NDIA

Celebrating 20 Years of Systems Engineering Excellence

20th Annual Systems Engineering Conference

Conference Program

October 23-26, 2017 | Waterford at Springfield | Springfield, VA
NDIA.org/systemsengineering

Welcome to the NDIA Systems Engineering Conference

On behalf of the National Defense Industrial Association's Systems Engineering Division, I would like to extend a very warm welcome to the 20th Annual Systems Engineering Conference. Yes, the 20th Annual – who knew when we started this conference 2 decades ago that we would continue to have important systems engineering issues to address? Well, perhaps most of you - because after all, technology keeps moving, our military capability continues to increase, the complexity of our systems continues to grow, and the threats we have to address continue to grow at an alarming rate.

For example, 20 years ago the term "Cybersecurity" wasn't addressed in DoD circles. Interoperability wasn't considered. Systems-of-systems weren't mentioned. And today, these are some of our hottest issues that the entire defense-industrial complex seeks to successfully address, not to mention affordability, sustainability and a host of other issues that continue to need attention.

This conference is the primary one in the US that brings together the engineering arms of the Office of the Secretary of Defense, the Services, many of the Federal Agencies, and the defense industrial complex to address and seek solutions to the issues we all face. Executives, managers and engineers from all of the major US defense contractors, as well as the principal engineering executives, managers and engineers from the Department of Defense and the Services and Federal Agencies are here, and dialog among us is critical to achieving a mutual understanding of the issues we collectively face and desperately need to solve. This conference provides an outstanding opportunity to have that dialog and exchange ideas, so please take maximum advantage of this opportunity.

And if there is anything that the conference committee, whose names are listed in the program, or I, or the outstanding NDIA staff can do to assist you, please let us know.

Bob Rassa
Manager, Engineering Programs
Raytheon Space & Airborne Systems

Dear Attendees, Speakers and Sponsors,

I would like to add my warm welcome to those attending the annual Systems Engineering Division conference. This year's conference marks the 20th anniversary of this prestigious event. I congratulate the NDIA Systems Engineering Division for their sustained, superior performance in producing a highly consequential event and applaud the many ways the division supports the Defense Department and defense community.

This conference is the premier event addressing the application of systems engineering principles to defense acquisition. As such, it is the main forum to exchange information and ideas among the Defense Department, the services, defense agencies, industry and academia.

I wish the best of experiences here at the conference, and look forward to many more years of division engagement with the community to promote and refine the systems engineering practice.

Sincerely

Herbert J. Carlisle
General, USAF (Ret)
President and CEO

20TH ANNUAL SYSTEMS ENGINEERING CONFERENCE

OCTOBER 23-26, 2017 | SPRINGFIELD, VA

INTRODUCTION

Considered the major annual systems engineering event focusing on the performance of DoD programs and systems, the National Defense Industrial Association's Annual Systems Engineering Conference offers content tailored to all levels of systems engineering (SE) professionals:

- Keynote Presentation
- Systems Engineering Executive Panels
    - DoD Executive Panel: Service Systems Engineering Leads discuss SE issues
    - DoD Executive Panel: Interagency Systems Engineering Activity
    - Industry Executive Panel: Industry Leaders discuss Systems Engineering issues
    - DoD Executive Panel: Service and Agency Program Managers discuss systems engineering issues
- Technical Breakout Sessions (2+ days)

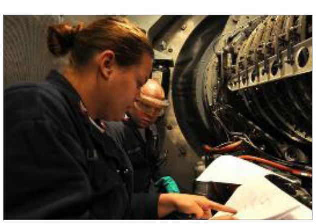
Demonstrating broad systems engineering community support, the conference is once again this year enjoying technical co-sponsorship by IEEE AES, IEEE Systems Council and the International Council on Systems Engineering.

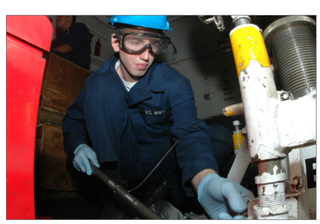
Further attesting to its value and relevance to Systems Engineering professionals within the defense industry, the conference continues to receive the support of the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

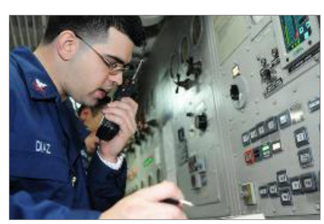
Major themes running through the three plus day agenda will include net-centric operations, data/information interoperability, system-of-systems engineering, cyber security and all aspects of system sustainment.

CONFERENCE OBJECTIVE

This conference seeks to create an interactive forum for Program Managers, Systems Engineers, Chief Scientists, Engineers, and Managers from the Requirements, Design, Verification, Support, Logistics and Test communities from both government and industry. The conference and the professional exchanges it will prompt will create opportunities to shape future policy and procedures.







BACKGROUND

The Department of Defense continues to seek ways to improve the acquisition of military equipment and capability to assist the warfighter in protecting the U.S. and its Allies around the world in a complex environment of ever-changing threats and conditions.

The Weapon Systems Acquisition Reform Act (WSARA) of 2009 defines Systems Engineering as a key enabler to effect improvements in defense acquisition and program execution that will produce more effective and affordable military systems. Previous DoD Better Buying Power initiatives, with their focus on achieving dominant capabilities through technical excellence and innovation, continued to emphasize the importance of engineering to the Department. The new administration seeks to increase military spending which will put additional onus on the defense industrial complex to achieve acquisition excellence, and systems engineering performance on the part of government and industry as partners is a key ingredient to success.

Systems Engineering is the “umbrella” engineering function that drives successful program execution and ensures an appropriate balance between requirements, performance, cost, schedule, and overall effectiveness and affordability. Systems Engineering principles embody strong technical and risk/opportunity management aspects for the acquiring Program Office as well as the prime and subcontractors. Strong emphasis on systems engineering throughout a program, especially in early development planning, is a key enabler of successfully fielding complex defense systems.

NDIA’s Annual Systems Engineering Conference explores the various roles of systems engineering from all aspects and perspectives—pragmatic, practical and academic—and brings key practitioners together to work on effective solutions to achieve a successful and affordable warfighting force.

CONFERENCE CHAIR

Mr. Robert Rassa
Director, Engineering Programs
Raytheon Company

DIVISION CHAIR

Mr. Frank Serna
Principal Director, Strategic Initiatives
Draper Laboratory

DIVISION VICE-CHAIR

Mr. Joseph Elm
Director of Engineering
L-3 Communications

NDIA PLANNING TEAM

Ms. Tammy Kicker, CMP
Director, Meetings & Events

Ms. Tina Fletcher
Meeting Planner, Meetings & Events

SCHEDULE AT A GLANCE

MONDAY, OCTOBER 23

8:00 am - 12:00 pm	Display Move In
12:00 pm - 5:30 pm	Registration
1:00 pm - 3:00 pm	Tutorials
3:00 pm - 3:30 pm	Networking Break
3:30 pm - 5:30 pm	Tutorials continue

TUESDAY, OCTOBER 24

7:00 am - 5:00 pm	Registration
7:00 am - 8:15 am	Networking Breakfast
8:15 am - 8:30 am	Opening Remarks: Bob Rassa, Raytheon; Frank Serna, Draper Labs
8:30 am - 9:30 am	Plenary Session Keynote: Vice Admiral Paul Grosklags, USN, Commander, Naval Air Systems Command
9:30 am - 10:00 am	Networking Break
10:00 am - 11:15 am	Executive Panel: DoD Systems Engineering
11:15 am - 12:30 pm	Executive Panel: Interagency Systems Engineering
12:30 pm -1:30 pm	Networking Luncheon
1:30 pm - 2:45 pm	Plenary Session Continues: Industry Executive Panel
2:45 pm - 3:00 pm	Presentation of Lt Gen Thomas R. Ferguson Systems Engineering Excellence Awards
3:00 pm - 3:30 pm	Networking Break
3:30 pm - 5:00 pm	Executive Panel: Program Managers
5:00 pm - 6:30 pm	Networking Reception

WEDNESDAY OCTOBER 25

7:00 am - 5:15 pm	Registration
7:00 am - 8:00 am	Networking Breakfast
8:00 am - 9:40 am	Concurrent Breakout Focus Sessions A
9:40 am - 10:15 am	Networking Break
10:15 am - 11:55 am	Concurrent Breakout Focus Sessions B
11:55 am - 1:00 pm	Networking Luncheon
1:00pm - 2:40 pm	Concurrent Breakout Focus Sessions C
2:40 pm- 3:15 pm	Networking Break
3:15 pm - 5:20 pm	Concurrent Breakout Focus Sessions D

THURSDAY OCTOBER 26

7:00 am - 5:15 pm	Registration
7:00 am - 8:00 am	Networking Breakfast
8:00 am - 9:40 am	Concurrent Breakout Focus Sessions A
9:40 am - 10:15 am	Networking Break
10:15 am - 11:55 am	Concurrent Breakout Focus Sessions B
11:55 am - 1:00 pm	Networking Luncheon
1:00 pm - 2:40 pm	Concurrent Breakout Focus Sessions C
2:40 pm- 3:15 pm	Networking Break
3:15 pm - 5:20 pm	Concurrent Breakout Focus Sessions D

TRACK OBJECTIVES

AGILE IN SYSTEMS ENGINEERING

Track Chairs: John Norton, *Raytheon Company*
Linda Maness, *Northrop Grumman Corporation*
Eileen Wrubel, *Software Engineering Institute*

Agile usage is becoming more prevalent within the government space. Lessons learned and ideas for implementation can be shared with those who are experienced in using Agile concepts. This track brings together practitioners with experience applying agile methods in a variety of disciplines and domains, with the goal of collaboration to expand their effective use in systems engineering and on defense programs

ARCHITECTURE

Track Chairs: Bob Scheuer, *The Boeing*
Ed Moshinsky, *Lockheed Martin Corporation*

Architecture is a key element in systems engineering. This track addresses architecture frameworks, strategies, and applications to improve system design, test, operations, and support.

COMPUTATIONAL RESEARCH & ENGINEERING ACQUISITION TOOLS AND ENVIRONMENTS (CREATE)

Track Chair: Douglass Post, *DoD High Performance Computing Modernization Program (HPCMP)*

The DoD HPCMP CREATE Program is a Tri-Service Program launched in 2006 by OSD and the HPCMP to develop and deploy eleven physics-based high performance computing software applications specifically to enable the DoD acquisition engineering community to design and analyze military ships, aircraft, ground vehicles, and radio frequency antennas. These tools enable engineers to generate an arbitrarily large number of design options (virtual prototypes expressed as digital product models) for design-space exploration, rapidly assess the feasibility and performance characteristics of each design option, and accurately predict the performance of each weapon platform with high-fidelity tools. With these tools, DoD engineers can identify design defects and performance shortfalls and fix them before metal has been cut, thus reducing costly rework and improving system performance. This reduces the cost, schedule, and risk of acquisition programs. The tools and computer time are available to DoD engineers (government and industry). The tools are being used by more than 180 DoD engineering organizations (government 40%, industry 50%, and other 10%--including academia) with over 1,400 users.

DEVELOPMENTAL TEST & EVALUATION (DT&E)

Track Chairs: Joe Manas, *Raytheon Company*

Developmental Test and Evaluation is a key aspect of successful systems engineering. This track addresses the entire continuum of test and evaluation from early planning to operational testing.

DIGITAL ENGINEERING/MODEL-BASED SYSTEMS ENGINEERING

Track Chair: Philomena Zimmerman, *DASD/SE*

Digital Engineering is an emerging set of practices for Systems Engineering and other engineering disciplines which has, at its core, the use of models (data, algorithms and/or processes) as a technical means of communication. When used properly, models can provide a cohesion across engineering activities, and cohesion with acquisition activities. When coupled with computational capabilities, resultant data from simulations can be used in decision-making at all echelons, and an increased level of insight and risk reduction in the end item can be achieved.

ENGINEERED RESILIENT SYSTEMS (ERS)

Track Chairs: Lois Hollan, *Potomac Institute*

Engineered Resilient Systems (ERS) is a Department of Defense priority initiative that seeks to transform engineering environments so that warfighting systems are more resilient and affordable across the acquisition lifecycle. The track will present new results across the ERS initiative including anchor technologies and computational representation.

EDUCATION & TRAINING

Track Chair: Don Gelosh, *Worcester Polytechnic Institute*

The Education and Training track for 2017 is an excellent collection of thirteen presentations from government, industry, and academia. The presentations describe a wide range of systems engineering workforce development activities from competency frameworks, cybersecurity skills, MBE and MBSE best practices, System of Systems guide and capstone marketplace to development of technical leaders.

ENTERPRISE HEALTH MANAGEMENT/PROGNOSTICS/ DIAGNOSTICS/RELIABILTY

Track Chairs: Chris Resig, *The Boeing Company*

The health of the system as a whole – the enterprise – is a critical function of systems engineering. This session will touch on some issues relating to the system health, including prognostics, diagnostics and reliability.

ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH)

Track Chairs: Sherman Forbes, *USAF*
Dave Schulte, *SAIC*
Lucy Rodriguez, *Booz Allen Hamilton*

The ESOH track provides a cross section of topics that reflect the many different Systems Engineering design considerations included under the DoDI 5000.02 acronym ESOH, as defined in MIL-STD-882E, the DoD Standard Practice for System Safety. This year, Mr. James Thompson, Director, Major Program Support (MPS), within the Office of the Deputy Assistant Secretary of Defense for Systems Engineering will be the ESOH track's keynote speaker. Mr. Thompson will share his perspectives on Risk, Issue, and Opportunity (RIO) Management and Independent Technical Risk Assessments (ITRAs). Mr. David Asiello, the Acquisition, Sustainability & Technology Programs lead in the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment will follow Mr. Thompson's presentation with a presentation focusing on how ESOH Risk Management is an integral part of the RIO Management Process and offering suggestions for improving the rigor, accountability, and visibility of ESOH risk management. There will be an extended question and answer period following Mr. Thompson's and Mr. Asiello's presentations to allow the audience to further explore the Acquisition and Sustainment Risk Management. The remainder of the ESOH track presentations will address specific acquisition ESOH issues, to include using Digital Engineering to manage ESOH risks and requirements, how to manage ESOH in Rapid Acquisitions, software system safety, hazardous materials regulations and management impacts on programs, environmental liabilities, environmental sustainability, and lessons learned about program office successes and failures in implementing the DoDI 5000.02 acquisition ESOH policy.

HUMAN SYSTEMS INTEGRATION (HSI)

Track Chair: Matthew Risser*, Pacific Science*
Patrick Fly*, The Boeing Company*

The HSI sessions include technical papers aligned with DoD HSI policy, standards and guidance. The goal is to address HSI implications in the design of complex systems in support of systems engineering and include HSI methods, metrics, and best practices, process improvements, applications and approaches to program integration.

INTEROPERABILITY/NET - CENTRIC OPERATIONS

Track Chairs: Jack Zavin*, OUSD/ATL*
John Daly*, Booz-Allen-Hamilton*

Interoperability is ability to operate in synergy in the execution of assigned tasks both within the DoD and its external mission partners. Net Centric Operations supports interoperability by providing the POPIM solution sets that allows the DoD and its mission partners to share information/data/knowledge when needed, where needed, and in a form they can understand and act on with confidence, while protecting it from those who should not have it. Net Centric Operations/Interoperability includes technologies such as Service Oriented Architecture, Data Center, Cloud Computing, information transport [e.g. internet, web, radios, data links], as well as both hardware and software [aka Information and Communicative Technology] together with people, operating alone or in organizations, as part of the System of Systems Systems Engineering.

MISSION ENGINEERING

Track Chair: Judith Dahmann*, MITRE*

Mission engineering (ME) is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects. This track focuses on current directions in Defense ME and approaches to applying SoS and SE approach to ME.

MODELING AND SIMULATION (M&S)

Track Chairs: David Allsop*, The Boeing Company*
Chris Schreiber*, Lockheed Martin Corpration*

The M&S Track highlights the use of models and simulations in the systems engineering process. Included are presentations on integrated environments, tools & technologies, and M&S applications in several SE process phases. Topics focused specifically on Digital Engineering/Model-based Systems Engineering are contained in a separate track on this topic.

PROGRAM MANAGEMENT

Track Chairs: Ken Nidiffer*, Software Engineering Institute*

Program Managers and chief Systems Engineers should be the “joined-at-the-hip” leads on all programs that wish to be successful. This session will address some of the issues that our program managers face in the execution of programs.

SOFTWARE ENGINEERING

Track Chairs: Ken Nidiffer*, Software Engineering Institute*

Software is often overlooked when talking systems engineering yet software is a key element of most designs today and must always be part of the systems engineer’s portfolio of responsibility. This session will highlight a few significant software development issues.

SYSTEMS ENGINEERING EFFECTIVENESS

Track Chairs: Tim White*, Raytheon Company*
Joe Elm*, L3 Technologies*

Systems Engineering Effectiveness is obvious to some and quite esoteric to others. The goal though, improving the value obtained for each SE dollar spent, is shared by each who joins the discussion. Please attend the SE Effectiveness track to learn how your peers are implementing practical measures to better quantify the benefits of Systems Engineering and its value to Product Users and Developers alike. Early and effective Systems Engineering has been shown to return excellent value to all project stakeholders. This Track will highlight the latest DoD policy and guidance, define new approaches, and provide some practical experiences to assist the DoD and defense industry SE community in achieving a quantifiable and persistent improvement in program outcomes through appropriate application of systems engineering principles and best practices.

SYSTEMS OF SYSTEMS (SOS)

Track Chairs: Judith Dahmann, *MITRE*
Rick Poel, *The Boeing Company*
Jennie Horn*, Raytheon Company*

The System of Systems track will feature papers highlighting development SoS engineering approaches, particular SoS SE application areas, and SoS tools and modeling, including SoS SE applied to defense missions in mission engineering. See directly related track in Mission Engineering, above.

SYSTEM SECURITY ENGINEERING (SSE)

Track Chairs: Holly Dunlap*, Raytheon Company*
Melinda Reed*, DASD/SE*

System Security Engineering has become one of the most important aspects in the design of DoD systems. This track will focus on system security engineering and a holistic approach to program protection.

Monday, October 23

8:00AM - 12:00PM	**Display Move In**
12:00PM - 5:30PM	**Registration Open**
1:00 PM - 5:30 PM	**Tutorials**

Track	Room	Session	1:00PM - 1:30PM	1:30PM - 2:00PM	2:00PM - 2:30PM	2:30PM - 3:00PM
Track 4	Gibson	**Tutorial: Modeling and Simulation (M&S)** 1C4	19696 Half-Day Tutorial: Modeling and Simulation in the Systems Engineering Process ▶ Dr. Jim Coolahan, Coolahan Consultants, LLC			
Track 5	Sellier	**Tutorial: Applying MIL-STD** 1C5	19702 Tutorial: Tutorial: Applying Focused MIL-STD-882E Software Safety Level of Rigor ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*			
Track 6	Korman	**Tutorial: Communication and Analysis** 1C6	19713 Effective Communication and Analysis in the Age of MBSE ▶ Mr. Ronald Kratzke, *Vitech Corporation*			

3:00PM - 3:30PM	**Networking Break**

Track	Room	Session	3:30PM - 4:00PM	4:00PM - 4:30PM	4:30PM - 5:00PM	5:00PM - 5:30PM
Track 4	Gibson	**Tutorial: Modeling and Simulation (M&S) Cont'd** 1D4	19696 Half-Day Tutorial: Modeling and Simulation in the Systems Engineering Process ▶ Dr. Jim Coolahan, Coolahan Consultants, LLC			
Track 5	Sellier	**Tutorial: Applying MIL-STD Cont'd** 1D5	19702 Tutorial: Applying Focused MIL-STD-882E Software Safety Level of Rigor ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*			
Track 6	Korman	**Tutorial: Communication and Analysis Cont'd** 1D6	19713 Effective Communication and Analysis in the Age of MBSE ▶ Mr. Ronald Kratzke, *Vitech Corporation*			

5:30PM	**Adjourn**

Tuesday, October 24

7:00AM - 5:00PM **Registration Open**

7:00AM - 8:15AM **Networking Breakfast**

8:15AM - 8:30AM **Opening Remarks**

Mr. Robert Rassa, *Director, Engineering Programs, Raytheon Company; NDIA Systems Engineering Conference Chair*

Mr. Frank Serna, *Principal Director, Strategic Initiatives, Draper Laboratory; Chair, NDIA Systems Engineering Division*

8:30AM - 9:30AM **Keynote Presentation**

VADM Paul Grosklags, *NAVAIR, Commander, Naval Air Systems Command*

9:30AM - 10:00AM **Networking Break**

10:00AM - 11:15AM **DoD Executive Panel: DoD Systems Engineering**

Moderator: Mrs Kristen Baldwin, *Deputy Assistant Secretary of Defense, Systems Engineering (Acting)*

Panelists:

- Col Laird Abbott, *USAF, Chief, Engineering and Force Management Division, Deputy Assistant Secretary for Science, Technology, and Engineering, SAF-AQR*
- Mr. William Bray, *USN, DASN RDT&E and Chief Systems Engineer*
- Mr. Douglas Wiltsie, *USA, Executive Director, SoSE&I, ASA ALT (invited)*

11:15AM - 12:30PM **Executive Panel: Interagency Systems Engineering**

Moderator: Ms. Kristen Baldwin, *Deputy Assistant Secretary of Defense, Systems Engineering (Acting)*

Panelists:

- Mr. Albert “Benjie” Spencer, *National Oceanic and Atmospheric Administration*
- Mr. Jon Holladay, *Technical Fellow for Systems Engineering, National Aeronautics and Space Admnistration*
- Mr. Kent Jones, Assistant Deputy Administrator for Systems Engineering and Integration, Defense Programs, DOE *National Nuclear Security Administration*
- Mr. Joseph Post, *Deputy Director, NAS Systems Engineering & Integration Federal Aviation Administration*
- Mr. James Tuttle, Deputy Director, CDS and Chief Systems Engineering, *Department of Homeland Security*

`

12:30PM - 1:30PM **Networking Luncheon**

1:30PM - 2:45PM **Industry Executive Panel: Model-Based Systems Engineering: How is it Helping?**

Mr. Frank Serna, *Principal Director, Strategic Initiatives, Draper Laboratory; Chair, NDIA Systems Engineering Division*

Panelists:

- Ms. Christi Gau Pagnanelli, *Director, BDS Systems Enginnering and Engineering Multi-Skilled Leadership, Boeing Defense, Space & Security*
- Mr. Randall Lum, *Corporate Director, Engineering, Northrop Grumman Corporation*
- Mr. Tim Walden, *Chief Engineer and Fellow, Lockheed Martin Corporate Engineering and Production Operations*
- Mr. Scott Welles, *Vice President, Booz Allen Hamilton*

2:45PM - 3:00PM **Presentation of Lt Gen Thomas R. Ferguson Systems Engineering Excellence Awards**

3:00PM - 3:30PM **Networking Break**

3:30PM - 5:00PM **Executive Panel: Program Managers**

Moderator: Col. David McIllece, USAF

Panelists:

- Col Edward Hospodar, USAF, *GPS User Equipment Senior Materiel Leader*
- COL Mike Milner, USA, *Armored Multi-Purpose Vehicle (AMPV) Program Manager*
- Col Amanda Myers, USAF, *Deputy Director, Global Reach Programs, Former C-17 System Program Manager*
- CAPT Seiko Okano, USN, *PEO Integrated Wardare Systems (IWS) 2.0 Program Manager*

5:00pm - 6:30pm **Networking Reception**

Wednesday, October 25

7:00AM-5:15PM **Registration**

7:00AM-8:00AM **Networking Breakfast**

Track	Chair	Session	8:00AM - 8:25AM	8:25AM - 8:50AM	8:50AM - 9:15AM	9:15AM - 9:40AM
Track 1	Singleton	**Human Systems Integration** 3A1	19516 Enhancing Future Soldier Systems through the use of the Systems Modeling Language to Incorporate Human Aspects into the Soldier as a System Definition ▶ Mr. Sean Pham, *U.S. Army ARDEC*	19641 HSI Best Practice Standard ▶ Dr. Patrick Fly, *The Boeing Company*	19739 The Human Systems Integration Partnership:: Delivering the HSI Capability to the Air Force Systems Engineering Process ▶ Mr. Derek Johnston, *United States Air Force*	19919 Adaptive Automation for UAV Pilot Vehicle Interfaces ▶ Mr. Jeff O'Hara, *Georgia Tech Research Institute*
Track 2	Miller	**Net Centric Operations & Interoperability** 3A2	19752 Kick Off/Context for NCO/I Track ▶ Mr. Jack Zavin, *DoD/OUSD(AT&L)*	19815 ISO/IEC/IEEE8 15288 System Interoperability Considerations ▶ Mr. John Daly, *Booz Allen Hamilton*	19759 JITC Executes DoD Mobility Field Assessments ▶ Mr. Khoa Hoang, *Joint Interoperability Test Command*	19764 Interface Management for Interoperability– from Theory to Modeling ▶ Mr. Matthew Hause, *PTC*
Track 3	Von Sternberg	**Engineering & Model-based Systems Engineering** 3A3	19819 DoD Digital Engineering Strategy ▶ Ms. Philomena Zimmerman, *Department of Defense*	19879 Model Centric Engineering Enabling a New Operational Paradigm for Acquisition ▶ Dr. Mark Blackburn, *Stevens Institute of Technology*	19853 Joint NDIA SSE & SwA Committee and Joint Federated Assurance Center, Government SwA Gap Analysis Workshop Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19855 MBSE and Systems Engineering Transformation ▶ Mr. Troy Peterson, *INCOSE*
Track 4	Gibson	**Modeling & Simulation** 3A4	19691 An Autonomous Sensor Tasking System ▶ Ms. Quintina Jones, *Raytheon Missile Systems*	19711 Best Practices for the Architecture, Design, and Modernization of Defense Models and Simulations ▶ Mr. Michael Heaphy, *AT&L/DMSCO*	19725 VV&A of Models and Simulations: The Power of Independent Cumulative Analyses ▶ Ms. Natalie Plotkin, *Raytheon Company*	19916 Formalized Execution of Model Integrated Descriptive Architecture Languages ▶ Mr. Gregory Haun, *Analytical Graphics, Inc.*
Track 5	Sellier	**Agile** 3A5	19877 Research Gone "Agile" A Case Study on Using an Enterprise Transformation Process to Enable Agile Methods in a Research Program ▶ Dr. Rosa Heckle, *The MITRE Corporation*	19726 Issues anOpportunities in Accelerated Software Development for Next Generation DoD Applications ▶ Dr. Craig Arndt, *Defense Acquisition University*	19755 A System Dynamics Model of the Scaled Agile Framework (SAFe) to Quantify the Effects of Management Decisions on Capability Development and Acquisition Outcomes ▶ Mr. Sean Ricks, *The MITRE Corporation*	19777 "Elicitation of Robust and Quality Agile User Stories Using QFD" ▶ Ms. Sabrina Ussery, *The George Washington University*
Track 6	Korman	**Software** 3A6	19745 Software Complexity Modeling ▶ Mr. Thuc Tran, *Capital One*	19749 Harnessing the Beast: Using Model Based Systems Engineering (MBSE) to Manage Complex Research Software Environments ▶ Ms. Jennifer Turgeon, *Sandia National Laboratories*	19758 Software Systems Maturity Analysis ▶ Mr. Christopher Dieckmann, *Idaho National Laboratory*	19816 Free and Open Source Tools to Assess Software Reliability and Security ▶ Mr. Lance Fiondella, *University of Massachusetts*

Wednesday, October 25 - Continued

9:40AM-10:15AM **Networking Break**

			10:15AM - 10:40AM	10:40AM - 11:05AM	11:05AM - 11:30AM	11:30AM - 11:55AM
Track 1	Singleton	**Human Systems Integration** / **Systems Security Engineering** 3B1	19784 A Wearable Vision+Inertial Navigation System for Assessing Volumetric Utilization and Task Geometry Efficiency ▶ Mr. Kevin Duda, *Draper Laboratory*	19740 Fisher vs. Taguchi Experimental Design Methods in Human Factors ▶ Ms. Sarah Ewing, *Idaho National Laboratory*	19854 NDIA Welcome and Review of Accomplishments ▶ Ms. Holly Dunlap, *Raytheon Company*	19881 DoD Cyber Resilient Weapon Systems ▶ Ms. Melinda Reed, *Department of Defense*
Track 2	Miller	**Net Centric Operations & Interoperability** / **Mission Engineering** 3B2	19923 Joint and Mission Partner Interoperability ▶ Mr. Mike Richards, *Joint Staff J6*	19499 Real Life Cloud Acquisition and Adoption Across Agencies and Cloud Providers ▶ Mr. Mun-Wai Hon, *Noblis*	19849 Mission Integration Management, NDAA 2017 Section 855 ▶ Mr. Robert Gold, *Department of Defense*	19838 Systems of Systems Engineering Technical Approaches as Applied to Mission Engineering ▶ Dr. Judith Dahmann, *MITRE*
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engineering** 3B3	19793 Model-Centric Decision Making: Insights from an Expert Interview Study ▶ Dr. Donna Rhodes, *Massachusetts Institute of Technology*	19890 Using MBSE to Communicate and Gain Acceptance of your Analysis ▶ Mr. Frank Salvatore, *Engility*	19795 New Innovations in Digital Systems Engineering ▶ Dr. Edward Kraft, *University of Tennessee Space Institute*	19920 Key MBSE Enablers with Examples ▶ Mr. Nicholas Driscoll, III, *Raytheon Company*
Track 4	Gibson	**CREATE Computational Research & Engineering Acquisition Tools and Environments** 3B4	20010 Digital Engineering (DE) and Computational Research and Engineering Acquisition Tools and Environments (CREATE) ▶ Ms. Philomena Zimmerman, *Department of Defense*	19721 CREATE: Accelerating Defense Innovation with Computational Prototypes and High Performance Computers ▶ Dr. Douglass Post, *DoD HPCMP*	19730 Physics-Based Simulation in Support of Acquisition program and Fleet Operations ▶ Mr. Steven Donaldson, *Naval Air Systems Command*	19728 Capstone: A Patform for Geometry, Meshing and Attribution Modeling for Physics-based Analysis and Design ▶ Dr. Saikat Dey, *US NRL Code 7131*
Track 5	Sellier	**Agile** / **Environment Safety & Occupational Health** 3B5	19902 Software Development Challenges in AFMC (Agile Software Development and Data Rights) ▶ Mr. Andrew Jeselson, *Air Force Materiel Command*		19701 Leveraging Cybersecurity Tools for Software Safety: Focusing (Some) Static Analysis on Safety-Critical Software ▶ Mr. Stuart Whitford, *Booz Allen Hamilton*	20028 Joint Software System Safety Implementation Guide ▶ Mr. Bob Smith, *Booz Allen Hamilton*
Track 6	Korman	**Systems Engineering Effectiveness** 3B6	19850 Engineering Autonomy ▶ Mr. Robert Gold, *Department of Defense*	19882 The Drive for Innovation in Systems Engineering ▶ Mr. Scott Lusero, *Department of Defense*	19814 DoD Systems Engineering Policy, Guidance and Standardization ▶ Ms. Aileen Sedmak, *Department of Defense*	19835 Helix: Understanding Systems Engineering Effectiveness through Modeling ▶ Ms. Nicole Hutchison, *Stevens Institute of Technology*

11:55AM - 1:00PM **Networking Luncheon**

Wednesday, October 25 - Continued

			1:00PM - 1:25PM	1:25PM - 1:50PM	1:50PM - 2:15PM	2:15PM - 2:40PM
Track 1	Singleton	**System Security Engineering** 3C1	19852 NDIA Cyber Resilient & Secure Systems Summit Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19839 Unified Architecture Framework (UAF) Profile for Risk Assessment Methodology ▶ Ms. Tamara Hambrick, *Northrop Grumman Corporation*	19913 Considerations to Address Dependably Secure System Function in System Capability, Requirements, and Performance Artifacts ▶ Mr. Michael McEvilley, *The MITRE Corporation*	19866 AF Cyber Campaign Plan - Weapon Systems Focus ▶ Mr. Daniel Holtzman, *U.S. Air Force*
Track 2	Miller	**Mission Engineering** / **System of Systems** 3C2	19706 Model Based Systems of Systems Engineering ▶ Mr. Francis McCafferty, *Vitech Corporation*	19868 Mission Threads: Linking Mission Engineering and Systems Engineering ▶ Dr. Greg Butler, *Engility Corp*	19718 Developing Standards for Systems of Systems (SoS) Engineering ▶ Dr. Judith Dahmann, *The MITRE Corporation*	19804 Scaling Model-Based System Engineering Practices for System of Systems Applications: Software Tools ▶ Ms. Janna Kamenetsky, The *MITRE Corporation*
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engineering** 3C3	19545 Pulling the Digital Thread with Model Based Engineering ▶ Mr. Christopher Finlay, *Raytheon Company*	19906 Modeling the Digital System Model Data Taxonomy ▶ Ms. Philomena Zimmerman, *Department of Defense*	19746 Developing and Distributing a CubeSat Model-Based Systems Engineering (MBSE) Reference Model – Interim Status #2 ▶ Dr. David Kaslow, *S.E.L.F*	19872 Enabling Design of Agile Security with MBSE ▶ Mr. Barry Papke, *No Magic*
Track 4	Gibson	**CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering** 3C4	19779 High-Fidelity Electromagnetic Modeling with CREATE-RF Tools ▶ Dr. Daniel Dault, *Air Force Research Lab*	19809 Physics Based Modeling & Simulation For Shock and Vulnerability Assessments - Navy Enhanced Sierra Mechanics ▶ Mr. Jonathan Stergiou, *Naval Surface Warfare Center, Carderock Division*	19823 The Role of CREATE-AV in Realization of the Digital Thread "Authoritative Truth Source" ▶ Dr. Edward Kraft, *University of Tennessee Space Institute*	19753 A Networked Frigate Concept Design Space Exploration Using the Rapid Ship Design Environment ▶ Dr. Douglas Rigterink, *Navel Surface Warfare Center, Carderock Division*
Track 5	Sellier	**Environment Safety & Occupational Health** 3C5	19912 DASD (SE) Risk, Issue, and Opportunity (RIO) Management and Independent Technical Risk Assessments (ITRAs) ▶ Mr. James Thompson, *Department of Defense*	19697 ESOH Risk Management ▶ Mr. David Asiello, *OASD(EI&E)*	19908 DoD Acquisition ESOH IPT Q&A Panel ▶ Mr. David Asiello, *OASD(EI&E)*	
Track 6	Korman	**Systems Engineering Effectiveness** 3C6	19790 Systems Engineering Research Needs and Workforce Development Study ▶ Dr. Dinesh Verma, *Systems Engineering Research Center (SERC)*	19744 Technical Performance Risk Management for Large Scale Programs ▶ Mr. Brian Davenport, *Raytheon Company*	19742 The Design of a Cone Penetrometer System ▶ Dr. Doris Turnage, *U. S. Army Engineer Research & Development Center*	19781 Additive Manufacturing – Challenges for the Systems Engineer and Program Manager ▶ Mr. William Decker, *Defense Acquisition University*

Wednesday, October 25 - Continued

2:40PM - 3:15PM **Networking Break**

			3:15PM - 3:40PM	3:40PM - 4:05PM	4:05PM - 4:30PM
Track 1	Singleton	**System Security Engineering** 3D1	19861 Cyber Resilient and Secure Weapon Systems Acquisition/Proposal Discussion & Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19771 When the Right Answer is Not What NAVSEA Normally Does ▶ Mr. Peter Chu, *NAVSEA 05*	19870 Can't We Just Get Along: Engineering Trade Decisions VS RMF at the System Level ▶ Mr. Don Davidson, *DoD CIO*
Track 2	Miller	**System of Systems** 3D2	19802 Scaling Model-Based System Engineering Practices for System of Systems Applications: Analytic Methods ▶ Dr. Aleksandra Markina-Khusid, The *MITRE Corporation*	19757 Defense System of Systems Gap Analysis ▶ Mr. Christopher Dieckmann, *Idaho National Laboratory*	19878 Enterprise Implications of Family of Systems (FoS) Acquisition ▶ Dr. Garrett Thurston, *Dassault Systemes*
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engineering** 3D3	19775 Digital System Model Ice ▶ Dr. David Hench, *Eagle Ray R&D*	19871 Enabling Repeatable SE Cost Estimation with COSYSMO and MBSE ▶ Mr. Barry Papke, *No Magic*	19888 MBSE to Address Logical Text-Based Requirements Issues ▶ Dr. Saulius Pavalkis, *No Magic*
Track 4	Gibson	**CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering** 3D4	19693 Program Management in CREATE for the Development of Large-scale Physics-based Software Development Projects for Engineering Design and Analysis ▶ Dr. Richard Kendall, *DoD HPCMP*	19704 Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles (CREATE-GV) ▶ Dr. Christopher Goodin, *U.S. Army ERDC*	19715 Physics-based, Multidisciplinary Analysis of Fixed-Wing Aircraft with HPCMP CREATE(TM)-AV/Kestrel ▶ Dr. David McDaniel, *DoD HPCMP/CREATE*
Track 5	Sellier	**Environment Safety & Occupational Health** 3D5	19770 Assessing the impacts of Amended Toxic Substances Control Act to the DoD Mission and the Defense Industrial Base Panel ▶ Ms. Amy Borman, *U.S. Army* ▶ COL Joseph Constantino *(SAF/IEE)* ▶ Mr. Shane Esola, *DCMA* ▶ Mr. Jim Rudroff, (ODASN(E)) ▶ Dr. Patricia Underwood, *OASD(EI&E)*		
Track 6	Korman	**Systems Engineering Effectiveness** 3D6	19738 Improving Effectiveness with respect to Time-To-Market and the Impacts of Late-stage Design Changes in Rapid Development Life Cycles ▶ Mr. Parth Shah, *George Washington University*	19716 Integrity System Security Engineering into System Engineering ▶ Mr. Ken Barker, *USAF*	19824 Implementation of the R&M Engineering Body of Knowledge ▶ Mr. Andrew Monje, *Department of Defense*

Wednesday, October 25 - Continued

			4:30PM - 4:55PM	4:55PM - 5:20PM	
Track 1	Singleton	**System Security Engineering** 3D1	19880 Engaging the DoD Enterprise to Protect U.S. Military Technical Advantage: Joint Acquisition Protection and Exploitation Cell Update ▶ Mr. Brian Hughes, *Department of Defense*	19798 Using Real Options Analysis to develop Resiliency in System Security Architectures ▶ Mr. Chris D'Ascenzo, *Defense Acquisition University*	
Track 2	Miller	**System of Systems** 3D2	19736 "Defense Acquisition System" System of Systems Engineering ▶ Mr. Larry Harding, *Idaho National Laboratory*		
Track 3	Von Sternberg	**Digital Engineering & Model-based Systems Engoneering** 3D3	19763 The Digital Engineering Journey ▶ Mr. Mathew Hause, *PTC*	19833 Digitalization of Systems Engineering –Examples and Benefits for the Enterprise ▶ Mr. Sanjay Khurana, *Dassault Systemes*	
Track 4	Gibson	**CREATE: Computational Research & Engineering Acquisition Tools and Environments Engineering** 3D4	19776 Weapons System Innovation through Workflow-based Computational Prototyping ▶ Mr. Loren Miller, *DataMetric Innovations, LLC*	19786 Rotorcraft Acquisition: Development of Modeling and Simulation Procedures ▶ Dr. Marvin Moulton, *U.S. Army*	
Track 5	Sellier	**Environment Safety & Occupational Health** 3D5	19770 Assessing the impacts of Amended Toxic Substances Control Act to the DoD Mission and the Defense Industrial Base Panel ▶ Ms. Amy Borman, *U.S. Army* ▶COL Joseph Constantino *(SAF/IEE)* ▶ Mr. Shane Esola, *DCMA* ▶ Mr. Jim Rudroff, (ODASN(E)) ▶ Dr. Patricia Underwood, *OASD(EI&E)*		
Track 6	Korman	**Systems Engineering Effectiveness** 3D6	19762 Decision-Driven Product Development ▶ Mr. Matthew Hause, *PTC*	19830 Are We Doing Enough in Requirements Management? ▶ Dr. Steven Dam, *SPEC Innovations*	

5:20PM **Adjourn**

Thursday, October 26

7:00AM-5:15PM **Registration**

7:00AM-8:00AM **Networking Breakfast**

			8:00AM - 8:25AM	8:25AM - 8:50AM	8:50AM - 9:15AM	9:15AM - 9:40AM
Track 1	Singleton	**System Security Engineering** 4A1	19796 Cyber Systems Risk – an Opportunity for Model Based Engineering & Design ▶ Dr. Jerry Couretas, *Booz Allen Hamilton*	19785 Cybersecurity As An Integral Part of Systems Engineering ▶ Mr. William Decker, *Defense Acquisition University*	19741 Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems ▶ Mr. Thomas McDermott, Jr., *Georgia Tech Research Institute*	19911 Achieving DoD Software Assurance (SwA) ▶ Mr. Thomas Hurt, *Department of Defense*
Track 2	Miller	**Developmental Test & Evaluation** 4A2	19792 An Approach to Verification of Complex Systems ▶ Dr. Wilson Felder, *Stevens Institute of Technology*	19925 Improving Distributed Testing with TENA and JMETC ▶ Mr. Ryan Norman, *TENA / JMETC*	19774 Identifying Requirements and Vulnerabilities for Cybersecurity; Or How I Learned to Stop Worrying and Love the Six-Phase Cybersecurity T&E Process ▶ Mr. David Brown, *Electronic Warfare Associates (EWA)*	19831 How Can We Use V&V Techniques in Early Systems Engineering? ▶ Dr. Steven Dam, *SPEC Innovations*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4A3	20009 Digital Engineering and ERS ▶ Mr. Robert Gold, *Department of Defense*		19845 ERS: Influencing Acquisition Innovation ▶ Dr. Owen Eslinger, *U.S. Army Engineer Research and Development Center*	19907 Scaling Data Analytics for ERS ▶ Mr. David Stuart, *U.S. Army Engineer Research and Development Center*
Track 4	Gibson	**Create: Computational Research & Engineering Acquisition Tools and Environments Engineering** 4A4	19887 Multi-Disciplinary Integration of ModSim for Navy Applications ▶ Dr. Greg Bunting, *Sandia National Laboratories*	19729 Academic Deployment of the HPCMP CREATE Genesis Software Package ▶ Dr. Robert Meakin, *U.S. DoD HPCMP*	19875 Secure Web-Based Access for Productive Supercomputing ▶ Ms. Laura Ulibarri, *Air Force Research Laboratory*	19800 CREATE-SH IHDE: Workflow Process Improvements for Hydrodynamics Characterization of Ship Designs ▶ Mr. Wesley Wilson, *Naval Surface Warfare Center, Carderock Division*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4A5	19773 Model Based Systems Engineering (MBSE) Considerations for Environment Safety and Occupational Health (ESOH) ▶ Mr. Leo Kilfoy, *MSC Software*	19772 A Pragmatic Approach to System Modeling for Hazard Identification and Risk Management ▶ Mr. Michael Vinarcik, *Booz Allen Hamilton*	19708 Unmanned System (UxS) Safety Engineering Precepts - an OSD Guide - update of the 2007 OSD UxS Safety Guide ▶ Mr. Michael Demmick, *NOSSA*	19754 Divergent Oscillating Refueling Probe on the HH-60G Pavehawk ▶ Mr. Joseph Jones, *SAF/AQRE*
Track 6	Korman	**Architecture** 4A6	19820 MOSA Considerations in Systems Engineering Through the Lifecycle ▶ Ms. Philomena Zimmerman, *Department of Defense*	19821 Implementing a MOSA to Achieve Acquisition Agility in Defense Acquisition Programs ▶Ms. Philomena Zimmerman, *Department of Defense*	19837 Challenges to Implementing MOSA for Major DoD Acqusition Programs ▶ Mr. Edward Moshinsky, *Lockheed Martin Corporation*	19778 Investigating Approaches to Achieve Modularity Benefits in the Defense Acquisition Ecosystems ▶ Dr. Navindran Davendralingam, *Purdue University*

Thursday, October 26- Continued

9:40AM-10:15AM Networking Break

			10:15AM - 10:40AM	10:40AM - 11:05AM	11:05AM - 11:30AM	11:30AM - 11:55AM
Track 1	Singleton	**System Security Engineering** 4B1	19853 Joint NDIA SSE & SwA Committee and Joint Federated Assurance Center, Government SwA Gap Analysis Workshop Summary ▶ Ms. Holly Dunlap, *Raytheon Company*	19698 Program Manager's Guidebook for Integrating Software Assurance into Defense Systems During the System Acquisition Lifecycle ▶ Dr. Kenneth Nidiffer, *Software Engineering Institute*	19735 Reducing Software Vulnerabilities – The "Vital Few" Process and Product Metrics ▶ Mr. Girish Seshagiri, *Ishpi Information Technologies, Inc.*	19910 DoD Joint Federated Assurance Center (JFAC) 2017 Update ▶ Mr. Thomas Hurt, *Department of Defense*
Track 2	Miller	**Education & Training** 4B2	19813 Shaping the Department of Defense Engineering Workforce ▶ Ms. Aileen Sedmak, *Department of Defense*	19794 Review of Best Practices for Technical Leadership Development ▶ Dr. Wilson Felder, *Stevens Institute of Technology*	19805 Development of a Defense Mission Engineering Competency Model ▶ Dr. Nicole Hutchison, *Stevens Institute of Technology*	19789 The Capstone Marketplace: Growing our Technical Workforce through Systems Oriented Senior Design Projects ▶ Ms. Megan Clifford, *Systems Engineering Research Center*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4B3	19844 Tradespace: Informed Decision making for Acquisition ▶ Mr. Timothy Garton, *Engineer Research and Development Center*	19834 Building an Agile Framework for the Analysis of Environmental Impacts on Military Systems ▶ Dr. Dharhas Pothina, *Engineer Research and Development Center*	19859 Introducing Lifecycle Cost to Early Conceptual Tradespace Exploration ▶ Mr. Erwin Baylot, *Engineer Research and Development Center*	19806 Overcoming the Government - Industry Collaboration Hurdle ▶ Dr. Patrick Martin, *BAE Systems*
Track 4	Gibson	**Create: Computational Research & Engineering Acquisition Tools and Environments Engineering** 4B3	19694 Software Engineering for Physics-based HPC Applications for Engineering Design and Analysis in CREATE ▶ Dr. Richard Kendall, *DoD HPCMP*	19703 Verification and Validation in CREATE Multi-Physics HPC Software Applications ▶ Dr. Lawrence Votta, *Brincos Inc.*	19709 DoD Risk Management Deficiencies...And How to Fix Them ▶ Mr. Richard Sugarman, *U.S. Air Force*	19724 Tools for Acquiring Highly Maintainable Software-Intensive Systems ▶ Dr. Barry Boehm, *USC*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4B5	19767 Rapid Equipping – Immediate Need to Equip and Protect Soldiers ▶ Mr. George Evans, *Prospective Technology Inc. (SAAL-PE/PTI ctr)*	19769 ESOH Risk Management and Applying MIL-STD-882E Principles to Programs that Deviate from Standard Acquisition Models ▶ Mr. Jefferson Walker, *Booz Allen Hamilton*	19732 Hazardous Materials Risk Management Using MIL-STD-882E ▶ Ms. Lori Hales, *Booz Allen Hamilton*	19836 Leveraging the International Aerospace Environmental Group (IAEG) Defense Acquisition Materials Declaration Process ▶ Ms. Karen Gill, *Booz Allen Hamilton*
Track 6	Korman	**Architecture** 4B6	19780 Cybersecurity and a Modular Open Systems Approach ▶ Mr. William Decker, *Defense Acquisition University*	19743 If System Architectures are So Useful, Why Don't We Use Them More? ▶ Mr. Robert Scheurer, *NDIA SE Architecture Committee*	19873 A Reverse Chronology of Evolutionary Architecture and Agile Development ▶ Mr. Thomas Mielke, *CACI International Inc.*	19903 Efficient Use of Enterprise and System Architecting in Combined Environment ▶ Dr. Howard Gans, *Harris Corporation*

Thursday, October 26 - Continued

11:55AM - 1:00PM **Networking Luncheon**

			1:00PM - 1:25PM	1:25PM - 1:50PM	1:50PM - 2:15PM	2:15PM - 2:40PM
Track 1	Singleton	**System Security Engineering** 4C1	19862 Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs ▶ Dr. Jeremy Muldavin, *Department of Defense*	19747 SSE Abstract: Developing Trust For a Secure Microelectronics Supply Chain ▶ Dr. Michael Fritze, *Potomac Institute for Policy Studies*	19731 SSE: Trusted Microelectronics Joint Working Group ▶ Dr. Brian Cohen, *Institute for Defense Analyses*	19700 Managing Risk with Trusted ASICs: Introducing to the SSE Community a Guidebook to Using Trusted Suppliers ▶ Mr. Jim Gobes, *Intrinsix Corp.*
Track 2	Miller	**Education & Training** 4C2	19811 Version 1.0 of the New INCOSE Competency Framework ▶ Mr. Don Gelosh	19515 A Proposed Engineering Training Framework and Competency Methodology ▶ Dr. Eric Dano, *BAE Systems*	19695 Educating Engineers or Training Technicians ▶ Mr. Zane Scott, *Vitech Corporation*	19734 Solving Cybersecurity Skills Shortage With Apprenticeships & Certifications – A Case Study ▶ Mr. Girish Seshagiri, *Ishpi Information Technologies, Inc.*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4C3	19783 The Language of Complexity: Ontology in Systems Design and Engineering ▶ Mr. Abe Wu, *Raytheon Missiles*	19846 Physics and Model Based Aerodynamic Design and Analysis at GA ▶ Mr. Pritesh Mody, *General Atomics Aeronautical Systems, Inc.*	20050 Automation and Integration for Complex System Design ▶ Mr. Scott Radon, *Phoenix Integration*	19825 Application of CREATE Tools for High Fidelity Design Space Exploration ▶ Mr. Antonio De La Garza, *Lockheed Martin Aeronautics Company*
Track 4	Gibson	**Program Management** 4C4	19751 A Capability Value Frontier in Support of Acquisition Approaches to Enable Military Effectiveness ▶ Dr. Marilyn Gaska, *Lockheed Martin Corporation*	19782 Technical Data Package and Intellectual Property Rights ▶ Mr. William Decker, *Defense Acquisition University*		19827 Policy Engineering: Applying Systems Engineering to Develop Better Policies ▶ Dr. Steven Dam, *SPEC Innovations*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4C5	19714 DoD's REACH Strategy and its Impact to Acquisition and Sustainment ▶ Dr. Patricia Underwood, *OASD(EI&E)*	19705 Environmental Liabilities for DoD Weapons Systems ▶ Ms. Patricia Huheey, *OASD(EI&E)*	19810 *Environmental Life Cycle Assessment of Commercial Transportation Activities* ▶ Ms. Sheila Neumann, *University of Texas at Arlington*	19699 LIfe Cycle Assessment: A Tool for Protecting Defense Assets ▶ Dr. Kelly Scanlon, *OASD(EI&E)*
Track 6	Korman	**Architecture** 4C6	19748 Advancing U.S. Marine Corps Warehouse Management Operations Through System Architecture and Analysis ▶ Mr. Christopher Melkonian, *Marine Corps Systems Command*	19828 From Architecture to Operations – Using Your Architecture Work in Operations ▶ Dr. Steven Dam, *SPEC Innovations*		

Thursday, October 26 - Continued

2:40PM - 3:15PM **Networking Break**

			3:15PM - 3:40PM	3:40PM - 4:05PM	4:05PM - 4:30PM
Track 1	Singleton	**System Security Engineering** 4D1	19864 Field Programmable Gate Array (FPGA) Assurance ▶ Mr. Ray Shanahan, *Department of Defense*	19891 Using Cyber Resiliency Frameworks to Engineer and Manage IT Services ▶ Dr. Subash Kafle, *The MITRE Corporation*	19863 Survey of Cyber Security Framework across Industries ▶ Mr. Ambrose Kam, *Lockheed Martin Corporation*
Track 2	Miller	**Education & Training** 4D2	19756 Teaching Executable Model-Based Engineering (MBE): Best Practices ▶ Mr. Matthew Cotter, *The MITRE Corporation*	19760 The Systems of Systems (SoS) Primer: A Guide to SoS for all Expertise Levels ▶ Ms. Laura Antul, *The MITRE Corporation*	19865 Breaking Out: Systems Engineering To Go ▶ Mr. Zane Scott, *Vitech Corporation*
Track 3	Von Sternberg	**Engineered Resilient Systems** 4D3	19712 Implementation of Clustering Analysis in Engineered Resilient Systems Tools for Enhanced Trade Space Exploration of Military Ground Vehicles ▶ Mr. Andrew Pokoyoway, *TARDEC*	19818 Tradespace Analysis and Exploration incorporating Reliability, Availability, Maintainability, and Cost ▶ Dr. Lance Fiondella, *University of Massachusetts*	19741 Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems ▶ Mr. Thomas McDermott, *Georgia Tech Research Institute*
Track 4	Gibson	**Program Management** 4D4	19847 Proactively Managing Supplier Relationships for an Integrated Product Development Program ▶ Ms. Beth Layman, *Layman & Layman*	19932 Improving Efficiency in Assembly, Integration and Test (AI&T) ▶ Mr. Jeff Juranek, *The Aerospace Corporation*	19842 "Other Transactions" - An Alternative to Business as Usual ▶ Mr. Richard Dunn, *Strategic Inst for Innovation in Govt Contracting*
Track 5	Sellier	**Environment, Safety & Occupational Health** 4D5	19766 ESOH Management in Agile and Rapid Acquisitions Using Digital Engineering ▶ Mr. Sherman Forbes, *SAF/AQRE*		
Track 6	Korman	**Enterprise Health Management** 4D6	19523 Mission-Based Forecasting for the Sustainment Enterprise ▶ Col Greg Parlier, USA (Ret.), *GH Parlier Consulting*		

Thursday, October 26 - Continued

			4:30PM - 4:55PM	4:55PM - 5:20PM	
Track 1	Singleton	System Security Engineering 4D1	19722 The Systems Challenges of Cybersecurity ▶ Mr. Jeffery Zili, *Vitech*	19895 Modeling Cyber Security ▶ Mr. Ambrose Kam, *Lockheed Martin Corporation*	
Track 2	Miller	Education & Training 4D2	19914 Bridging the Gap to MBSE ▶ Mr. James Baker, *Sparx Systems*	19719 Introducing Cyber Resiliency Concerns Into Engineering Education ▶ Mr. Thomas McDermott, *Georgia Tech Research Institute*	
Track 3	Von Sternberg	Engineered Resilient Systems 4D3	19781 Additive Manufacturing – Challenges... Program Manager ▶ Mr. William Decker, *DAU Huntsville*	20051 Model-Based Engineering: Opportunities, Risks, and Best Practices ▶ Dr. Marc Halpern, *Gartner, Inc.*	

5:20PM **Adjourn Conference**

SILVER SPONSORS

IBM®

At IBM Research, we invent things that change the world. We are pioneering promising and disruptive technologies that will transform industries and society, including the future of AI, blockchain and quantum computing.

We are driven to discover. We are home to more than 3,000 researchers in 12 labs located across six continents. Scientists from IBM Research have produced six Nobel Laureates, 10 U.S. National Medals of Technology, five U.S. National Medals of Science, 6 Turing Awards, 19 inductees in the National Academy of Sciences and 20 inductees into the U.S. National Inventors Hall of Fame.

Our teams are pushing the boundaries of science to uncover tomorrow's breakthroughs for national security, economic growth and jobs. We are especially focused on microelectronics as a national critical resource. The semiconductor industry is a foundational industry for modern society. Semiconductors enable all electronics; they are at the base of the electronics food chain and make digital life – every electronics system in the world – possible. Technological leadership in semiconductor research, development, design and manufacturing is vital for economic growth and especially for national security.

LOCKHEED MARTIN

"Headquartered in Bethesda, Maryland, Lockheed Martin is a global security and aerospace company that employs approximately 97,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services."

Raytheon

Raytheon Company is a technology and innovation leader specializing in defense, security and civil markets throughout the world. With a history of innovation spanning more than 90 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems; as well as a broad range of mission support services.

THANK YOU TO OUR SPONSORS

IBM®

jama software

LOCKHEED MARTIN

Raytheon

Pulling the Digital Thread with Model Based Systems Engineering

10/25/2017

Chris Finlay
finlayc@raytheon.com
401.842.2691

Stacy Gottesman
smgottesman@raytheon.com
520.794.8474

Julie DeMeester
julied@raytheon.com
978.858.4759

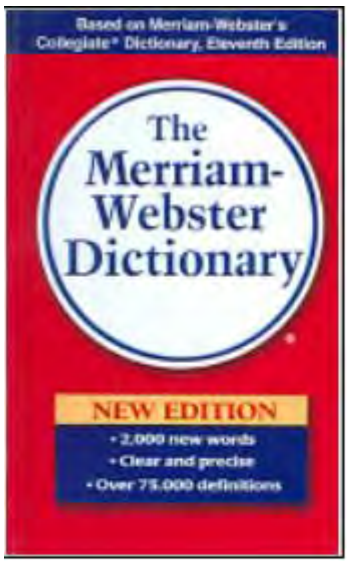
Raytheon

Agenda

- MBE Vision
- Digital Thread Process
- Creating the Systems Digital Thread
- Pulling the Digital Thread through SW Development
- Pulling the Digital Thread through HW Development
- Benefits
- Lessons Learned

First... Some definitions

Digital Thread vs. Digital Twin



The ***digital thread*** refers to a **collaborative engineering framework** that digitally connects data flow and data views of a system throughout its lifecycle across traditionally “siloed” engineering functions.

The ***digital twin*** refers to a physics-based set of digital models representing a physical system, its surrounding environment and real time data feeds. The digital twin represents each unique as-built system instance and operational and environmental data unique to that specific serial number it represents.

This Paper focuses on the Digital Thread

Raytheon

Model Based Engineering

*Engineering solutions composed as a set of models **linked** through an **information** infrastructure forming a **Digital Thread** that provides **authoritative source of truth***

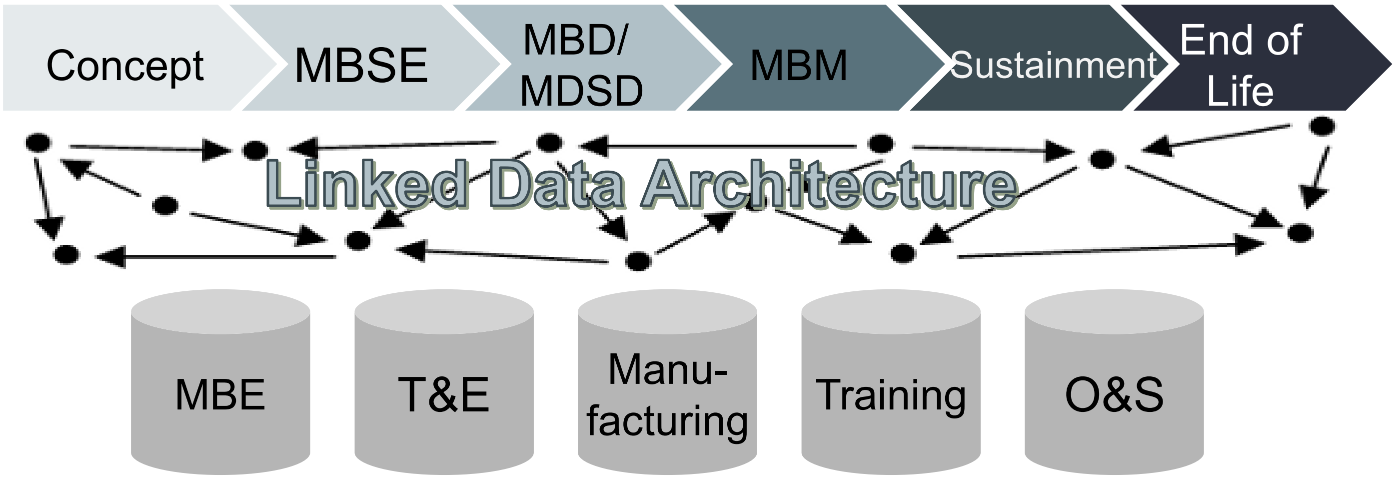
- Our model data is then turned in to **actionable information** as part of the overall design processes
- Our models become the source of information for deliverable documents which are **produced automatically**
- **Design decisions** are then **linked** and **consistent** across the solution space

The Models are the Master

Raytheon

Digital Thread Process

- Provides end-to-end information flow across the product lifecycle
- Enables a digitally linked data architecture (OSLC-enabled)
- Determines "what" information is important
- Enhances value-stream mapping and eliminates "air gaps"



MBSE = Model Based Systems Engineering
MBD = Model Based Definition
MDSD = Model Driven SW Development
MBM = Model Based Manufacturing

Provides actionable information through upstream and downstream impact analysis

Raytheon

System Digital Thread

Inputs

- Requirements
- Stakeholders
- Designers
- Testers
- Manufacturing
- Environment

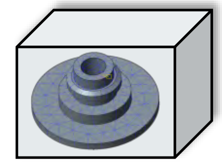
Tools and Techniques

System Design

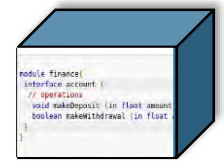
- Requirements Allocation and Flowdown
- SysML, UML Models
- Modeling Environment (Rhapsody, Magic Draw, etc.)
- Performance Analysis (Matlab)
- Architecture Frameworks (DODAF, etc)
- Collaborative Environment
- Automation (modeling, reporting, etc.)

Outputs

- Product Arch
- HW/SW Specs
- Req. Allocation
- Trade Studies
- Test Arch
- Interface Def.



Hardware Design



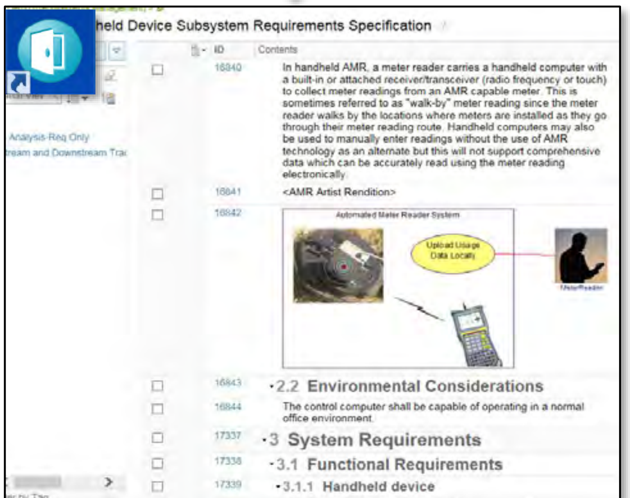
Software Design

System Test

MBSE enables our system design process to yield more accurate and consistent digital thread outputs

Creating the System Digital Thread

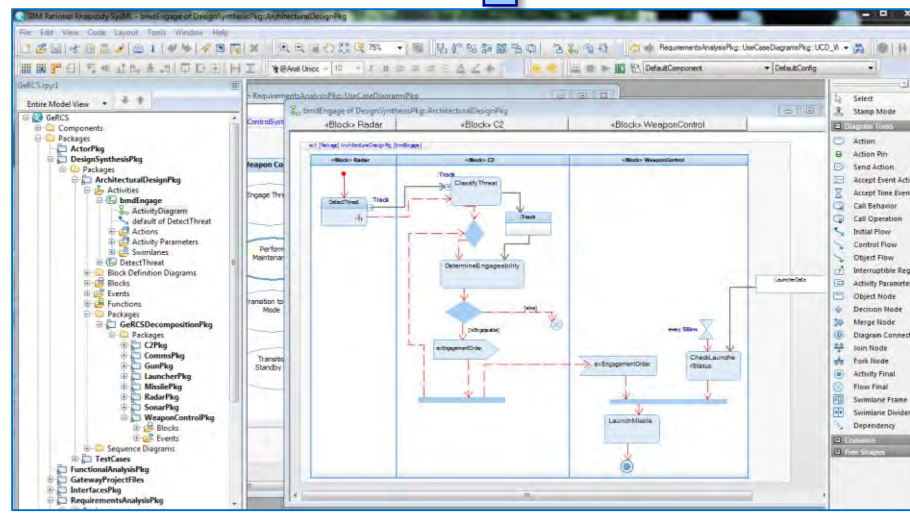
Requirements



Requirements Allocations/Flowdowns - digital linkages between requirements in a requirements management tool (DNG)

- System Requirements
- Software Requirements
- Hardware Requirements
- Test Requirements

SysML Models



Generate Integrated SysML Model - typically in Rhapsody or MagicDraw. Power Point and Visio SysML diagrams **do not** count

Use Case Modeling

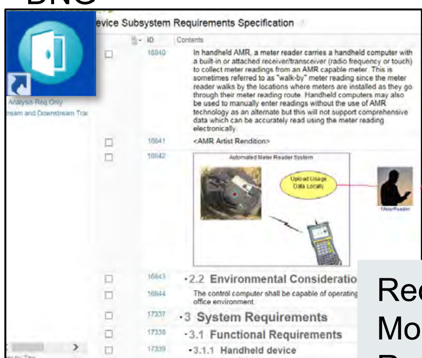
- System Use Cases
- Behaviors
- Interfaces
- Functions

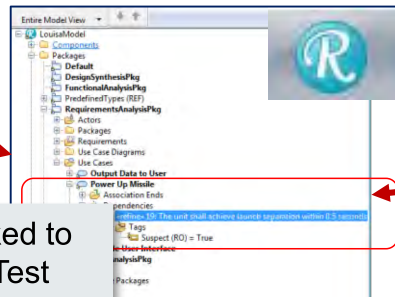
Raytheon

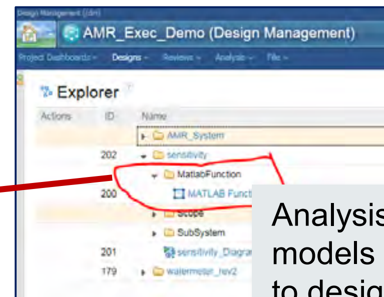
Creating the System Digital Thread

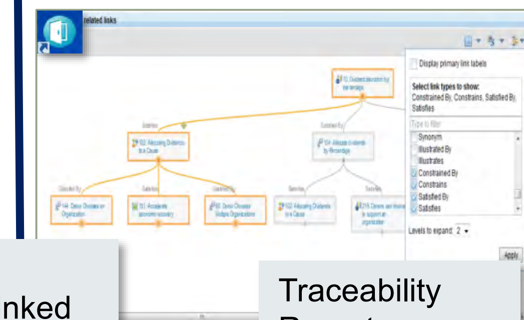
Requirements → System Models → Performance Analysis | Automated Digital Thread Reporting

DNG









Reqs linked to Models, Test Reports

Analysis models linked to design models

Traceability Reports across all artifacts

Requirements Allocations/Flowdowns - digital linkages typically between requirements and the SysML/UML models, HW Design Models, test Artifacts (RQM) and analysis models

System Design Model Traceability – digital linkages between SysML models and other models such as UML models, HW design models, Test Artifacts and analysis models

Automated Report Generation – reports are generated automatically using the tools that contain the digital linkages.

- Software Requirements
- Hardware Requirements
- Test Requirements

Reporting Actionable Information

- Requirement Traceability
- Verification Matrix
- Impact Analysis

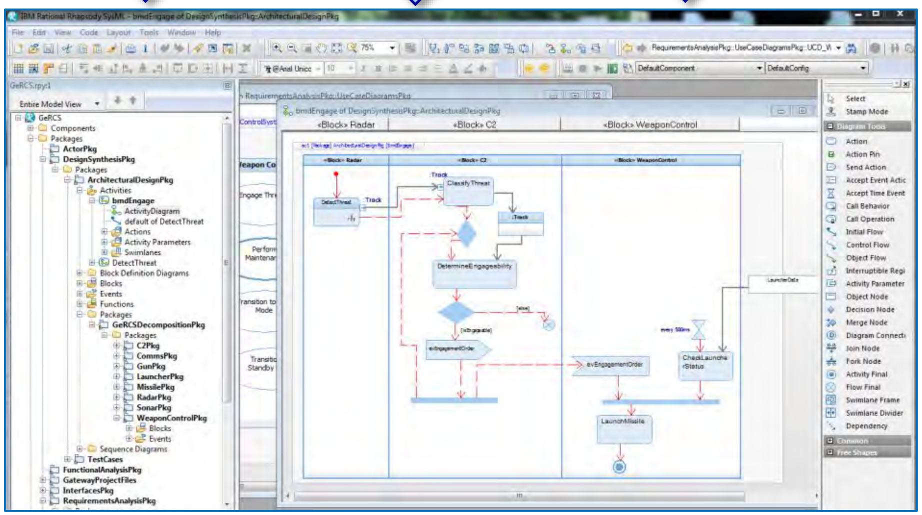
Raytheon

Creating the System Digital Thread

SysML Model

Requirements Links

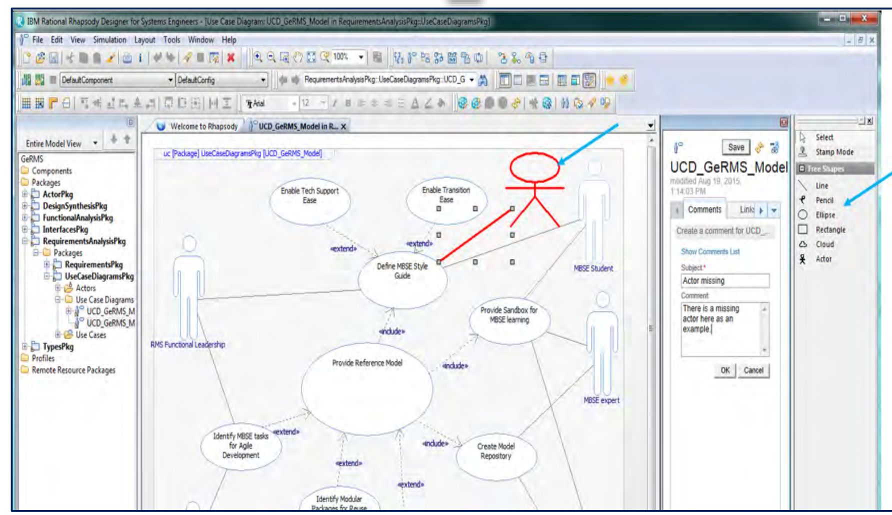
Performance Analysis Links



Generate Integrated SysML Model - typically in Rhapsody or MagicDraw. Power Point and Visio SysML diagrams **do not** count

- System Use Cases
- Behaviors
- Interfaces
- Functions

Reviewed Models and Digital Thread



Perform Model Based Peer Reviews - typically in Rhapsody Design Manager (RDM) for Rhapsody or Collaborator for MagicDraw.

Team Reviews

- Web-based (Don’t need design tool)
- Comment directly on model (eliminate air-gap)
- Archives with Model View Versions

Creating the System Digital Thread

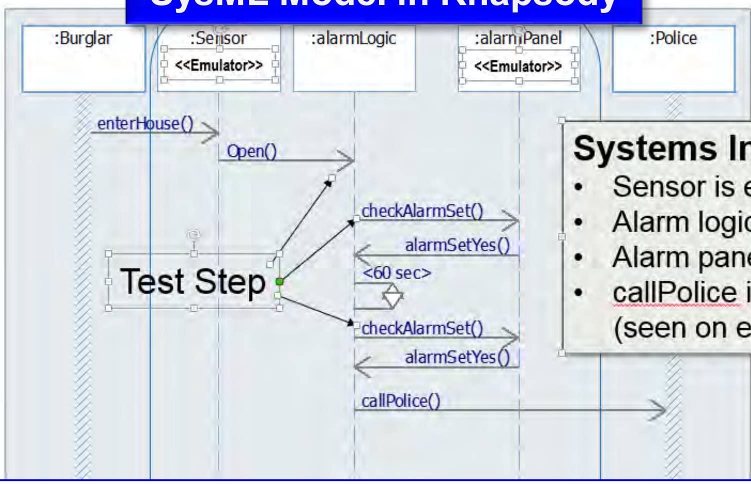
System Models

Requirements (DNG/DOORS)

Test Plans and Procedures

Test Result Reports and Metrics

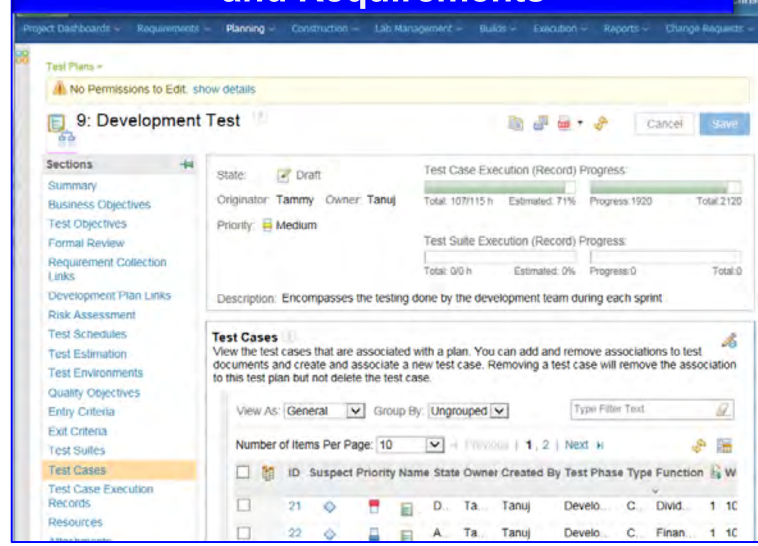
SysML Model in Rhapsody



Systems Integration SIL:

- Sensor is emulator
- Alarm logic is software
- Alarm panel is emulator
- callPolice is output message (seen on emulator)

Test Artifacts (RQM) Linked to Models and Requirements



Model Driven Testing - Test Sequences, Vectors and Stimulators defined in models. Test artifacts (e.g., cases, plans, procedures) link to the model(s) to define the scope and interactions required for each test event.

Test Defintion- Test artifacts (e.g., cases, plans, procedures) linked requirements and model. Documents and reports automatically generated

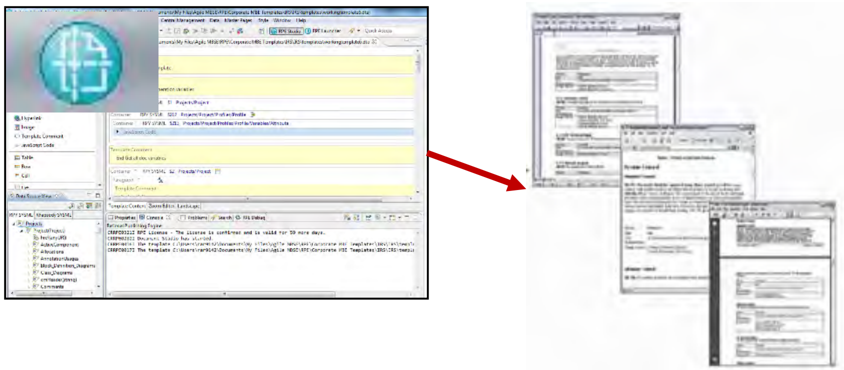
Test Artifact Development

Raytheon

Maintaining the System Digital Thread

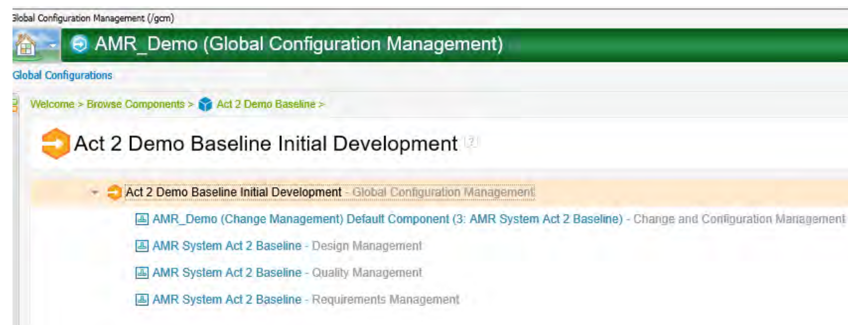
Requirements | System Models | Test Artifacts

RPE



Automatic Creation of Derivative Artifacts - typically with Rational Publishing Engine (RPE) for Rhapsody

Requirements Baseline | System Models Baseline | Test Artifacts Baseline



CM of Models – Configures baselines across multiple contributing applications forming a “configuration of configurations”

Keeping the Digital Thread maintained is just as important as creating it in the first place

Getting Actionable Information Out

Digital Thread Impact Analysis

Note:
Garbage In = Garbage Out

Digital Thread rapidly and confidently identifies potential upstream and downstream impacts to design modifications.

Raytheon

Software Digital Thread

Inputs

- SW Rqmts
- System Arch
- Trade Studies
- Test Architecture
- Interface Definition

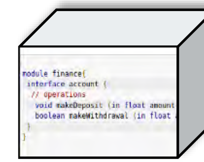
Software Design

Tools and Techniques

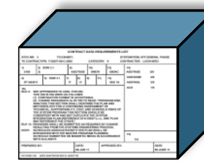
- Software Requirements Flowdown
- UML Models
- Software Modeling Environment (Rhapsody, Magic Draw, Eclipse, etc.)
- Code Generation
- Continuous Integration and Test
- Automation (Code, CDRLs, Reports, etc.)

Outputs

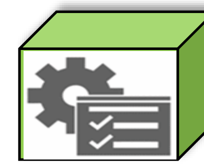
- SW->SE Trace
- Software Arch
- Data Model
- Design Artifacts
- Source Code
- Integration Tests



Generated Software



Generated CDRLs



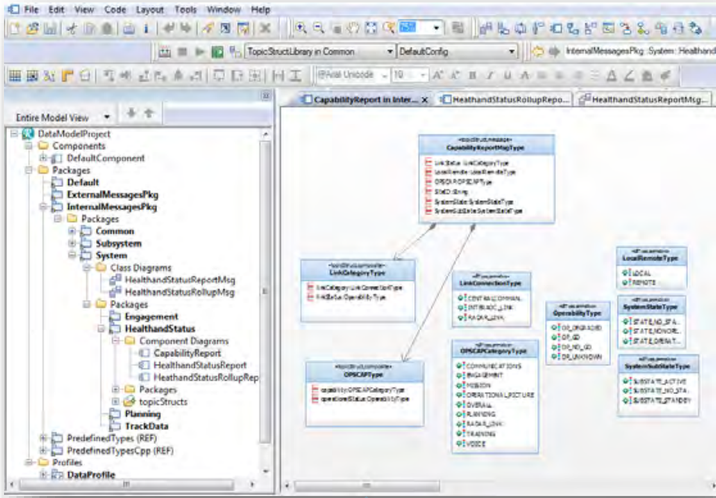
Automated Tests

Connecting the Digital Thread across engineering functions further enhances design consistency

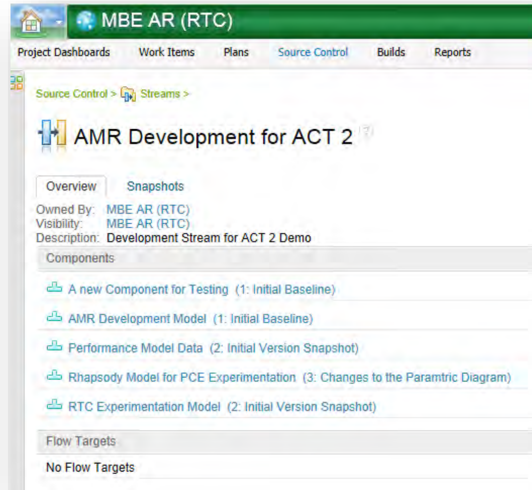
Raytheon

Pulling the Digital Thread through Software

Create Software & Data Model in Rhapsody/RDM



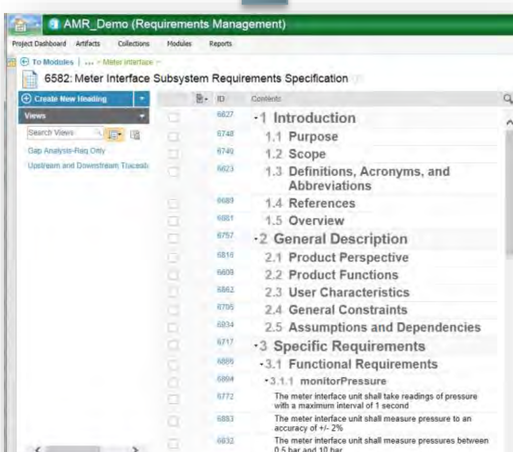
Manage/Track Changes in RTC



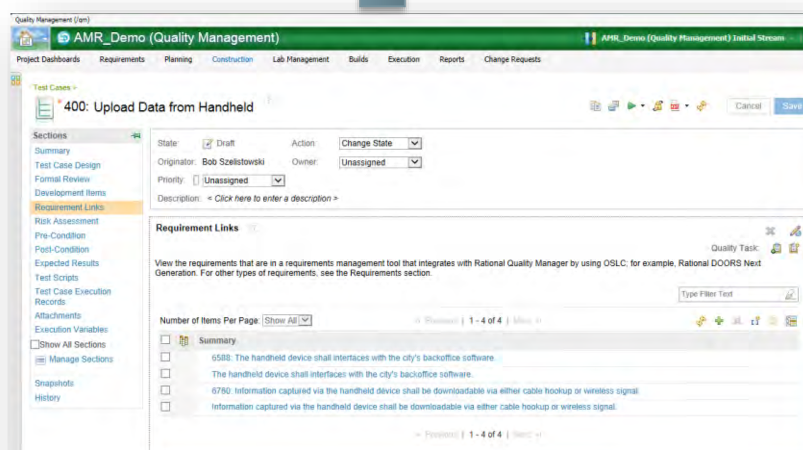
Code Generated from Model

Trace to Model

Continuous IV&V



Validated by Test Case



Requirements in DNG

Test Cases & Execution Results in RQM

HW Digital Thread

Inputs

- HW Rqmts
- System Arch
- Trade Studies
- Test Architecture
- Interface Definition
- Functional Decomp

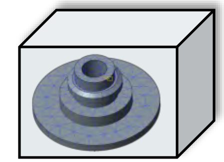
Hardware Design

Tools and Techniques

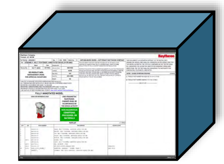
- Hardware Requirements Flowdown
- HW Models (3D CAD, FEA, Schematics, etc..)
- HW Modeling Environment (Creo, Mentor, etc…)
- Modeling Standards
- Derivative Artifact Generation (3D PDF, neutral model formats)
- Digital Thread Integration Platform
- Multi-physics Co-Simulation platforms

Outputs

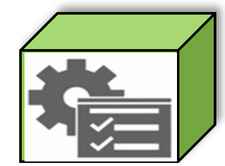
- HW->Sys Trace
- HW Arch
- HW Models
- Design Artifacts
- Integration Tests



Hardware Design



Technical Data Package

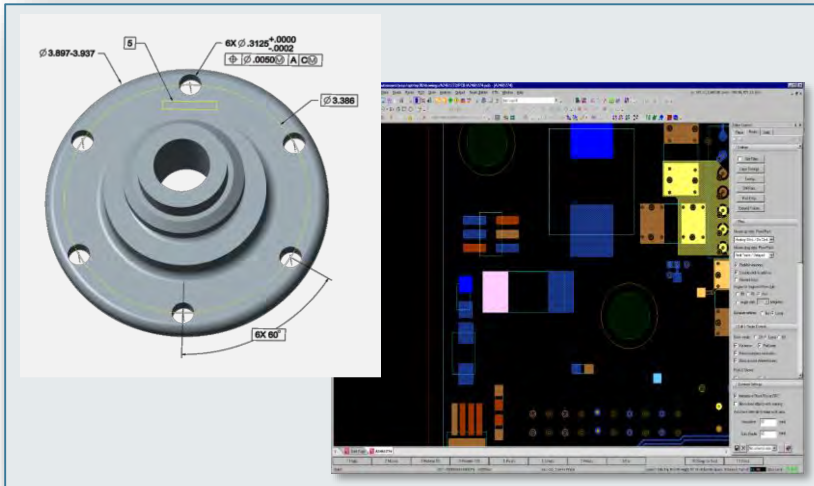


Digital Twin Artifacts

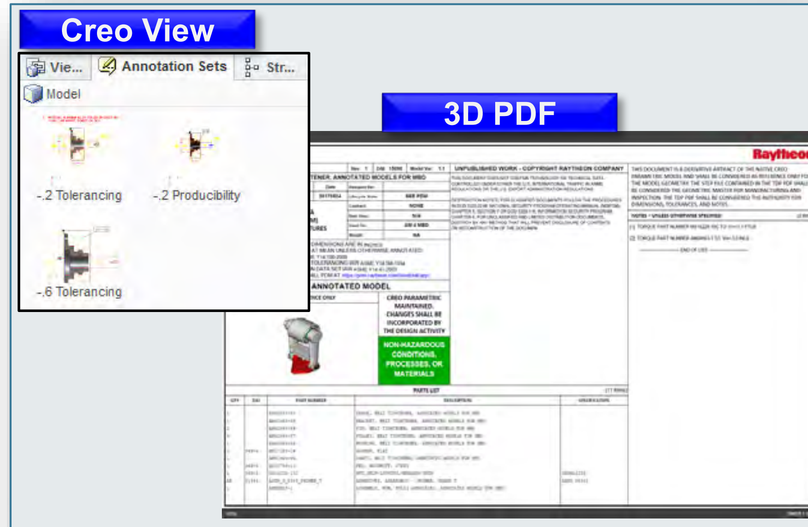
The HW Digital Thread provides the basis for Model Based Manufacturing and the Digital Twin

Pulling the Digital Thread through HW

Create ME/EE Design Models



Model Based Peer Reviews

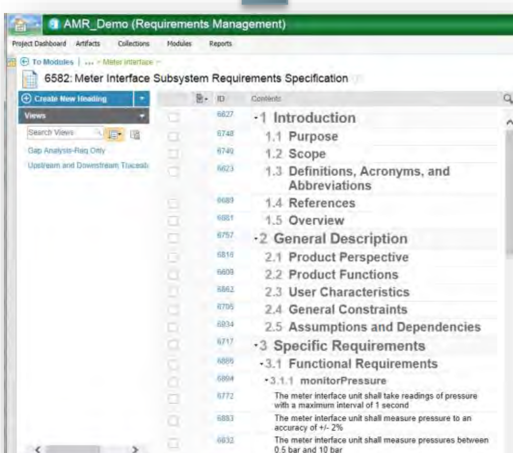


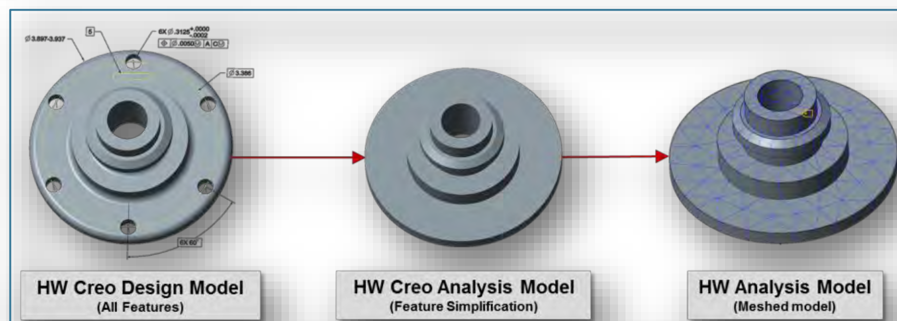
Derivative Artifacts Generated from Model

Trace to Model

Design Analysis and Optimization

Validated by Test Case





HW Requirements in DNG

Analysis Models Linked and Sourced to Design Model

MBE Digital Thread Benefits

- Because information is linked and does not live as stove-piped information in documents or disconnected models…
  - **Eliminate manual transfers**, data redundancy and increase data integrity (*removes "air gaps")*
  - **Provides automated impact analysis** on proposed changes
  - Facilitates **traceability of design decisions** for life of design
  - Make **changes in one place** and propagate change through linkages (lowers risk of missing key work products or causing disconnects / escapes
  - Can perform **early and continuous design refinement** with easy cross reference to design details
  - Models may be **re-used** across disciplines, across the life cycle of a program and across programs
  - Enforced rigor **reduces risk** associated with system complexity
  - **Communicate more effectively** across stakeholders because of the graphical nature of many types of models. (*shift defect detection curve to the left*)
  - Facilitates **knowledge transfer** of our system design decisions.

Raytheon

Lessons Learned

- Technology is still emerging, we can't do everything we need to yet to eliminate all the "air gaps"
- Some 3rd party OEMs collaborate more openly with others
  - Digital Thread will only survive if tools integrate with each other through common standards… no one tool meets all needs
  - Need more collaboration amongst the tool vendors
- Customers are starting to ask for MBSE/MBE specifically in RFPs ☺… RFP language does not accurately reflect common MBE conventions or specifies the MBE digital thread vision but does not reflect the current state of technology ☹
- There is still a cultural barrier both within industry and with the Customer on MBE adoption. Good news is that we are all making headway

NDIA 20th Annual Systems Engineering Conference (23-25 Oct 2017) Presentation #19770

TSCA Panel: Assessing the impacts of Amended Toxic Substances Control Act (TSCA) to the DoD Mission and the Defense Industrial Base.

Sustainable Hazardous Material Management:

- ***Manage/minimize risks & identify safer alternatives to toxic chemicals while ensuring performance to meet mission requirements***
  - ***Protect Human Health and the environment***
  - ***Reduce costs of regulation; hazardous waste storage and disposal, worker protection, and future liabilities***
  - ***Stimulate innovation – research and development on chemicals of importance to DoD mission.***

- ***Risk Evaluation for Existing Chemicals under Amended TSCA***
  - **Purpose: "Determine whether a chemical substance presents an *unreasonable* risk to health or the environment under the *conditions of use* (of the chemical substance)"**
- ***"Conditions of Use"***
  - **Means the circumstances under which a chemical substance is intended, known or reasonably foreseen to be manufactured, processed, distributed in commerce, used, or disposed of.**
  - **Intended to avoid past practices of assessing only narrow uses of a chemical substance but towards a more inclusive approach to chemical substance management**
  - **Intent is not on individual uses (to prioritize chemicals) but on substances that present a potential hazard and potential route to exposure under the "conditions of use".**
- ***End User Considerations:***
  - **Uses/Disposal – Applications/Performance; Management/Controls; Alternatives/Transitions(Implementation)/Resourcing.**
    - **Hazardous Chemicals are widely used in connection with all phases of the System Acquisition process.**
    - **System/Performance-Driven Requirements for use:**
      - **Contained in technical manuals, specifications, etc., that govern the processes and procedures for weapon systems operations and support.**
  - **Conditions Affecting Replacement or Elimination**
    - **Commercial availability of potential viable (equal to or improved performance) alternatives for specific applications.**
    - **Potential alternative(s) are less hazardous to personnel safety and environment under management and control processes and practices.**
    - **Cost/Resourcing impact analysis of potential alternative chemicals/processes.**

TSCA Panel: Assessing the impacts of Amended Toxic Substances Control Act (TSCA) to the DoD Mission and the Defense Industrial Base.

Process to identify items containing chemicals targeted by amended TSCA rules

- *Identify National Stock Numbers (NSNs) and associated applications in use which contain chemicals targeted by proposed TSCA rules.*
- *HMIRS -- Serves as the DoD SDS Repository as mandated by the DODI 6050.05*
  - Data is maintained by each service data stewards for items that they manage or locally purchase
  - HMIRS recently (30 June) went through migration to HMIRS NextGEN
  - Contains SDS/PDS images and associated data
  - Provide unique serial number per stock number and product formulation (e.g. DVGBX)
- *Navy builds full HMIRS records (logistics, SDS, and chemical data) in HMIRS for NSNs and only SDS and logistics for Local Stock Numbers (LSNs)*
- *Search HAZMAT Information Resource System (HMIRS) for products containing targeted chemicals in reportable quantities (≥ 1% or ≥ 0.1% for carcinogens).*
- *Using NSNs, determine Navy procurement, Systems HAZMAT Lists status, and technical requirements.*
- *Calculate concentration of each targeted chemical in each NSN using percentages specified on the Safety Data Sheet (SDS).*
- *Identify technical POCs for applications. Identify prior substitution details.*
- *Contact technical POCs with recommended substitutes.*
- *If substitute is accepted, update technical documentation.*
- *If substitute is not accepted, document reason.*

Amended TSCA:

- Shifts the burden of demonstrating chemical safety — all chemicals, old and new — to chemical manufacturers, processors and manufacturers of the finished goods -- ***engage industry suppliers.***
- Mandates that the EPA prioritize and evaluate "high priority" chemicals according to an aggressive and judicially enforceable schedule -- ***plan/streamline the internal review processes of chemical substances.***
- Mandates EPA's review and evaluation of these chemicals, and many others determined to be "high priority" which will have significant impacts on the chemicals reviewed, their uses and applications and availability -- ***engage specifiers and systems engineering.***
- With change comes opportunity e.g. new sustainable products & technologies -- ***encourage innovation*** in more sustainable and less environmentally impactful chemistries/formulations.

NDIA Systems Engineering Conference

NDIA System Security Engineering Committee

October 2017

Holly Dunlap

Raytheon

NDIA SSE Committee Chair

Holly.Dunlap@Raytheon.com

Welcome

- Purpose of NDIA & SSE Committee
- Introductions
- SSE Track Agenda Review
- System Security Engineering Committee 2017 Accomplishments

SE Division Mission

- ***To promote the widespread use of systems engineering (SE) in the Department of Defense (DoD) acquisition process in order to achieve affordable and supportable weapon systems that meet the needs of the military users. To provide a forum for the open exchange of ideas and concepts between government, industry and academia. To develop a new understanding of a streamlined SE process.***
- ***The SE Division seeks to effect good technical and business practices within the aerospace and defense industry. It focuses on improving delivered system performance, including supportability, sustainability, and affordability. The division emphasizes excellence in systems engineering throughout the program life cycle and across all engineering disciplines and support functions.***

Introductions & Around the Room

NDIA SSE Track Review

NDIA SSE Committee Accomplishments

- **NDIA SSE Committee Accomplishments**
  - NDIA Cyber Resilient & Secure Systems Summit, April 18 – 20th
  - NDIA SSE & SwA Co-Sponsored with the Joint Federated Assurance Center (JFAC) a (2) Day Government SwA Gap Analysis Workshop. June 22nd & 23rd.
  - Acquisition Language

NDIA Cyber Resilient & Secure Weapon System Summit Purpose

NDIA Systems Engineering Division held a "Top SE Issues Workshop", August 2016

Cyber Resilient & Secure Weapon Systems was identified as a Top SE Issue

System survivability in a cyber contested operational mission environment is critical. We need to elevate the system security risk to the program risk register to ensure a security focus. We need well defined methods, processes, standards, metrics and measures, along with skilled professionals to integrate system security into our product development lifecycle.

Top SE Issue: Cyber Resilient & Secure Weapon Systems

- **Due to the evolving and persistent cyber system security threat that impacts our interconnected systems, focused attention is required. The following main points also include tenants of engineered resilient systems and mission assurance:**
  - **System Security risks** must be added to the **program risk register** to ensure that security doesn't get traded away to system technical capabilities and cost reduction efforts.
  - Well defined **metrics** and **measures** are needed to conduct trades: cost, risk, and performance.
  - **CONOPS** and **SoS** along with **System critical mission threads** are essential to initiate and focus the system mission functional criticality analysis.
  - **Integration of the security specialties** into the **system security architecture view** needs to be defined and methods developed.
  - NIST SP 800-160 establishes a foundation for System Security Engineering best practices. We need to develop **education and awareness training** to include a range of proficiencies for different **security specialties** with experience in mission system platforms and embedded systems, along with a **range of acquisition professionals.**

Top SE Issue Report Recommendation

- **NDIA System Security Engineering Committee with support from the NDIA Systems Engineering Division to convene a joint government/industry activity such as a workshop or summit, to dialog the relevant issues.**
  - **A Summit** is recommended to bring Government, Industry, and FFRDC working groups together to share **developments, strengths, gaps, opportunities, and recommendations**. The NDIA System Security Engineering Committee hosted a 3 day NDIA Program Protection Summit in May 2014 and is preparing for a Spring 2017 follow-up.
  - The new System Survivability KPP values are intended to define objective values for a capability solution and derived from operational requirements of the system. **Connecting the SS KPP, Cyber Resiliency metrics**, and **System Security Specialty Risk Mitigations** offers a compelling means to conduct risk, performance, cost trades and compare one solution to another.
  - **Verification** and **validation criteria** need to be identified and methodologies established to achieve same.
  - **Cyber Resilient** and **Secure System** requirements **SOW & RFP** along with **Sections L&M** evaluation criteria guidance needs to be matured with metrics and measures to ensure a holistic approach for managing system security risks.

NDIA SSE Committee Meeting Agenda
June 28, 2017 Guest Speakers

- **AF SES Cyber Technical Director**
  - Mr. Daniel Holtzman, Cyber Resiliency Office for Weapon Systems (CROWS) AFLCMC/
- **OSD SE PPP Deputy Director, Ms. Melinda Reed**
  - Mr. Michael McEvilley, Mitre on behalf of Melinda Reed
- **AF Aircraft Cyber Threat Working Group (ACTWG)**
  - Col Masterson, Deputy Associate Director of Engineering & Technical Management Deputy Director, Cyber Resiliency Office for Weapon Systems (CROWS) AFLCMC/
- **University of Virginia, Systems Engineering Research Center (SERC)**
  - Mr. Peter Beling

NDIA Government SwA Gap Analysis Workshop

Sponsors: NDIA SSE & SwA Committee & OSD Joint Federated Assurance Center (JFAC)

Background:

In July 2016, the JFAC SwA Technical Working Group identified 63 DoD capability gaps that prevent the effective planning and execution of software assurance within the DoD acquisition process. The gaps were organized into seven categories:

(1) life cycle planning and execution; (2) SwA technology; (3) policy, guidance, and processes; (4) resources; (5) contracting and legal; (6) metrics; and (7) federated coordination

As chair of the JFAC Steering Committee, Ms. Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineer (DASD(SE)), recently approved the analysis and directed the Technical Working Group to develop a strategy to address the identified gaps.

In February 2017, a Defense Science Board Task Force issued a report on cyber supply chain with two (out of a total of 25) overarching recommendations to USD(AT&L):

(1) Strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that systems are designed, fielded, and sustained in a way that reduces the likelihood and consequence of cyber supply chain attacks.

(2) Direct development of sustainment Program Protection Plans for critical fielded weapons systems. Military Service Chiefs should designate fielded weapons systems for development of initial sustainment PPPs to demonstrate their effectiveness.

NDIA Government SwA Gap Analysis Workshop Objectives:

NDIA

Generate feedback from industry on the recent DoD and Defense Science Board Task Force reports on SwA capability gaps within the DoD.

Collect industry's SwA challenges and capability gaps as you develop, sustain, and support our Nation's warfighting capabilities.

Provide JFAC with industry input to prioritize existing and future funding to address the Department's capability gaps.

Workshop pre-work

- **DSB Task Force report on Cyber Supply Chain**
- **JFAC SwA TWG Capability Gap Analysis**
- **Voice of Customer (VOC) Gap Analysis Worksheet & Instructions**

AF SSE Acquisition Language Guidebook Review & Comment

NDIA

United States Air Force

Systems Security Engineering (SSE)
Acquisition Language Guidebook
24 March 2017
VERSION 1.1

Distribution Statement D: Distribution authorized to DoD and U.S. DoD contractor
Administrative or Operational Use, determined 24 March 2017. Other requests for this do
shall be referred to AFLCMC/EZS (aflcmc.en-ez.weapon.systems.ia.team@us.af.mil).

Table of Contents

3

AF System Security Engineering Acquisition Language Guidebook

Please submit comments by July 15, 2017 to: Cory.L.Ocker@Raytheon.com and copy Holly.Dunlap@Raytheon.com using the Comment Resolution Matrix.

You are also welcome to send your comments to the AF directly.

AFLCMC/EN-EZ System Security Engineering Team (aflcmc.en-ez.weapon.systems.ia.team@us.af.mil).

Systems of Systems Engineering Technical Approaches as Applied to Mission Engineering

Dr. Judith Dahmann

Dr. Aleksandra Markina-Khusid

Janna Kamenetsky

Laura Antul

Ryan Jacobs

Topics

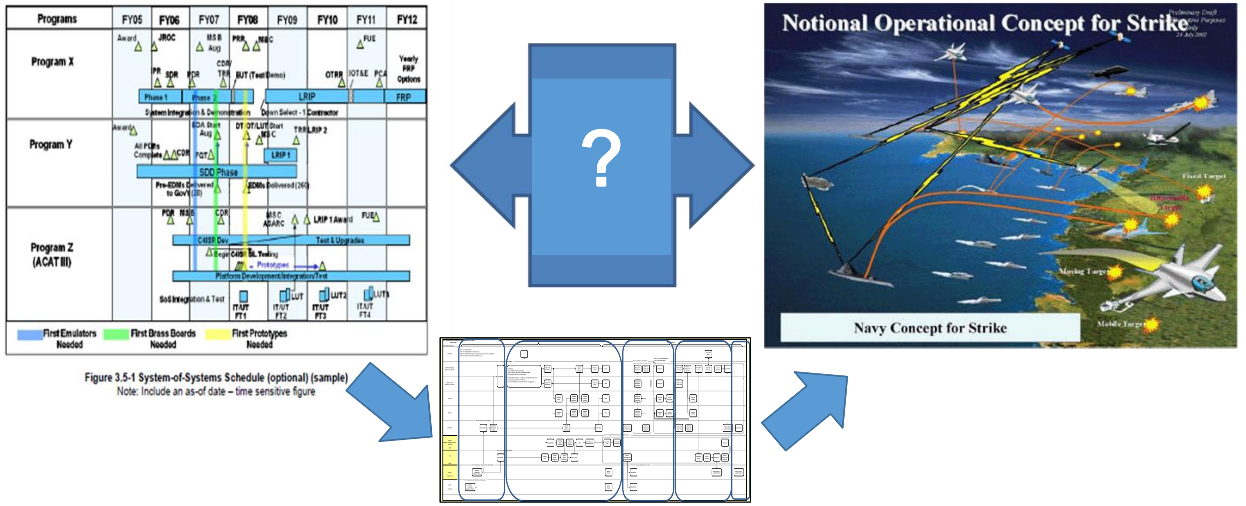
- **Mission engineering (ME)**
- **The relationship between system of systems engineering (SoSE) and ME**
- **Particular challenges of SoSE applied to missions**
- **Some SoSE technical approaches which address these challenges**

Mission Engineering Challenge

- Systems are acquired to meet user needs in a mission context
- Mission operations are supported by sets of systems (or systems of systems) which work together to achieve mission objectives
- Systems supporting each role in a mission (i.e. kill chain) will vary over the course of the operation and be used for multiple missions

System Acquisition

Operations



Mission/SoS
Architecture/Engineering

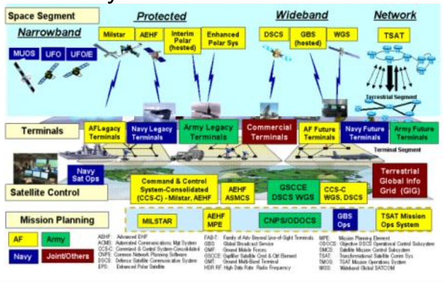
Mission Engineering is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects

Defense Acquisition Guide Ch 3

MITRE

Systems of Systems in Defense

Military Satellite Communications



Missions

Sets of systems working together to provide a broader capability or mission

Tactical Vehicle

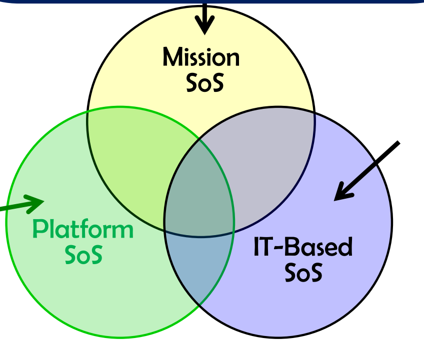
Platforms

A military platform (e.g. ship, aircraft, satellite, ground vehicle) equipped with independent systems (e.g. sensor, weapons, communications) needed to meet platform objectives

Operations Center

Information Technology

Networked information systems to support operations within or across platforms or systems to meet mission or capability objectives



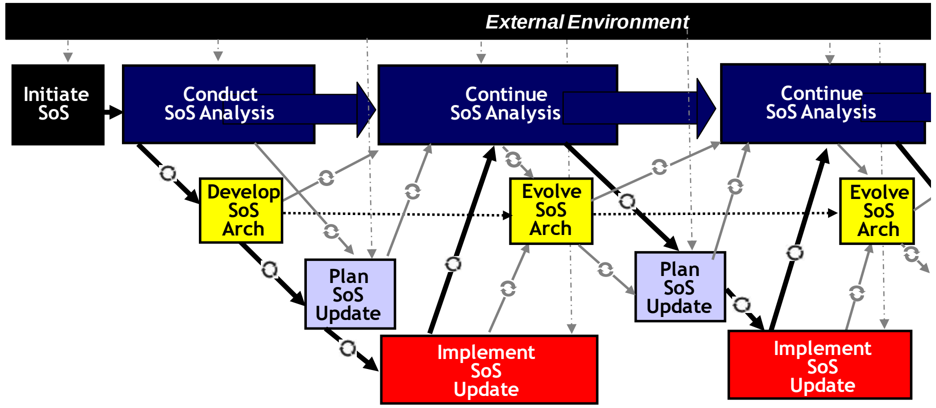
Considerations in mission SoS

- Mission environment
  - Mission context - variable physical environments, threats and non-material elements - critical in driving SoS for missions
- Composition
  - Execution of missions is based on the employment of the set of systems available and appropriate for the mission environment
  - Performance needs of a system in the Mission SoS may vary depending on the performance of other systems in the SoS (‘AKA ‘Float and Flow’)
- Mission ‘webs’ versus ‘threads’
  - While there may be a logical sequence of actions for a mission, in practice there are sets of systems which support missions under different situations

MITRE

SoSE Wave Model Applied to ME

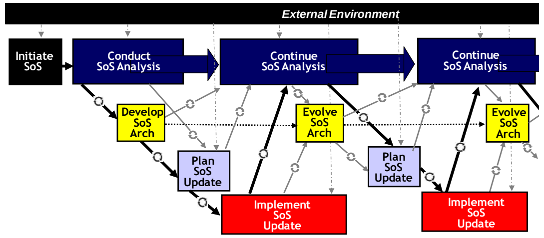
Define the mission including mission threads and mission context (*Includes mission objectives, CONOPs, scenarios, key functionality, threat*)	Conduct SoS Analysis
Identify current systems supporting the mission and how they are employed (*How are we implementing the mission today?*)	
Assess mission performance to assess how well current systems work together meet mission objectives	
Identify gaps from a mission effectiveness perspective and fault isolate the source of gaps	
Identify and assess options for improving the mission effectiveness (*Including changes in how the systems are employed as well as new or different systems, systems updates and non-material considerations*)	Develop SoS Architecture
Guide systems acquisitions, from requirements through implementation to test and maintenance to assure effective mission execution	Plan SoS Update
Conduct mission level integration and test	Implement SoS Updates
Monitor mission effectiveness with changes in mission context, scenarios and threat capabilities	



Like other SoS, SoS for missions

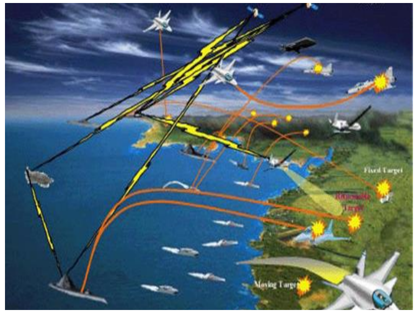
- Are ***not 'designed'*** top down, green field systems
- ***Evolve over time*** based on changing capability needs and systems
- Engineering follows the an **evolutionary** '***wave***' process versus traditional system 'V'

Mission Engineering
SoSE Engineering to Meet Mission Objectives



Baseline current SoS Against **Mission Objectives**
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Evaluate options and **trades across the SoS** to improve or sustain mission performance
- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces



Implement changes in systems, integrate and test updated SoS **mission capability**

Negotiate with systems to make changes to support **mission performance** improvement
- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

MITRE

Key Activities in ME Process

A key starting point for ME is understanding current state of mission

– Operational mission objectives and CONOPS (mission threads)
– Current and planned systems
– Identifying critical, priority mission gaps

Baseline current SoS Against **Mission Objectives**

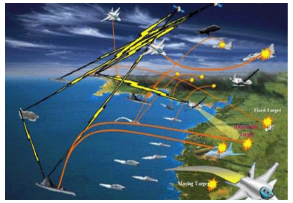
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Technical assessment of options and trades

– Fault isolating sources of gaps
– Assessing alternative approaches to addressing capability gaps

Evaluate options and **trades across the SoS** to improve or sustain mission performance

- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces



Implement changes in systems, integrate and test updated SoS **mission capability**

Tracking implementation, integration and test

– Given independence of systems and development schedules

Negotiate with systems to make changes to support **mission performance** improvement

- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

Planning and funding coordinated changes in systems

– 'Capability package' which cross systems owners and development schedules

MITRE

Key Activities in ME Process

A key starting point for ME is understanding current state of mission

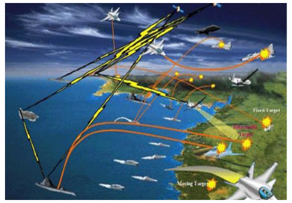
– Operational mission objectives and CONOPS (mission threads)
– Current and planned systems
– Identifying critical, priority mission gaps

Technical assessment of options and trades

– Fault isolating sources of gaps
– Assessing alternative approaches to addressing capability gaps

Baseline current SoS Against **Mission Objectives**
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Evaluate options and **trades across the SoS** to improve or sustain mission performance
- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces



Implement changes in systems, integrate and test updated SoS **mission capability**

Negotiate with systems to make changes to support **mission performance** improvement
- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

Tracking implementation, integration and test

– Given independence of systems and development schedules

Planning and funding coordinated changes in systems

– ‘Capability package’ which cross systems owners and development schedules

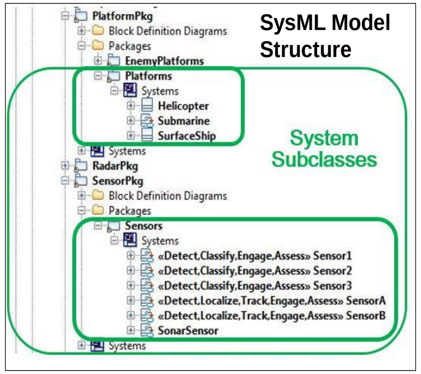
SoSE Technical Approaches to Address ME

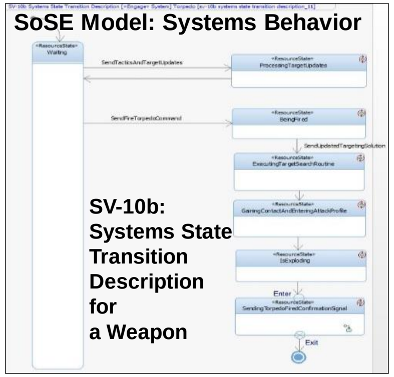
Technical assessment of options and trades
- Fault isolating sources of gaps
- Assessing alternative approaches to addressing capability gaps

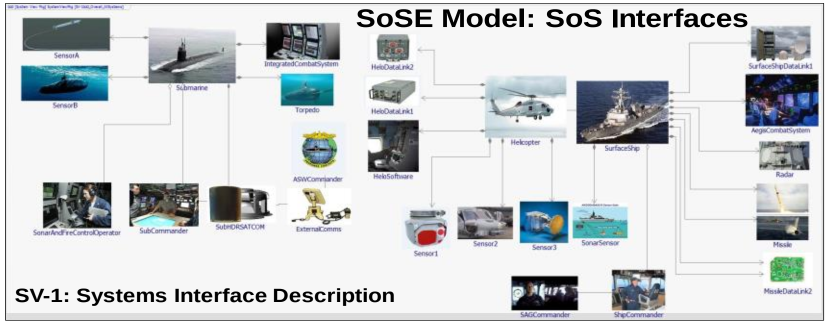
- **Mission environment**
- **Composition**
- **Mission 'web'**

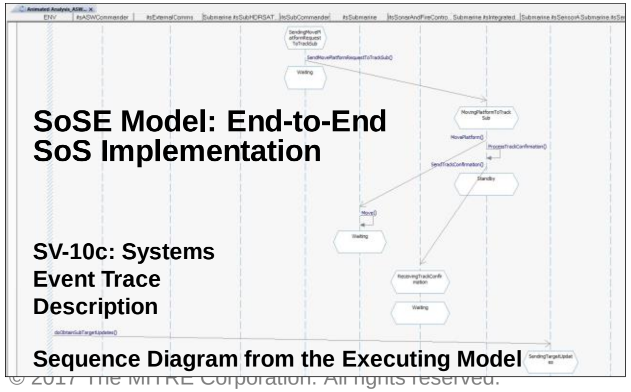
- **Scalable model-based approaches to SoS architecture representation**
- **Analytic approaches to SoS architecture assessment**
- **Assessing impacts of SoS architecture changes on operational mission outcomes**

Model-Based SoSE





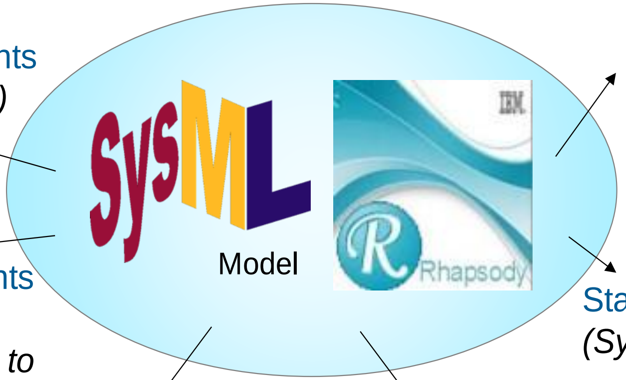




- **For SoSE purposes, SysML model represents an unambiguous, structured, executable, digital representation of the SoS system architecture**

Architecture Elements *(Systems Structure)*

Single Data Repository *(For Future Analysis and Testing Activities)*

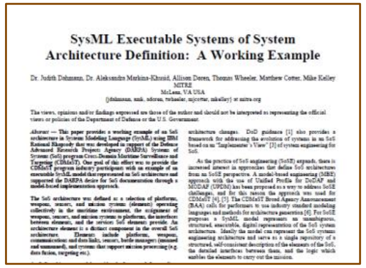


Mapping of Architecture Elements to Operational Activities *(Structure to Behavior)*

State Machine Diagrams *(Systems Behavior)*

Operational Activities *(Systems Behavior)*

Element Interactions via Model Execution *(Verification, Validation, and Visibility)*



"SysML Executable Systems of Systems Architecture Definition: A Working Example"

IEEE International Systems Conference
http://2017.ieeesyscon.org/

MITRE

Model-Based SoSE

Why is this important for mission engineering?

- The systems composed into an SoS architecture to support a mission are typically drawn from a **variety of specialty areas** (sensors, weapons, platforms, communications) and **diverse organizations** which bring **various perspectives** to the mission
  - ***Specificity*** provided by models can help avoid misunderstandings about system behavior, system interactions/interfaces (*Have I addressed all the needed interfaces to execute the end to end sequence of actions? Value of executable)*
- A model allows for representation of the complexity of the interrelations among systems in the mission, reflecting the variety of paths in the '***mission web***'
- It is important to have a ***commonly understood representation*** providing both the mission engineer and the constituent systems engineers a cross cutting integrated view across the systems and how they are expected to be employed in a mission context
  - Value of ***standards***-based modeling approaches

Sequence Diagram from the Executing Model

http://2017.ieeesyscon.org/

MITRE

Scalable Model-Based SoSE

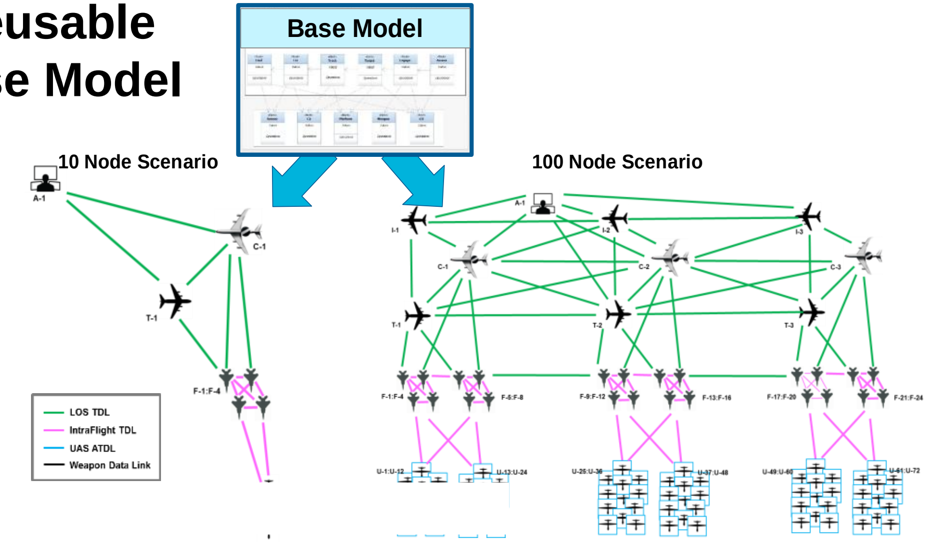
See NDIA paper XYZ for technical details

- **A key enabler of model-based SoSE is the ability to efficiently develop large complex SoS architecture model**

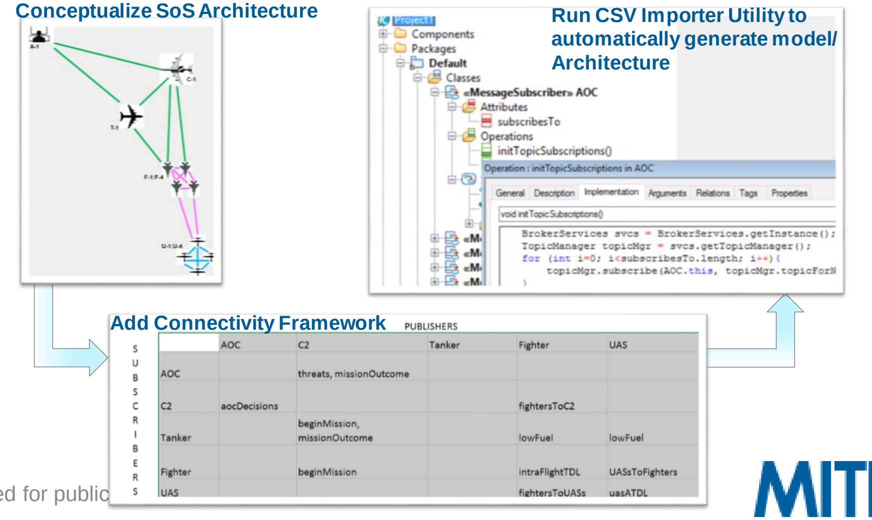
The effort required to build SoS architecture models can be reduced by starting the modeling process with a reusable **base model template**, independently of the architecture size

Tools can facilitate integration of SoS connectivity information into MBE tools, tightening the coupling between subject matter experts (SMEs), software engineers, and analysts -- comma separated variable (CSV) **importer tool**

Reusable Base Model



CSV Importer



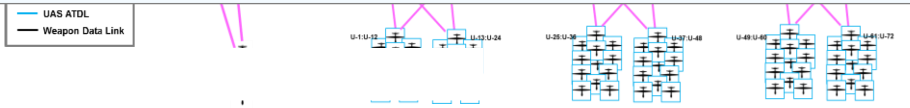
MITRE

Scalable Model-Based SoSE

See NDIA paper 19804 for technical details

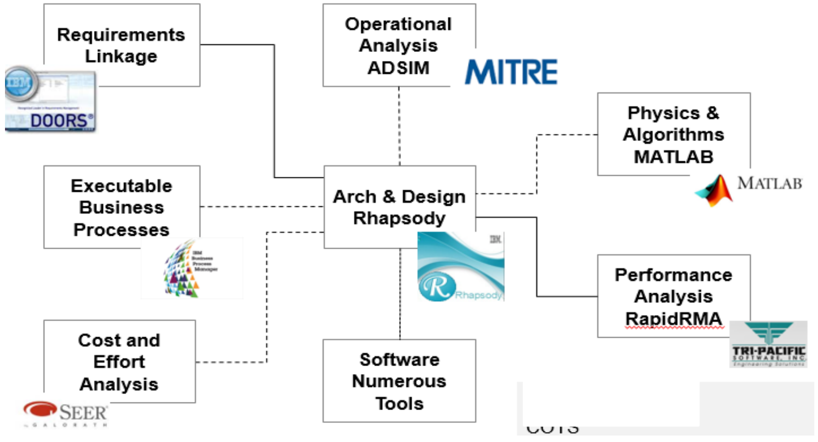
Why is this important for mission engineering?

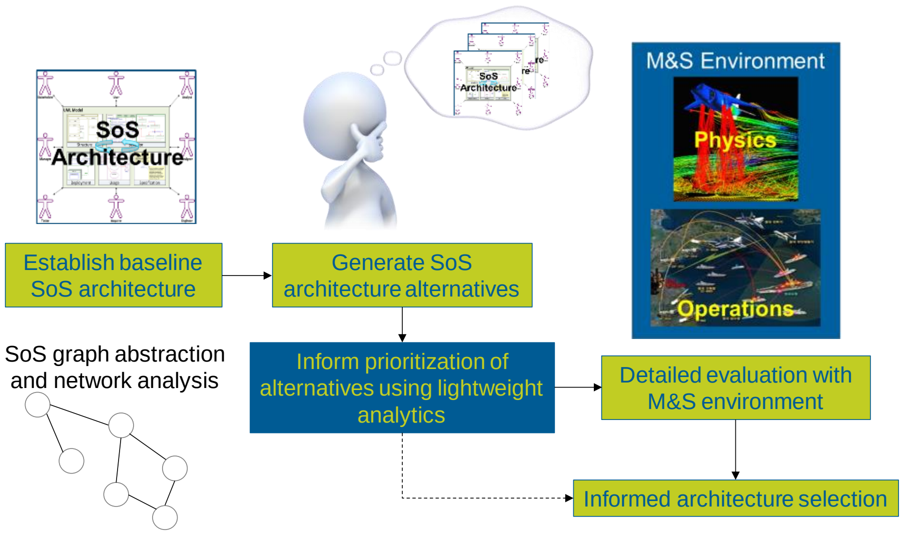
- Missions can be large and comprise many systems, and the time required to develop a model framework for each mission architecture can raise the ***cost of entry*** for use of models to support mission engineering
- Gathering the ***needed data*** to understand the current state of a large mission can be difficult given the diversity of knowledgeable mission stakeholders.
  - Providing ***intuitive tools*** to allow stakeholders to share knowledge in a way familiar to them can build confidence and speed knowledge gathering
  - Automated transform ***directly into a model*** again lowers the cost of entry for large mission architecture, and reduces likelihood of errors or misunderstandings



I	Tanker	missionOutcome	lowFuel	lowFuel
B E	Fighter	beginMission	intraFlightTDL	UASsToFighters
R S	UAS		fightersToUASs	uasATDL

Analytic Approaches to SoS Architecture Assessment (1 of 2)

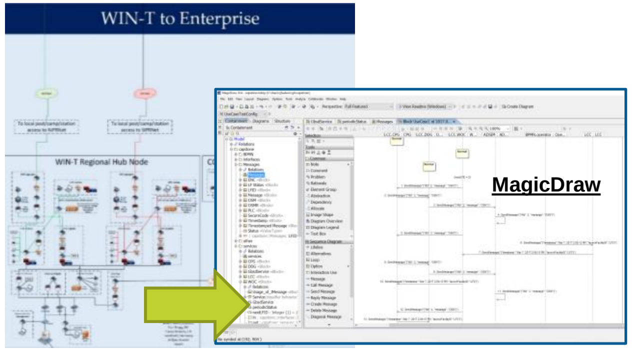


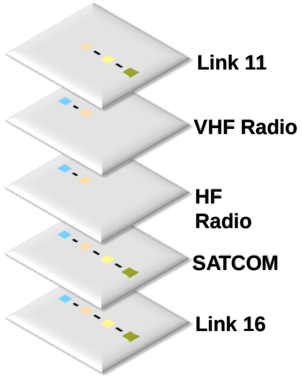


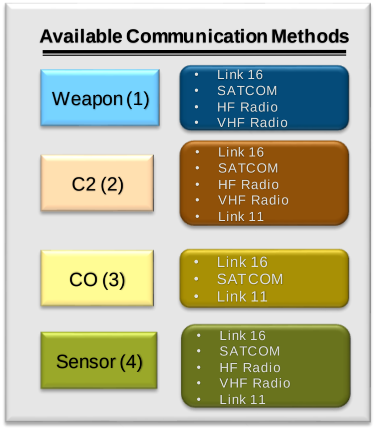
- **Representing SoS architecture in a model opens the options for analysis**
  - Interfacing a SoS model with other tools to assess performance, cost, other aspects of the SoS, provides a shared representation of the architectures for analysis from different perspectives
  - Developing approaches to assess alternative architectures is a challenge for the perspective of scalability
  - How do you identify viable options for more detailed analysis when there is such a large trade space?

Analytic Approaches to SoS Architecture Assessment (2 of 2)

Thread Simulation

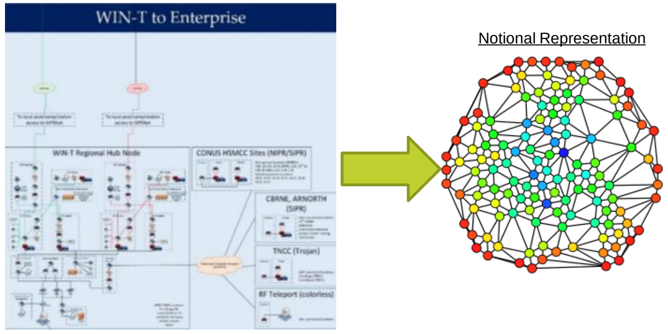






Identify Patterns and Inform Mitigation Strategies

Graph Theoretic Approach

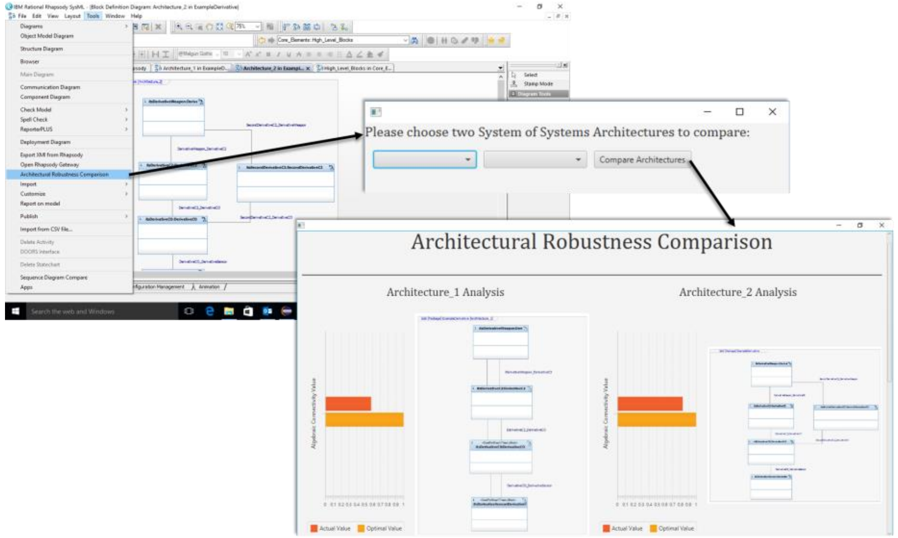


	VHF Radio		HF Radio		Link 11			Link 16				SATCOM			
VHF Radio	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0
	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
HF Radio	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0
	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0
Link 11	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0
	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0
	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1
Link 16	1	0	1	0	0	0	0	0	1	0	0	1	0	0	0
	0	1	0	1	1	0	0	1	0	1	0	0	1	0	0
	0	0	0	0	0	1	0	0	1	0	1	0	0	1	0
	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1
SATCOM	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0
	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0
	0	0	0	0	0	1	0	0	0	1	0	0	1	0	1
	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0

VHF Radio | Link 16 | Link 11 | HF Radio | SATCOM

Identify vulnerable assets within the Army Network Architecture

- **Use of architecture data in a graph theoretic analysis**



See NDIA paper 19802 for technical details

MITRE

Analytic Approaches to SoS Architecture Assessment

Thread Simulation

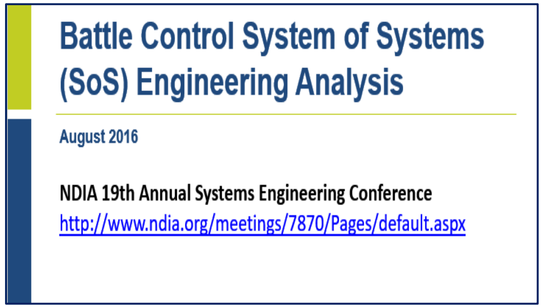
Why is this important for mission engineering?

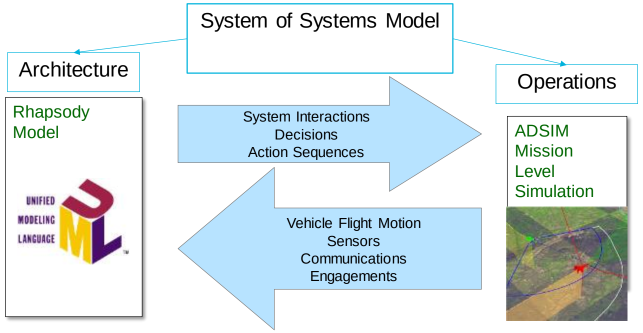
- Scale and complexity of missions require trades across multiple metrics and many solution options
- Lightweight analytic tools leverage architecture data to enable an initial quantification of mission impacts due to architecture changes
- This initial analysis can be used to filter out undesirable architecture options prior to investing resources to assess options with more detailed modeling and simulation tools

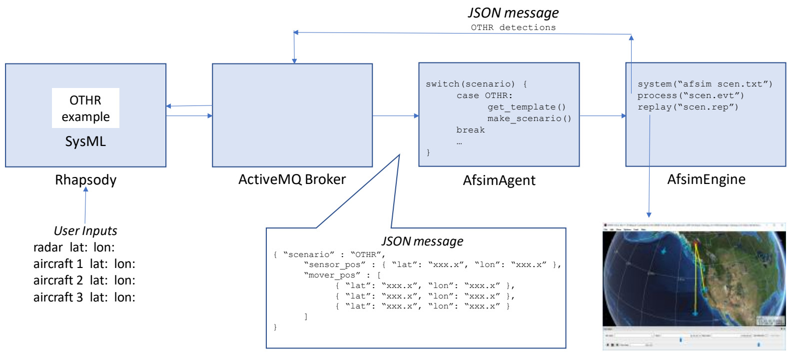
Identify vulnerable assets within the Army Network Architecture

Linking SoS Architecture to Operational Outcomes

- **Effectiveness of SoS for missions is based on mission outcomes**
  – SE analysis of SoS for missions addresses the technical feasibility of the SoS options
  – Analyzing alternative SoS architectures or specific SoS compositions also needs to consider the impact on mission outcomes, typically addressed in operational simulations or test environments
  – This includes ***developing automated interfaces between architecture models and operational simulations***, allowing for analysis of the effectiveness of the SoS in representation scenarios, following proposed concepts of employment
  – Examples include Rhapsody to ADSIM, more recently to AFSIM


Battle Control System of Systems (SoS) Engineering Analysis
August 2016
NDIA 19th Annual Systems Engineering Conference
http://www.ndia.org/meetings/7870/Pages/default.aspx





Linking SoS Architecture to Operational Outcomes

Why is this important for mission engineering?

- Mission engineering is all about achieving user operational capability
- Ensuring technical feasibility is an important prerequisite – it is key that systems work together as planned based on engineering across the systems supporting the mission
- But it is key that the mission SoS composition is fit for purpose in the mission environment – physical, threat, etc. – and when executed leads to the expected mission outcomes under anticipated conditions
- Mission SoS architectures can be complex, and it can be time consuming and error prone to have to manually instantiate these in today's operational simulations
- Automating this facilitates the conduct of the analysis of the mission effect or proposed or alternative SoS compositions, and it allows operators and commanders to see the proposed composition in their operation context

Summary

- Mission engineering is an application of SoSE with specific driving characteristics
- As SoSE technical approaches and tools evolve, they provide valuable capabilities to enable technically based approaches to addressing mission engineering challenges

Abstract

In the US Department of Defense there is increased interest in **mission engineering - the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.** The Components have implemented mission engineering in areas where there is a critical interest in achieving mission capability such as ballistic missile defense or naval mission areas, and there is growing interest in addressing a broad set of mission areas through the implementation of mission integration management - the coordination all the programmatic elements - matching funding, schedules, technical improvements, resources (technical staff, development and test infrastructure, M&S etc.) across the relevant mission systems and supporting systems to develop, test, and field a phased set of mission capabilities. **One element of this is engineering of the systems of systems supporting the mission area.**

This presentation outlines the **key activities** involved in mission engineering and describes **opportunities for application of systems of systems engineering technical approaches** to these activities to provide the engineering base for mission integration and mission management. In particular, mission engineering often emphasizes the definition of the key activities need to execute the mission in the form of **mission threads or kill/effects chains and assessing gaps in mission performance.** Less attention has been paid to the various **patterns of mission activities and the engineering required to identify and assess alternatives to addressing the gaps and engineering the SoS to implement the preferred approach**. Drawing on work within the MITRE Systems Engineering Technical Center's model based engineering center, this presentation will present approaches to developing, representing and evaluating systems of systems architectures using model based methods and evaluating SoS configurations to address the functional needs of the mission which provide a set of approaches to supporting mission engineering.

INCOSE: TRANSFORMATION STRATEGIC OBJECTIVE

Troy A. Peterson
INCOSE Assistant Director
Systems Engineering Transformation
troy.peterson@incose.org
Vice President & Technical Fellow
System Strategy, Inc. (SSI)

20th Annual Systems Engineering Conference

Systems Engineering

The Essence of the Next Industrial Revolution

"The world is entering the Fourth Industrial Revolution. Processing and storage capacities are rising exponentially, and knowledge is becoming accessible to more people than ever before in human history. The future holds an even higher potential for human development as the full effects of new technologies such as the Internet of Things, artificial intelligence, 3-D Printing, energy storage, and quantum computing unfold."

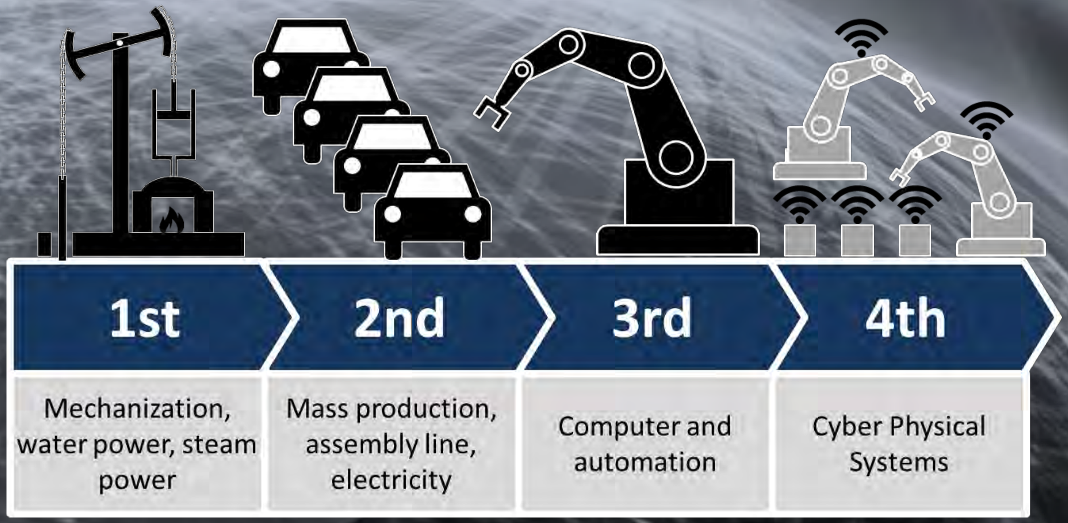
The Global Information Technology Report
Innovating in the Digital Economy
World Economic Forum

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

24 October 2017

Digital Transformation

Industrial Revolution



INCOSE
International Council on Systems Engineering

Deep Shift
Technology Tipping Points and Societal Impact

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Six Megatrends

As a foundation to its work, the council sought to identify the software and services megatrends which are shaping society, and their associated opportunities and risks.

People and the internet
How people connect with others, information and the world around them is being transformed through a combination of technologies. Wearable and implantable technologies will enhance people's "digital presence", allowing them to interact with objects and one another in new ways.

Computing, communications and storage everywhere
The continued rapid decline in the size and cost of computing and connectivity technologies is driving an exponential growth in the potential to access and leverage the internet. This will lead to ubiquitous computing power being available, where everyone has access to a supercomputer in their pocket, with nearly unlimited storage capacity.

The Internet of Things
Smaller, cheaper and smarter sensors are being introduced – in homes, clothes and accessories, cities, transport and energy networks, as well as manufacturing processes.

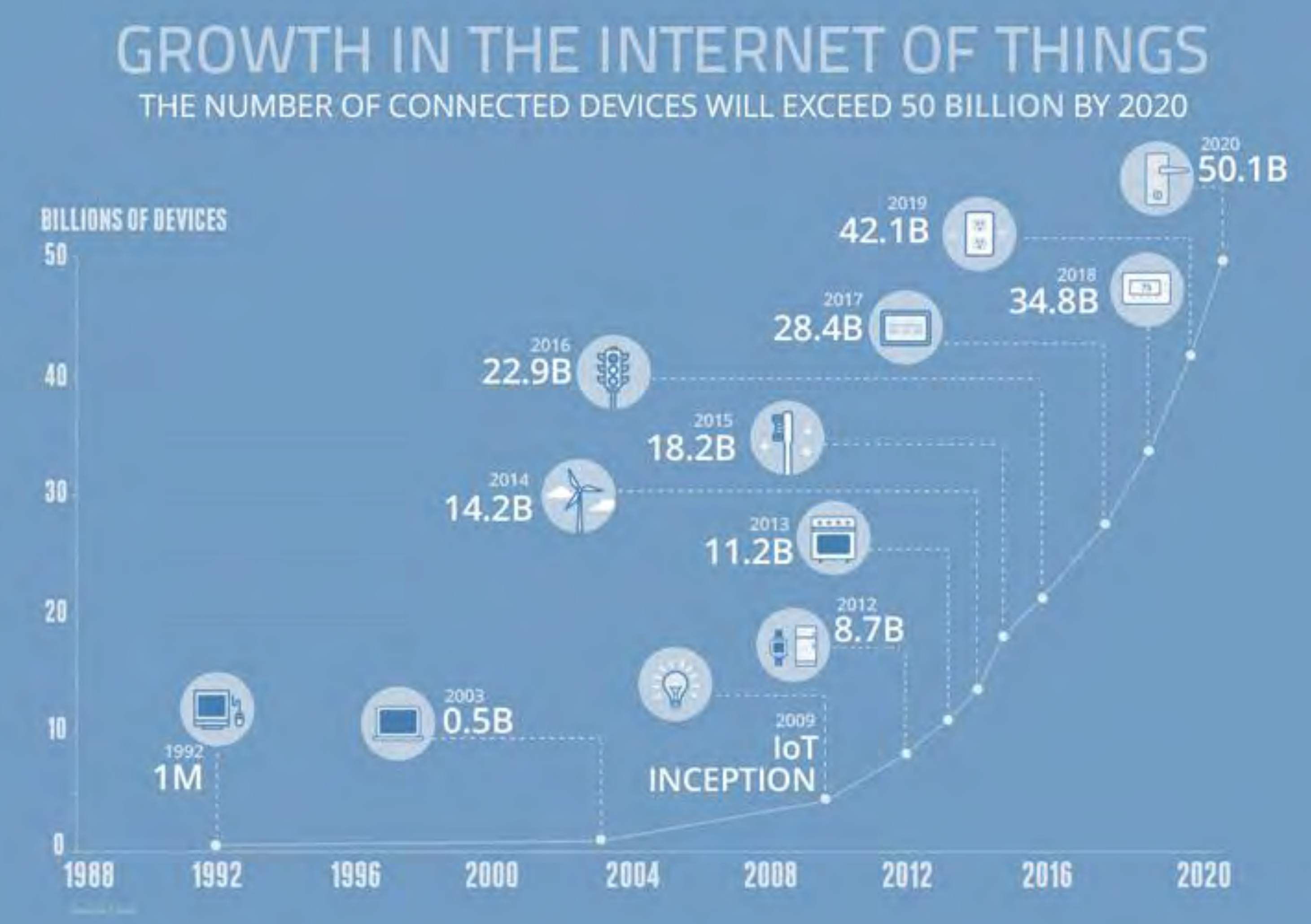
Artificial intelligence (AI) and big data
Exponential digitization creates exponentially more data – about everything and everyone. In parallel, the sophistication of the problems software can address, and the ability for software to learn and evolve itself, is advancing rapidly. This is built on the rise of big data for decision-making, and the influence that AI and robotics are starting to have on decision-making and jobs.

The sharing economy and distributed trust
The internet is driving a shift towards networks and platform-based social and economic models. Assets can be shared, creating not just new efficiencies but also whole new business models and opportunities for social self-organization. The blockchain, an emerging technology, replaces the need for third-party institutions to provide trust for financial, contract and voting activities.

The digitization of matter
Physical objects are "printed" from raw materials via additive, or 3D, printing, a process that transforms industrial manufacturing, allows for printing products at home and creates a whole set of human health opportunities.

Trends: Internet of Things and System Interactions

The interconnection of products is ubiquitous, occurring across domains and with systems we use every day creating a complex web of interdependent systems.

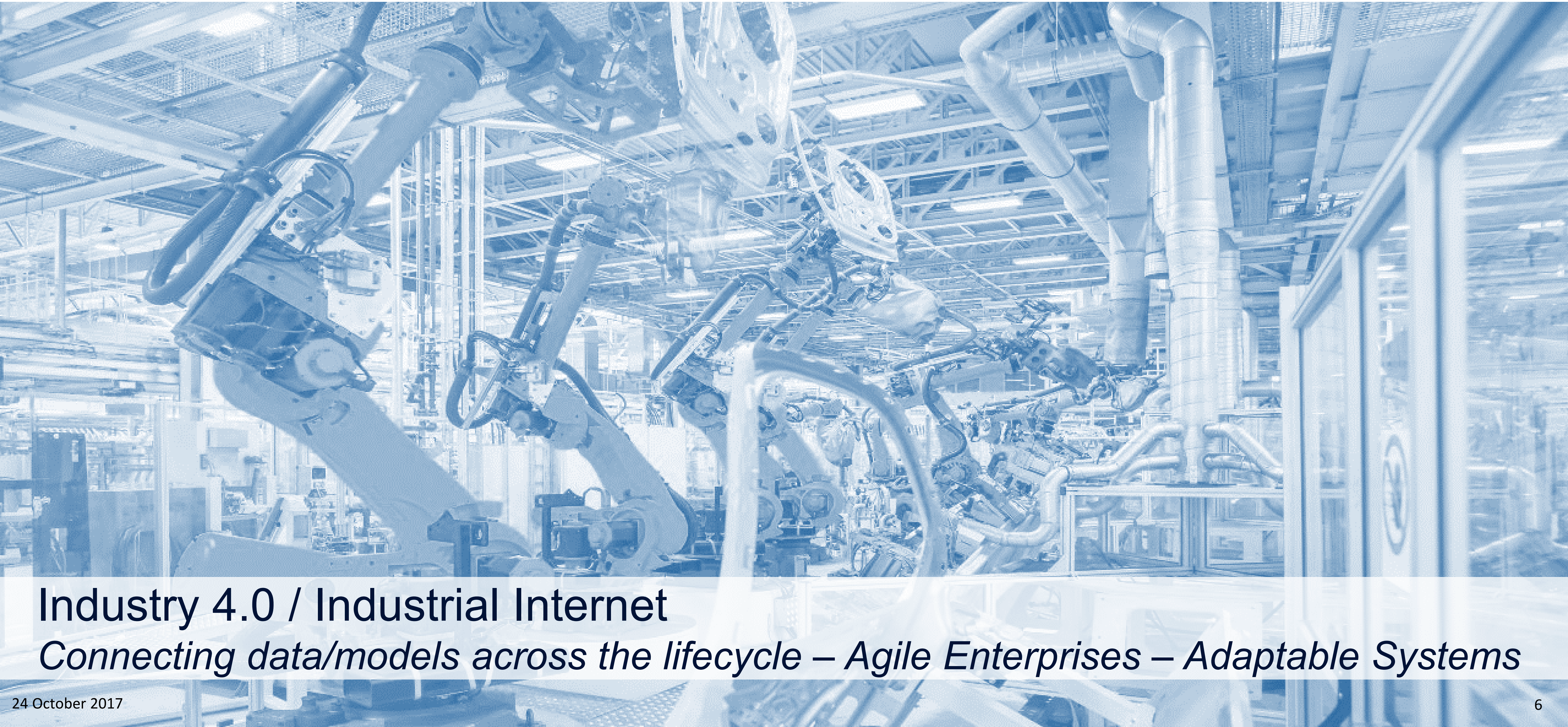


Trends: Analytics and Data Science

Analytics – Data Science - Visualization:

Improving Systems and Shared Human Understanding

Trends: Industrial Revolution / Industry 4.0



Industry 4.0 / Industrial Internet

Connecting data/models across the lifecycle – Agile Enterprises – Adaptable Systems

Trends: Cyber Physical System Security

Cyber-Physical System Security

Intertwined cyber and physical, vast state space, new vulnerabilities

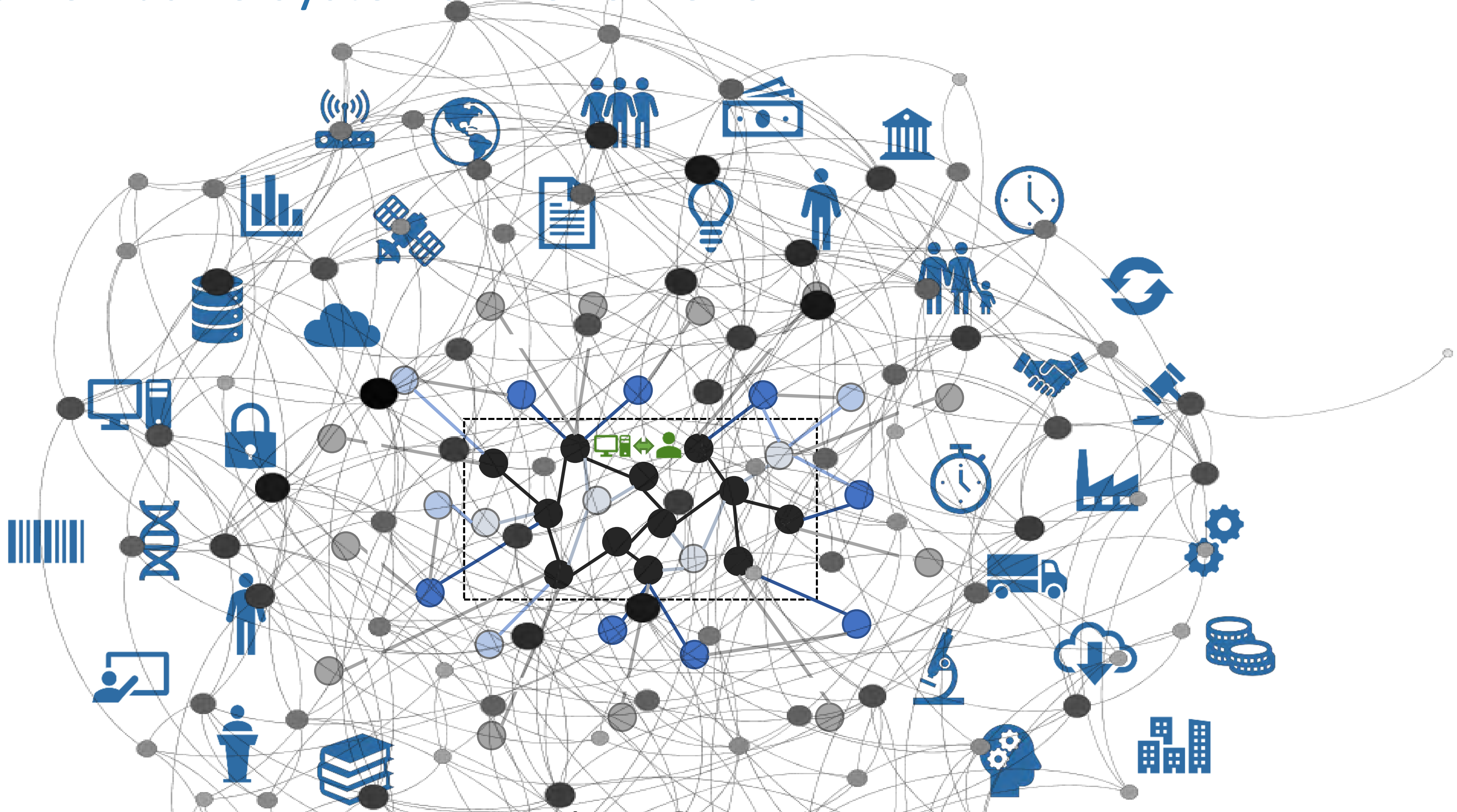
Trends: Artificial Intelligence

Augmented & Artificial Intelligence

Human – machine interactions solving complex problems

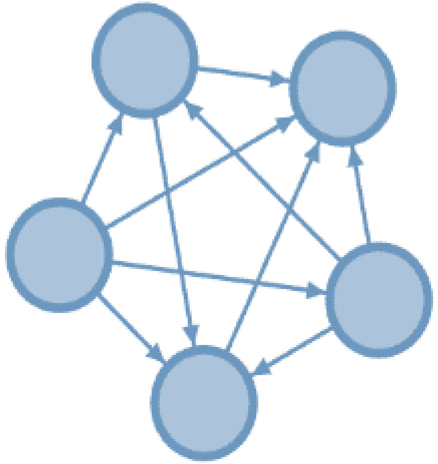
Smart, Interconnected, Complex, Dynamic…

The Pervasive Systems Phenomenon



System Elements & Interactions
External Elements & Interactions
Increased Density of System Elements & Interactions
Increased Density of System External Elements & Interactions
Increased Interactions Between External Elements
Expanding System Domain Boundary Increasing Interactions

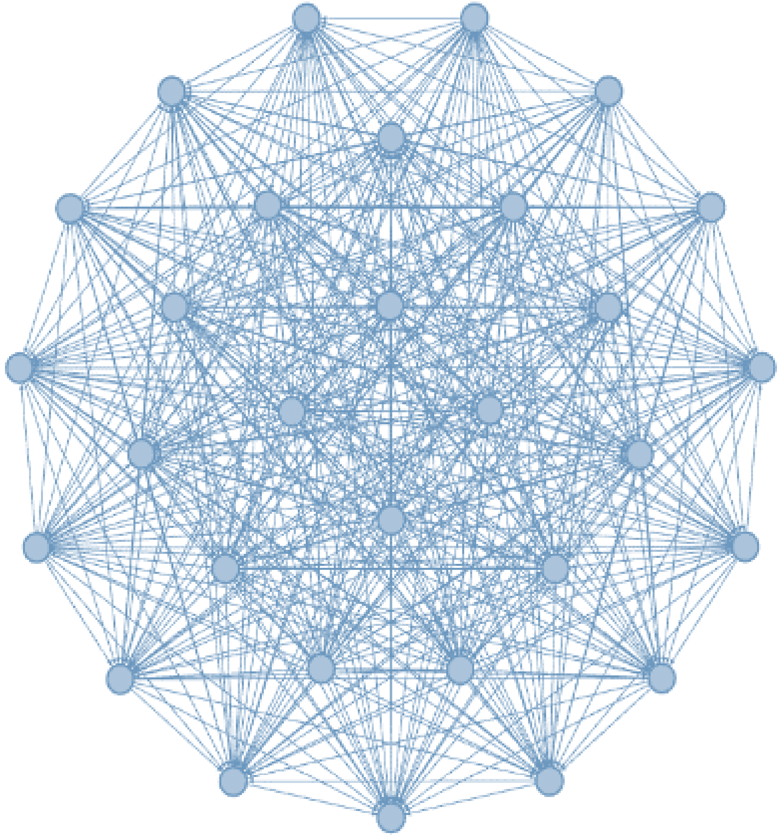
System Phenomenon & Complexity



Nodes = 5

Potential Links = 10

Networks = 2^{10} or 1024



Nodes = 30, potential links = 435, unique configurations = 2^{435}

Number of known atoms in the universe ~ 2^{158} and 2^{246}

Quote on System Challenges Today

"Today more and more design problems are reaching insoluble levels of complexity."

"At the same time that problems increase in quantity, complexity and difficulty, they also change faster than before."

"Trial-and-error design is an admirable method. But it is just real world trial and error which we are trying to replace by a symbolic method. Because trial and error is too expensive and too slow."

Christopher Alexander,
Notes on the Synthesis of Form[1],

1. Christopher Alexander, "Notes on the Synthesis of Form" Harvard University Press, Cambridge Massachusetts, 1964

Rethinking Systems Conceptualization

- The rapid increase in Cyber-Physical Systems is changing the way we develop, manage and interact with systems.
- The National Science Foundation (NSF) describes Cyber-Physical Systems (CPS) as “engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components”
- They tightly intertwine computational elements with physical entities across domains
- The NSF notes that CPS challenges and opportunities are both significant and far-reaching.
- To address these challenges the NSF is calling for methods to conceptualize and design for the deep interdependencies inherent in Cyber-Physical Systems.

Transforming Systems Engineering

Systems engineering will lead the effort to drive out unnecessary complexity through well-founded architecting and deeper system understanding

A virtual engineering environment will incorporate modeling, simulation, and visualization to support all aspects of systems engineering by enabling improved prediction and analysis of complex emergent behaviors.

Composable design methods in a virtual environment support rapid, agile and evolvable designs of families of products. By combining formal models from a library of component, reference architecture, and other context models, different system alternatives can be quickly compared and probabilistically evaluated.

From: Model-based systems engineering has grown in popularity as a way to deal with the limitations of document-based approaches, but is still in an early stage of maturity similar to the early days of CAD/CAE.

To: Formal systems modeling is standard practice for specifying, analyzing, designing, and verifying systems, and is fully integrated with other engineering models. System models are adapted to the application domain, and include a broad spectrum of models for representing all aspects of systems. The use of internet-driven knowledge representation and immersive technologies enable highly efficient and **shared human understanding** of systems in a virtual environment that span the full life cycle from concept through development, manufacturing, operations, and support.

INCOSE's Transformation Strategic Objective

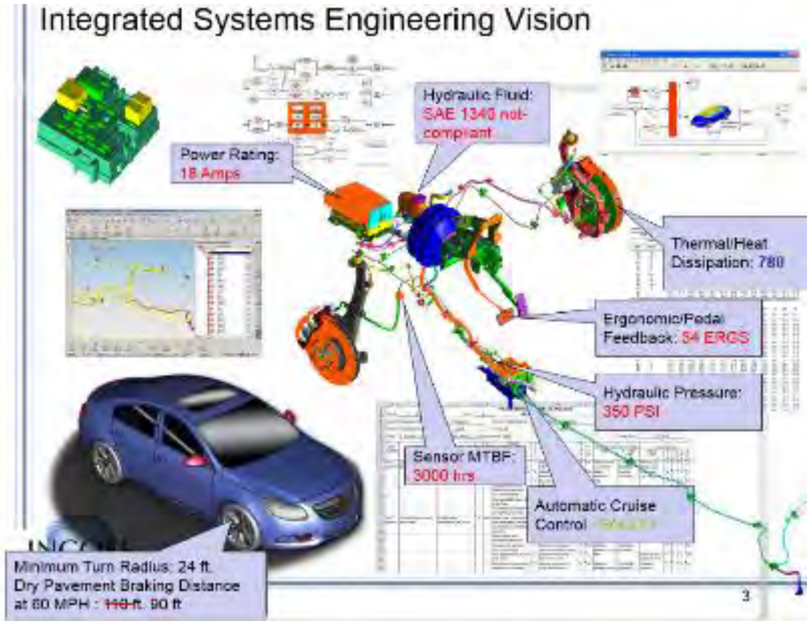
Objective:

INCOSE accelerates the transformation of systems engineering to a model-based discipline.

- Accelerates:
  - Understand the hype cycle[1] and bridge the chasm[2]…
  - Empower others to enlighten and influence adoption

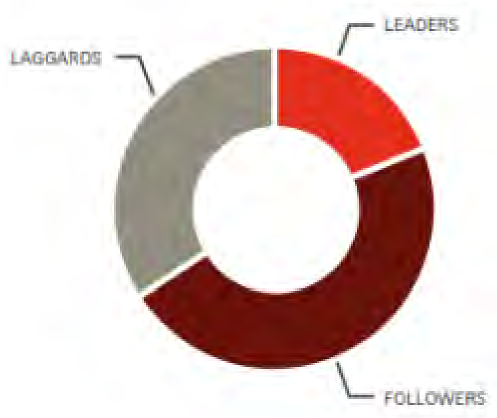
- Transformation:
  - A marked change, as in appearance or character, usually for the better[3]. e.g. documents to models
  - Lead and support the community in crossing the chasm

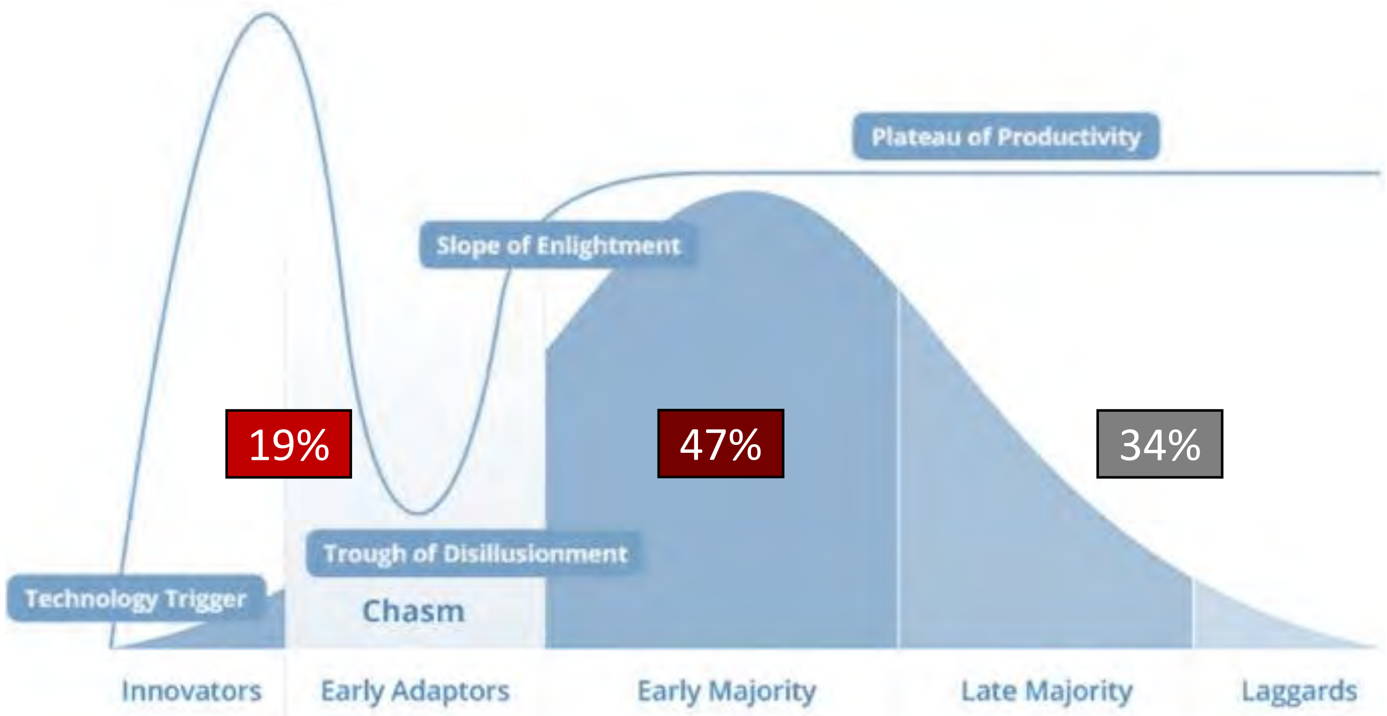
- Model Based Discipline
  - System models of all types
  - Modeler Collaboration and Model Integration



1. Hype Cycle is a branded graphical presentation developed and used by IT research and advisory firm Gartner
2. Moore, Geoffrey A. "Crossing the Chasm – and Beyond" Strategic Management of Technology and Innovation Third Edition 1996
3. Excerpted from The American Heritage Dictionary of the English Language, Third Edition 1996 by Houghton Mifflin Company
4. Friedenthal, Sandy and Sampson, Mark - MBSE Initiative Overview - http://www.omgwiki.org/MBSE/doku.php

Accelerating: Technology Adoption – Hype and Chasm





Rating of company's digital maturity in leadership and management[5]

More than 80% of respondents are either followers or laggards

Acceleration is very much about sharing, communicating and learning

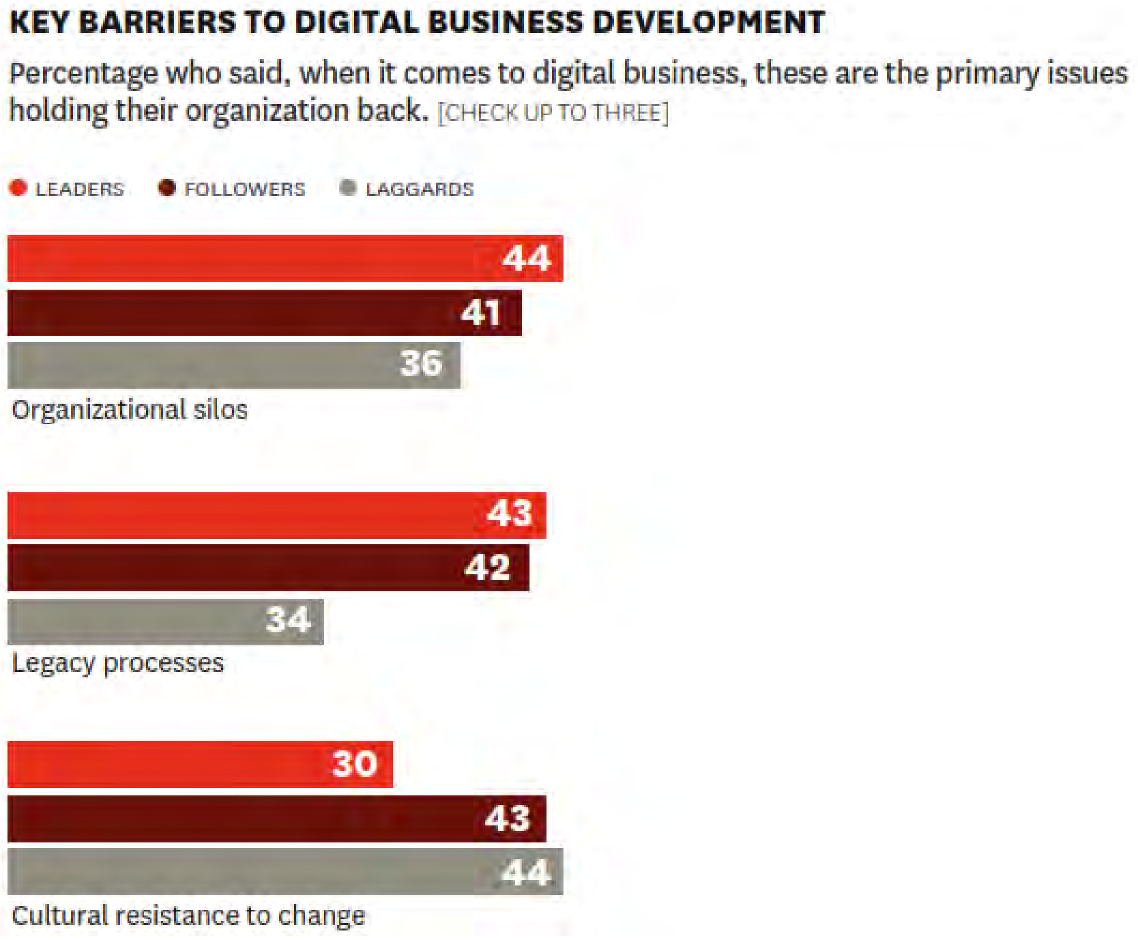
Where would you plot your organization today?

1. Hype Cycle is a branded graphical presentation developed and used by IT research and advisory firm Gartner
2. Hype Cycle Graphic: https://en.wikipedia.org/wiki/Hype_cycle
3. Moore, Geoffrey A. "Crossing the Chasm – and Beyond" Strategic Management of Technology and Innovation Third Edition 1996
4. Hype Cycle, Chasm Combined Graphic: http://www.datameer.com/blog/big-data-analytics-perspectives/big-data-crossing-the-chasm-in-2013.html
5. Driving Digital Transformation: New Skills for Leaders, New Role for the CIO, Harvard Business Review

Transformation: Driving Digital Transformation[1]

Keys to Digital Transformation (HBR Report)

- Start from the customers perspective
- Digital leadership starts at the top
- Engage in a discussion of trends
- Think about agile
- Use examples to make it real
- Need a foundation of trust
- Use KPIs for sharing knowledge
- Break down walls wherever possible
- Need digital coaches or maters
- Create appropriate learning forums



1. Driving Digital Transformation: New Skills for Leaders, New Role for the CIO, Harvard Business Review

Transformation: Change Management and Leadership

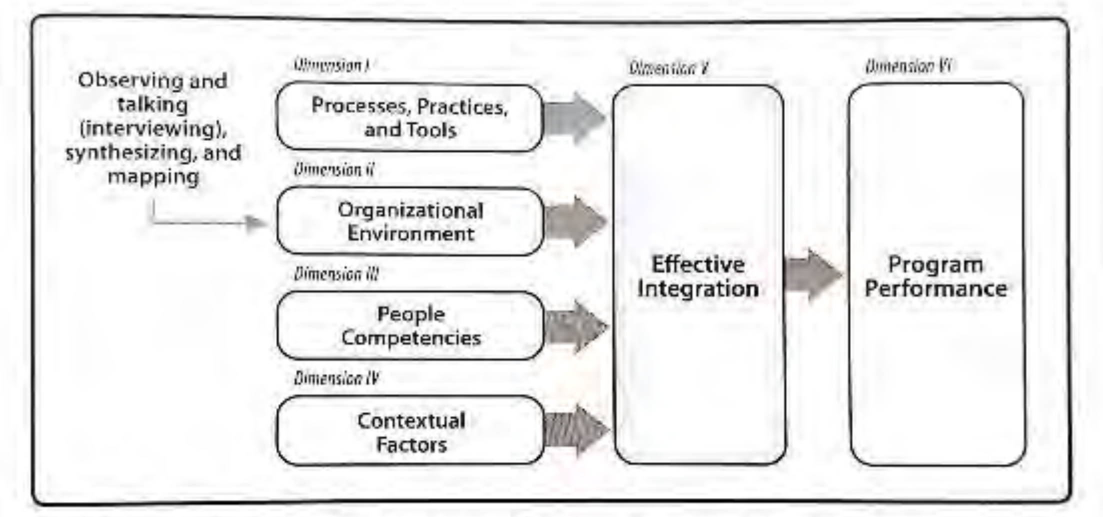
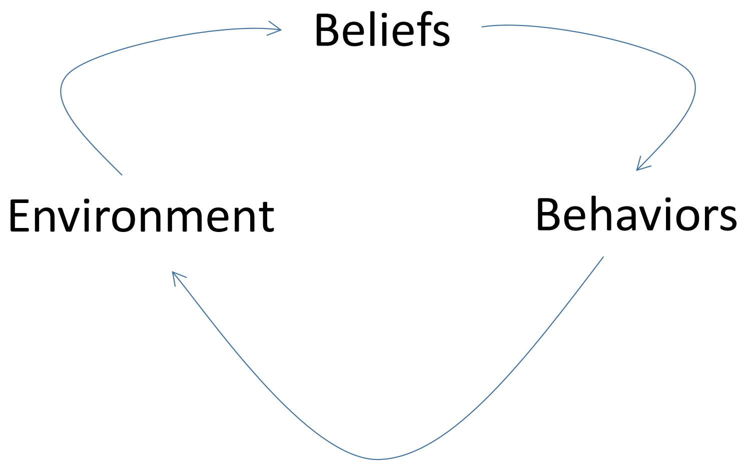


Figure 15-1: The dimension of the Integration Framework in view for initial engagement activities

Consider key dimensions of change

- People, Process, Tools/Technology, Infrastructure, and Governance
  - Integrate dimensions of change
  - Addresses dimensions in parallel
  - Leverage concurrency to encourage cross dimension trades
  - Build ownership at the grass-root level

Transformation is all about changing peoples environment, beliefs and behavior.



Transformation: Digital impact on Change Management

Changing Change Management:

- 70% of Change Management programs fail to achieve their goals largely due to employee resistance and lack of management support
- When people are truly invested in change it is 30% more likely to stick
- Mastering the art of changing quickly is now a critical competitive advantage
- Competitive advantage will accrue to companies with the ability to set new priorities and implement new processes quicker than their rivals.

Five key areas to make internal change efforts more effective:

- 1. Provide just in time feedback – right information at the right time
- 2. Personalize the experience – tailor information to the user
- 3. Sidestep hierarchy – network, open, short circuit long chains of communication
- 4. Build community & shared purpose – dashboards, visuals and gamification
- 5. Demonstrate Progress – Communicate progress and status, move forward

Ref: Changing Change Management - McKinsey & Company, July 2015

Model Based Discipline: The Next Evolutionary Step

Model Based Discipline

- Models are not new to us
- In some ways we’re going “back to the future”
- Transformation is not a wholesale change
- Model based is the next evolutionary step
- A transformation whose time has come

Understand the Current State

- Take inventory of current state of transition and progress toward becoming a model based discipline

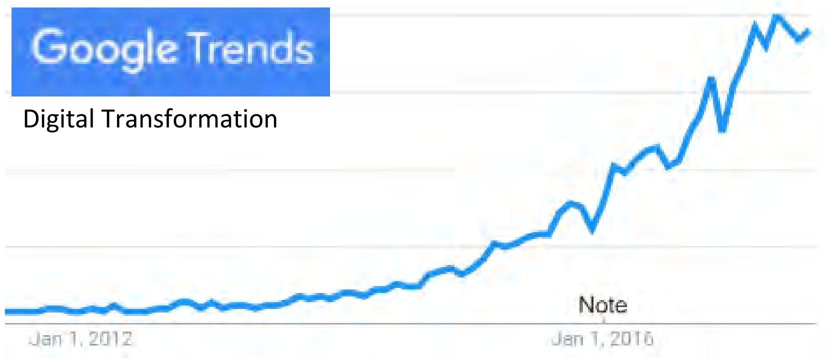
Envision and define the future state of SE:

- See Vision 2025,what are the business objectives, metrics, stakeholders, technologies, priorities etc.

"Make sure that those, *'Ideas whose time has come'*, get launched today."

Model Based Discipline: What do we mean by MBSE

- What do we mean by:
  - Model Based Systems Engineering
  - Model Based Engineering
  - Model Based Development
  - Model Based Design
  - Model Centric Engineering
  - Model Based Methods
  - Digital Engineering
  - Digital Design
  - Digital Thread
  - Digital Twin
  - Digital Tapestry



Model Based Discipline: Systems Engineering Domains

Model based methods apply to more than models of the Target System…

3

System of Innovation Domain

(System of Interest)

- Management of 2
- Innovation Processes
- Governance
- Policy Makers
- Training and Education
- Enterprise Systems
- Financial Systems

2

System Management Domain

- Life Cycle Mgmt. of Target System
- Target System Development
- Support Processes
- Manufacturing
- Distribution
- Infrastructure
- Marketing
- Et al

1

Target System / System of Interest (SOI)

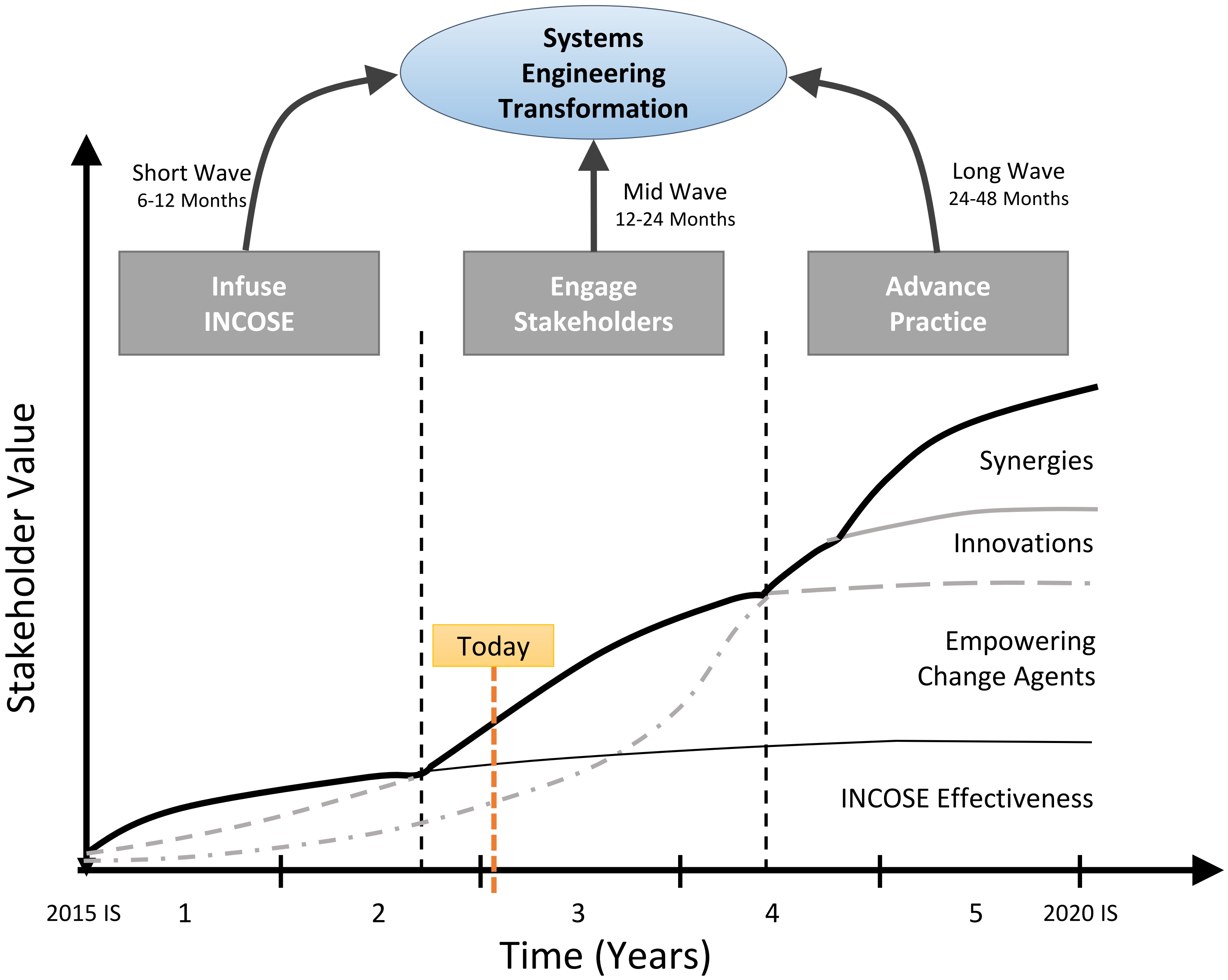
Transformation Strategy Overview

- Vision
- Mission
- Mission Areas
- Goals
- Objectives

Vision	Systems Engineering is acknowledged as a model based discipline		
Mission	INCOSE accelerates the transformation of systems engineering to a model-based discipline		
Mission Area #	1	2	3
Mission Area	Infuse INCOSE	Engage Stakeholders	Advance Practice
Mission Area	What can INCOSE Do?	What is practiced and needed?	What is possible?
Goals	Infuse model based methods throughout INCOSE products, activities and WGs	Engage stakeholders to assess the current state of practice, determine needs and values of model based methods	Advance stakeholder community model based application and advance model based methods.
Objective 1 Foundations	Inclusion of model based content in INCOSE existing/new products (Vision, Handbook, SEBoK, Certification, Competency Model, etc.)	Define scope of model based systems engineering with MBE practice and broader modeling needs	Advance foundational art and science of modeling from and best practices across academia, industry/gov. and non profit.
Objective 2 Expand Reach	Expand reach within INCOSE of MBSE Workshop; highlight and infuse tech ops activities with more model based content (products, WGs etc.)	Identify, categorize and engage stakeholders and characterize their current practices, enablers and obstacles	Increase awareness of and about stakeholders outside SE discipline of what is possible with model based methods across domains and disciplines (tech/mgmt)
Objective 3 Collaborate	Outreach: Leverage MOUs to infuse model based content into PMI, INFORMS, NAFEMS, BIM, ASME and others, sponsoring PhD Students, standardization bodies, ABET	Build a community of Stakeholder Representatives to infuse model based advances into organizations practicing systems engineering.	Initiate, identify and integrate research to advance systems engineering as a model based discipline
Objective 4 Assessment/ Roadmap	Assess INCOSE's efforts (WG, Objectives, Initiatives etc.) for inclusion of model based methods across the Systems Modeling Assessment/Roadmap	Engage stakeholder community with Systems Modeling Assessment/ Roadmap to better understand the state of the practice of MBSE. Push and pull content from stakeholders (change agents and the "to be convinced")	Provide baseline assessment framework, Systems Modeling Roadmap, to create a concrete measure of current state of the art of what's possible/what's the potential.

Strategy Notional Timeline

- Mission Areas
- Internal Short Wave
- External Mid Wave
- Advancing Long Wave
- Waves Run Concurrently
- Activities build on each other
- Important to fully engage stakeholder this next year. Pilot Assessment & Roadmap this CY and kick-off more broadly at 2017 IW.

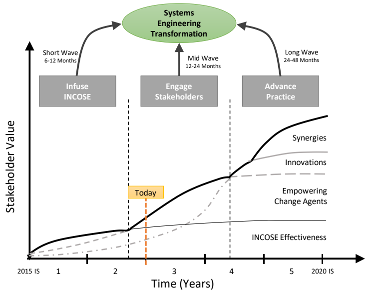


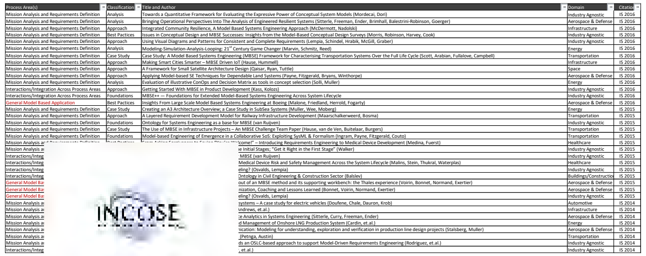
Transformation – Objectives & Initiatives

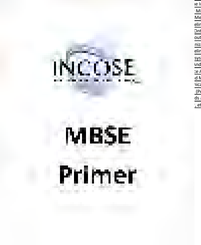
New/Related Developments
- SE Ontology Effort with SERC, JPL et al.
- MBSE Initiative Challenge Team for Digital Artifacts
- MSE Challenge team for Production & Logistics Systems Modeling
- MBSE Initiative for V&V of models in collaboration with ASME
- 2018 IS MBSE Workshop “TED Talks” & Case Studies

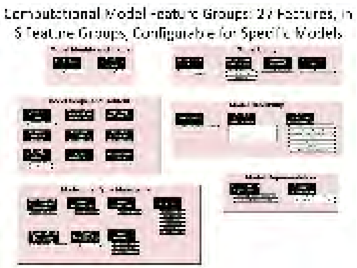
Products Under Development
- Model Based Exemplars
- Assessment Roadmap Model Features
- INCOSE MBSE Primer
- Value Briefing / Case Studies / ROI
- Webinar planned for November

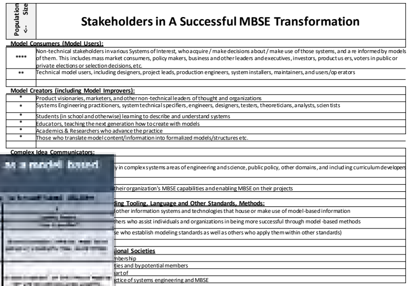
Accomplishments
- Strategy & Action Plan
- Stakeholder List
- Assessment Roadmap
- Enablers & Roadblocks
- Web search improvements
- Transformation website created
- Integration of MBSE throughout IW
- Many professional society and company briefings on Systems Engineering Transformation

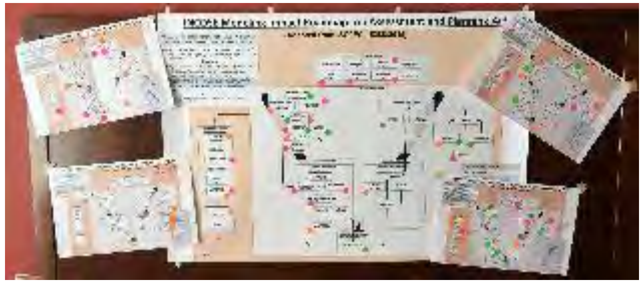




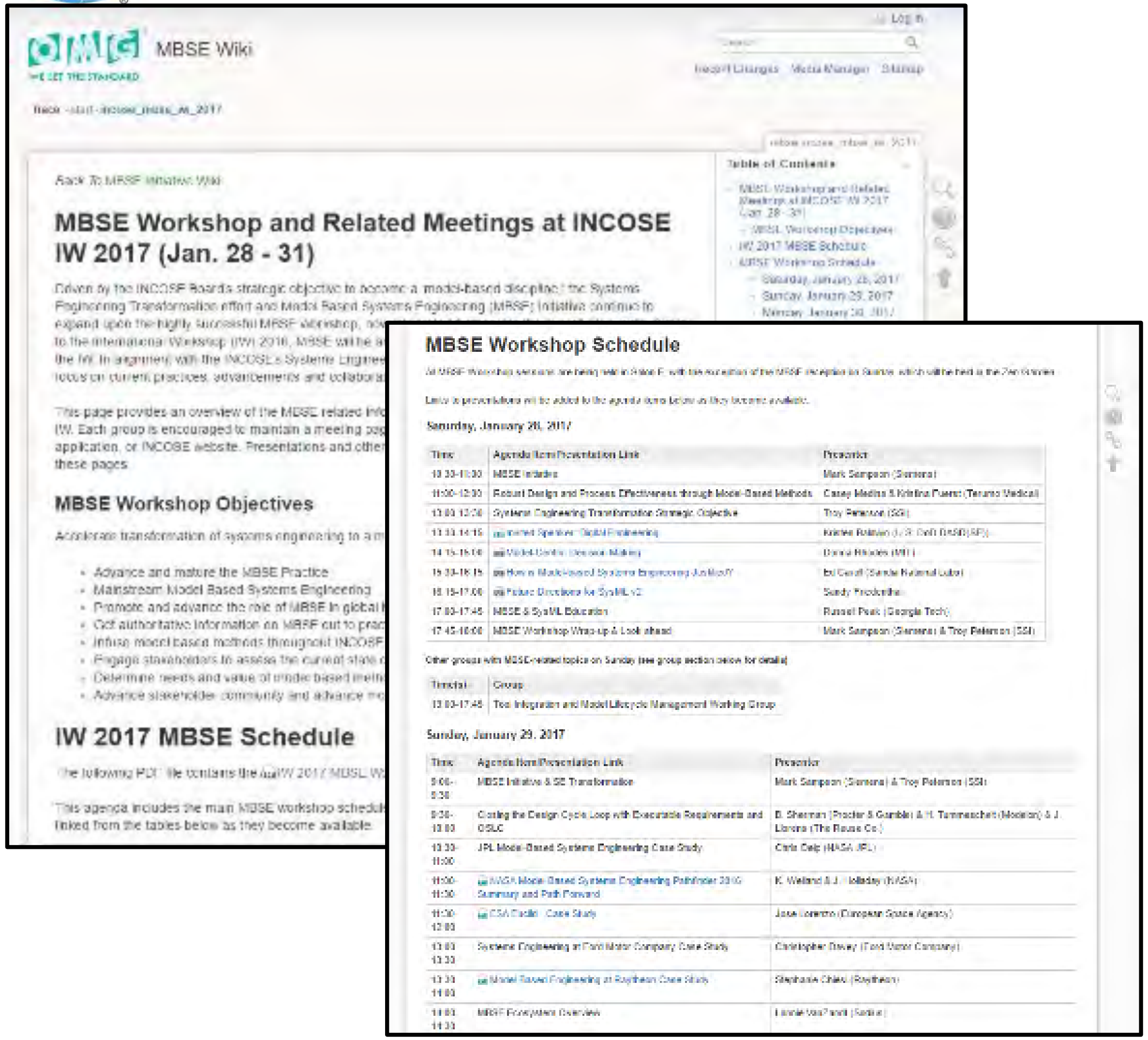




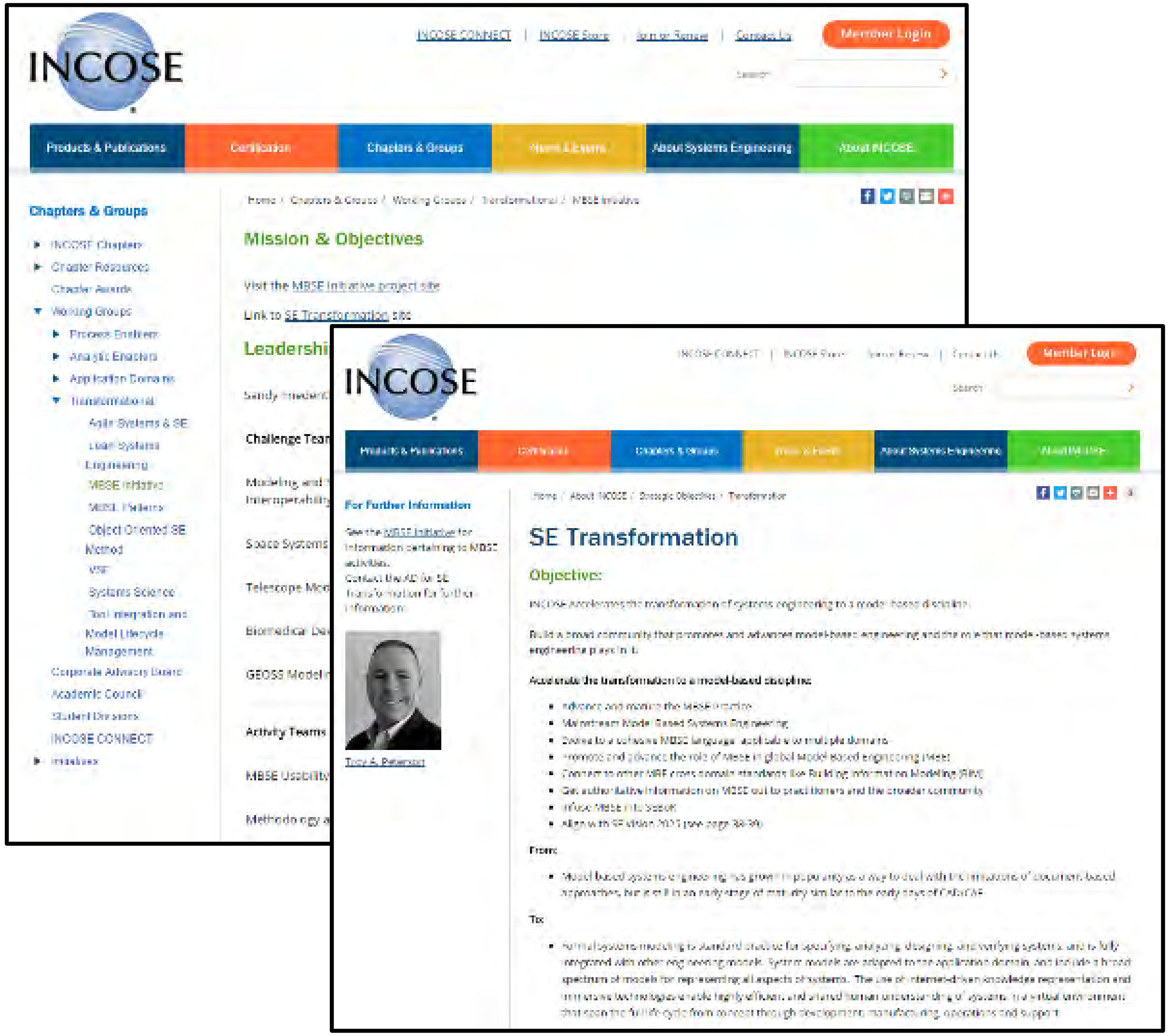




MBSE Wiki and Website



http://www.omgwiki.org/MBSE/doku.php?id=mbse:incose_mbse_iw_2017



http://www.incose.org/about/strategicobjectives/transformation

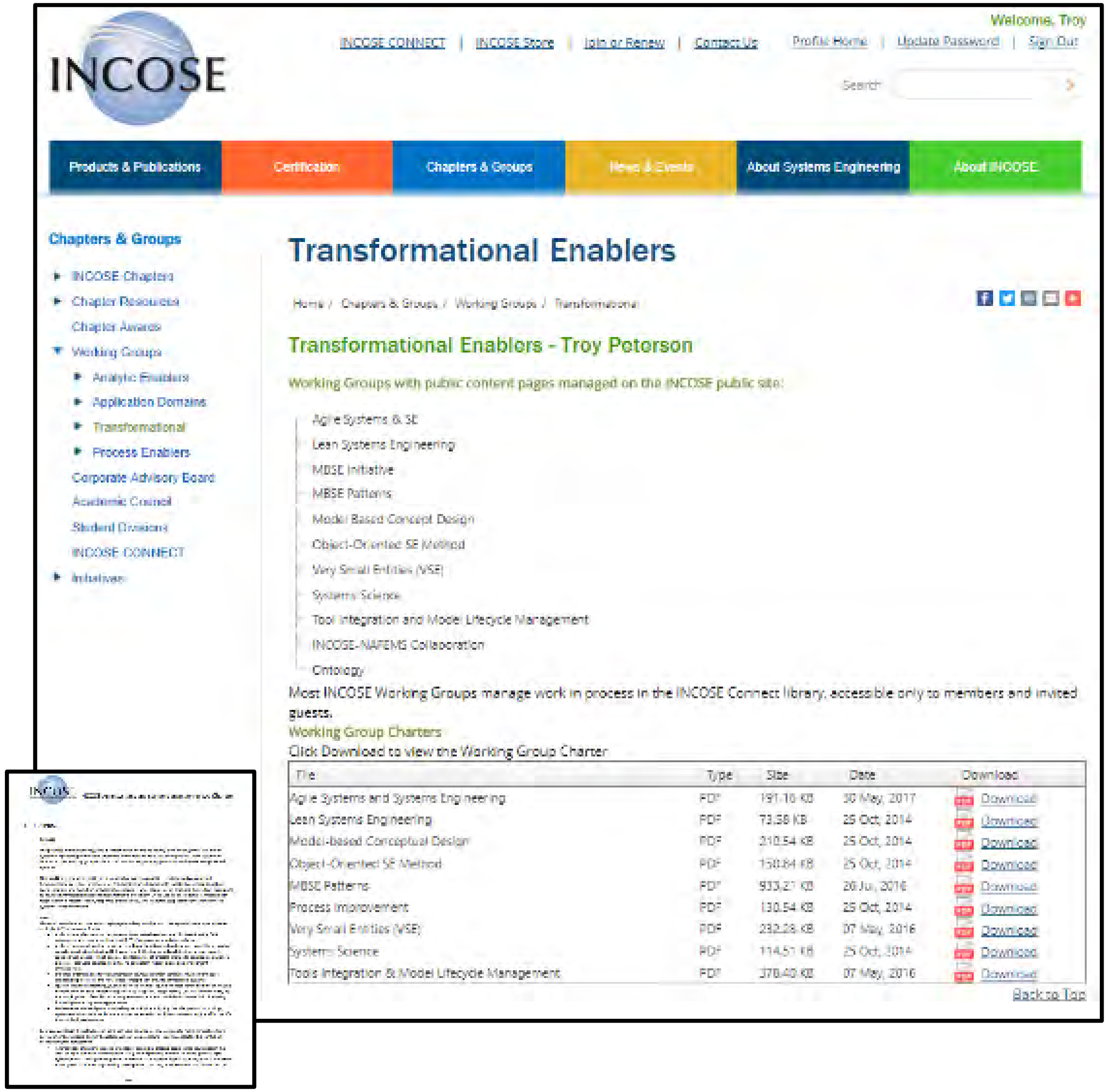
Accomplishments: Website / Discoverability Improvements

Transformational Working Groups (WG)

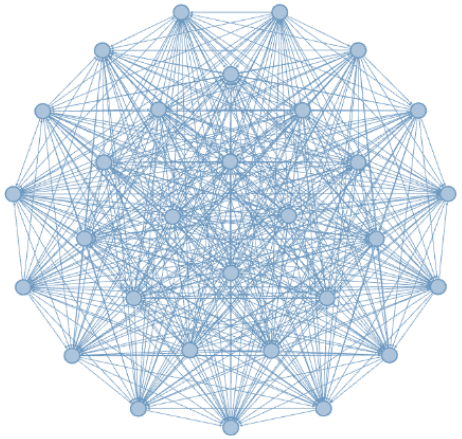
- Agile Systems and Systems Engineering
- Lean Systems Engineering
- Model Based Systems Engineering Initiative
- Model-based Conceptual Design
- Object-Oriented SE Method
- MBSE Patterns
- Very Small Entities (VSE)
- Systems Science
- Tools Integration & Model Lifecycle Management
- INCOSE-NAFEMS Collaboration
- Ontology

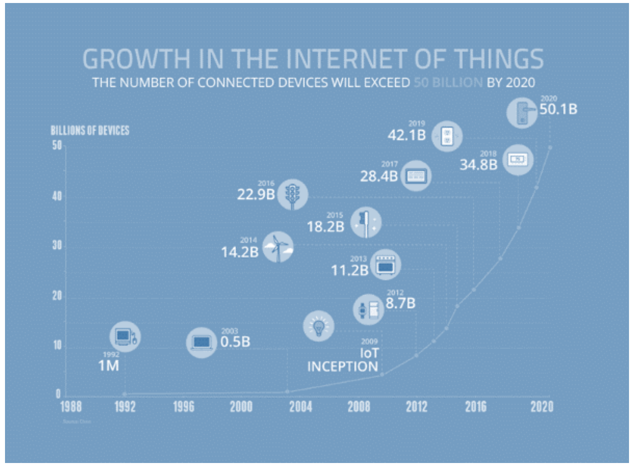
Visit site for WG charters and to learn more

http://www.incose.org/ChaptersGroups/WorkingGroups/transformational



Overcoming the Challenge





…the only simplicity to be trusted is the simplicity to be found on the far side of complexity

Alfred North Whitehead (1861-1947)

Simplicity does not precede complexity but follows it.

Alan Perlis (1922 – 1990)

Out of intense complexities intense simplicities emerge

Winston Churchill (1874 – 1965)

Simplicity is complexity resolved.

Constantin Brancusi (1876-1957)

Fools ignore complexity. Pragmatists suffer it. Some can avoid it. Geniuses remove it.

Alan Perlis (1922 – 1990)

Any intelligent fool can make things bigger and more complex… It takes a touch of genius – and a lot of courage to move in the opposite direction.

Albert Einstein (1879 – 1955)

A genius! For 37 years I've practiced fourteen hours a day, *and now they call me a genius!*

Pablo de Sarasate (1844 – 1908)

Lesson: Endure complexity, add tireless effort, and a touch of genius…

“It is not necessary to change. Survival is not mandatory.”

W. Edwards Deming

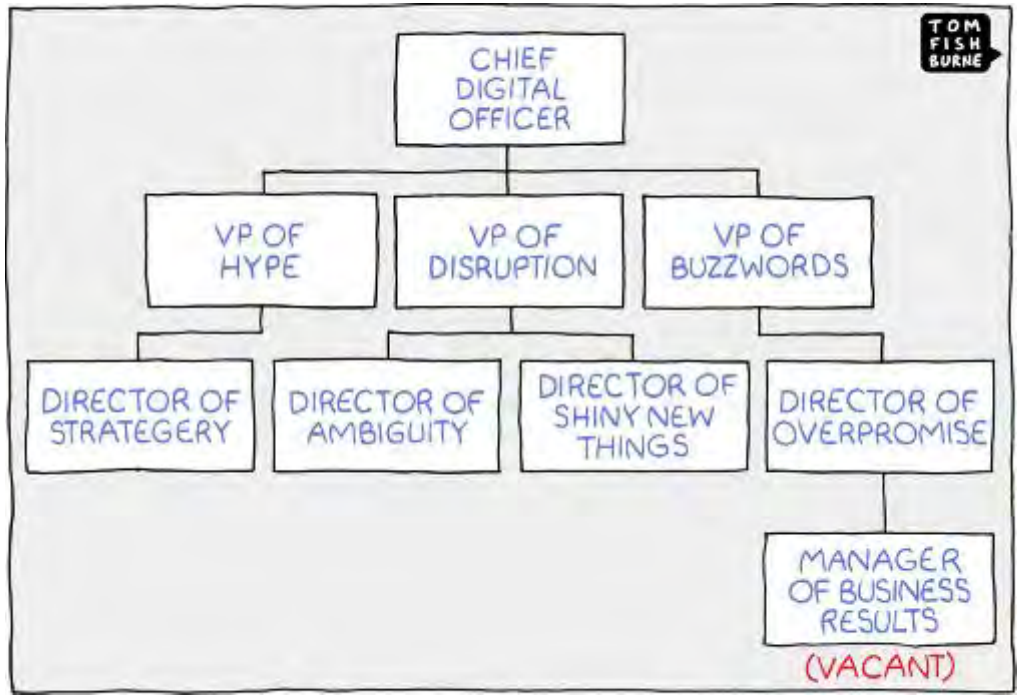
INCOSE’s Transformation Strategic Objective:

http://www.incose.org/about/strategicobjectives/transformation

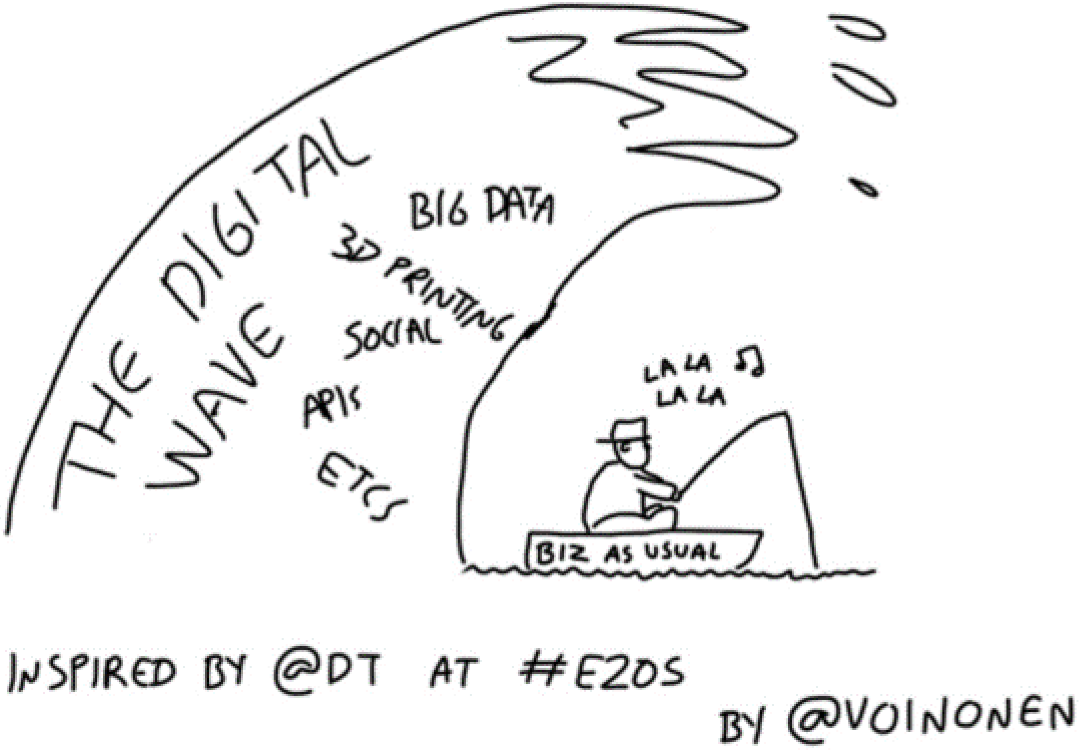
Engage as a Transformation Stakeholder Representative, visit:

http://www.incose.org/about/strategicobjectives/transformation

Q&A



Digitally Zealous



Digital Denial

Troy Peterson Bio

Troy Peterson

Vice President
tpeterson@systemxi.com
313.806.3929

Troy Peterson is Vice President and co-founder of System Strategy, Inc. a systems consulting business. Previous to this role Troy was a Booz Allen Fellow and the firm's Chief Systems Engineer responsible for instituting capabilities to manage complexity, engineer resiliency and speed innovation.

Troy has led several international projects and large teams in the delivery of complex systems. His experience spans commercial, government and academic environments across all product life cycle phases. Recent engagements include Contingency Basing, the Ground Combat Vehicle (GCV), Mine Resistant Ambush Protected (MRAP) vehicle and developing engineering capability within organizations responsible for research, development, acquisition and system of systems engineering and integration.

Troy's impact has led to his appointment to six different boards to improve engineering education and method application. He frequently speaks at leading engineering conferences and was recently appointed by INCOSE as the lead for transforming Systems Engineering to model based discipline.

Prior to joining Booz Allen, Troy worked at Ford Motor Company and as an entrepreneur operating a design and management consulting business. Troy received his B.S. in Mechanical Engineering from Michigan State University, his M.S. in Technology Management from Rensselaer Polytechnic Institute, and an advanced graduate certificate in Systems Design and Management from the Massachusetts Institute of Technology (MIT). He holds INCOSE Systems Engineering, PMI Project Management, and ASQ Six Sigma Black Belt certifications.

Copyright for INCOSE Vision 2025 use and references

Copyright

- This product was prepared by the Systems Engineering Vision 2025 Project Team of the International Council on Systems Engineering (INCOSE). It is approved by the INCOSE Technical Operations for release as an INCOSE Technical Product.
- Copyright ©2014 by INCOSE, subject to the following restrictions:
- Author use: Authors have full rights to use their contributions in a totally unfettered way with credit to the INCOSE Technical Product.
- INCOSE use: Permission to reproduce this document and to prepare derivative works from this document for INCOSE use is granted provided this copyright notice is included with all reproductions and derivative works.
- External Use: This document may be shared or distributed to non-INCOSE third parties. Requests for permission to reproduce this document in whole are granted provided it is not altered in any way.
- Extracts for use in other works are permitted provided this copyright notice and
- INCOSE attribution are included with all reproductions; and, all uses including derivative works and commercial use, acquire additional permission for use of
- images unless indicated as a public image in the General Domain.
- Requests for permission to prepare derivative works of this document or any for commercial use will be denied unless covered by other formal agreements with INCOSE. Contact INCOSE Administration Office, 7670 Opportunity Rd., Suite 220, San Diego, CA 92111-2222, USA.
- Service marks: The following service marks and registered marks are used in this document:

U.S. Air Force

Integrity - Service - Excellence

AF Cyber Resiliency Office for Weapon Systems (CROWS)

NDIA Systems Engineering Conference

Mr. Danny Holtzman, HQE
Cyber Technical Director
SL, Cyber Security Engineering & Resiliency
daniel.holtzman.1@us.af.mil

25 October 2017

Cyber Resiliency – A War Winning Capability

Overview

- AF Cyber Campaign Plan
- Cyber Resiliency Office for Weapon Systems (CROWS)
- Technical Integration & Governance
- Cyber Resiliency S&T Needs
- An Authorizing Official Perspective

AF Cyber Campaign Plan (CCP) Bottom Line Up Front

- **AF Cyber Campaign Plan's (CCP) overall mission has two goals:**
  - **#1 "Bake-In" cyber resiliency into new weapon systems**
  - **#2 Mitigate "Critical" vulnerabilities in fielded weapon systems**

- **Established the Cyber Resiliency Steering Group (CRSG)**
  - **8 voting members (SAF/AQR, LCMC, SMC, NWC, AFTC, Intel, SAF/CISO, & 24AF/CV)**
  - **Governance body to guide the AF Cyber Campaign Plan (CCP)**

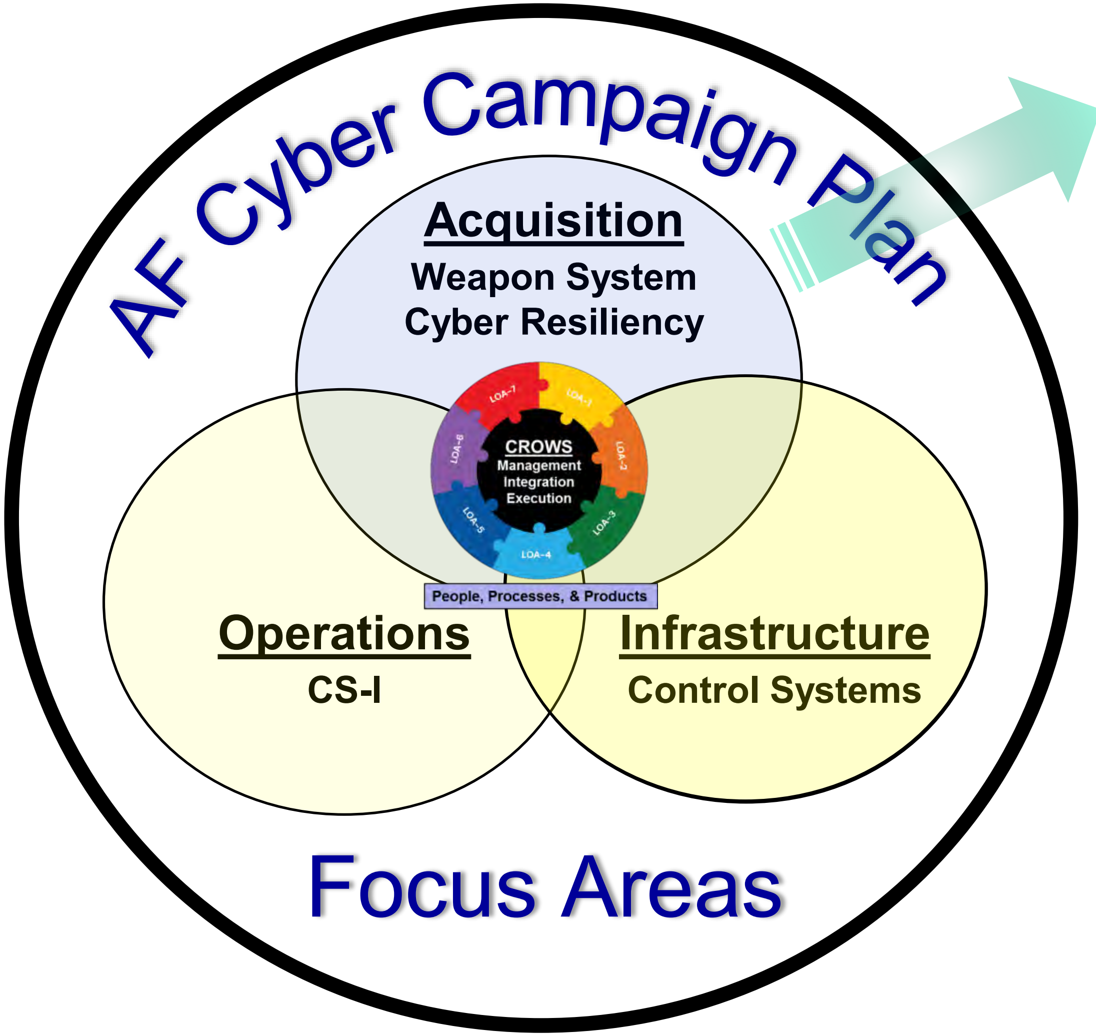
- **Established dedicated office to manage execution → Cyber Resiliency Office for Weapon Systems (CROWS)**
  - **Executing 7 Lines of Actions**
  - **Manage/execute the NDAA 1647 Weapon System Assessments and Mitigations**

- **Coordination with:**
  - **Cyber Squadron Initiative (Operational)**
  - **Industrial Control Systems (ICS) cyber protection measures (Infrastructure)**
  - **Test and Evaluation (infrastructure & capability growth)**

Collaborate, Integrate and Execute

AF Cyber Campaign Plan (CCP)

Weapon System Vision, Mission and Goals



Vision

Cyber resiliency ingrained in AF culture

Mission

Increase cyber resiliency of Air Force weapon systems to maintain mission effective capability under adverse conditions

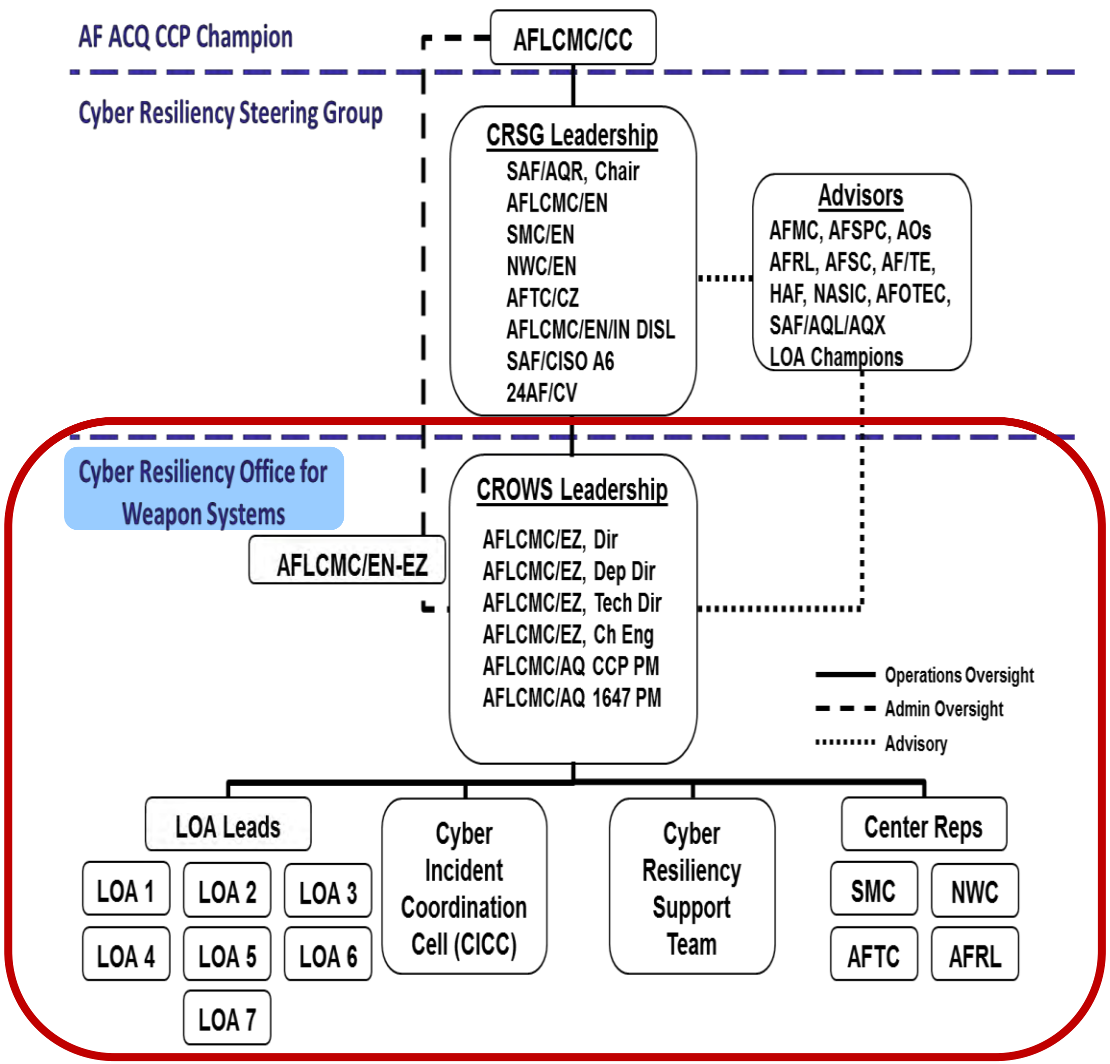
Goals

#1 "Bake-In" cyber resiliency into new weapon systems

#2 Mitigate "Critical" vulnerabilities in fielded weapon systems

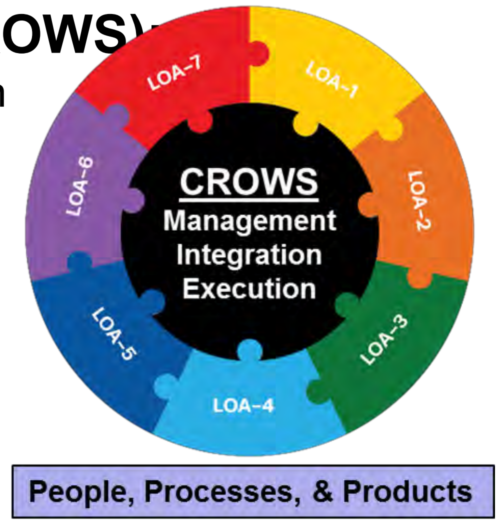
Cyber Resiliency Office for Weapon Systems (CROWS)

- Charter
  - Stakeholder signatures
  - AFLCMC/CC approval
- Scope
  - Weapon system cyber resiliency support for the acquisition community
  - CRSG/CROWS will collaborate and leverage the other CCP efforts to maximize the benefits for the AF mission and stakeholders



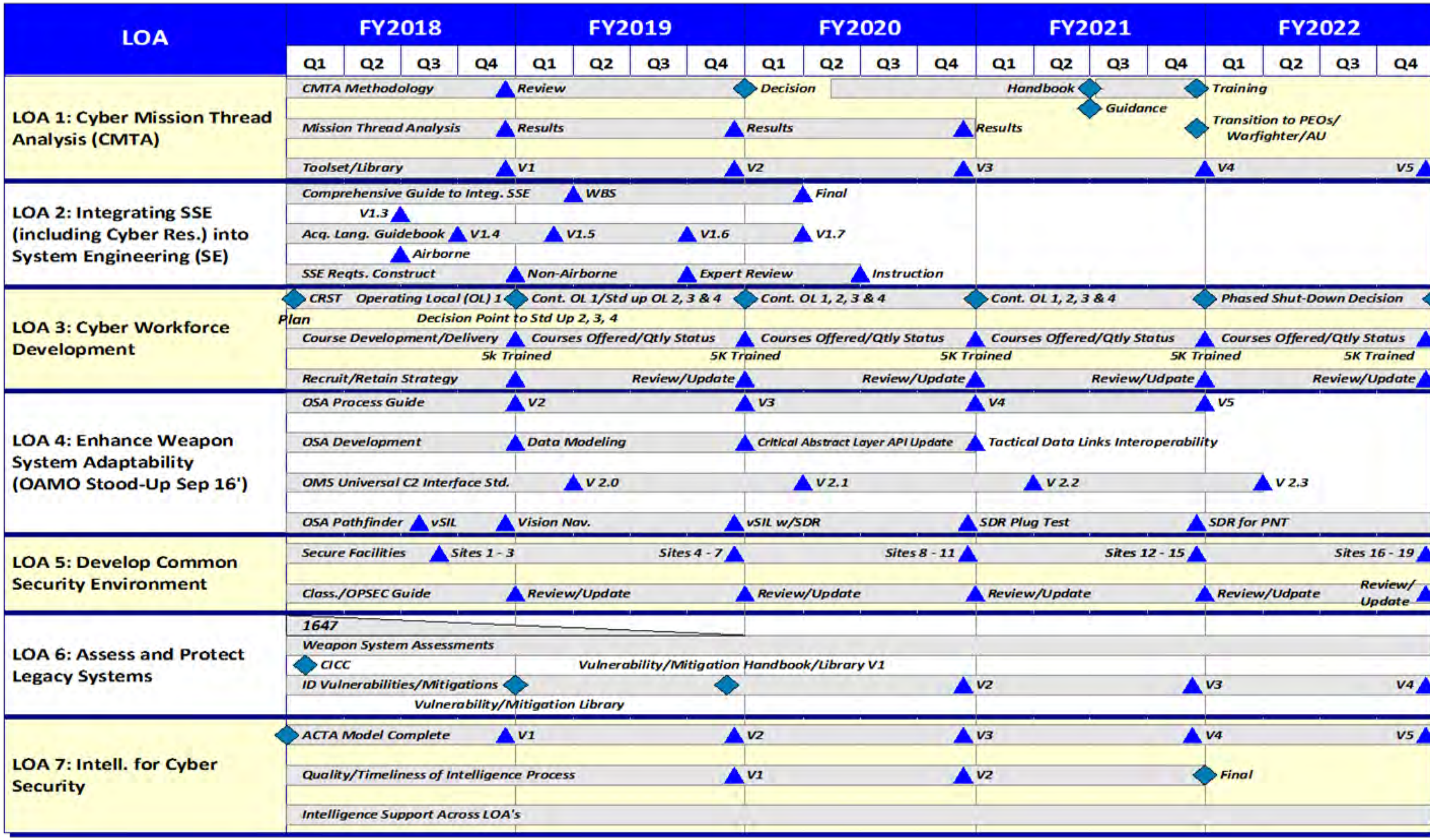
Weapon System Cyber Campaign (CCP) Overview

- **Cyber Resiliency Office for Weapon Systems (CROWS):**
  - Execution of Acquisition/Weapon System Cyber Campaign Plan
  - Execution of NDAA 1647 weapon system assessments
- **7 Lines of Action (LOAs)**
  - LOA 1: Cyber Mission Thread Analysis
  - LOA 2: Integrate SSE/Cyber Resiliency into SE
  - LOA 3: Cyber Workforce Development
  - LOA 4: Weapon System Agility & Adaptability
  - LOA 5: Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Cyber Intel Support



- **Cyber Resiliency Steering Group (CRSG):**
  - Weapon System CCP Guidance and Direction
  - 8 Voting Members:
    - SAF/AQR (Chari), LCMC, SMC, NWC, AFTC, Intel, SAF/CISO, 24AF

Weapon System Cyber Campaign Plan Schedule



Cyber Resiliency for Weapon Systems

Technical Integration & Governance

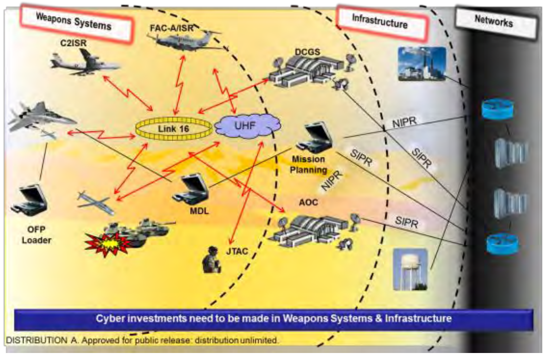
Mr. Daniel C. Holtzman, HQE
SL, Cyber Security Engineering & Resiliency

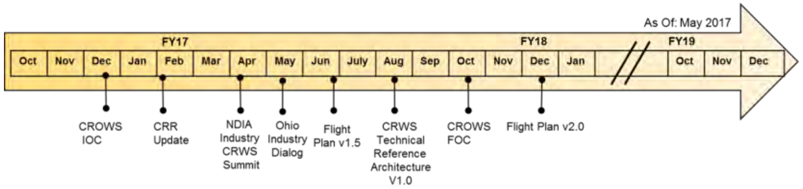
Cyber Resiliency for Weapon Systems On Going Alignment of Efforts

- ✓ **CR Technical Reference Architecture (CR-TRA)**
  - Framework for Cyber Resiliency in Weapon Systems
- ✓ **CR Technical Flight Plan (CR-RFP)**
  - Alignment of Technical Work Program
- ✓ **CR Advisory Council (CR-TAC)**
  - Alignment to Technical Flight Plan, Staffing/Comment adjudication, Technical recommendations, Technical Coordination/Reviews
- ✓ **FFRDC/UARC Collaboration**
  - AF Security Engineering Team (AFSET)
- ✓ **PEO / Programs**
  - Cyber Resiliency Review (Bi Annual)
  - PEO Directors of Engineering (DOE) Council
- ✓ **Industry**
  - Engagement via NDIA SE/SSE/T&E Committee's
  - Cyber Resiliency for Weapon Systems Round Table
- ✓ **Service's, OSD, Academia, NIST**

Cyber Resiliency Government Reference Architecture

- CR Technical Reference Architecture (CR-TRA)
- CR Technical Flight Plan (CR-TFP)
- CR Technical Advisory Council (CR-TAC)





Technical Advisory Council (CRWS-TAC)
- Chair – AF Cyber Technical Director
- CO Chair – AFCISO

Criteria	**Design**	**Hardware**
Observables	**Operate**	**Software**
Behaviors	**Maintain**	**Carbon Based Units**

Communications & Collaborations On Going Efforts

- Information Sharing
  - Classification
  - Configuration Management
  - Mechanism/Process
  - Expectation Management
- Cyber Flash
  - Within Organization
  - External to Organization

- FFRDC/UARC – AFSET
  - Nine FFRDC/UARCs
- Industry – NDIA SE/SSE/TE Committee
  - 2017 NDIA Cyber Resiliency Summit
  - 2018 AF/Industry CRWS Round Table
- **CRWS Round Table**
  - Quarterly Industry Sponsored / Hosted
  - Adoption of Anti Tamper Model (as applicable)
- YOUR IDEAS HERE !!

Establishing an AF / Industry Cyber Resiliency for Weapon Systems Round Table

Technical Integration & Governance

Cyber Resiliency for Mission Assurance Requires an Integrated, Holistic Strategy

Metrics – Reporting metrics and measuring progress

Acquisition – Policy & processes for acquiring secure resilient systems (contracting language)

S&T – Address longer term gaps by aligning AF research agenda

Intel – Communicating and sharing cyber threat information to acquisition programs, S&T and Test Community

Workforce Education & Training – Across ALL Centers for awareness, technical expertise

Sustainment – Processes and methods to ensure and improve the security posture of operational systems

T&E – Effective ways of testing protection and resiliency & allocating appropriate resources

Risk Management - A Temporal perspective

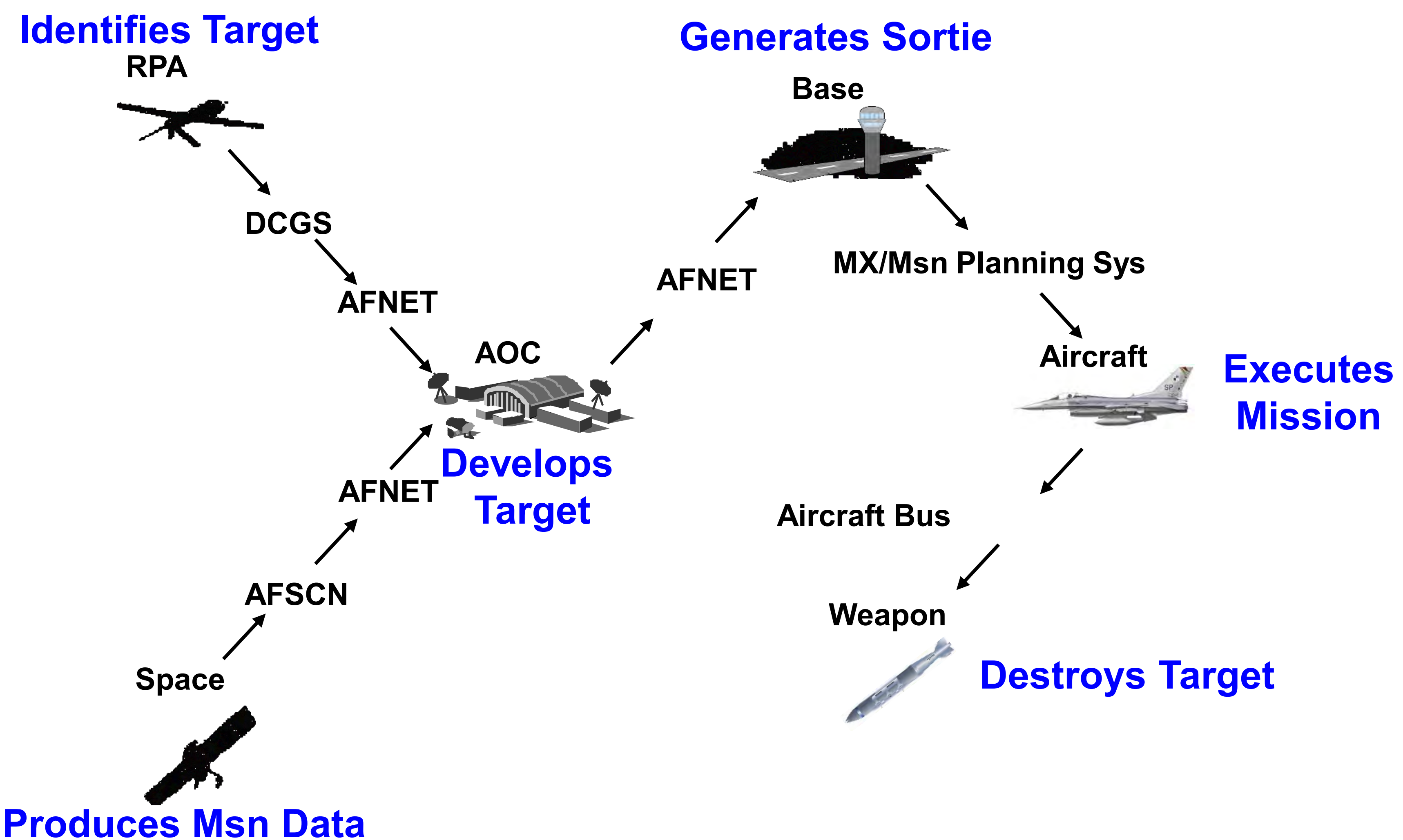
Technical Risk Management Vs. Operational Risk Management

Acquisition Risk Views		Operational Risk Views	
Low	High	Low	High

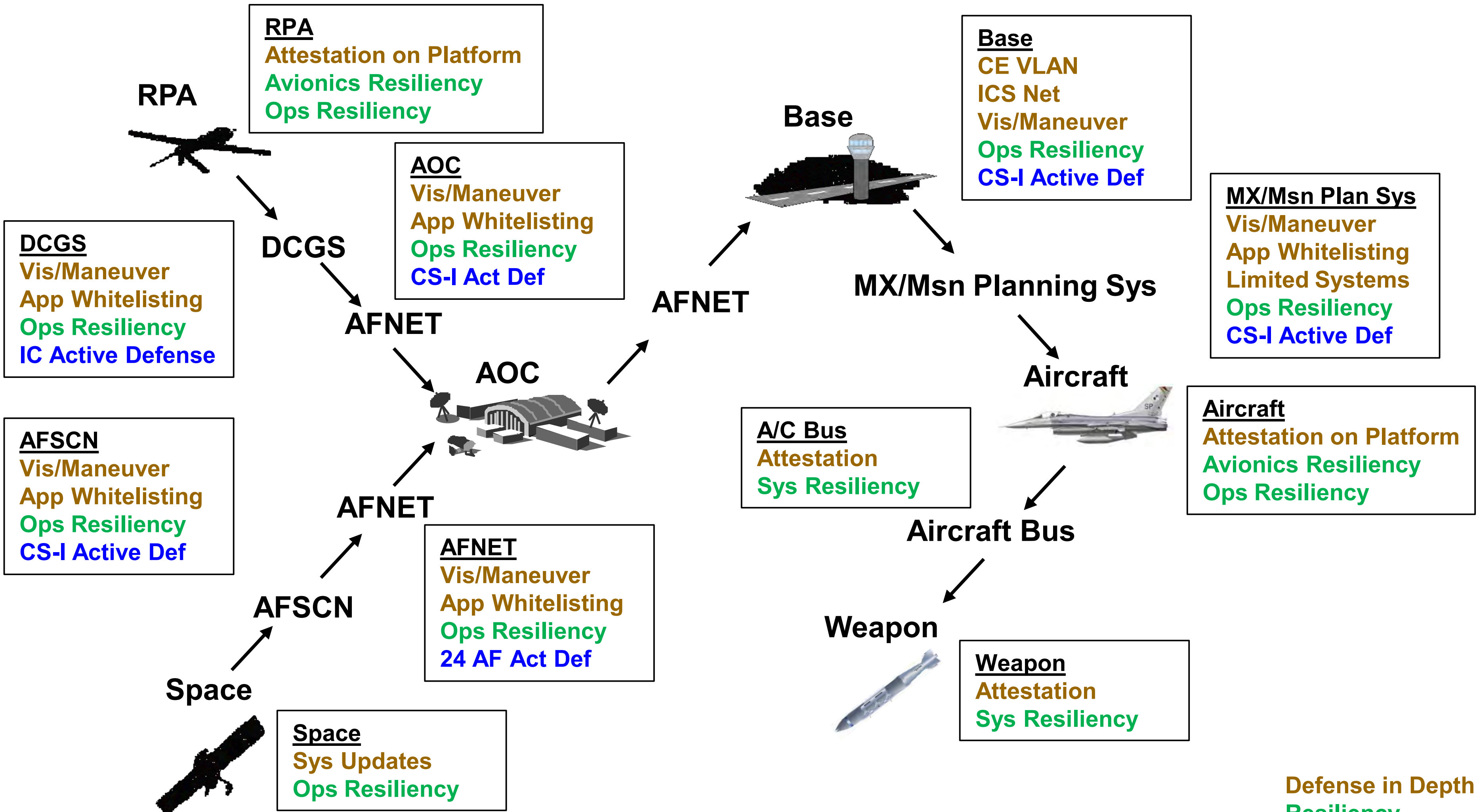
- Manage risks through system engineering and requirements throughout Lifecycle
- Bake security in and establish an initial security posture and burn tech. risk down
- Validate security is “good enough to operate” – issue ATO
- Accept that Systems operate in contested environments in ways not indented
- Over time systems are not as secure due to obsolesce/patching/resources/etc.

Risk view is different at different points in time

Cyber Resiliency Government Reference Architecture
Simple AF Mission Example



Cyber Resiliency Government Reference Architecture
Five Year Vision (aka "To Be")



Defense in Depth
Resiliency
Active Defense

Cyber Resiliency Technical Flight Plan (CR-TFP)

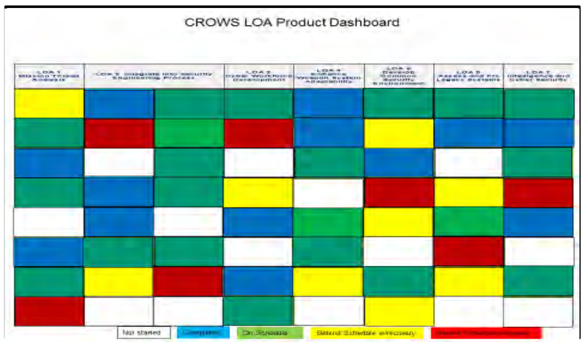
Level 0
Technical Flight Plan
Strategic Objectives

	FY17	FY18	FY19	FY20
LOA 1	2.3,3.1,5.1	2.1,2.2,3.2,5.1,5.2	2.1,2.4,3.3,4.1,4.2,5.1,5.2,6.1	
LOA 2	1.1,1.6	1.3,1.5		1.2,1.4,1.7,2.1,2.2,3.2
LOA 3	1.1,2.1,2.3,3.1,3.2,3.3 3.4,3.5,3.6	1.2		
LOA 4 LOA 5	1,2,3,4	5		
LOA 6	1.1,1.2,1.3,1.4,1.5,1.6,3.1,3.2,4.1,4.2,4.3,4.4	3.3		
LOA 7	1.1,1.2,2.1,2.3,3.1,3.2, 3.3	2.2		4.1
	1.1,1.2,2.2,2.3,3.3,5.1,6.1,6.2,7.1,7.2,7.3 ,8.1,8.2	2.1,2.4,3.1,3.2,3.3,6.2,6.3	2.4,6.2	2.4,5.1

Cyber Resiliency Technical Flight Plan Detail Level

- L0 Technical Flight Plan
- L1 LOA Product Dashboard
- L2 LOA Flight Plan Summaries
- L3 LOA P3 Details
- L4 LOA Action Plans

Level 1
Yearly High Level
Product Dashboard



OA	Objective	Task	Actions/Products	P3	FY15	FY16	FY17	FY18	FY19	FY20	BCRD
1	1	1.1	Mission Thread Identification		Complete						
		1.2	Mission Thread Prioritization		Complete						
		1.3	Mission Thread Evaluation Scope			X					
	2	2.1	Complete RAND's Framework/Process for assessing and communicating Cybersecurity Risk		Complete						
		2.2	Identify current/ongoing CMTA Frameworks or Processes to understand strengths, weaknesses, and limitations as it relates to Cybersecurity			X					
		2.3	Incorporate adversary Cyber Threat intelligence into CMTA Framework/Process			X					
		2.4	Finalize and approve common CMTA Methodology					X			
	3	3.1	Determine Cyber Threat risks to the systems participating in the mission thread.			X					
		3.2	Recommend possible mitigations and program actions for risks identified in Task 3.1			X	X				
		3.3	Identify possible common mitigations and program actions for risks identified in Task 3.2				X				
		3.4	Provide feedback and lessons learned regarding the effectiveness of the CMTA Framework and process based on experience exercising it			X	X	X			
	4	4.1	Feed analytical results and recommendations to the portfolio management community, users, and to the Communication Squadron Next initiative for enteprise consideration				X				
	5	5.1	Develop and coordinate plan to incorporate Cyber CMTA Reviews and Checklists into current policy/processes				X				
		5.2	Develop a configuration management approach for developing, cataloging, sustaining, maintaining, and governing mission threads and tools			X					

Level 2 & 3
P3 - People, Process, Products

Level 4
Multi Year
Action Plans

Line of Action 1 Action Plan
Mission Thread Analysis

Line of Action 2 Action Plan
Integrating SSE into Systems Engineering

Line of Action 3 Action Plan
Cyber Workforce Development

Line of Action 4 Action Plan
Enhanced Adaptability

Line of Action 5 Action Plan
Common Security Environment

Line of Action 6 Action Plan
Assess & Mitigate Legacy Systems

Line of Action 7 Action Plan
Intelligence for Cyber Security

Weapon System Cyber Reporting

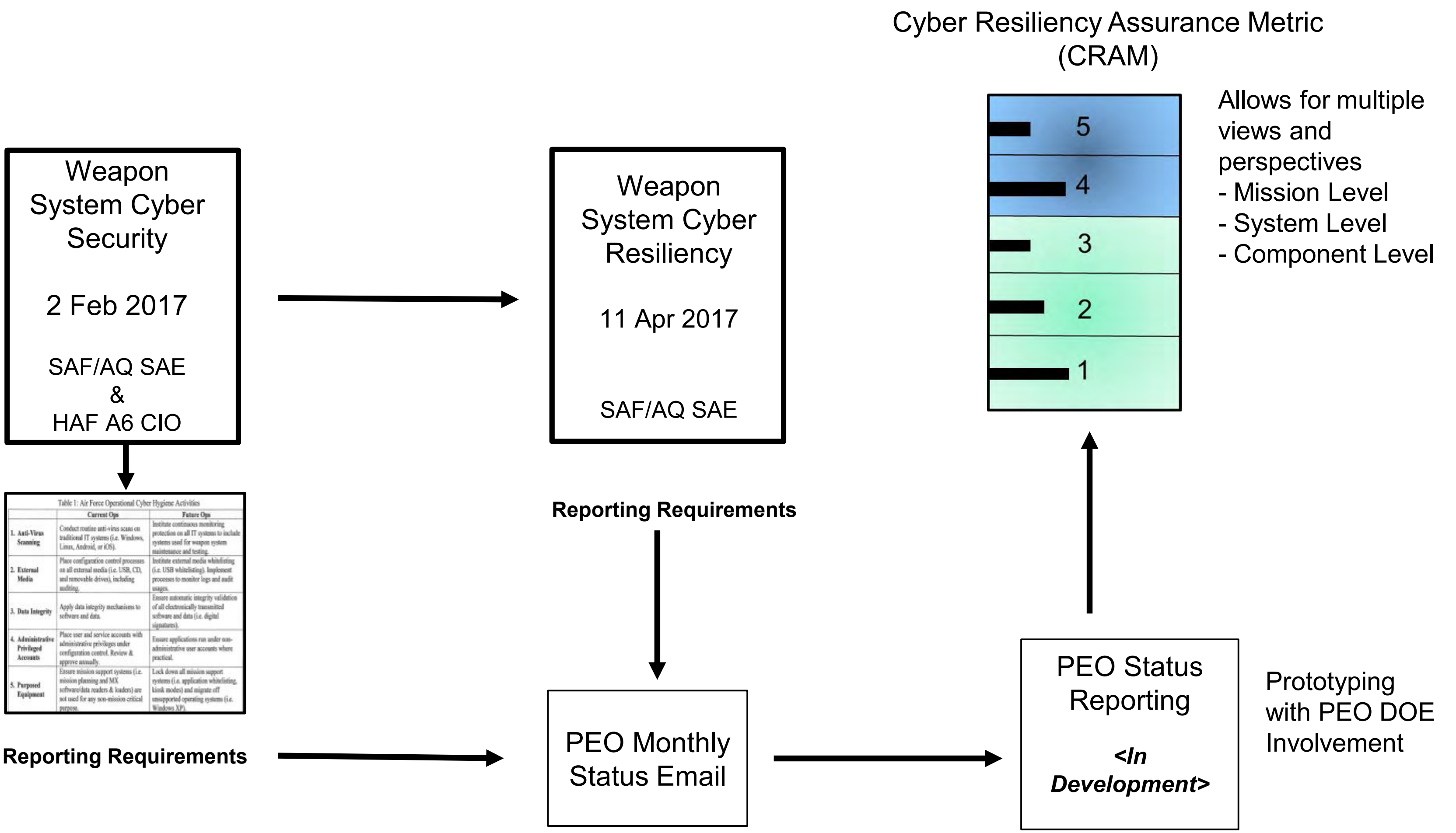


Table 1: Air Force Operational Cyber Hygiene Activities

	Current Ops	Future Ops
1. Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
2. External Media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
3. Data Integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data (i.e. digital signatures).
4. Administrative Privileged Accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
5. Purposed Equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Weapon System Integrated Reporting and Metric

Cyber Resiliency Assurance Metric (CRAM)

- Integrated Metric – Focus is on Cyber Assurance in Mission context
  - Incorporates all available risk assessments - Evidentiary Analysis & Data based
  - Linked to Cyber Hygiene Reporting requirements and Authorizations (e.g. ATO, ATC)
- Based on Risk analysis and Confidence factors – Risk Management vs Compliance
- Provides for Situational Awareness of Cyber Assurance over Time
  - WS CR Dashboard in development

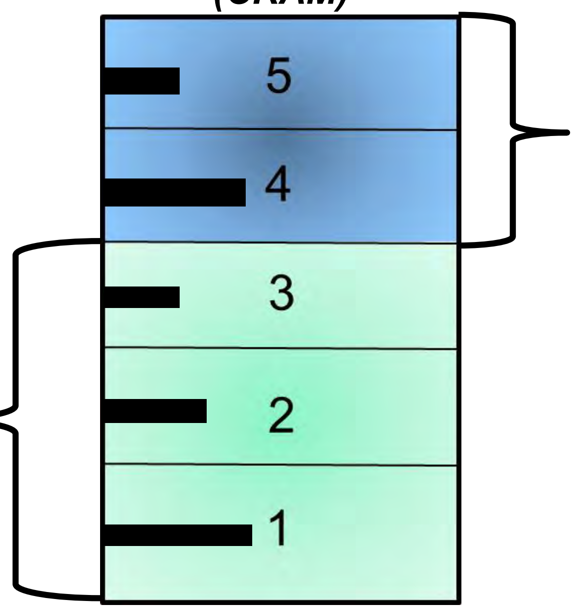
Cyber Hygiene

- Builds in Security
- Assumes a set of known "Knowns"

Table 1: Air Force Operational Cyber Hygiene Activities

	Current Ops	Future Ops
1. Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
2. External Media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
3. Data Integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data (i.e. digital signatures).
4. Administrative Privileged Accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
5. Purposed Equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Cyber Resiliency Assurance Metric (CRAM)



Cyber Resiliency

- Buys down Risk
- Assumes Unknowns Happen
- Enables ability to Play Hurt
- Operational Contingency

Cyber S&T Thoughts

- Engineering Cyber Resilience in Weapons Systems
  - Criteria, Observables, Behaviors – What does Cyber Resiliency look like?
  - Requirements, Cost, Measures & Metrics – How to specify and measure Cyber Resiliency?
  - Acquisition Language, Design Standards – How to execute and implement Cyber Resiliency?

- Need to Secure
  - Software
  - Hardware
  - Integrated SW & HW
  - Carbon Based Units

- To Securely
  - Design & Develop Capabilities
  - Operate System/Missions
  - Maintain and Sustain Capabilities

Enable Cyber Mission Assurance

- Defining the problem space
  - Criteria
  - Observables
  - Behaviors

- To Define the Needs:
  - Mitigations
  - Capabilities
  - Investment Areas

Identify the Gaps

- Solutions and S&T needs follow Gaps

Cyber S&T Needs

- Automated Continuous Monitoring
- Persistent monitoring at bus level
- Supply Chain Risk Management scalability
- Awareness Education & Training
- Autonomy at the application level
- Automated vulnerability enumeration
- Use of autonomy in detection and response
- Measurement and attestation of system-of-system stack
- Software Assurance
- Automated Software Analysis & Repair
- Secure Operating System
- Autonomous Analysis & Detection
- Real Time Human in the loop HW simulations
- Threat detection & continuous monitoring
  - SWaP-C constrained environment

Initial Set Defined 2017

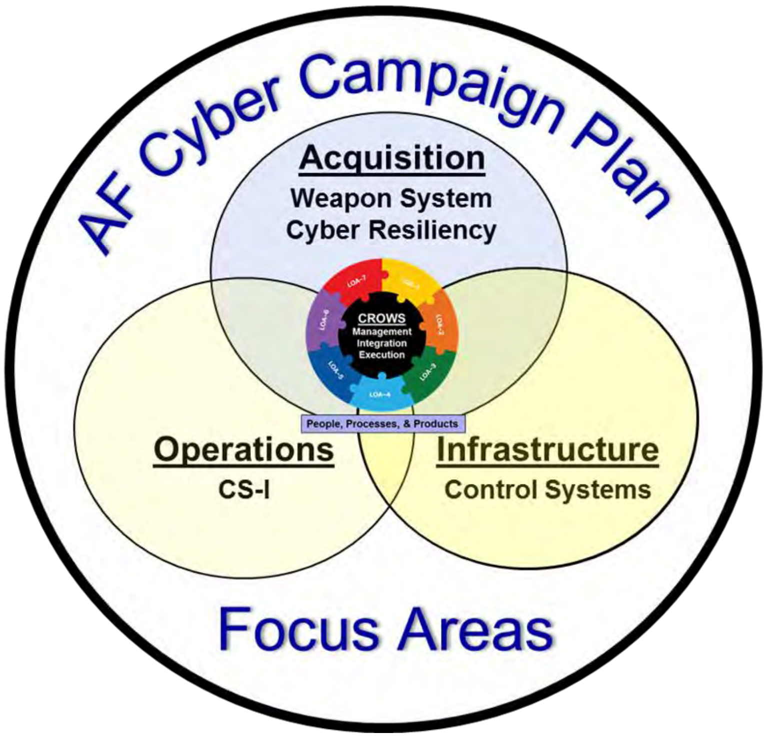
Summary

- **Challenge: Cyber resiliency impacts all AF missions -- new threats require new approaches to improve mission assurance**

- **Cyber Campaign Plan addresses this challenge in an integrated, holistic manner to enable AF to address cyber resiliency by:**
  - Making cyber security/resiliency a requirement in all weapon system acquisition programs
  - Assisting program managers to ensure cyber security/resiliency is fully considered and implemented in all aspects of acquisition programs across the lifecycle
  - Ensuring cyber security and resiliency becomes engrained in the AF acquisition culture

- **We are already seeing results due to awareness, training, TT&Ps, and identifying key enterprise vulnerabilities/mitigation solutions**

Authorizing Official (AO) Perspective



Mr. Daniel C. Holtzman, HQE
Command & Control (C2)
And
Rapid Cyber Acquisition (RCA)
Authorizing Official
daniel.holtzman.1@us.af.mil

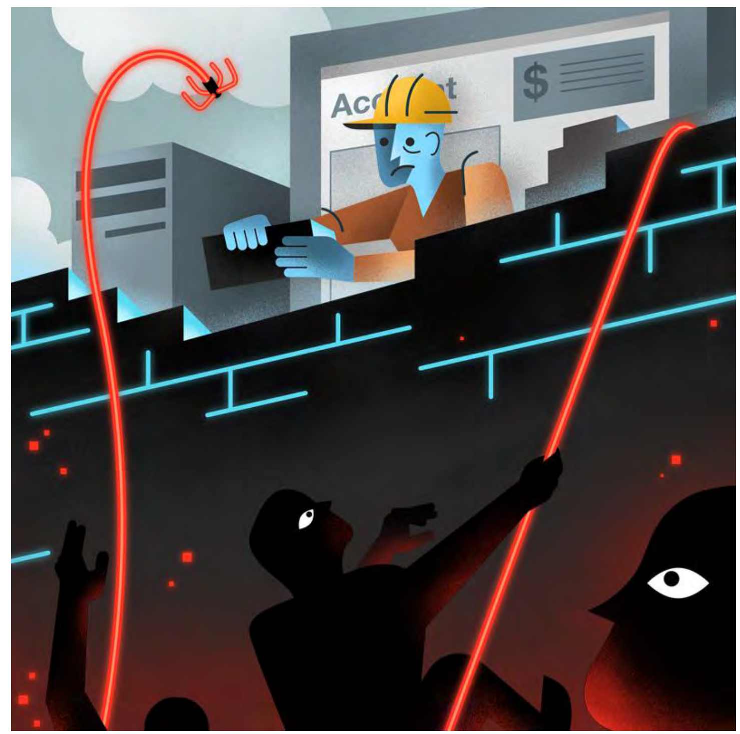
25 October 2017

Cyber Resiliency – A War Winning Capability

Weapon System Security & Resiliency

- Security & Resiliency are symbiotic
  - Each have objectives but can't achieve success without the other
  - Neither are sufficient alone to provide mission assurance
- Resiliency is the ability to play hurt

Can you take a punch?



USB port for Aircraft

Everything that connects to an Aircraft acts like an USB Port

- **All Access points need to be considered**
- **Need to ensure chain of trust and confidence**
- **There are no "Air Gaps" in the 21 Century**

Bottom Line Up Front
C2 & RCA Authorizing Official Objectives

- Objectives
  - Make decisions faster, Make transparent decisions, Foster reciprocity
  - Facilitate risk management, from acquisition through operations & sustainment
  - Enable Program Managers, to advance Cyber Security & Cyber Resiliency

- Enablers
  - Set clear requirements and increase agility in decision making process – Decision Briefing
  - Programs bring standard System Engineering - Evidentiary Analysis & Data
  - Provide programs with single AO POC for each Weapon System – Streamline expectations
  - Focus Cybersecurity on risks that matter – Risk Management vs Compliance perspective

- Collaborative Execution
  - Cyber Risk Assessors (CRA), formerly called SCA, are focused on assessing risks
  - Authorizing Official is focused on informing enterprise decision makers on Risks
  - Partnerships with PEO's, DOEs, PMs, Users, and Sustainers enables a holistic approach
  - Focus is on risk identification and management – Programs & AOs
  - Enable Cyber Resiliency – Foster Mission Assurance

Increase Decision Making Ability & Focus on Risk Management

C2 & RCA implementation approach

- Integration of Cyber Risk into program Risk
- Agile Decision Making
- System Engineering based approach
  - Evidentiary Analysis and Data driven
- Risk Confidence Index
  - Enables Risk Management vs compliance
- Collaborative Execution

Quick Look
Week 1

Assessment of target environment

Review existing Analysis & documentation

Start threat and Initial Risk Assessment

Week 2-3

Identify Risk based on target environment

Select Security features/Requirements based on Initial Risk Assessment

Weeks 3-4

Verification of Security Requirements

Real Time risk Assessment(s)

Weeks 5-6

Authorization decision

POA&M development

Ongoing monitoring for changes

Continuous Monitoring for ongoing risk assessment

Goal: Integrate Cyber Security into Acquisition, Operations, Sustainment Culture

C2 & RCA MAR Dashboard

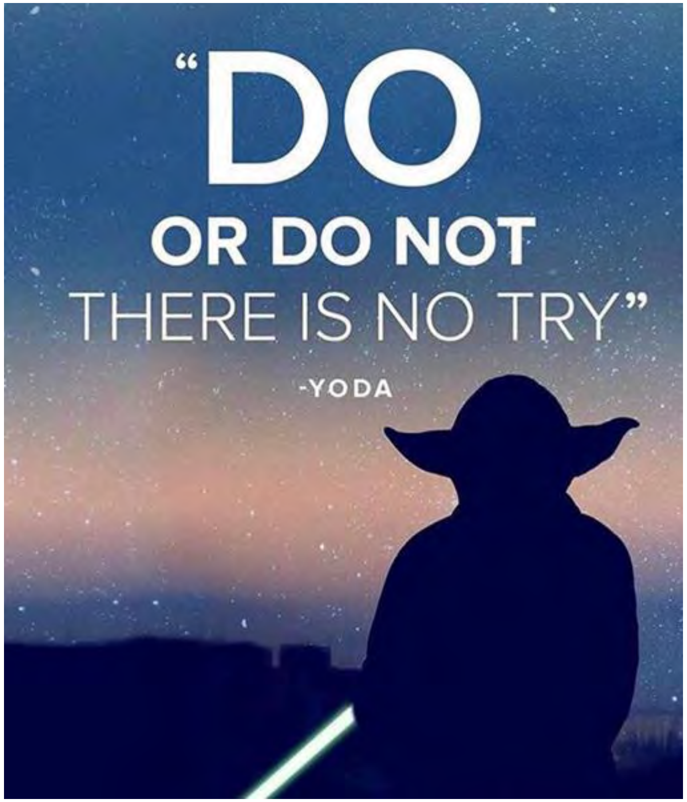
(In Development)

- **BLUF: Execute C2 & RCA AO responsibility as any other – Cost, Schedule, Performance**
- **Quarterly PMR with CIO – Asses C2 & RCA AO enterprise, Big Rocks, Issues/Opportunities**
- **Monthly reviews with Users (e.g. PEOs, MAJCOMS, Other Stakeholders)**
- **90 Day look ahead – Proactive vs Reactive**

ProgramName	RequestorOfficeSymbol	PEO_MAJCOM	DecisionType	DateExpires	SCA Signed	AO Signed
Unit Command and Control	HBBC	HB	ATO	11/21/2017	5/31/2017	6/2/2017
AF Common Computing Environment in Amazon GovCloud (Production), Version 1.1.1	HNII	AFLCMC	ATO	12/1/2017	5/24/2017	6/2/2017
Unit Command and Control	HBBC	HB	IATT	9/29/2017	4/24/2017	4/24/2017
AF-Doctrine Next (AWS GovCloud IL2)	HNI	AFLCMC	ATO	3/30/2018	3/23/2017	3/24/2017
Battlefield Control System-Tyndall	A3	AETC	ATO	3/31/2020	3/22/2017	3/22/2017
DCGS Integration Backbone	HBBI	AFLCMC	ATO	8/16/2019	3/7/2017	3/17/2017
AF Common Computing Environment (AWS GovCloud)	HNII	AFLCMC	IATT	9/1/2017	2/28/2017	3/2/2017
Battlefield Airborne Communications Node	HNA	AFLCMC	ATO	2/17/2020	2/17/2017	2/17/2017
Fixed Base Weather Observation System	HBAW	AFLCMC	ATO	1/15/2018	2/16/2017	2/16/2017
Fixed Based Weather Observation System	HBAW	AFLCMC	[illegible]	1/15/2018	2/16/2017	2/17/2017
Air Execution Information Services	HBBC	AFLCMC/HB	[illegible]	9/1/2017	2/1/2017	2/16/2017
Joint Mission Planning System 1.5.200	HBD	[illegible]	ATO	1/12/2018	1/23/2017	1/23/2017
FPS-117 Essential Parts Replacement Program	HBZIA	AFLCMC	ATO	2/2/2018	1/20/2017	1/27/2017
JSTARS Mission Maintenance Trainer	HBG	AFLCMC	ATO	3/31/2018	1/18/2017	1/24/2017
Airborne Warning and Control System Internet Protocol Enabled Communication	HBS	AFLCMC	IATT	4/30/2017	1/17/2017	1/23/2017
Agile Core Services	HBBC	[illegible]	IATT	9/1/2017	1/11/2017	1/23/2017
Air Tasking Order Management System	[illegible]	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Airspace Management Application - Airspace Information Service	[illegible]	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
C2AOS-C2IS Air Status	[illegible]	AFLCMC/HB	IATT	9/1/2017	1/11/2017	1/23/2017
Integrated Air and Missile Defense	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Joint Air Defense System Integrator	[illegible]	AFLCMC	ATO	10/1/2017	1/11/2017	1/12/2017
Joint Surveillance Target and Attack Radar Imagery Configuration Management System	HBG	AFLCMC	ATO	3/31/2018	1/11/2017	1/24/2017
Map Abstraction Layer	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Request Information Services Command and Control	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017

INITIAL

Questions & Discussion



Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the <u>Cyber Resiliency of Military systems</u> to be:
  - The ability of weapon systems ***to maintain mission effective capability*** under adversary offensive cyber operations
  - To ***manage the risk*** of adversary cyber intelligence exploitation
- Weapon systems differ from general administrative and business IT systems in ways that matter for implementing Cyber Resiliency

Cyber Campaign Plan FOCUS

Weapon Systems

Software/Hardware Design

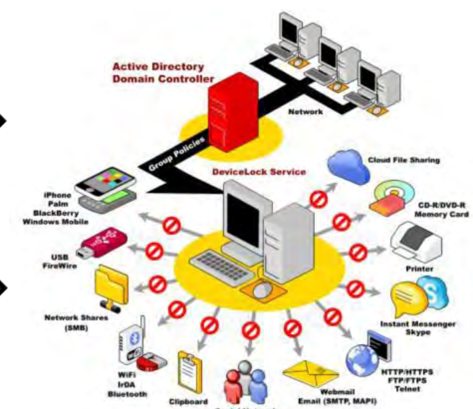
Government control ↔ COTS

Architectures

Diverse ↔ Common

Interfaces

Customized ↔ Standardized



IT Systems

Cyber Resiliency

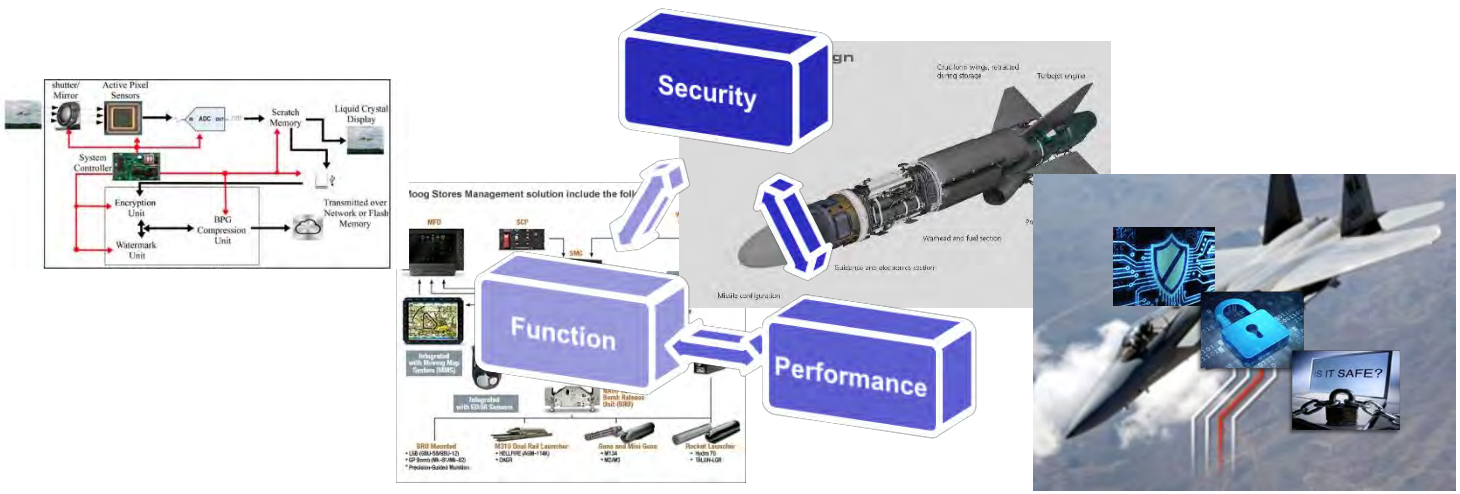
- Definition (What does it mean?)
  - Cyber Resiliency = ***<u>The ability to provide required capability despite adversity</u>***, that impacts the Cyber aspects of the Systems
  - "Cyber Aspects" = Software, Firmware and data in electronic form and the associated hardware
- Cyber Resilience, like system security, is an end goal:
  - And just like security having protection mechanisms (aka controls) that do not necessary combine to make one "adequately secure",
  - Having a set of resilience techniques and a framework for their application does not necessary combine to make one "resilient".

Design, Secure, Assess
Build, Secure, Assess

Bolted-on

COST

Baked-in



Best Countermeasure

- Cyber security will improve as system design improves.
- Essentially, if built properly, security will be an **inherent property**

- Best **countermeasures:**
  - Better design (Bake it in)
  - Proper use of technology (Plan for Resiliency)
- **Enable** systems:
  - To be resilient to rapid change

Change
&
Diversity

Weapons System Cybersecurity Guidance Operational Cyber Hygiene Activities

	Current Operations	Future Operations
Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
External media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
Data integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data. (I.e. digital signatures).
Administrative privileged accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
Purposed equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Public Release Approval

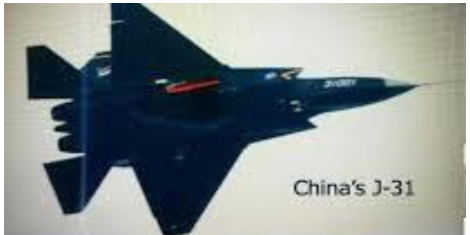
Case Number: 2017-0421 (original case number(s): AFIMSC-2017-0039; 66ABG-2017-0114) The material was assigned a clearance of CLEARED on 23 Oct 2017. If local policy permits, the Review Manager for your case, Deborah Powers, deborah.powers@us.af.mil, will prepare a hard copy of the review and will forward it via mail or prepare it for pick up.

Engaging the DoD Enterprise to Protect U.S. Military Technology Advantage

Brian Hughes
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

These are Not Cooperative R&D Efforts



M-16

QBZ-95

HUMVEE

Dongfeng EQ2050

Reaper

Yìlóng-1

Case History: Titanium Dioxide

Walter Liew, a naturalized American citizen, business owner, and technology consultant stole DuPont's protocols for producing its superior titanium white from 1997 through 2011

- DuPont developed $2.6B per annum Titanium Dioxide business – recognized as world leader
  - Processes created in 1940s but spent $150M year to improve processes by 1%
    - Near monopoly on the manufacturing techniques
  - Shielded its titanium dioxide process
    - Guards
    - Escorted Visitors
    - Documents and blueprints controlled
  - Starting in 1990's China began seeking ways to illegally acquire DuPont's methods
    - China accounts for approximately 25% of the demand

Liew was convicted in 2014 on each of twenty counts with which he was charged and sentenced to serve 15 years in prison, forfeit $27.8 million in illegal profits, and pay $511,667.82 in restitution

Bottom Line Up Front

- Adversary is targeting our Controlled Technical Information (CTI)
- DoD is emphasizing protection activities to encompass the full range of threats and vulnerabilities across the acquisition life cycle
- The Joint Acquisition and Protection and Exploitation Cell (JAPEC) enables a comprehensive analysis of protections for DoD's critical programs and technologies (CP&T) and addresses shortfalls
- Significant amount of technical expertise resides in the Defense Industrial Base (DIB)
- The DIB is not only critical to protecting that information but helping DoD identify which information it should protect

Partnership between DoD and DIB is vital

Agenda

- **DoD Efforts to Safeguard Controlled Technical Information (CTI)**

- **Know the Environment**

- **Stakeholder Dialogue**

- **Defense Industrial Base (DIB)'s Role in the Process**

Addressing the Loss of CTI

Risk = f (threat, vulnerabilities, consequences)

Goals:

- **Enable information-sharing, collaboration, analysis, and risk management between acquisition, Law Enforcement (LE), Counterintelligence (CI), and Intelligence Community (IC)**
  - Connect the dots in the risk function (map blue priorities, overlay red threat activities, warn of consequences)
- **Integrate existing acquisition, LE, CI, and IC information to connect the dots in the risk function - linking blue priorities with adversary targeting and activity**
  - Many sources and methods are relevant (e.g., HUMINT, joint ventures)
  - Cyber is only one data source
- **Focus precious resources**
- **Speed discovery and improve reaction time**
- **Ultimately, evolve to a more proactive posture**

JAPEC Mission: Integrated Analysis

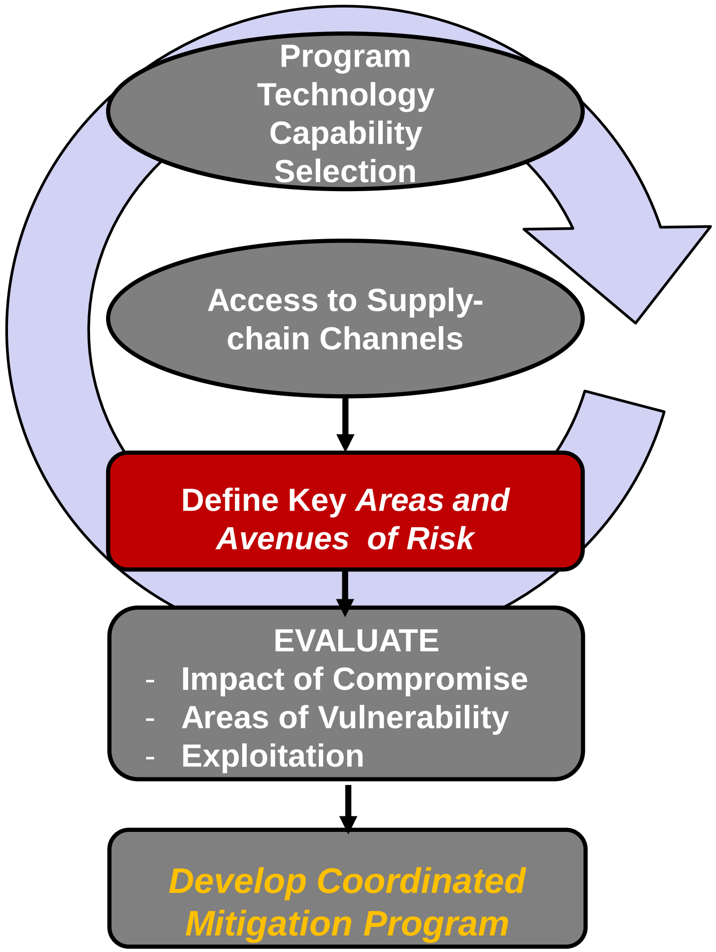
The Joint Acquisition and Protection and Exploitation Cell (JAPEC) integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage.

Identifying Critical Programs and Technologies for Proactive Protection

ACQUISITION
- Identify DoD's Critical Acquisition and Technology
- Link technologies across the enterprise
- Identify protection methods
- Educate the workforce

SECURITY
- Integrate CI/Security posture
- Coordinated Security Classification Guides
- Onsite protection at DIB
- Contractor threat education

COUNTERINTELLIGENCE/ LAW ENFORCEMENT
- Collect against adversary activity
- Field presence
- Facility security analysis
- CI threat assessment
- Investigations & Prosecution



REQUIREMENTS
- Revise requirements based on change in threat

INTELLIGENCE
- Identify adversary technologies needs

DIB
- Understand Supply Chain
- Proactive approaches
- Improve Information Sharing w/ DoD

CIO/NETWORK SECURITY
- Tiered IT security controls
- Enroll in threat sharing forums

JAPEC projects demonstrated the effectiveness of an integrated iterative approach. JAPEC methods complement other DoD efforts.

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- **Know the Environment**
- Stakeholder Dialogue
- Defense Industrial Base (DIB)'s Role in the Process

Understanding Your Supply Chain

- **Increase level of concern for DoD's protection priorities throughout the supply chain**
  - Includes vendors, mergers, acquisitions, subsidiaries
- **Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States dtd 21 July 2017**
- **Within 270 days**
  - (a) identifies military and civilian materiel, raw materials, and other goods essential to national security;
  - (b) identifies manufacturing capabilities essential to producing goods identified pursuant to subsection (a) of this section, including emerging capabilities;
  - (c) identifies defense, intelligence, homeland, economic, natural, geopolitical, or other contingencies that may disrupt, strain, compromise, or eliminate supply chains of goods identified pursuant to subsection (a) of this section (including as a result of the elimination of, or failure to develop domestically, capabilities identified pursuant to subsection (b) of this section) and that are sufficiently likely to arise so as to require reasonable preparation for their occurrence;
  - (d) assesses resiliency and capacity of manufacturing and defense industrial base and supply chains of the United States to support national security needs

How well do you know your supply chain?

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- **Stakeholder Dialogue**
- Defense Industrial Base (DIB)'s Role in the Process

Dialogue with Protection Stakeholders

- **Compliance with existing rules & regulations is necessary but not sufficient**
  - Protection is more than completing a checklist
- **What is crucial to your organization delivering the desired capability?**
  - Identify who, what and where at each facility
    - FSO may not be well positioned to speak to this
  - Are there links with other programs, especially if programs are in a different Military Department?
    - Informing all involved parties helps focus IC, CI, and LE resources
  - Are there plans to market the same technology to other Military Departments or Government Agencies?
    - Government regulations and laws protect business proprietary
- **DoD/DIB information sharing improves the US' ability to focus priorities on most critical technologies**
  - Timely reporting to DoD which includes more than cyber incidents
  - Information sharing forums enable you to learn from other's experiences

Adversary is Dynamic and Active

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- Stakeholder Dialogue
- **Defense Industrial Base (DIB)'s Role in the Process**

DIB Role

- **Identify crucial elements for protection up front**
  - Requires coupling technical know how with CI/LE expertise
  - Develop and implement training that focuses specifically on CTI handling and protection requirements
- **Do you have your own list of technologies crucial to you?**
- **Report**
  - Cyber incidents
  - Suspicious contacts
  - Media Theft and Loss
  - Insider Threats
- **Consider joining the DIB CS program**
  - Enables Government to Industry information sharing
  - Join and contribute to the DIB CS program at http://dibnet.dod.mil/
  - Share cyber forensic reports with DoD
- **Maintain an open dialogue with all the protection stakeholders**
  - Counterintelligence, Law Enforcement, Network Security, etc.
  - Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting at http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf

The DIB is a critical partner in preventing unauthorized access to precious U.S. intellectual property and manufacturing capability by adversaries

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Questions

Mr. Brian D. Hughes

Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451

Engineering
Cyber Resilient Weapon Systems

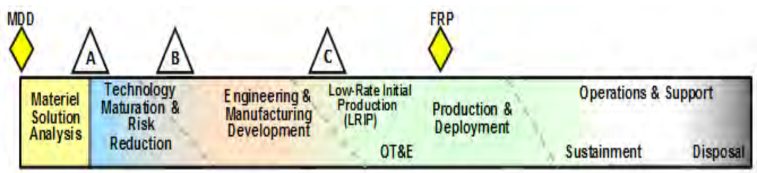
Melinda K. Reed
Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

Ensuring Cyber Resilience in Defense Acquisition Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - Found in programs, organizations, personnel, networks, systems, and supporting systems
  - Inherent weaknesses in hardware and software can be used for malicious purposes
  - Weaknesses in processes can be used to intentionally insert malicious hardware and software
  - Unclassified design information within the supply chain can be aggregated
  - US capability that provides a technological advantage can be lost or sold
- ***Consequences:***
  - Loss of technological advantage
  - System impact – corruption and disruption
  - Mission impact – capability is countered or unable to fight through

Access points are throughout the acquisition lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Key Protection Activities to Improve Cyber Resiliency

Program Protection & Cybersecurity

DoDI 5000.02, Enclosures 3 & 14

DoDM 5200.01, Vol. 1-4 **DoDM 5200.45** **DoDI 8500.01**

DoDI 5200.39 **DoDI 5200.44** **DoDI 5230.24** **DoDI 8510.01**

Technology

What: A capability element that contributes to the warfighters' technical advantage (Critical Program Information (CPI))

Key Protection ActivityU

- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Activity:

- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

Goal: Protect key mission components from malicious activity

Information

What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Activity:

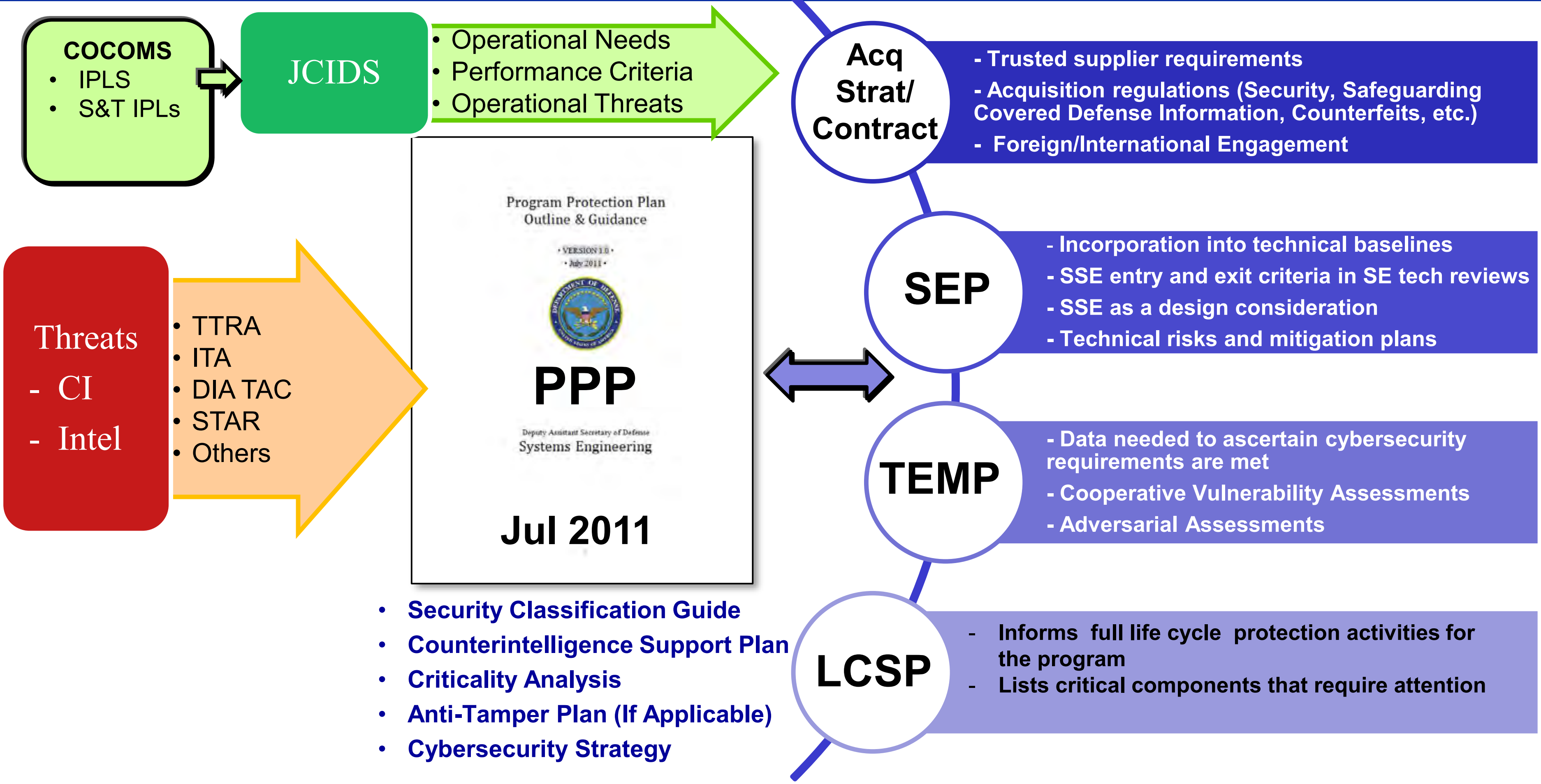
- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

Goal: Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: https://www.acq.osd.mil/se/initiatives/init_pp-sse.html

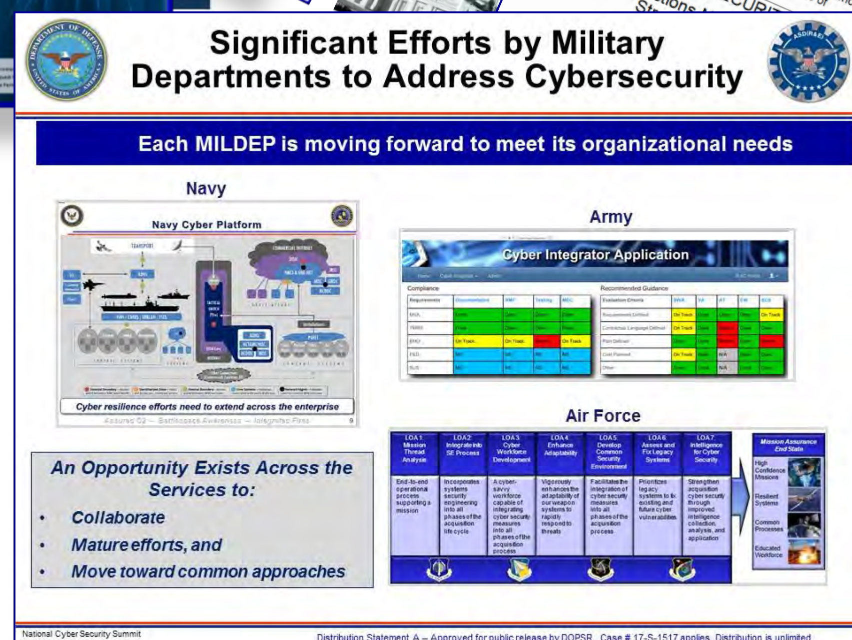
Program Protection and Cybersecurity Relationship to Key Acquisition Activities



Program Protection and Cybersecurity Considerations Are Integrated In All Aspects of Acquisition

Cybersecurity Is Everyone's Responsibility

Cybersecurity is not just an IT / network issue. We must translate Cyber IT / Network practices, standards, etc. into physical system requirements.



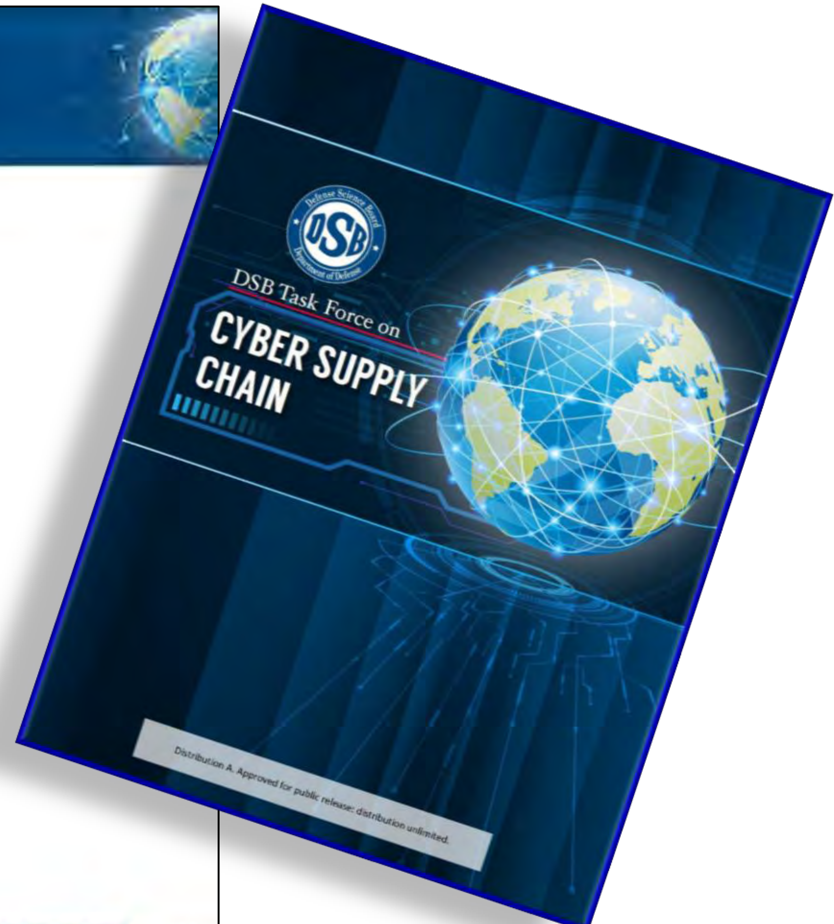
Recommendations from Defense Science Board

Summary of Recommendations

Five categories for improvement

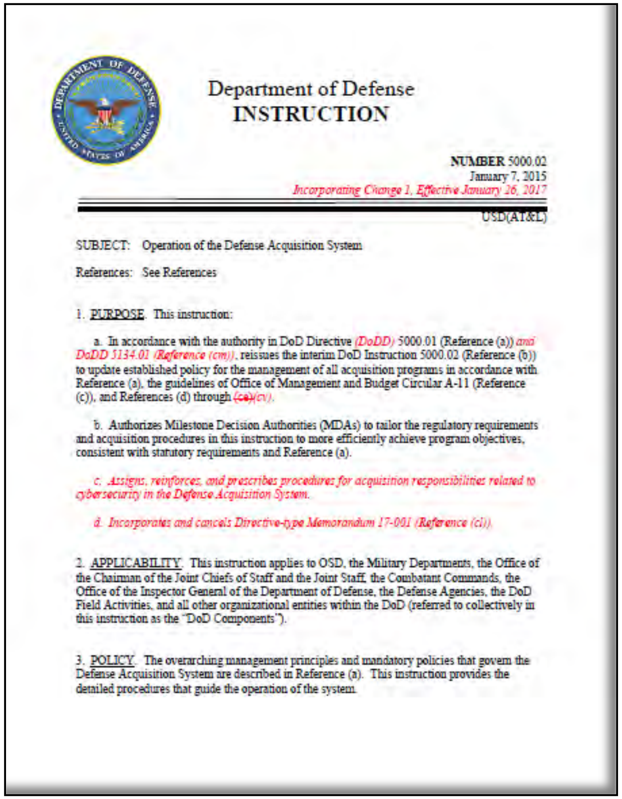
1. Understand supply chain risk
   - Expand vulnerability assessments
2. Mitigate potential vulnerabilities
   - Improve detection and reporting
3. Approach acquisition differently
   - Enhance program protection planning
   - Improve timeliness of supplier vetting
   - Improve system engineering
   - Use JFAC and JAPEC effectively
   - Consider cybersecurity impact of COTS products and components
4. Support life-cycle operations
   - Establish sustainment PPPs for fielded systems
   - Collect and act on parts vulnerabilities
5. Pursue technical solutions

DSB TASK FORCE ON CYBER SUPPLY CHAIN 11



Publicly-released report published Feb 2017
Available at: https://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF

Cybersecurity in Acquisition



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 1, Effective January 26, 2017

USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive *(DoDD)* 5000.01 (Reference (a)) *and DoDD 5134.01 (Reference (cm))*, reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through ~~(ce)~~*(cv)*.

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

c. Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.

d. Incorporates and cancels Directive-type Memorandum 17-001 (Reference (cl)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

Acquisition workforce must take responsibility for cybersecurity from the earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal

Scope of program cybersecurity includes:

– Program information Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system.

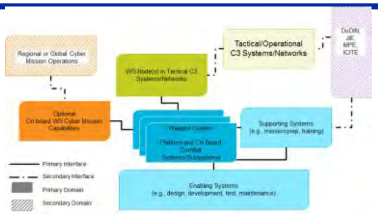
– Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations

– Networks Government, Government support activities, and contractor owned and operated unclassified and classified networks

– Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems

Codified in DoDI 5000.02, Enclosure 14, Jan 26, 2017

Design for Cyber Threat Environments



Activities to mitigate cybersecurity risks to the system include:

- **Allocate cybersecurity and related system security requirements to the system architecture and design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:**
  1. Manages access to, and use of the system and system resources.
  2. Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning).
  3. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment.
  4. Monitors, detects and responds to security anomalies.
  5. Maintains priority system functions under adverse conditions; and
  6. Interfaces with DoD Information Network (DoDIN) or other external security services.

DoDI 5000.02, Enclosure 14 establishes a threshold for what to address

Implementation: Engineering Cyber Resilient Workshops

Workshop 1 Findings
1. Requirements derivation is a challenge area
2. Require clarity on Risk Acceptance
3. Assessments should be integrated with and driven by SE Technical Reviews

Workshop 2 Findings/Actions
1. Definitions, Taxonomy & Standards Framework
2. Knowledge Repository
3. Consolidated Risk Guide
4. Assessment Methods
5. Needs Forecasting
6. Industry Outreach

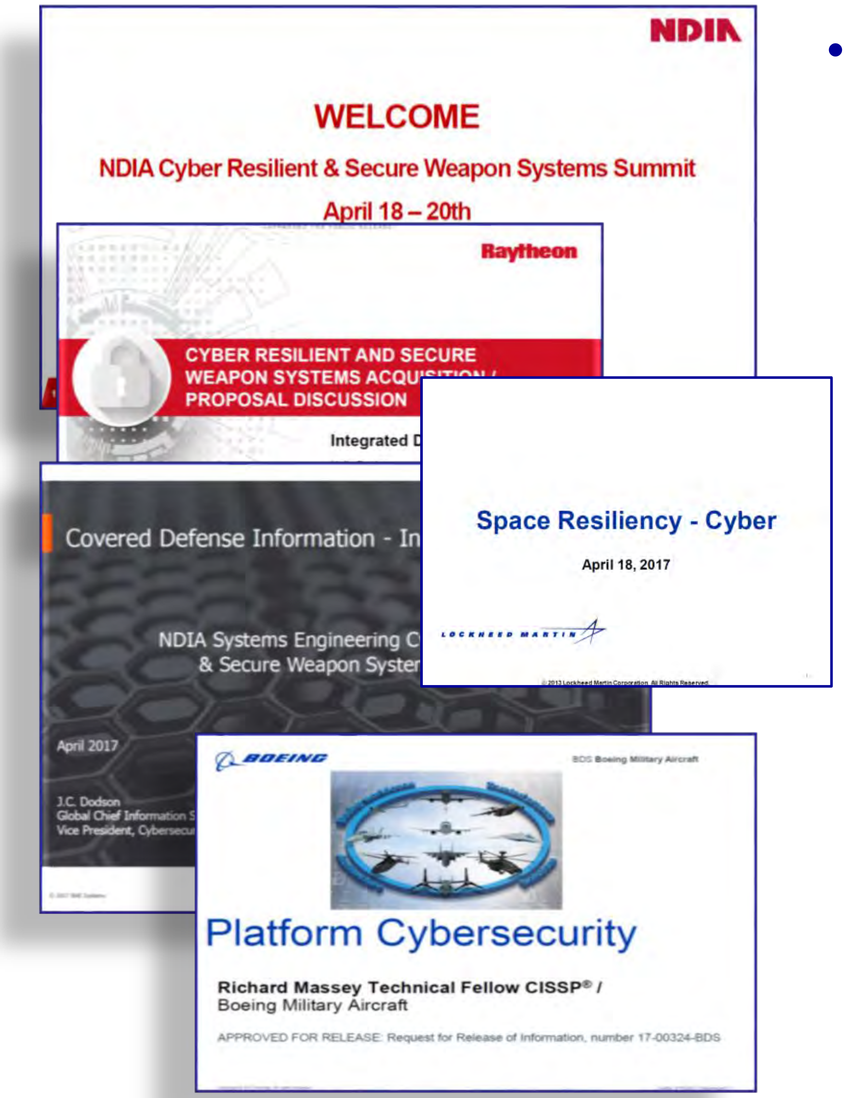
Workshop 3 Findings/Actions
1. Establish DAU CRWS CoP; facilitate definitions, taxonomy standards
2. Develop Risk, Issues, & Opportunities engineering cyber appendix
3. Align assessment approaches
4. Explore S&T opportunities
5. Address Workforce needs
6. Industry Outreach

Workshop 4 (Aug 2017)
Theme: Changing the Culture / Method: Leverage existing engineering approaches

- **Technical Performance Measures and Metrics**
  - Develop Engineering Guidebook
  - Identify TPMs affected by Cyber actions
- **System Engineering Technical Reviews**
  - Validate that existing SETR criteria is sufficient for secure and resilient system design and sustainment
- **Leveraging System Safety**
  - Identify threshold of acceptable risk
  - Quantify the security-driven risk
- **Cyber Resilient Software**
  - Establish an outline to identify engineering design and analysis considerations for the software in secure and resilient weapon systems
- **Risk, Issues, and Opportunity (RIO) Guide**
  - Develop appendix for Cyber Risk

Addressing Recurring Challenges:
Design Guidelines, Implementation, Engineering Assessment

NDIA SE Cyber Resilient Summit and Secure Weapon System Summit
April 18-20, 2017



- **Initial Industry Outreach Aligned with CRWS Series**
  - Industry implementation lessons learned
  - Emphasized need for consistency across communities
  - Discussed approaches to risk acceptance
  - Offered thoughts on implementing safeguards on manufacturing floor
  - Offered areas for improvements to methods, standards, processes, and techniques for cyber resilient & secure weapon systems
  - Thoughts on addressing sustainment challenges

Joint Federated Assurance Center: Software and Hardware Assurance

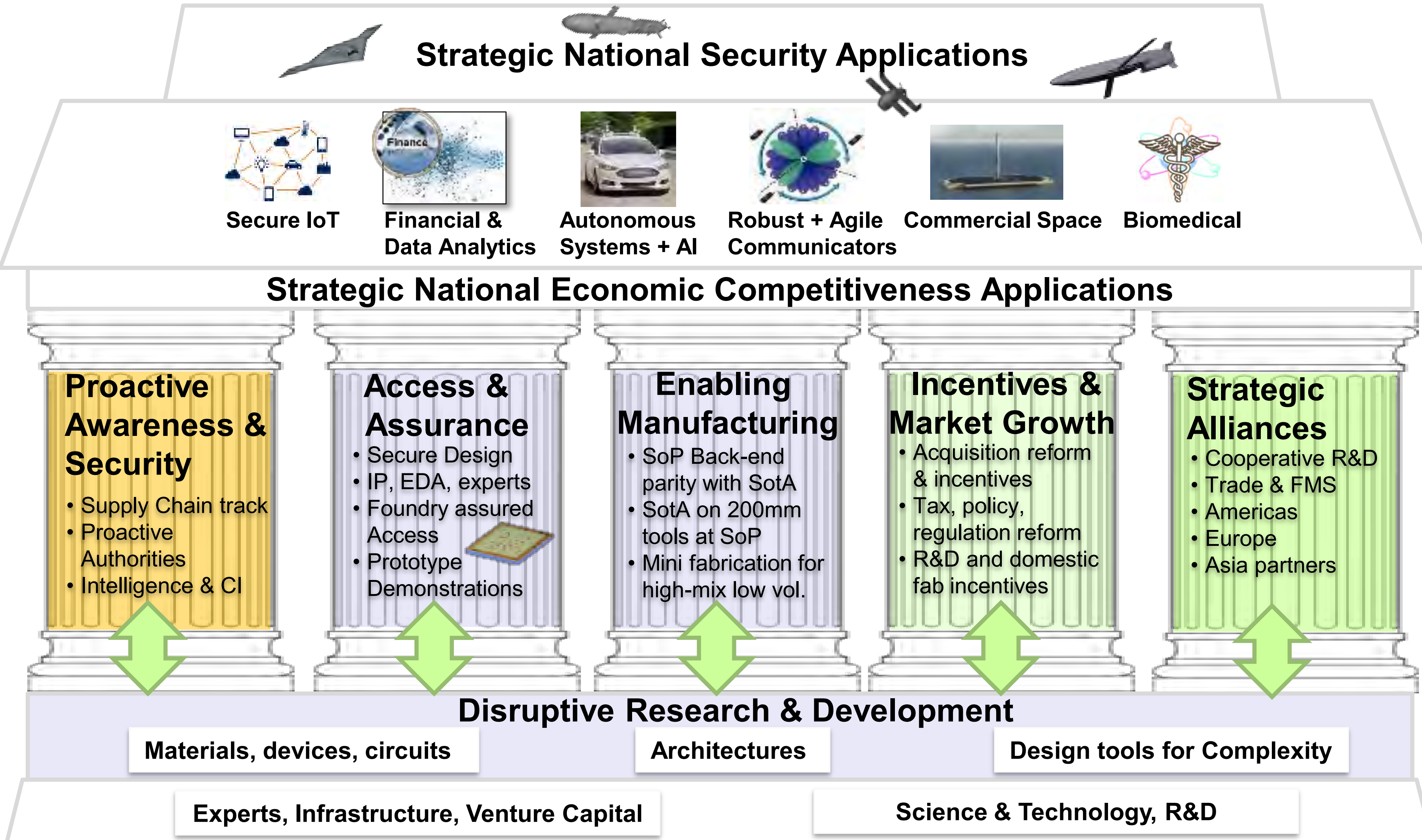
- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities to:**
  - Provide SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to PM's to mitigate risk of malicious insertion

- **JFAC Coordination Center is developing SwA tool and license procurement strategy to provide:**
  - Enterprise license agreements (ELAs) and ELA-like license packages for SwA tools used by all DoD programs and organizations
    - Initiative includes coordinating with NSA's Center for Assured Software to address potential concerns about the security and integrity of the open source products
  - Automated license distribution and management system usable by every engineer in DoD and their direct-support contractors

- **Lead DoD microelectronic hardware assurance capability providers**
  - Naval Surface Warfare Center Crane
  - Army Aviation & Missile Research Development and Engineering Center
  - Air Force Research Lab

Moving Towards Full Operational Capability
JFAC Portal: https://jfac.army.mil/ (CAC-enabled)

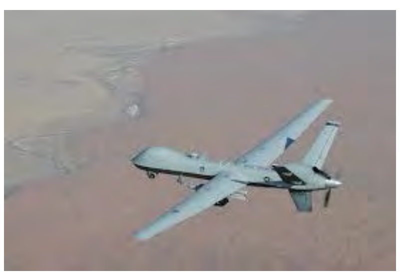
US Microelectronics Security and Innovation



These Are Not Cooperative R&D Efforts

U.S. HUMVEE

China's Dongfeng EQ2050



U.S. Reaper

China's Yìlóng-1

Protecting DoD's Unclassified Information

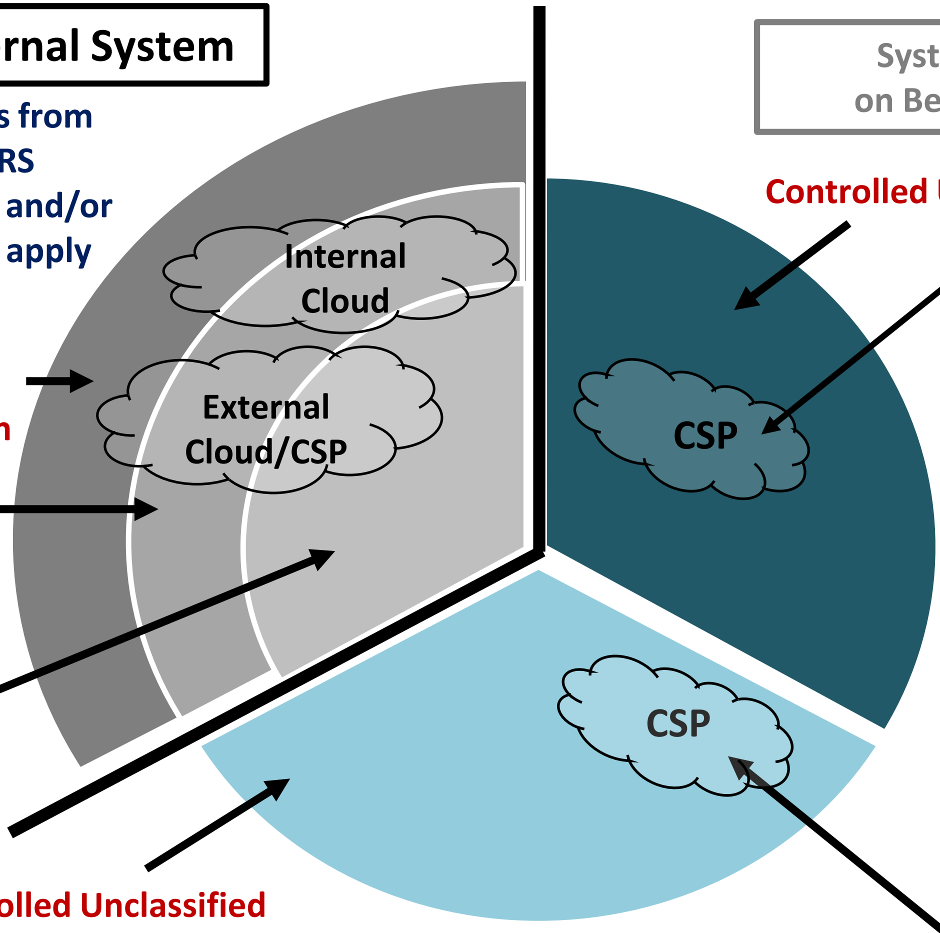
Contractor's Internal System

Security requirements from NIST SP 800-171, DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21 apply

Federal Contract Information

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information



System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

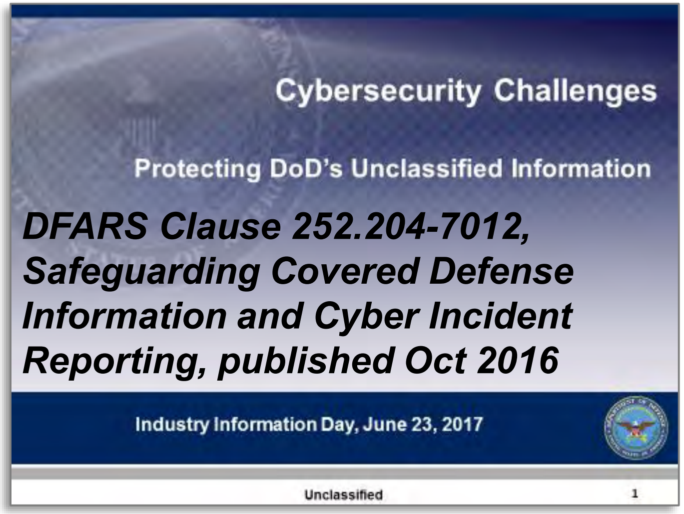
Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

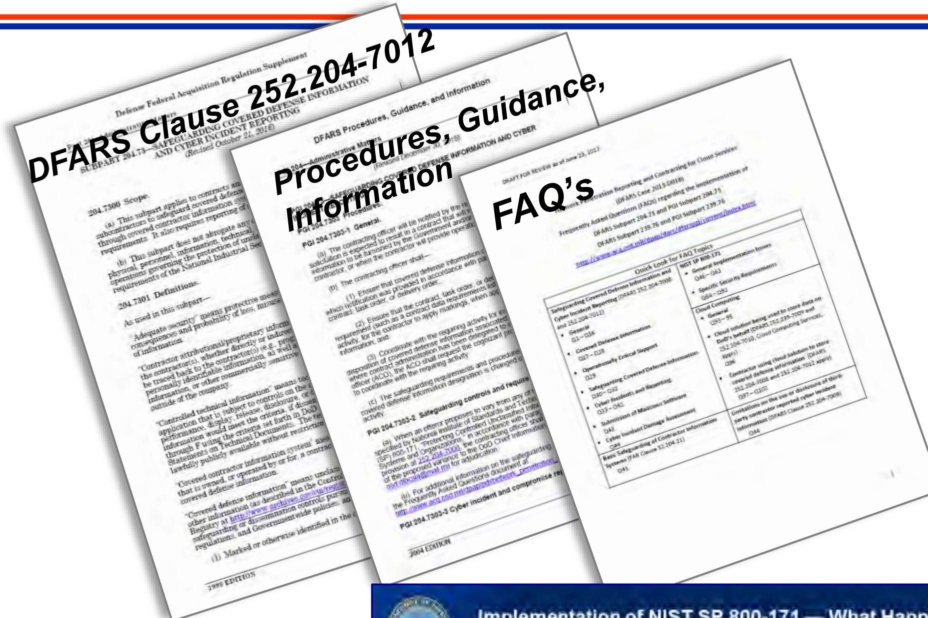
DoD Owned and/or Operated Information System

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

Contract Regulation for Safeguarding Covered Defense Information



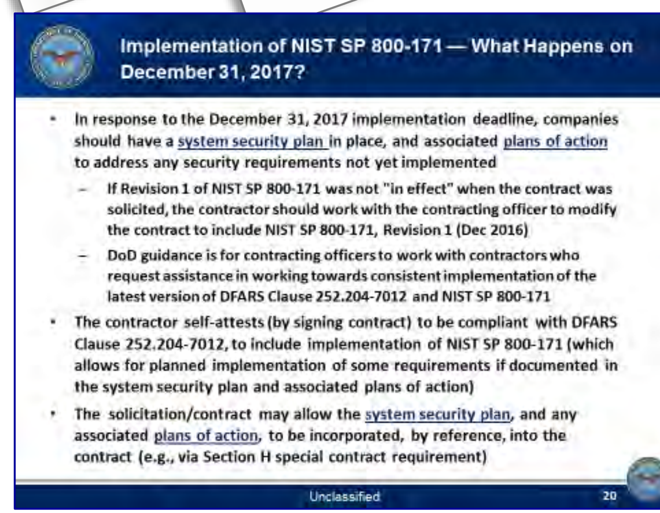


Purpose:

- Establish minimum requirements for contractors and subcontractors to safeguard DoD unclassified covered defense information and report cyber incidents on their contractor owned and operated information systems

Contractor is required to:

- Implement NIST SP 800-171 Controls for unclassified non-Federal Information Systems
- Report cyber incidents affecting covered defense information
- Submit malware when discovered
- Submit media when requested by DoD
- Flow down Clause to subcontractors when covered defense information is on subcontractor networks



Implementation of NIST SP 800-171 — What Happens on December 31, 2017?

- In response to the December 31, 2017 implementation deadline, companies should have a system security plan in place, and associated plans of action to address any security requirements not yet implemented
  - If Revision 1 of NIST SP 800-171 was not "in effect" when the contract was solicited, the contractor should work with the contracting officer to modify the contract to include NIST SP 800-171, Revision 1 (Dec 2016)
  - DoD guidance is for contracting officers to work with contractors who request assistance in working towards consistent implementation of the latest version of DFARS Clause 252.204-7012 and NIST SP 800-171
- The contractor self-attests (by signing contract) to be compliant with DFARS Clause 252.204-7012, to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the system security plan and associated plans of action)
- The solicitation/contract may allow the system security plan, and any associated plans of action, to be incorporated, by reference, into the contract (e.g., via Section H special contract requirement)

Unclassified 20

Cybersecurity in DoD Acquisition Regulations page:

http://dodprocurementtoolbox.com/ for Related Regulations, Policy, Frequently Asked Questions, and Resources

Cybersecurity for Advanced Manufacturing Systems

NDIA

Operational Technology Environment

ICS systems are long-lived capital investments (15-20 year life)

"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing jobs bring executable code into system

Technical data flowing through the system is highly valued by adversaries

10 NDIA Cybersecurity for Advanced Manufacturing Joint Working Group April 20, 2017

Challenges in DoD and the Manufacturing Environment are Cross Cutting

Cyber Community of Interest Roadmap Key Capability Areas

Embedded, Mobile, and Tactical Systems (EMT)

Assuring Effective Missions	Assess and control the cyber situation in mission context
Agile Operations	Dynamically reshape cyber systems as conditions/goals change, to escape harm

Resilient Infrastructure	Withstand cyber attacks, and sustain or recover critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

Cyber Modeling, Simulation, and Experimentation (MSE)

(MSE & EMT) cross-cutting areas in analysis of Joint Chiefs of Staff Cyber Gaps

Program Protection and Cybersecurity in Acquisition Workforce Training

- **ACQ 160: Program Protection Overview**
  - Distance learning (online); ~3 days
  - Provides an overview of program protection concepts, policy and processes, includes overview of DFARS 252.204-7012
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM
  - **Course deployed on DAU website on 15 Aug 2016**

- **ENG 260: Program Protection Practitioner Course (est. deployment Summer 2018)**
  - Hybrid (online and in-class); ~1 week
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes, including PM responsibilities for implementing DFARS 252.204-7012

Defense Acquisition University

Effective program protection planning requires qualified, trained personnel

Summary

- **Each system is different; approaches must be tailored to meet the requirement, operational environment and the acquisition**
  – We will embed cybersecurity risk mitigation activities into the acquisition program lifecycle

- **We must bring to bear policy, tools, and expertise to enable cyber resiliency in our systems**
  – Translate IT and network resiliency to weapon system resiliency
  – Establish system security as a fundamental discipline of systems engineering

- **Opportunities for government, industry and academia to engage:**
  – How can we thoughtfully integrate cybersecurity practices in existing standards for embedded software?
  – How can we better integrate program protection and cybersecurity risks into program technical risks?
  – Can we establish system requirements that restricts a system to a set of allowable, and recoverable behaviors?
  – How can we carefully engineer stronger resiliency in systems that are being modernized?

Systems Engineering: Critical to Defense Acquisition










PP/SSE Initiatives Webpage

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

JFAC Portal

https://jfac.army.mil/ (CAC-enabled)

For Additional Information

Ms. Melinda Reed

ODASD, Systems Engineering

571-372-6562

melinda.k.reed4.civ@mail.mil

Program Protection and Cybersecurity in DoD Policy

DoDI 5000.02 Operation of the Defense Acquisition System

– Assigns and prescribes responsibilities for Cybersecurity, includes security, to the acquisition community
– Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD; PM will submit PPP for *<u>Milestone Decision Authority approval</u>* at each Milestone review

DoDI 5200.39 Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation

– Establishes policy and responsibilities for identification and protection of critical program information
– Protections will, at a minimum, include anti-tamper, exportability features, security, cybersecurity, or equivalent countermeasures.

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

– Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to <u>vulnerabilities in system design</u> or <u>subversion of mission critical functions or components</u>

DoDI 4140.67 DoD Counterfeit Prevention Policy

– Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

– Establishes the DoD Cybersecurity Program, the DoD Principal Authorizing Official and Senior Information Security Officer to achieve cybersecurity through a defense-in-depth approach that integrates personnel, operations, and technology

An Adaptive Automation Approach for UAV UI Concept Development

Jeff O’Hara, Senior Research Scientist
Stuart Michelson, Research Engineer II
Georgia Tech Research Institute,
Human Systems Engineering Branch

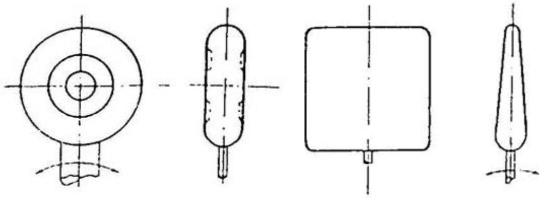
NDIA Systems Engineering Conference
24OCT2017

Georgia Tech Research Institute
Problem. Solved.

Background

- High loss rate of U.S. Military UAVs
- Numerous ergonomic / automation causal factors (Source: USAF SAB):
  - 80% of Predator mishaps involved human error due to fundamental design issues.
  - Warning/status messages buried layers deep.
  - Complex automation (22 steps to turn on the autopilot on the Predator).
  - $4.5M Predator lost due to pilot accidentally selected the engine kill switch instead of the landing gear switch.
- Analogous in terms of maturity to early manned cockpit design (systematic control shape coding analyses fixed a spate of B-17/B-25 crashes).
- Need a Systems Engineering approach to higher order human/automation system design.

B-17 Flap and Gear Handle



Modern Shape Coding

Challenging Emergent Requirements Driving the Need for Automation

Georgia Tech Research Institute

- New UAV Combat Missions:
  - Airborne Electronic Attack (AEA)
  - Air to Ground (A/G)
  - Air to Air (A/A)
- New User Interface Goals:
  - Single Pilot for multiple UAVs
  - Multiple user interactions (ground troops, manned air).

UAV kill by Tactical High Energy Laser (THEL) 2011

- Derived Requirements Mandate the use of Automation:
  - Single pilot mismatch with available attention span over multiple vehicles and multiple users.
  - Human reaction time mismatch (reactive jamming of enemy radar pushes automated response requirements)
  - Human computational limit reached (pilot is overmatched trying to compute fuel burn vs. rerouting requirements for signature management, etc.).

UAV Current Automated Capability

Georgia Tech Research Institute

UAV: "an aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming."

(US DoD Definition: JP 1-02)

- Current UAVs have very limited autonomy (e.g. preprogrammed flight to regain a lost link, auto land).
- Designers are struggling with adding more, incrementally.

MQ-1 Predator GCS

What to Automate – and what to NOT.

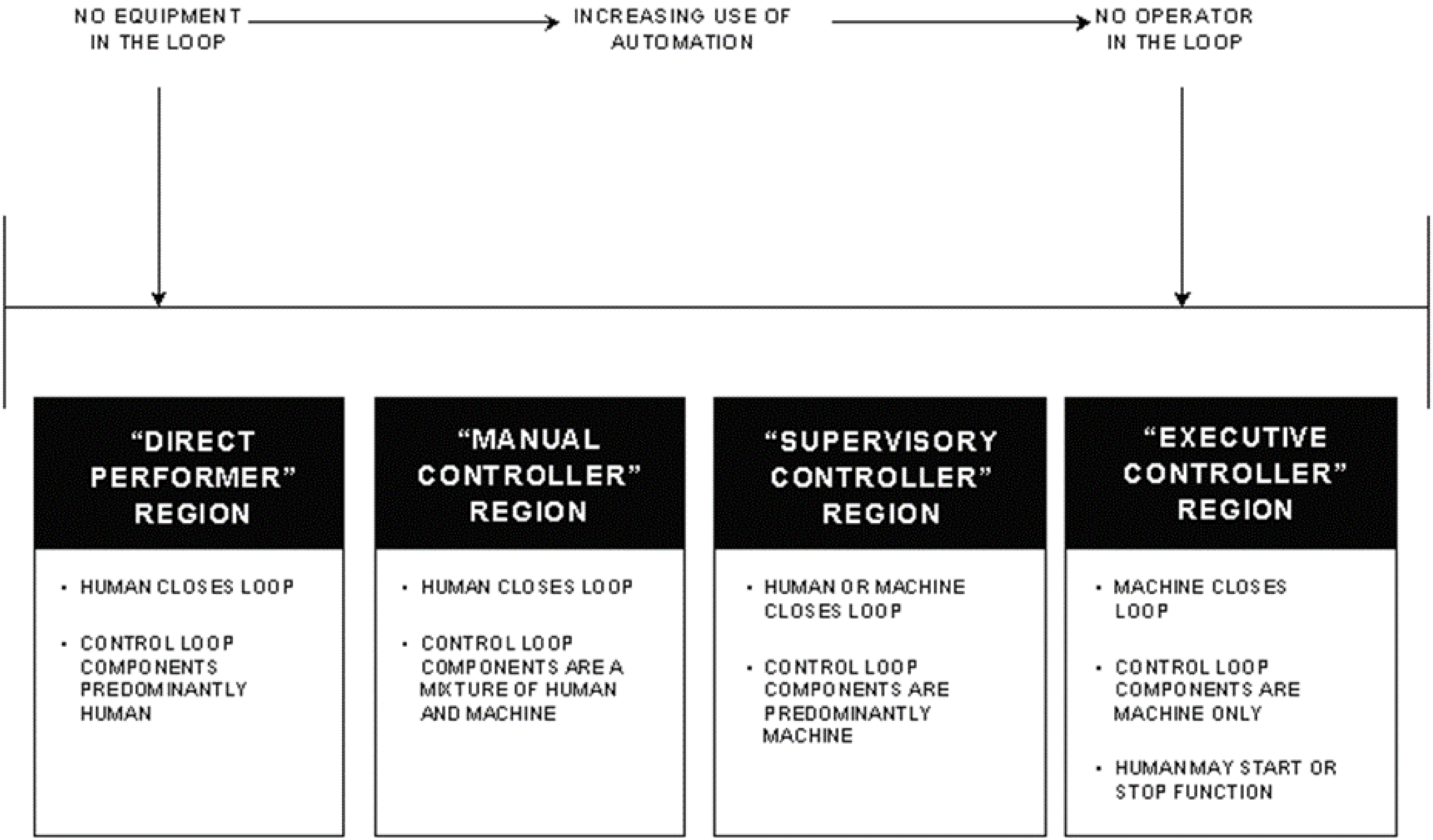
- The appropriate Systems Engineering question is not "how to design man out", but rather "which functions and tasks are appropriate to automate, and how?".
- Factors include:
  - Tactically significant timelines
  - Latency in the control loop (Observe/Orient/Decide/Act – OODA)
  - Need for human oversight and control – with weapons releases.

B-21 Raider

- The next step is to recognize the need for automation to manage automation itself.

Operator Role Theory of Automation
(Folds, 1995)

Georgia Tech Research Institute



System of Systems Approach

- Need a system of systems engineering approach across applications - to adaptive automation.
- Perform MTA/Task Decomposition and apply Operator Role Theory to determine mission elements.
- Determine which elements will exceed human spans of capability.
- Determine the modes of interaction between automation, and the overarching control loop tasks.
- Determine where **Executive level automation** is best suited to arbitrate or interpolate or monitor, and where the tasks are best suited for humans.

Executive Agent Example

Georgia Tech Research Institute

The Executive Agent

- Monitors automation managers within UAVs.
- Monitors coordinated tactics across UAV platforms.
- Compares weighted impacts of conflicting automation.
- Auto performs defined tasks / alerts pilot for other tasks.

+ N

The Datalink Manager

- Monitors datalink latency and quality against calculated range.
- Multiple links (UAV/UAV, UAV/manned, UAV/GCS, etc.)
- Alerts when nearing lost link.
- Sets flight path to regain link.

The Signature Manager

- Monitors ownship multispectral vis against known threat sensors.
- Continuously computed during maneuvering.
- Alerts when near high Pd.
- Sets flight path to avoid.

Executive Agent With the OODA Loop

- Monitor (“Observe/Orient”)
- Adjudicate (“Decide”).
- Recommend (or “Act”).
- Inform: elevate urgent advisories (would inform, then prompt, then warn).
- Perform specific-to-general reasoning related to induction, synthesis, and integration tasks.
- Perform general-to-specific reasoning related to deduction, analysis, and differentiation.
- Return the pilot to the role of a tactician.

Summary

- The piecemeal use of automation may be worse than having none.
- By equipping proposed future multiple combat UAV control systems with agile, Executive level controllers which can rapidly perform multivariate, weighted arbitrations between systematically integrated automation, time critical combat tasks can be met within the multiple UAV control paradigm.

An Adaptive Automation Approach for UAV UI Concept Development

Jeff O'Hara
404-407-8507
Jeffrey.ohara@gtri.gatech.edu

Stuart Michelson
404-407-6162
stuart.michelson@gtri.gatech.edu

Georgia Tech Research Institute
Electronic Systems Laboratory
400 Tenth St. NW
Atlanta, GA 30332-0840

Abstract

Despite decades of industry experience in the design of Unmanned Aerial Vehicle (UAV) control systems and their user interfaces, a combination of factors persist that produce a significant and unacceptable loss rate of UAVs due to poor user interfaces. One significant element is the current focus of human systems design on lower-order User Interfaces (UI) at the expense of investing in the design of an adaptive higher level integration to relieve inattentive or overtaxed operators of significant functionality as required, and to perform time-critical tactical tasks which humans cannot perform or for which they are not well suited. The approach proposed is one which defines the respective roles of user interactions with adaptive policy manager automation to address the loss of vehicles and mission failures. Specific policy manager automation elements are explored which will enable the system to flexibly assume or release UAV vehicle or systems functionality based on operator action/saturation in a number of mission areas. A notional Executive automation controller design approach is outlined to meet time critical information integration and mission task requirements.

Introduction and Historical Background

Despite decades of industry experience in the design of Unmanned Aerial Vehicle (UAV) control systems and their user interfaces, a combination of factors persist that produce a significant and unacceptable loss rate of UAVs due to poor user interfaces. By way of comparison to the progression of manned aircraft pilot vehicle interfaces, the UAV UI field has failed to progress as rapidly, being somewhat stalled at an equivalent of a 1940's state of the art with design foci on improved detailed level UI (menus, knobs, switches, screens), rather than on addressing systematic higher order user-system automation design.

In the 1940s, manned aircraft human engineering underwent a radical change in design philosophy with the work of human factors engineering pioneers such as Alphonse Chapanis, who applied engineering psychology to correct basic cockpit design flaws. The classic example of application of early engineering psychology analyses is the effort to mitigate a rash of bomber gear up crash landings. Human factors engineers redesigned landing gear handles to be shaped like wheels and reshaped flap handles shaped like flap handles for tactile discriminability by pilots who were visually focused on performing landing tasks. These were point design solutions, but were systematically applied through the cockpit and were eventually incorporated into the military standard system (Roscoe, 1995).

A systematic review in 2011 by the U.S. Air Force Scientific Advisory Board found a number of significant ergonomics and automation deficiencies in several current UAV Ground Control Systems (GCS), including poorly mechanized autopilot interfaces as well as "classic" pilot vehicle interface deficiencies. One example recalled the 1945 bomber crashes; the crash of one $4.5 million Predator UAV was directly caused by a pilot mistakenly choosing the "kill engine" switch instead of the adjacent landing gear switch (Morely, 2012). That a Predator pilot was even able to mistake (let alone be allowed to actuate in flight) the "kill engine" switch for the landing gear switch would seem to indicate the lack of a systems engineering analytical approach to user interface requirement definition.

Other studies have confirmed the apparent lack of a systematic design approach. A 2007 Air Force Research Lab study found that up to 80% of Predator mishaps alone involved human error, including poor documentation, crew coordination mistakes and training, and serious fundamental human factors design issues with GCSs. For example, it apparently took 22 key strokes to turn on the autopilot on early Predators; warning, caution and advisory messages were buried under layers of noncritical interfaces, resulting in situations where the pilot receives few if any alerting cues to emergencies. More than 400 US UAVs have crashed since 2001 (including midair collisions) and due to these causes, which contributed to lack of pilot awareness of or correct responses to weather, fuel status, data link strength, and high terrain (Craig, 2012).

Looking forward, UAV missions are expanding and multiplying into roles (such as Airborne Electronic Attack and Air to Air engagements) which stress rapidity of decision making in a complex shifting combat environment. Emergent warfighter UAV design goals are trending toward requirements for single user command and control of multiple heterogeneous UAV platforms with separate mission taskings, as well as requirements for cooperative control between a GCS and an off board user (such as a front line soldier or pilot). A Human Systems Integration (HSI) design approach limited to lower order point design switch and display issues or merely complying with military standard compliance audits does not address the systems engineering challenges from these needs. These new requirements present more challenging problems such as issues with single user task saturation and vigilance and how user system automation can augment a human user to prevent mishaps and enable mission success. This paper will summarize an approach to provide a framework for an adaptive, operator centric automation framework for future and retrofit naval UAV designs.

The approach recommended is two faceted; the first is the need for individual, adaptive automated policy managers focused on specific mission tasks (especially those needing rapid calculation or constant monitoring). The second is the need for an overarching Executive manager to provide rapid arbitration and coordination during time-critical combat operations. The end goal is to return the user to the role of tactician, automating first order calculations (e.g. fuel, terrain avoidance) but with a higher order automated process to ensure a coordinated response to human tactical direction.

Progress towards Adaptive GCS Automation

Two historically prevalent approaches to UAV GCS design have been followed. One approach focused on provision of controls duplicating manned aircraft interfaces (e.g. the approach used from 1940's designs up through the MQ-1 Predator). The other provided direction of the vehicle through graphical map cues (evolving from hard copy strip charts to present day point and click graphical interfaces to direct flight to a point). Either approach offers the potential for the uncoordinated application of multiple instances of automation (e.g., an automated route planner will disagree with an automated terrain avoidance system – and will present disharmonious results to the user from separate displays). The risk, then, is that attempts to add automation to GCS designs (within either design paradigm) will impose additional new tasks and roles on the user to monitor multiple automated systems across multiple vehicles, thus increasing the risk of significant error. For example, trending UAS human errors have been noted to include (Johnson, 2007):

1. Loss of operator situational awareness (SA) of airspace and traffic.
2. Operator-induced Air Vehicle loss of fuel/loss of link, leading to vehicle loss.
3. Loss of operator SA of altitude, airspeed, vehicle status, and clearance to terrain.

Operator Role Theory (Folds, 1995) posits a spectrum of human and automation shared roles in systems control (see Figure 1, below). Where no automation is present, the user is acting in a "Direct Performer" situation. With automation present but with the user performing information synthesis and control of the system, the system is running in a "Manual Control" region. With predominantly automated control loop processes and user monitoring and adjustment, the system is in a "Supervisory Controller" region, and finally, in the "Executive Controller" region of automation, the human is not in the control loop at all, save for a start/stop function

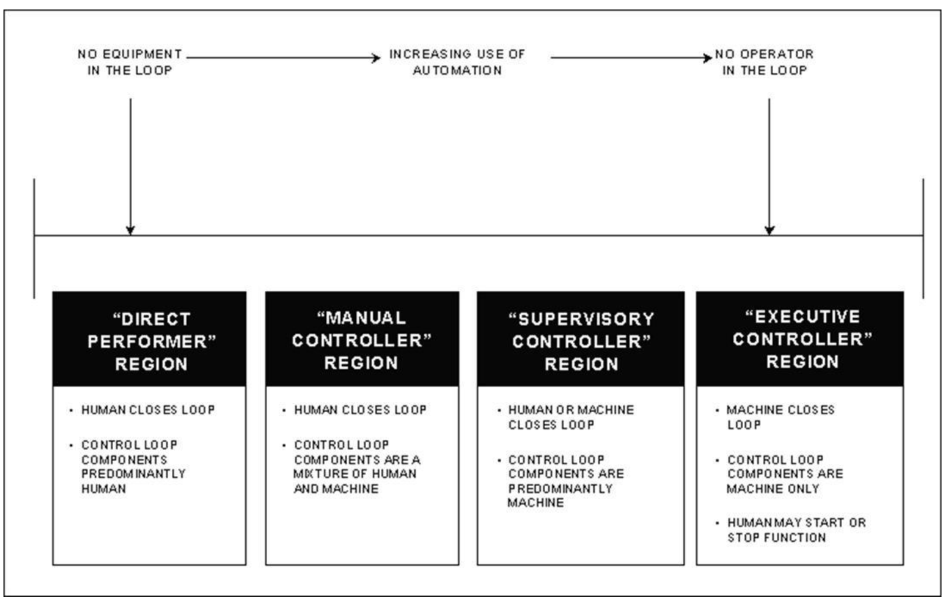


Figure 1 Continuum of Operator and Automation Roles

The classic example of Executive level control is cell phone tower switching, which takes place at an Executive level (human interaction with this automated element is generally limited to seeing the signal strength bar on their phone). Currently, GCS designs incorporate a mix of automation from in various automation control regions, with varying success. The move towards multiple UAV GCS control will only exacerbate existing problems without adoption of a new element of automation to aid the user in automation management. Newer GCS designs are undertaking to provide adaptive automaton which provides tools for automatic flight routing, route deconfliction, and calculation of weapons engagement zones, SAM shot avoidance cues, and so forth based on integrated "at a glance" presentations (Johnson, 2007).

Mission Growth Forces an Approach with an Executive

As with the cell phone example, the Executive automation role is well proven in manned combat aircraft. Airborne electronic warfare jammers react immediately, for example, to defeat incoming enemy missiles by automatically applying radar jamming techniques. The system executes the protective action because the pilot doesn't have the reaction time (let alone the surplus workload capacity) to manually employ the equipment. Particularly for pilots who may be tired or inattentive, the sudden leap in activation from being a system monitor to dealing with an emergency can lead to lapses and errors. Thus, a higher level requirement exists for a controller capability which looks across automated subsystems for multiple UAVs, accessing data to predictively analyze trends and threats in a coordinated manner, without the potential for boredom or fatigue.

To match the required UAV UI demands, a comprehensive shift to a system of systems engineering approach to adaptive automation – across applications – is recommended. With multiple UAVs aloft in a highly dynamic battlespace (where UAVs may be used not just for long counterinsurgency patrols, but as targeting and/or weapons platforms in air to air combat), automation needs to be considered as more than a family of decision making tools, but as an integrated system itself. A human systems engineering approach which applies operator role theory (Folds, 1995) to define a UAV system of systems will effect an order of magnitude improvement in combat efficiency and effectiveness. The approach proposed specifically advances the definition of multi-mission adaptive automation to address the impacts of (1) highly complex mission tasking (2) too many vehicles to manually monitor at once and (3) short engagement timelines.

Elements of the Integrated Solution: Policy Managers and an Executive

Automation should relieve humans from boring housekeeping tasks, prevent their inattention or raw information saturation from causing loss of vehicle and mission failure conditions, and allow humans to do that which they do best (make tactical judgments). Specific automation "policy" managers should be considered for collaborative integration in a fused GCS implementation. Many automation elements have already been fielded as separate tools in manned and unmanned aircraft. However, to implement enough of them, over multiple UAVs, with newly emergent requirements for tactical engagement accuracies and timelines, additional Executive level automation is needed.

Each policy manager has a role to play as individual automated elements under an Executive, which would supplement the monitoring and arbitration task set currently allocated to the human. An Executive would be able to quantitatively perform that role across multiple UAVs, and would be able to meet far tighter accuracy and speed requirements. The Executive must be able to resolve a best fit solution for the active UAV platforms given preplanned mission constraints by performing multivariate, weighted, arbitrations across the lines of the subordinate policy managers. Example potential individual automation elements include Auto Ground Collision Avoidance System (AGCAS) Protection, Auto Traffic Collision Avoidance Protection, Auto Envelope Protection, Auto Airspace Protection, Auto Datalink Protection and Auto Signature Protection (among a host of other functions). It is useful to examine how two (a Datalink Manager and a Signature Manager) interact.

The Datalink Manager monitors established UAV to GCS, UAV to UAV, and UAV to manned mission partner datalink latency and strength against calculated range limits. It then provides a real time calculated assessment of the probability of loss of link(s) as well as quality factors. (Link latency, as an example quality factor, will impact the ability of the vehicle to perform time critical tactical tasks). Based on this, as well as the availability of alternative links, this policy manager automatically shifts and configures data links In an integrated automation system, the Datalink policy manager will need arbitration with the Signature and other managers to regain signal while ensuring the "lost" AV avoids maneuvers which compromise detection or survivability.

The Auto Signature Protection manager provides real time computed signature management to ensure that the UAV remains either undetected or unengageable by threat systems. Based on preplanned settings, the Signature policy manager would provide a spectrum of adaptive actions from advisories to cautions to warnings to auto heading/alt changes based on flight paths past the minimum allowable approach range toward threats. This automation manager would consider the use of terrain and range line of sight effects in making an aspect/course/altitude change input; the signature policy manager would (in the proposed integrated system) make inputs in favor of or against course changes (whether automated or manual) to ensure that requested courses would not inadvertently generate a fatal shot solution from an enemy missile site. Yet obviously, some third party agent is necessary to perform the rapid, multivariate comparison and arbitration tasks between all these agents, if a human cannot possibly interpolate and calculate quickly enough.

The Need for an Executive Agent

While separately, individual automation elements may be useful, the emergence of far more complex combat requirements requires users to interpolate and integrate the many information variables (such as signature, envelope, and fuel as well as datalinks and weapons control) for multiple controlled UAVs, during multiple weapon engagements with hostile moving targets. USAF Colonel John Boyd, father of the Observe, Orient, Decide, and Act (OODA) loop model of tactical engagement, noted that the key to combat aircraft survival and autonomy is the ability to adapt to change rapidly and to capitalize on calculated advantages faster than one's opponent – to "get within the enemy's OODA loop" (Boyd, 1976). With such a varied range of automated policy managers, conflict arbitration via human or automated means is necessary. Because a single human cannot meet the analytical and computational requirement to comparatively perform the cross application functions for multiple UAVs within a tactically significant timeline for multiple controlled vehicles, the GCS must be equipped with an overarching Executive Agent.

Such an Executive would constantly monitor the individual policy managers for each UAV and adjudicate recommended automated actions based on preplanned algorithmic responses for most cases; the Executive would both provide more urgent advisories (would inform, then prompt, then warn) to cue user intervention based on the severity of impact of the problem within a tactically significant timeline (e.g. the UAV is headed for a threat, turn the UAV to avoid detection, and finally maneuver the UAV to defeat an engagement). In Boyd's terms, the control loop authority (human or Executive) must perform general-to-specific reasoning - deduction, analysis, and differentiation, while also performing specific-to general reasoning related to induction, synthesis, and integration tasks (Boyd, 1976).

In most cases, the Executive would employ hierarchical weightings to arbitrate between conflicting policy managers to prioritize actions emphasizing one mission aspect over another (such as a prioritizing lack of UAV detection over choosing the most fuel-efficient return route). In all cases, Executive arbitration of the policy managers would follow mission constraint settings selected during mission planning by the user (even if only for default settings) and consent for key tasks (e.g. weapons free status within approved engagement constraints) would necessarily be required.

Conclusion

By equipping proposed future multiple combat UAV controlling systems with agile, Executive level controllers which can rapidly perform multivariate, weighted, arbitrations, time critical combat tasks be met within the multiple UAV control paradigm. Significant further mission task analysis and requirements decomposition is necessary to ensure that further platform specific top level and detailed level design requirements are properly decomposed and allocated.

Works Cited

Boyd, John R. "Destruction and Creation". (3 September 1976).U.S. Army Command and General Staff College.

Folds, Dennis, and Mitta, Deborah. "Using Operator Role Theory to Guide Function Allocation in System Development", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 1 October 1995.

Johnson, R, et al. "Testing Adaptive Levels of Automation (ALOA) for UAV Supervisory Control" (March 2007). AFRL-HE-WP-TR-2007-0068. OR Concepts Applied (ORCA) for Air Force Research Laboratory, Human Effectiveness Directorate, Wright Patterson AFB OH 45433.

Michelson, Stuart. "A survey of the human-centered approach to micro air vehicles". Chapter 90, Springer Handbook of Unmanned Aerial Vehicles 2013.

http://www.springerreference.com/docs/navigation.do?m=Handbook+of+Unmanned+Aerial+Vehicles+(Engineering)-book256

Morely, Jefferson. "Boredom, terror, deadly mistakes: Secrets of the new drone war". Salon.com, 3 April 2012.

http://www.salon.com/2012/04/03/boredom_terror_deadly_mistakes_secrets_of_the_new_drone_war/

Roscoe, Stanley. "The Adolescence of Engineering Psychology", Volume 1, 1997, Human Factors History Monograph Series, Steven M. Casey, Editor, the Human Factors and Ergonomics Society, Santa Monica CA.

Whitlock, Craig. “Drone crashes mount at civilian airports”. Washington Post, 30 November 2012.
http://www.washingtonpost.com/world/national-security/drone-crashes-mount-at-civilian-airports-overseas/2012/11/30/e75a13e4-3a39-11e2-83f9-fb7ac9b29fad_story.html

Always a Step Ahead
ARDEC
ARMAMENTS

Enhancing Future Soldier Systems through the Use of the Systems Modeling Language to Incorporate Human Aspects into the Soldier as a System Definition

Presenter: Sean F. Pham
Shauna M. Dorsey, Frank B. Torres, Dana E. Perriello

NDIA Systems Engineering Conference, 25 October 2017

UNPARALLELED
COMMITMENT
& SOLUTIONS
Act like someone's life depends on what we do.

U.S. ARMY
U.S. ARMY RDECOM
U.S. ARMY ARMAMENT RESEARCH, DEVELOPMENT & ENGINEERING CENTER
US ARMY NATICK SOLDIER RD&E CENTER

Soldier as a System

Problem: The U.S. Army has historically focused on the development and optimization of Soldier **equipment**, leading to integration challenges between Soldiers and their equipment.

Best:

- Unmanned aerial vehicles
- Operational rations
- Organization/leadership
- Quality of life standards, etc.

It's not just about Soldier equipment. We must also understand and predict the performance of the ***full system***, inclusive of the Soldier, his/her equipment, and the tasks he/she must perform.

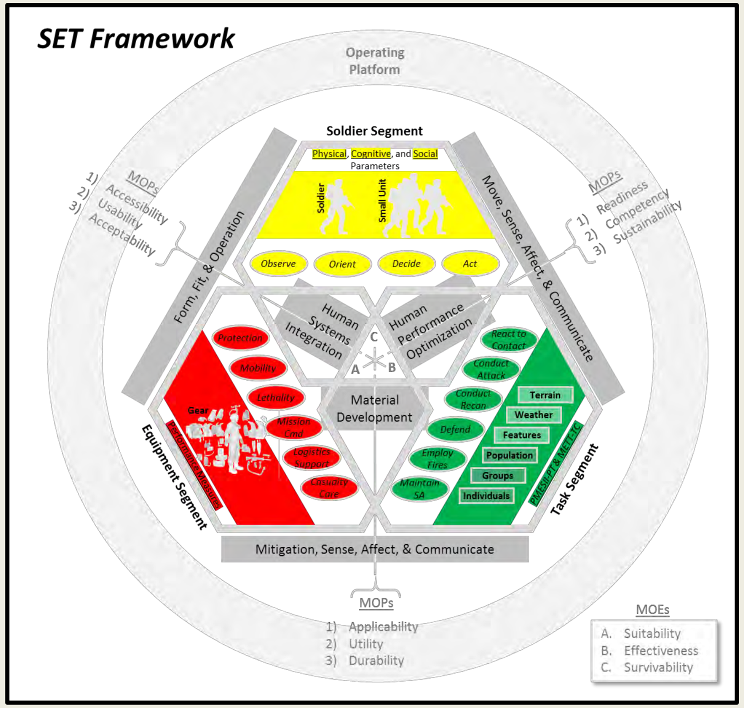
Objectives: Create a principle-based Soldier architecture and framework to enable a **system level tradeoff analysis** of the Soldier as a System (SaaS) domain.

- Create the **foundation for design parameters** for the next generation of Soldier systems and subsystems, which considers the complete **Soldier as a System** with the full complement of equipment, the human performance capabilities, and the mission tasks.

Anticipated Outcomes:

- Increased efficiencies and optimized performance of the Soldier as a System.
- Enterprise approach across Soldier-Small Unit Science and Technology (S&T) efforts, combat developers, and acquisition communities.

Purpose: Utilize Systems Engineering tools and processes to allow stakeholders across the Soldier Enterprise to manage the overwhelming complexity of the Soldier as a System domain.

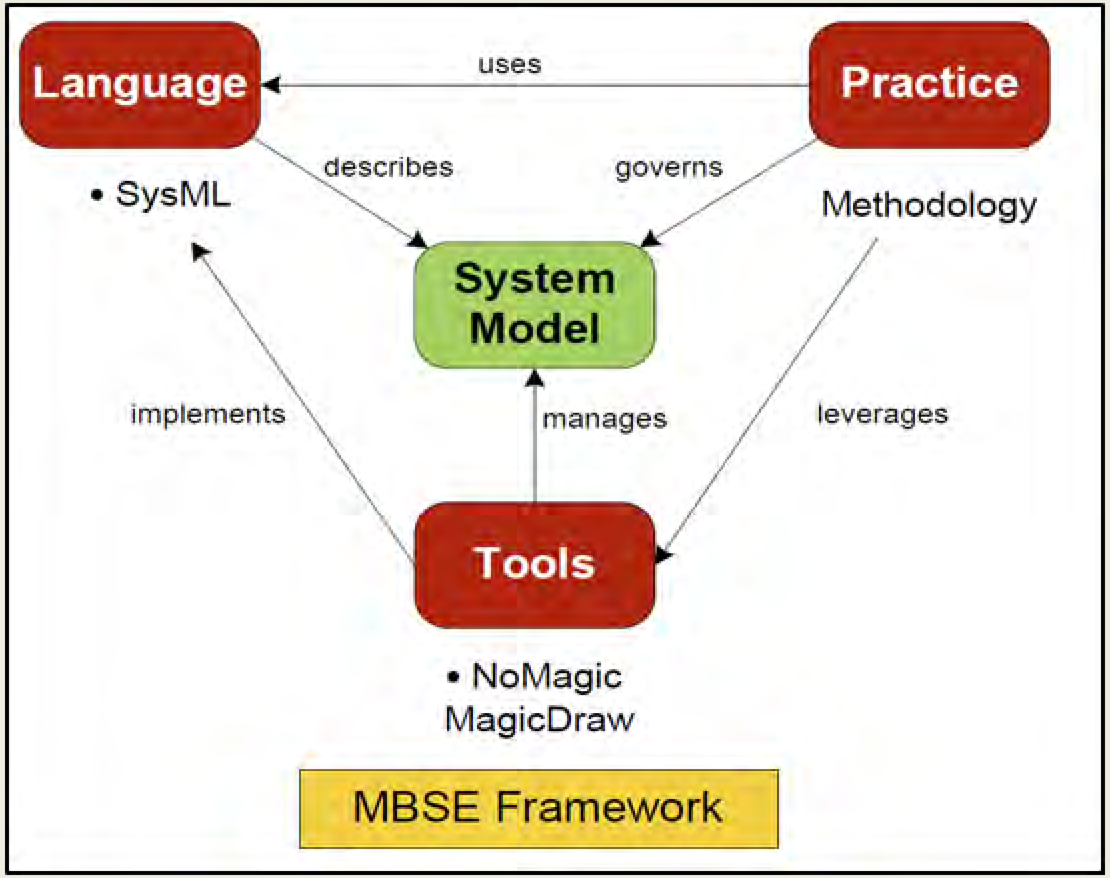


Soldier System Engineering Architecture (SSEA) is integrating these tools and processes for the Soldier Enterprise.

Model Based SE to Define SaaS Domain

Model Based Systems Engineering (MBSE): A Systems Engineering practice that uses **models** as the primary means of information exchange between engineers, rather than document-based.

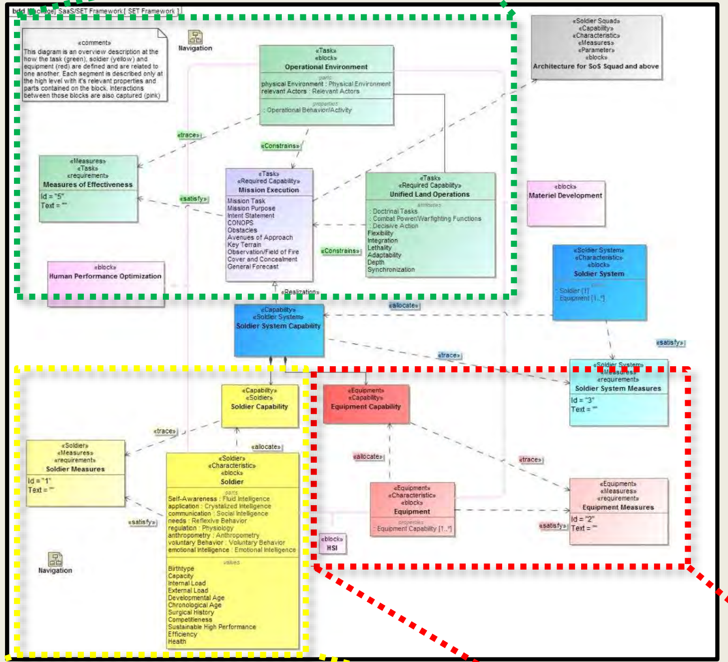
- MBSE allows for:
  - Graphically rich architectural product development of complex systems.
  - Relationship visualizations.
  - Interactive traceability handling.
  - Commonality of data and information throughout the project and across related projects.
  - Movement from document centric to model centric.



MBSE provides graphical views of SE products to inform SSEA trade analysis.

Soldier as a System Models

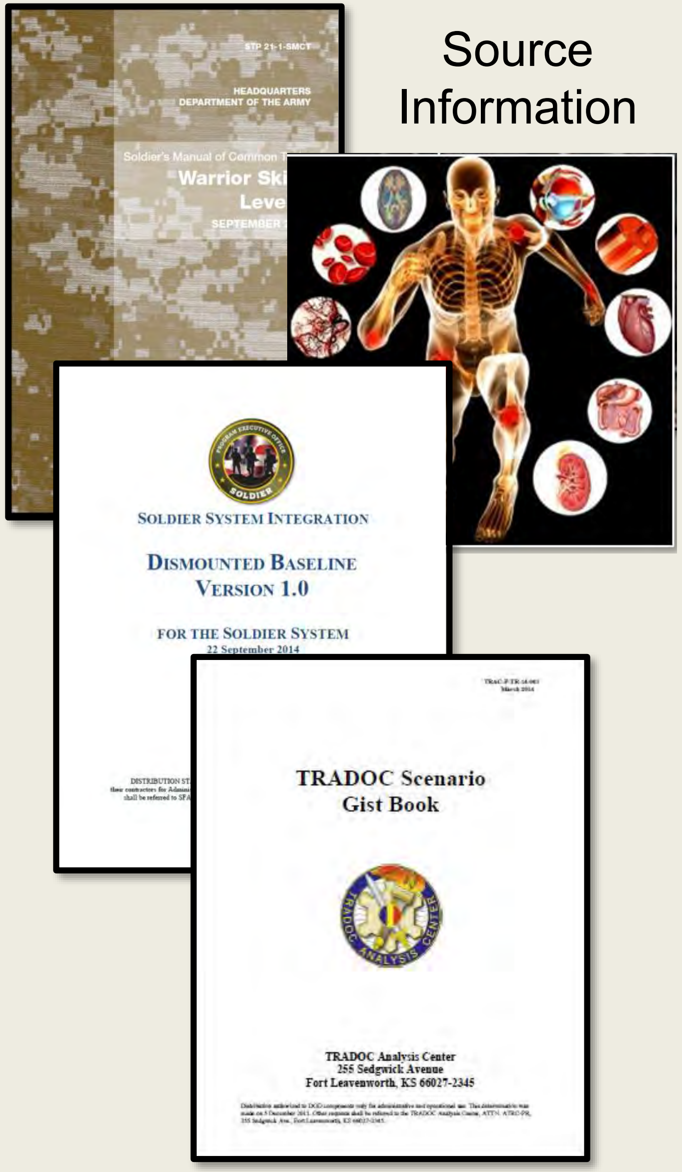
- The **System Model**:
  - **Characterizes** the Soldier as a System (SaaS) **domain** in terms of the human dimension, materiel solutions, and operational environment (i.e., the Soldier, Equipment, Task [SET] framework).
  - Formalizes the **definition** of the **SaaS** domain.
    - → Elements of the Soldier, Equipment, and Task, along with their interactions and interrelationships.
- **System Modeling Language (SysML)**:
  - **Captures the system model** and **defines the boundaries** of the system space.
    - → Enables decomposition of the SaaS domain and establishes a common vocabulary.
  - Provides a **common underpinning for SSEA**, allowing **stakeholders** to further **understand** their piece of the SaaS domain and its impact points over the full system space.



SysML SaaS Model Value Proposition

1. Comprehensive Reference Model
   - Provides a centralized focal point to **understand the elements** and **relationships** within the Soldier as a System (SaaS) domain.
     - Enables SSEA stakeholders/users to know where their products, decisions, and solutions fit in the domain and what they impact or what impacts them.
2. Standardized Soldier as a System Documentation
   - **Common language** to translate between technical, programmatic, and user communities.
     - Supports understanding and communication to facilitate informed decisions.
3. Starter Model for Model Based Systems Engineering (*future*)
   - Reduces rework, acclimates new team members, builds on lessons learned, and supports **sharing of knowledge** across communities.

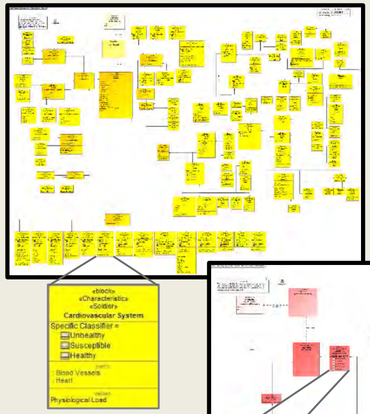
SOLDIER AS A SYSTEM MODELS



Source Information

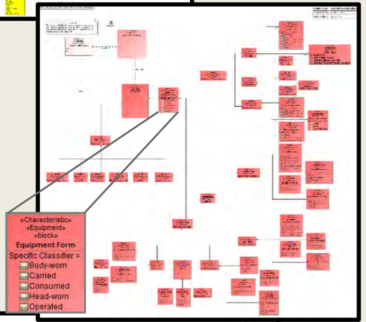
Soldier Model

Defines: *Anthropometric, Physiological, Behavioral, and Intelligence Elements*



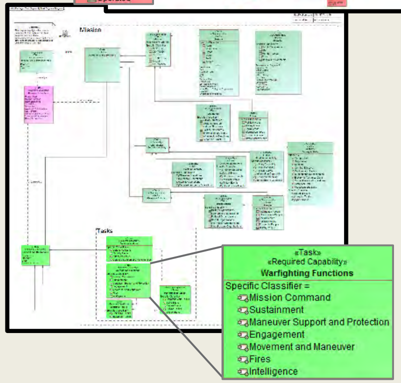
Equipment Model

Defines: *Structural and Behavioral Elements*



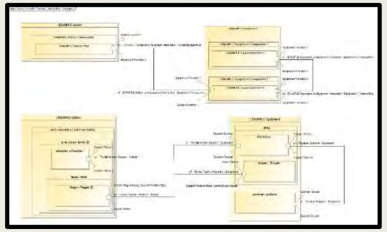
Task Model

Defines: *Physical Environment, Relevant Actors, Operational Behavior, and Unified Land Operations*



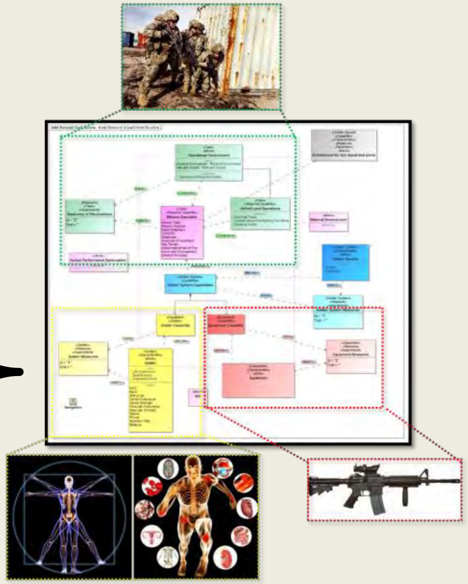
Interaction Model

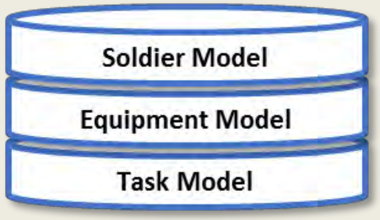
Defines: *Connections, Ports (structural), Interfaces (behavioral), and Flow (parametric)*



Integrate into the SaaS Reference Model

Fully-Integrated Reference Model



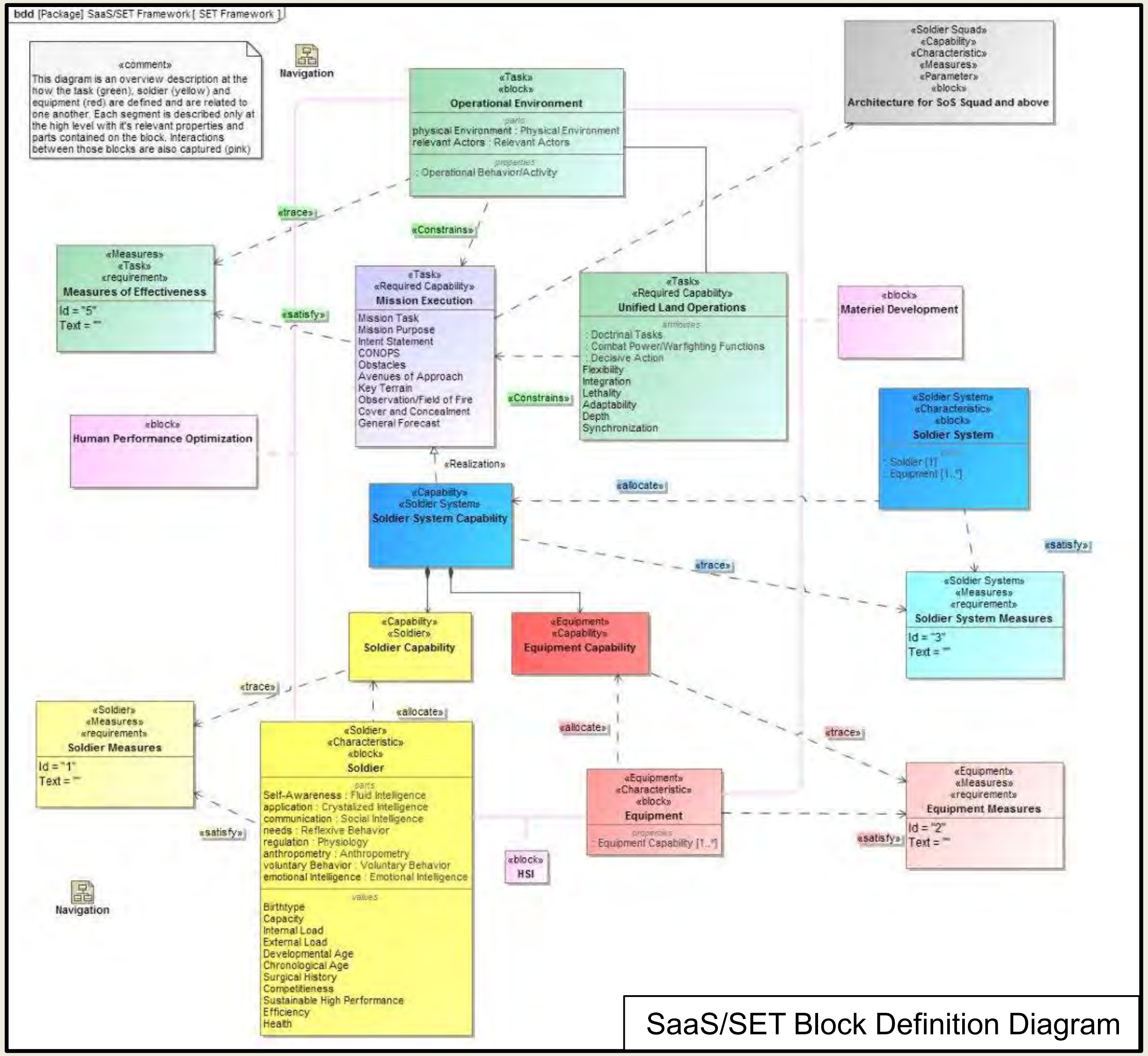


TeamWorks Server

U.S. ARMY RDECOM

SaaS Model Structure

- Purpose of the Model Structure:
  - Define the domain/system space (SaaS) and boundaries.
  - Serve as a central hub for the defined SaaS components and relationships.
    - Comprised of the soldier system within an operational context.
    - Displays any interrelationships between the primary model components.



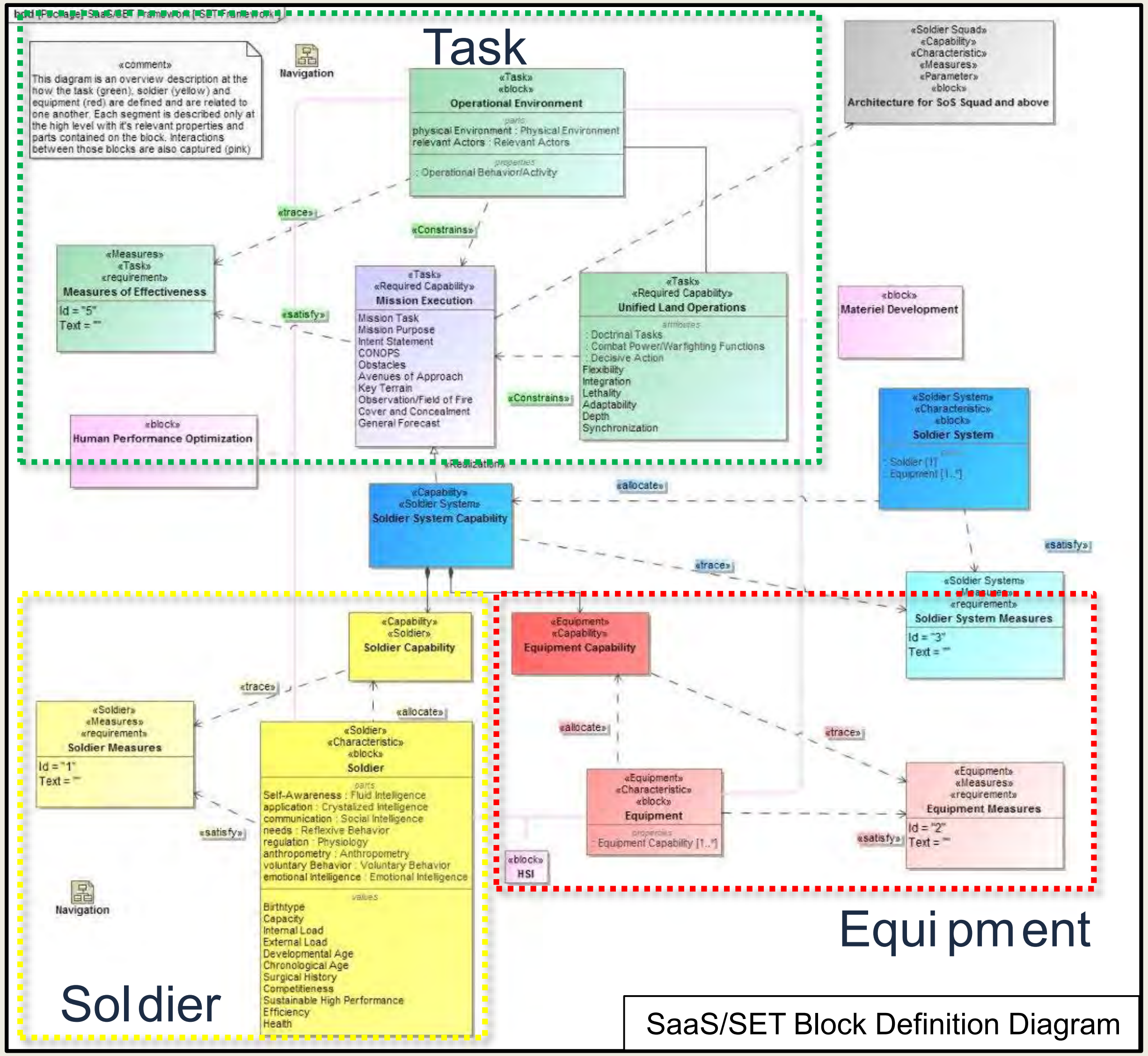
SaaS/SET Block Definition Diagram

U.S. ARMY RDECOM

SAAS MODEL STRUCTURE

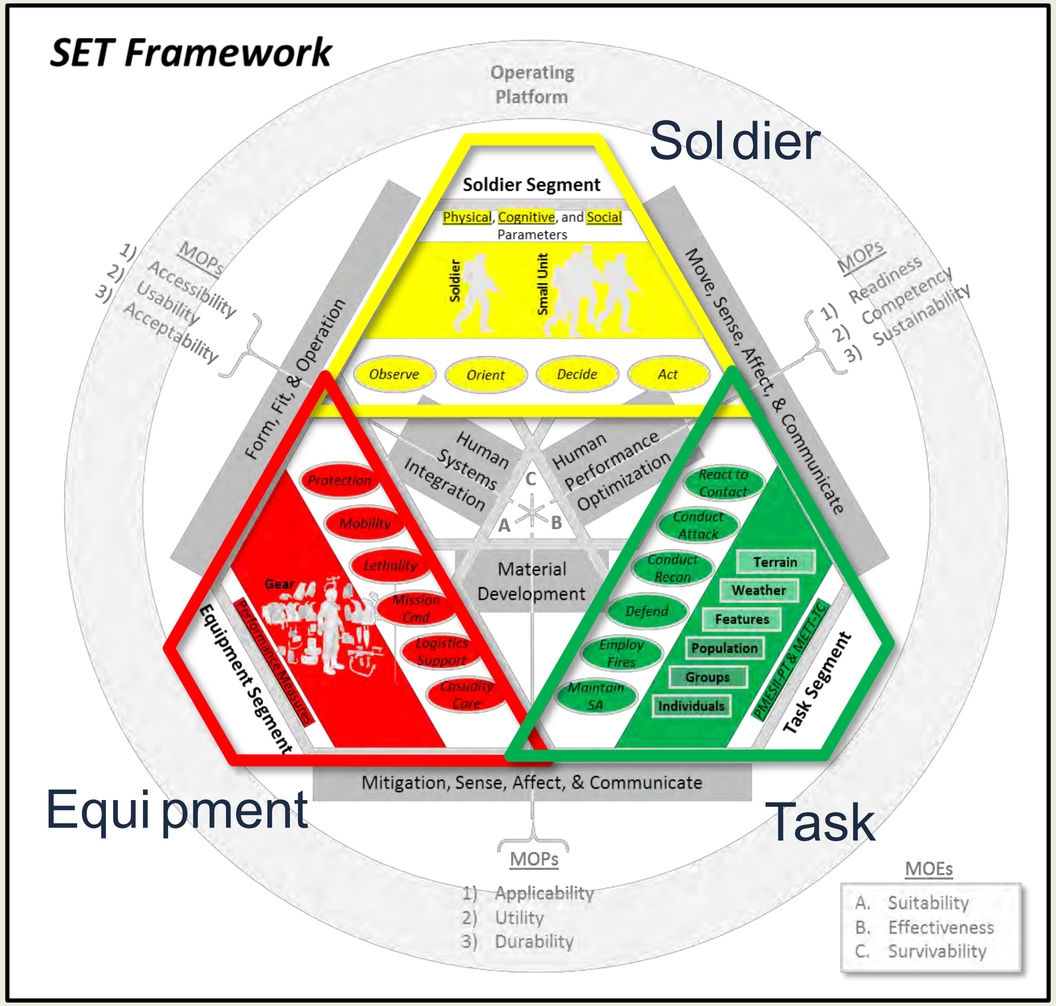
US ARMY NATICK SOLDIER RD&E CENTER ARDEC

Scenario: Soldier engaging an enemy target.



SOLDIER, EQUIPMENT, AND TASK SEGMENTS

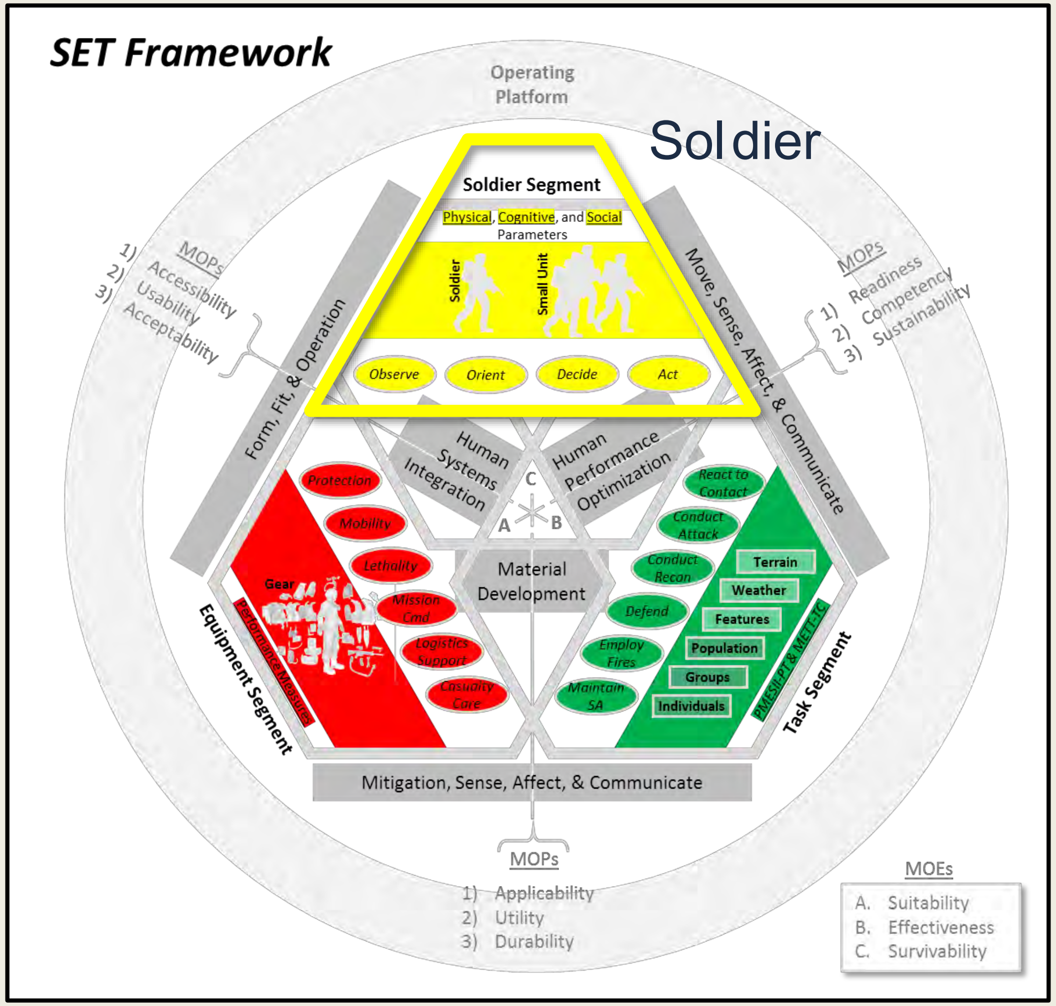
<u>Purpose</u>: Define the elements and relationships contained within Soldier, Equipment, and Task (SET) segments of the Soldier as a System (SaaS) model.



SOLDIER SEGMENT OF THE MODEL

Purpose: Define the elements and relationships within the human dimension, which includes cognitive, physical, emotional, and social parameters to further characterize the Soldier.

UNCLASSIFIED//DISTRIBUTION A



Soldier as a System: Soldier Segment of the Model

Four Main Components:

1. *Anthropometry – Physical structures of the human*
2. *Physiology – Internal regulatory systems of the human*
3. *Behavior – Voluntary (i.e., cognitively founded) and reflexive (i.e., "hard-wired") behaviors*
4. *Intelligence – Fluid (i.e., creativity and learning), crystalized (i.e., prior skills and knowledge), social, and emotional intelligence*

Component Classifiers:

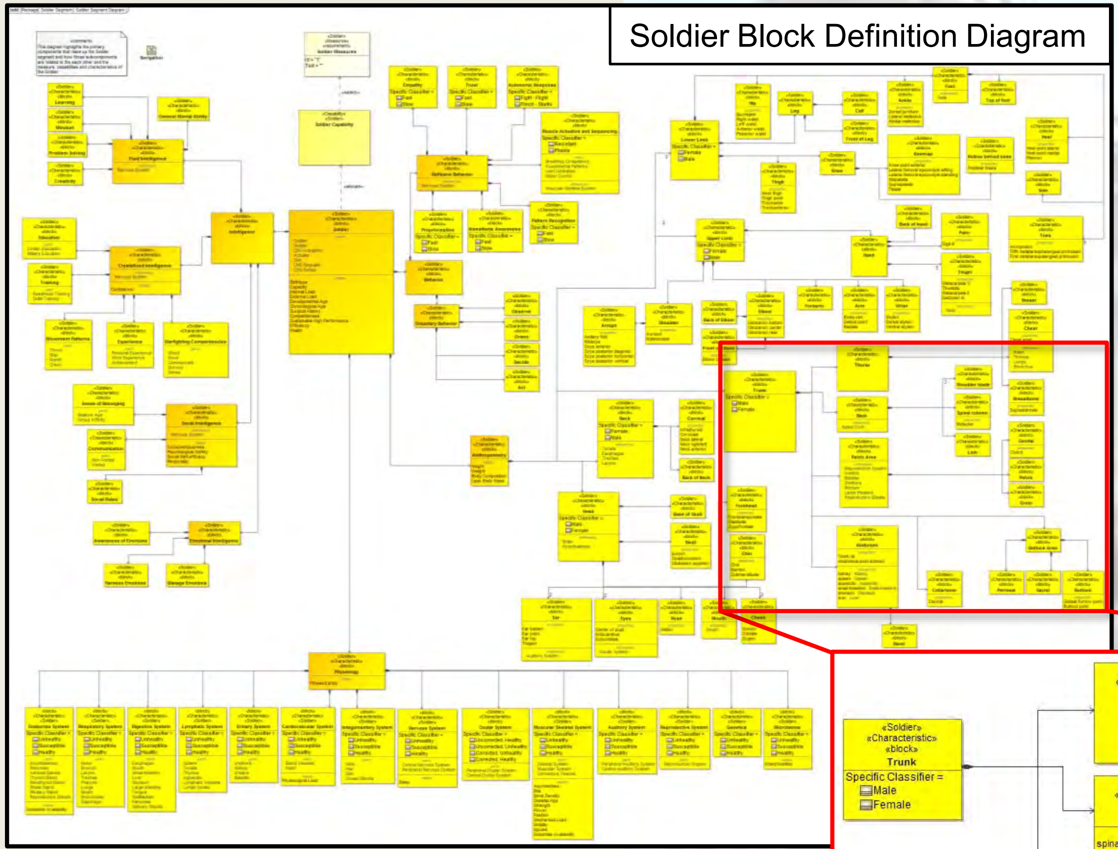
- *Size and shape*
- *Health state*
- *Response*
- *Creativity and learning*
- *Education and experiences*
- *Communication style*
- *Emotions*

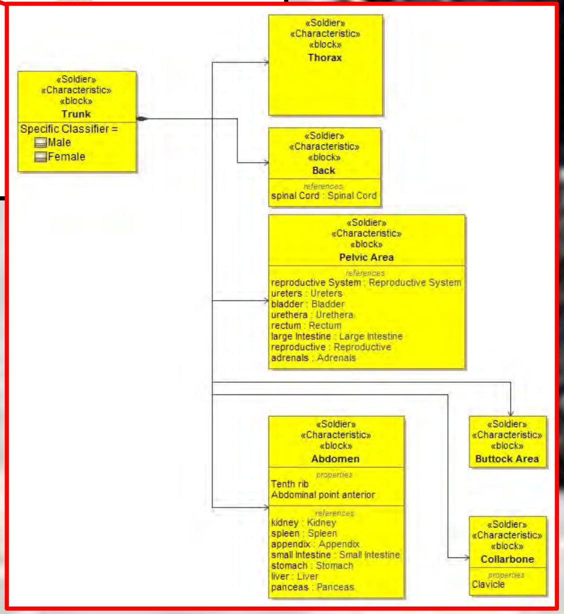
Ports / Interactions (examples):

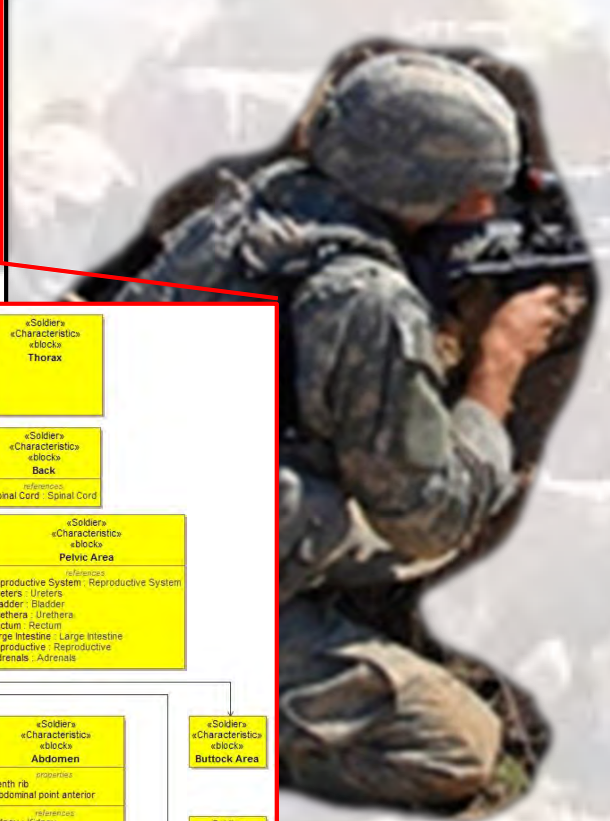
- *Shoulder / Support, Stabilize*
- *Hand / Support, Secure*
- *Finger / Control Magnitude, Actuate*
- *Eye / Signal Sense*
- *Body / Support, Secure, Attach*

SOLDIER AS A SYSTEM: SOLDIER SEGMENT OF THE MODEL

Soldier Block Definition Diagram







Soldier Anthropometrics

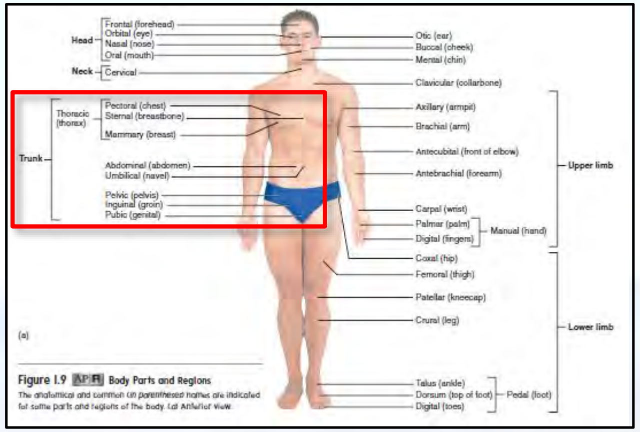


Figure 1.9 Body Parts and Regions
The anatomical and common (in parentheses) names are indicated for some parts and regions of the body. (a) Anterior view.

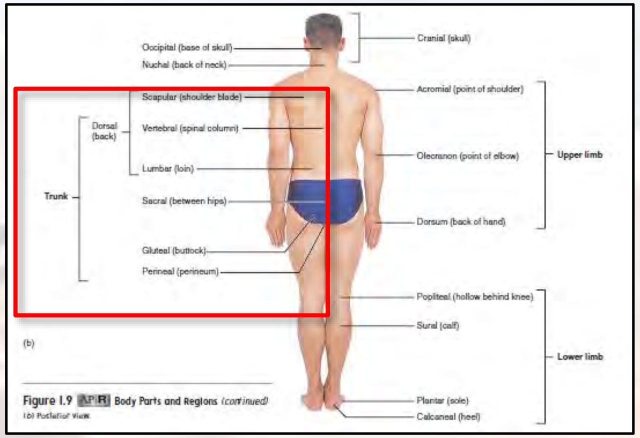


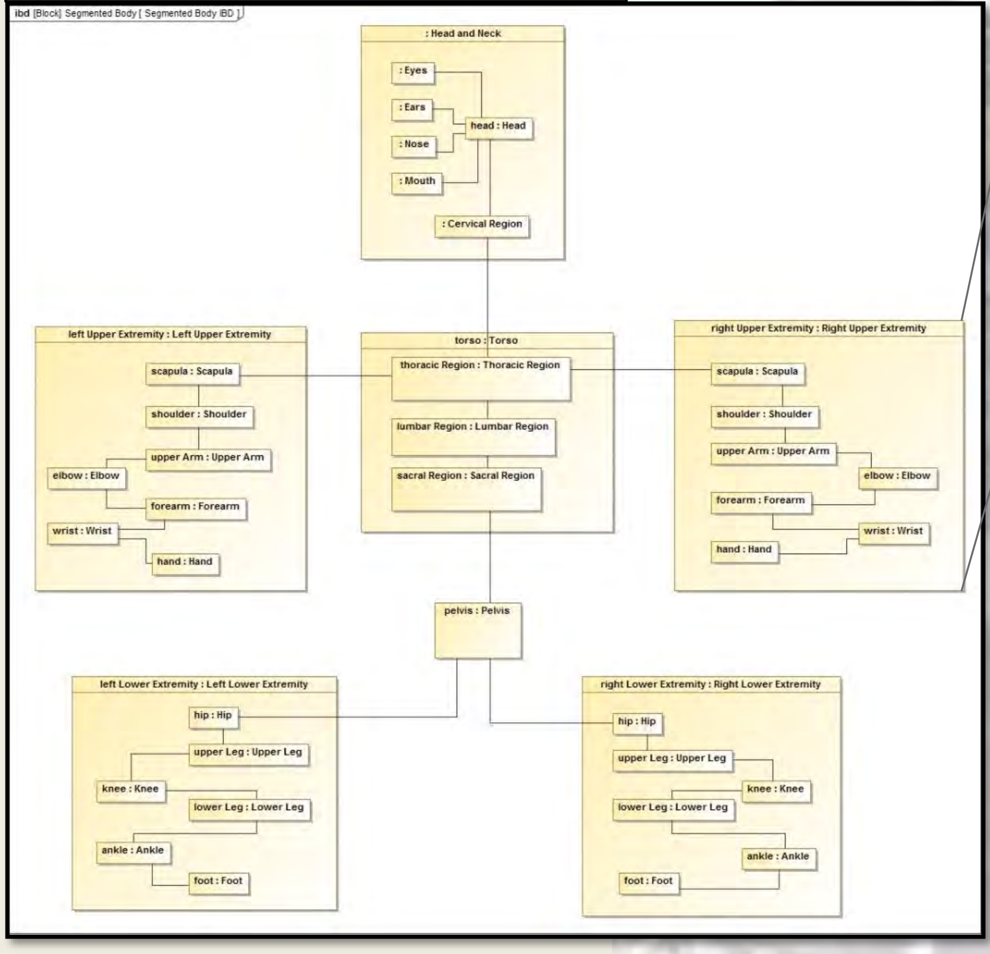
Figure 1.9 Body Parts and Regions (continued)
(b) Posterior view.

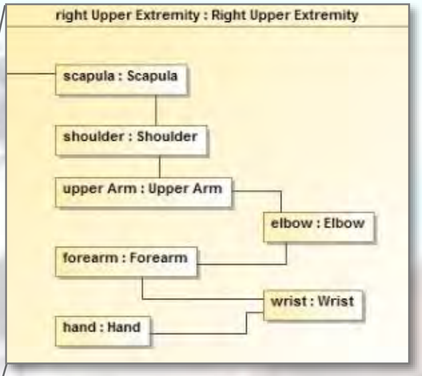
VanPutte CL, et al. Seeley's Essentials of Anatomy and Physiology, 9th Ed. 2014.

Gordon CG, et al. 2012 Anthropometric Survey of U.S. Army Personnel. NSRDEC. 2012.

SOLDIER AS A SYSTEM: SOLDIER SEGMENT OF THE MODEL

Segmented Body Internal Block Diagram



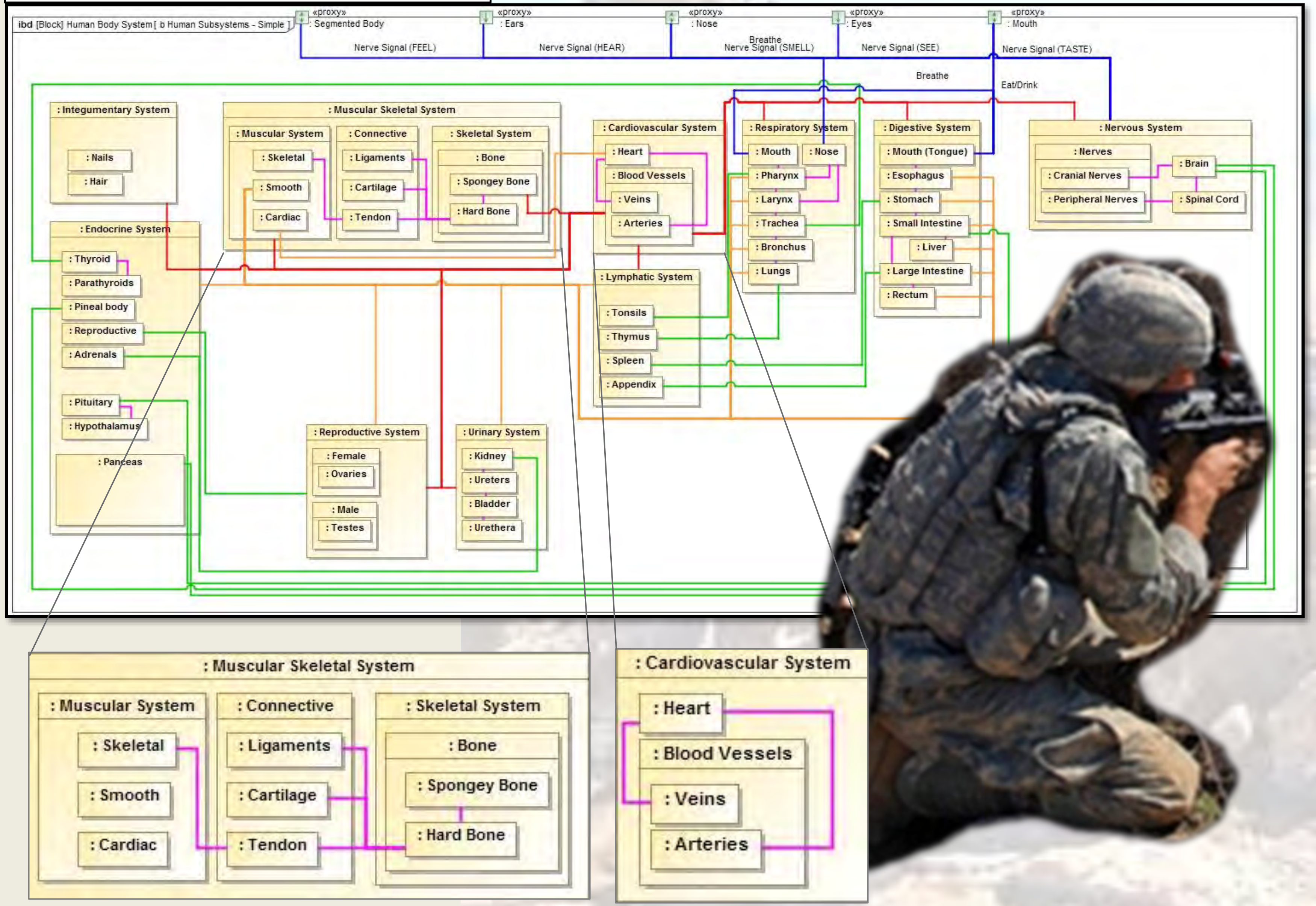


<u>Purpose</u>: Provide a decomposition of the physical anatomical regions of the human body and the connections between those regions of the human body.

<u>Application</u> (*future*): Show the "connections" between the anatomical body regions and allow for further parameterization and alignment to support future modeling capabilities.

Soldier as a System: Soldier Segment of the Model

Human Subsystem Internal Block Diagram

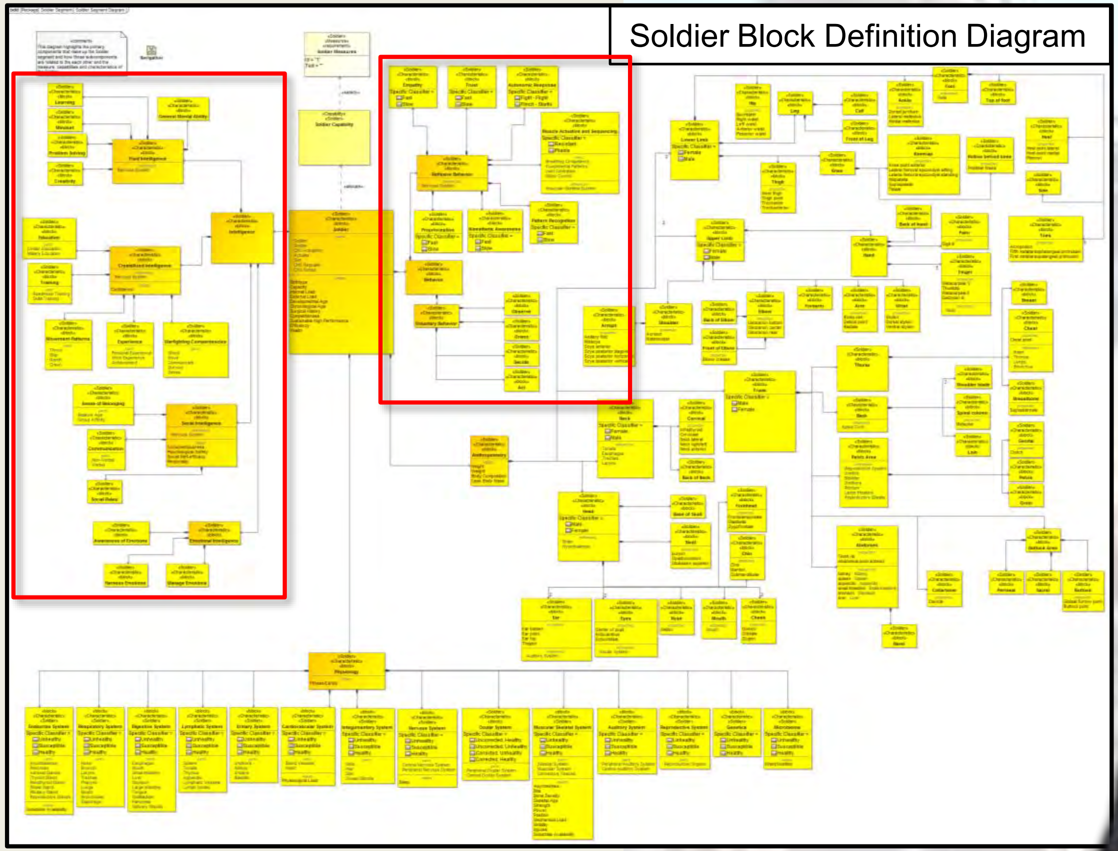


Purpose: Provide a breakdown of the internal regulatory subsystems within the human body and the corresponding anatomical connections between the systems.

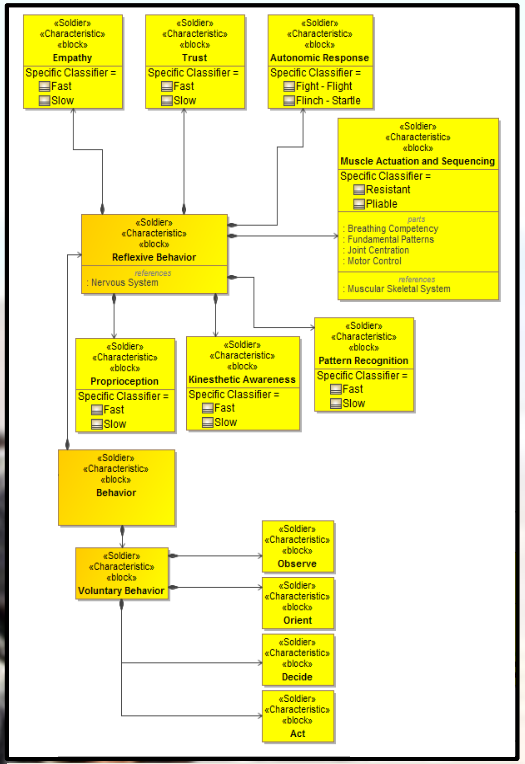
Application (*future*): Model the connections between the outside world and the internal regulatory systems of the human body.

Soldier as a System: Soldier Segment of the Model

Soldier Block Definition Diagram

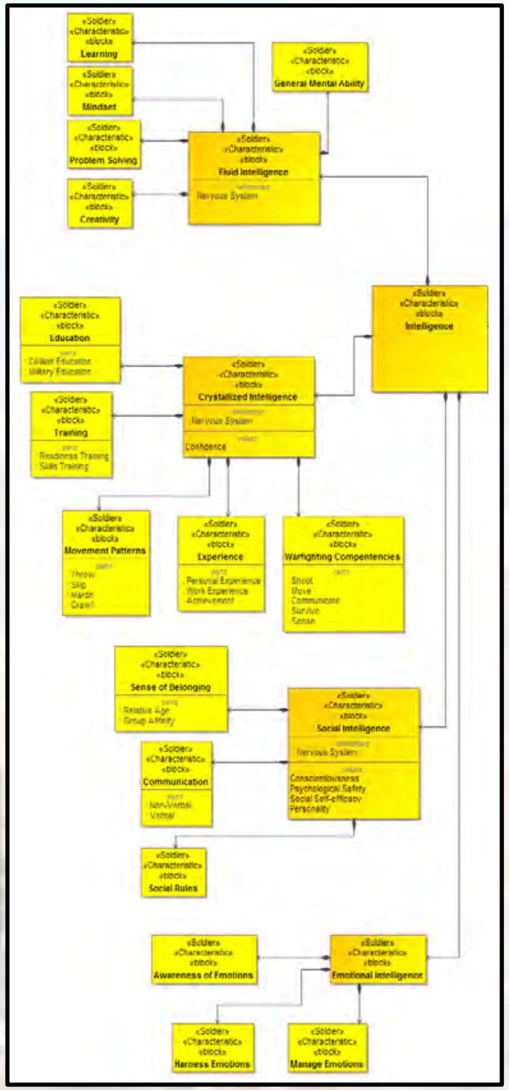


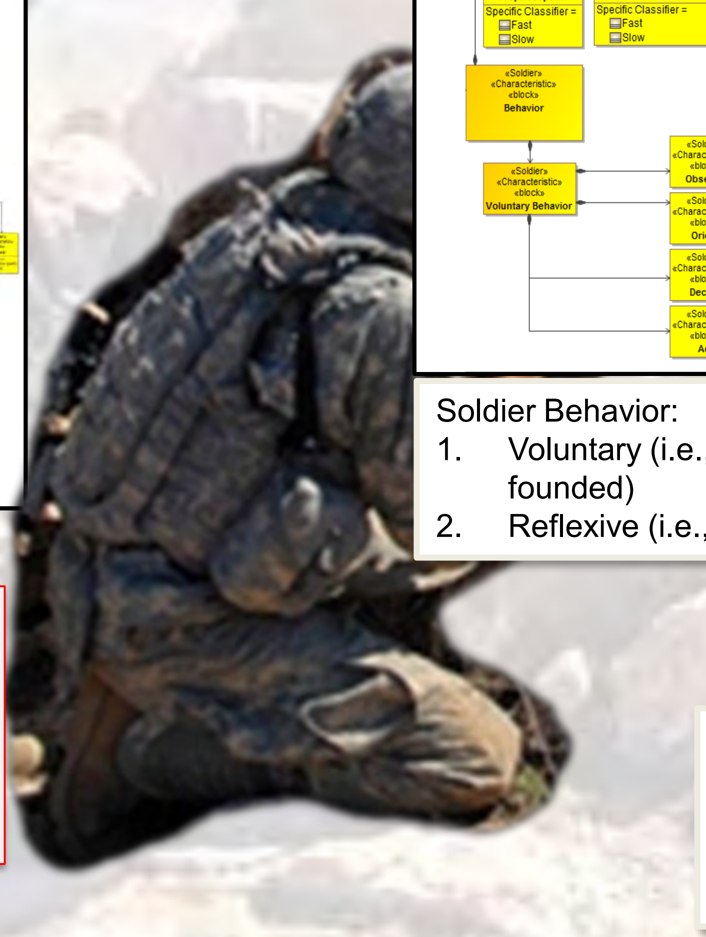
Soldier Behavior



Soldier Behavior:
1. Voluntary (i.e., cognitively founded)
2. Reflexive (i.e., “hard-wired”)

Soldier Intelligence



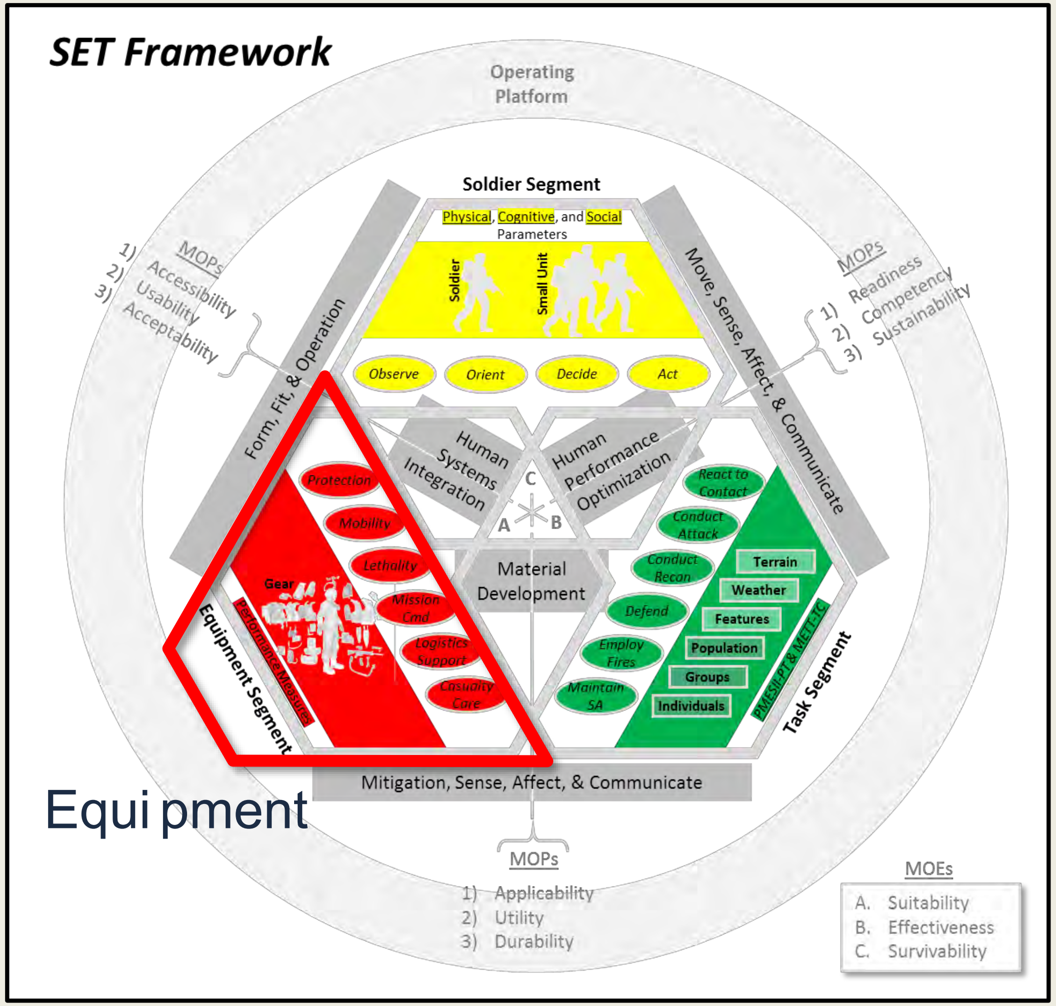


Explore the dynamics of Soldier behaviors and intelligence and how these components interact with the Equipment and operational Tasks.

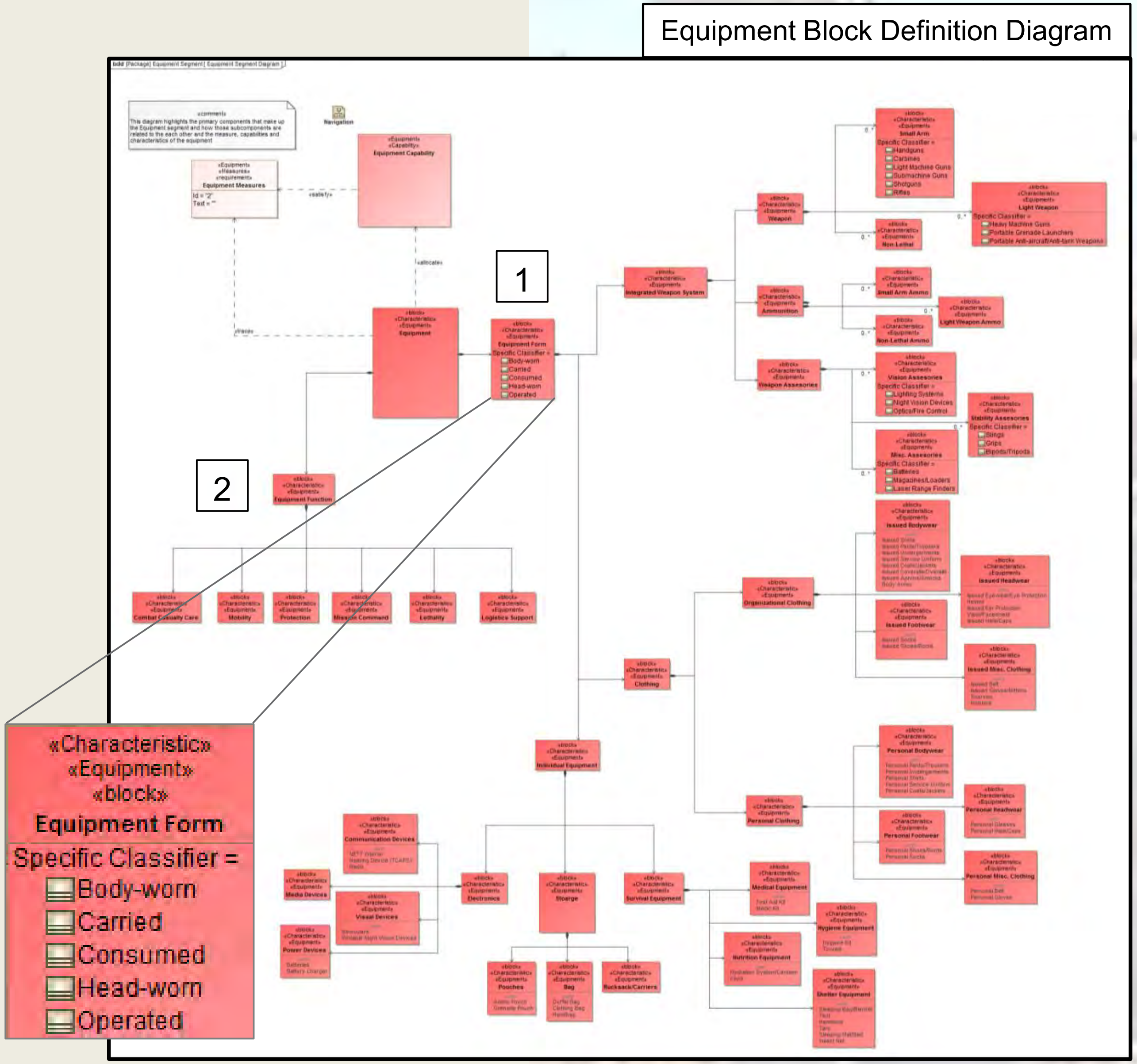
Soldier Intelligence:
1. Fluid (i.e., creativity and learning)
2. Crystalized (i.e., prior skills and knowledge)
3. Social
4. Emotional

Equipment Segment of the Model

Purpose: Define the elements and relationships within the material development dimension, including the type, form, and function of the equipment and how it relates back to its requirements.



Soldier as a System: Equipment Segment of the Model



Two Components:

- *Equipment Form – Integrated weapon system, clothing, and individual equipment*
- *Equipment Function – Combat casualty care, mobility, protection, mission command, lethality, logistics support*

Component Classifiers:

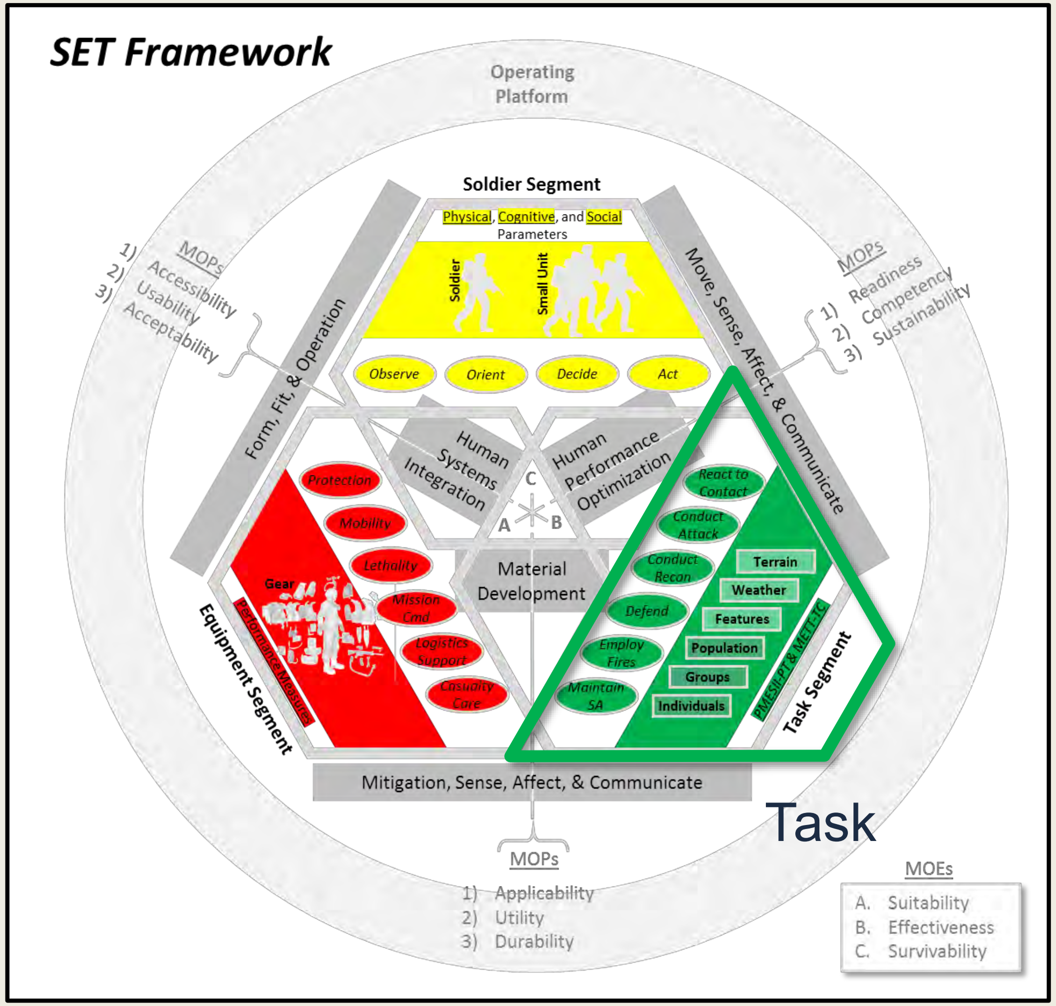
- *Forms of Equipment*
  - *Body-worn*
  - *Carried*
  - *Consumed*
  - *Head-worn*
  - *Operated*

Ports / Interactions (examples):

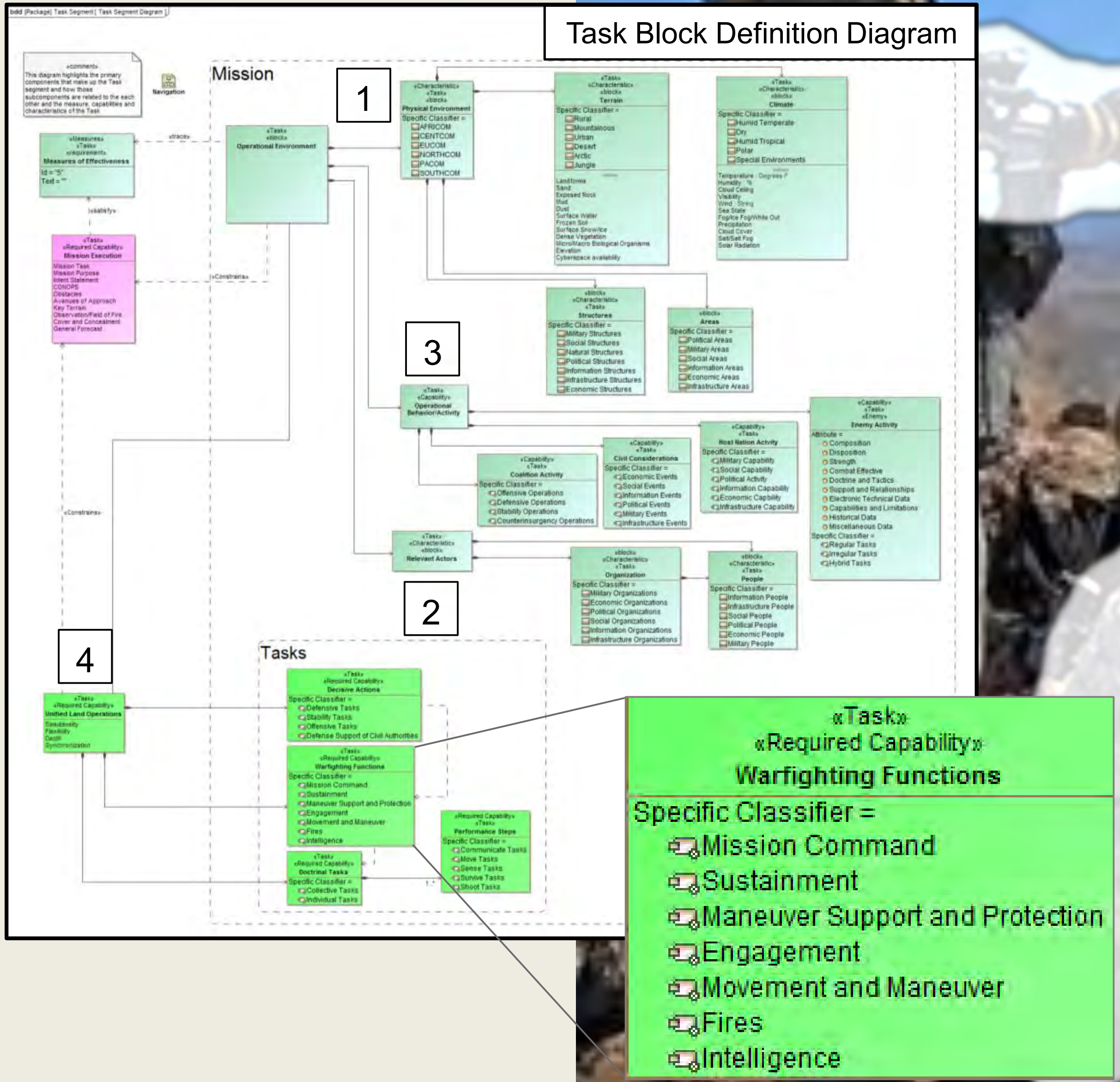
- *Buttstock / Support, Secure*
- *Improved Outer Tactical Vest / Support, Stop, Protect*
- *Rucksack / Provision, Store, Hold*
- *Close Combat Optic / Channel, Import, Allow*
- *Eye Protection / Control Magnitude, Regulate*

Task Segment of the Model

Purpose: Define the elements and relationships that the Soldier will encounter within a specific operational environment. This focuses primarily on doctrinal mission elements and parameters.



Soldier as a System: Task Segment of the Model



Four Components:

1. *Physical Environment – Terrain, climate, structures (man-made or natural), and regional areas*
2. *Relevant Actors – Organizations and people*
3. *Operational Behavior and Activity – Coalition, host nation, and enemy activities, along with civil considerations*
4. *Unified Land Operations – Characterizes decisive actions, warfighting functions, and doctrinal tasks*

Component Classifiers:

- *Types of:*
  - *Terrain and climate*
  - *Physical structures and areas*
  - *Groups and personnel*
  - *Operational variables (HAMO)*
  - *Operational activities*
  - *Threats and actions*
  - *Tasks and functions*

Soldier System Interaction Approach

Purpose: Standardize methods and elements to depict the relationships between the Soldier, Equipment, and Task segments of the SaaS model.

Interaction: Soldier Shoulder to Rifle Buttstock in an active "engagement" position.

Soldier Shoulder: Secured

Human Force
Surface for Physical Contact

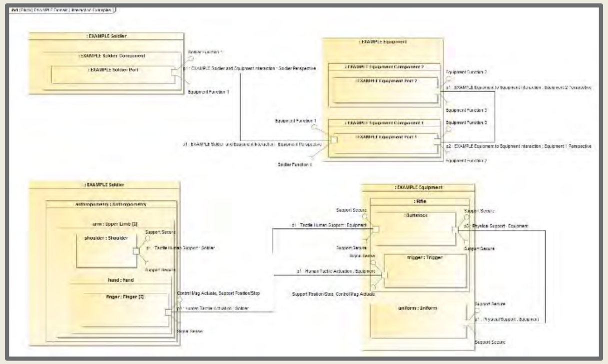
Rifle Buttstock: Stabilized

Mechanical Force
Surface for Physical Contact
Tactile Signal

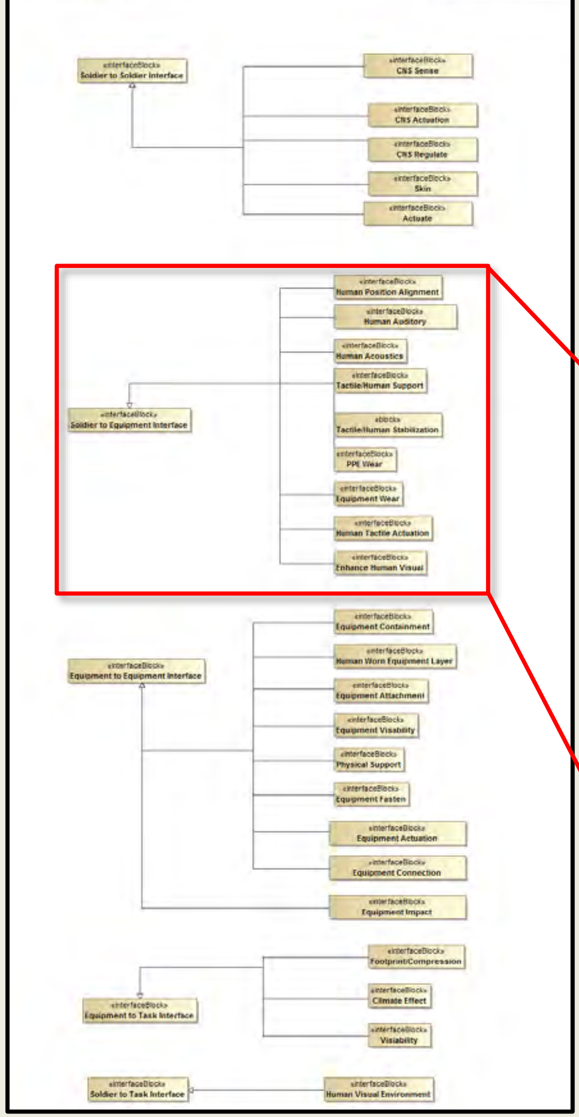
Otto K and Wood K. Product Design: Techniques in Reverse Engineering and New Product Development, 1st Ed. 2000.

SOLDIER SYSTEM INTERACTION APPROACH

Implementation of Relationships into SysML

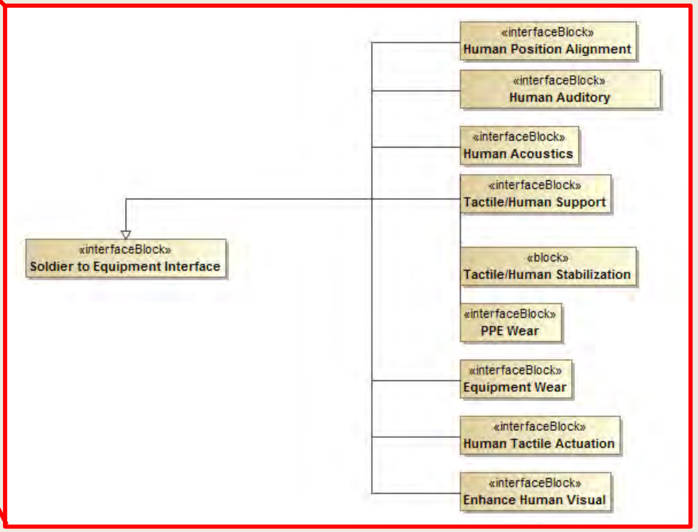


Interaction Library



Approach to Capture Relationships in SysML:

- Represented the interaction information in SysML as model elements.
- Created a library of common interactions which consisted of reusable relationships.
- Provided a reference of the details of the interaction mechanism that the database will leverage for their configuration building.



Describe a wide array of SET relationships using Interaction Library.

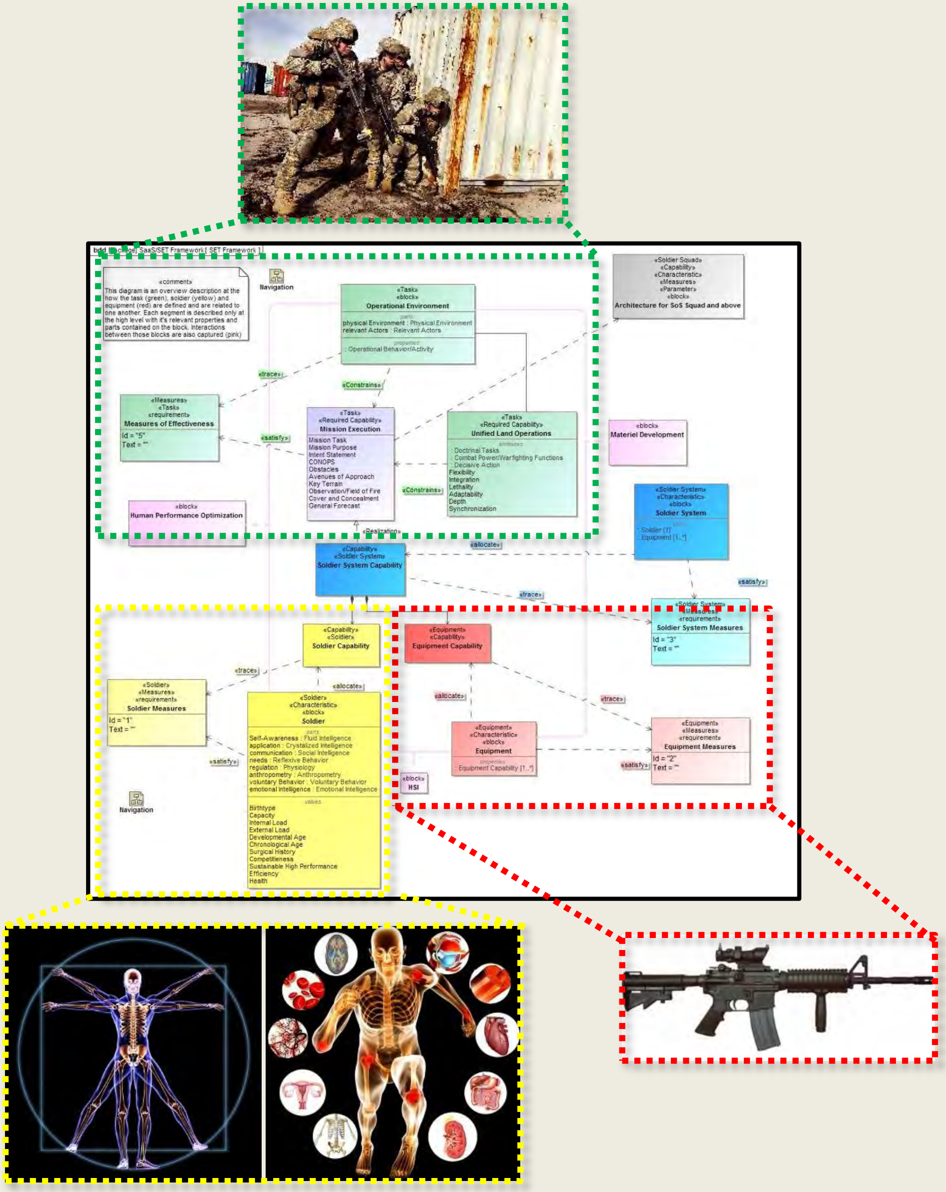
Otto K and Wood K. Product Design: Techniques in Reverse Engineering and New Product Development, 1st Ed. 2000.

U.S. ARMY RDECOM

CONCLUSIONS

US ARMY NATICK SOLDIER RD&E CENTER ARDEC

- A MBSE approach can be used to capture and display the meaningful content and relationships within a complex system of systems (i.e., the SaaS), which include elements related to the Soldier, equipment, and task capabilities.
- Human systems integration aspects are captured to further depict the relationships between the Soldier and their equipment in an operational context.
- SaaS SysML models can be used as a tool to improve decision making through a better understanding of Soldier-equipment interactions, leading to the optimization of future Soldier systems.



ACKNOWLEDGEMENTS

U.S. Army Armaments Research, Development, and Engineering Center (ARDEC):

- Shauna Dorsey
- Frank Torres
- Dana Perriello
- David Chau

U.S. Army Natick Soldier Research, Development, and Engineering Center (NSRDEC):

- David Krasnecky (STO Manager)
- Michael Curry (Draper)
- Axel Rodriguez
- Joseph Patterson
- Roger Schleper (Draper)
- John Turkovich (Draper)

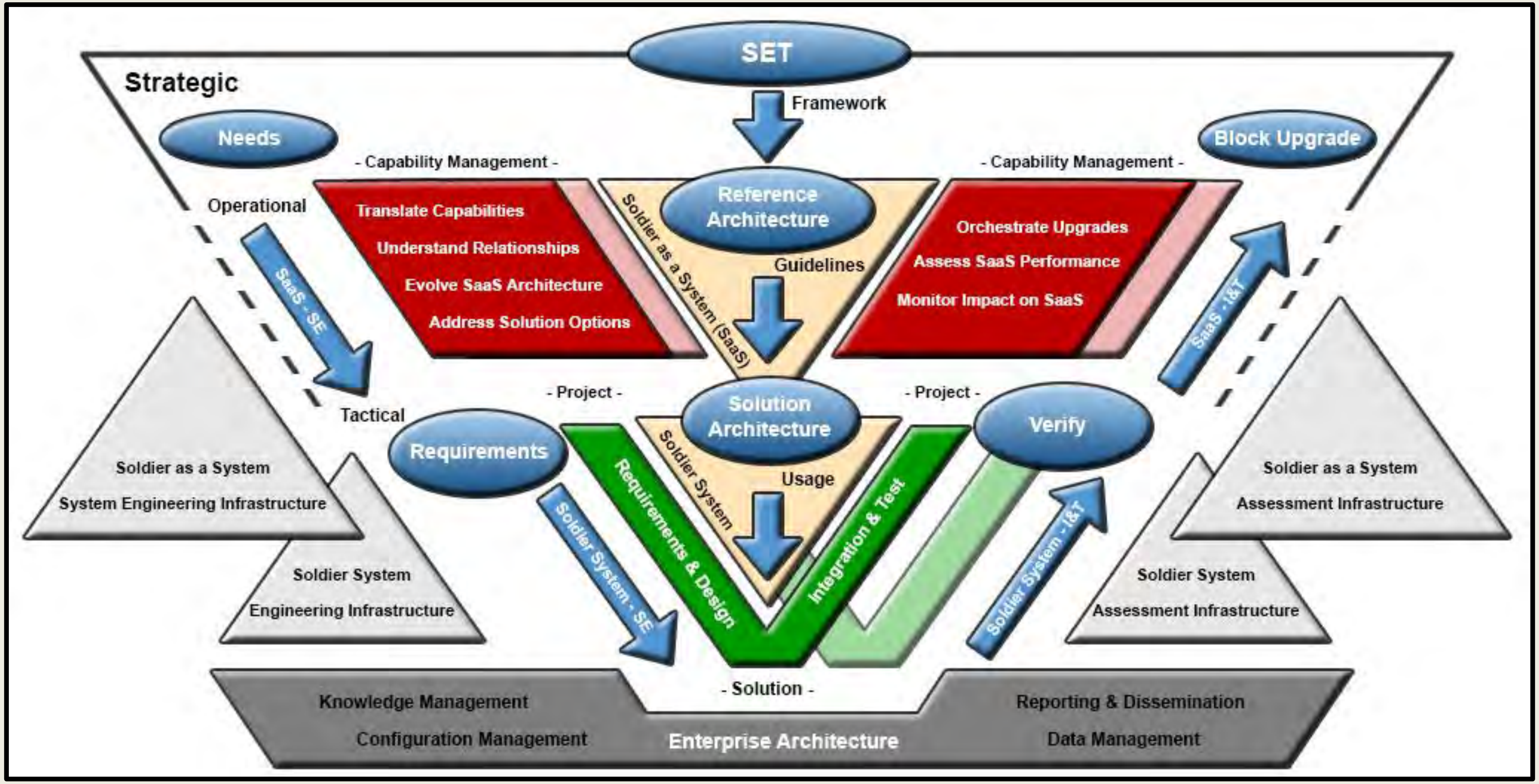
Other Government Agencies:

- Army Research Lab (ARL)
- Aberdeen Test Center (ATC)
- Communications-Electronics Research, Development, and Engineering Center (CERDEC)

THANK YOU

BACKUP SLIDES

Role of Systems Engineering in SSEA: The SE processes developed for SSEA have been selected to analyze, design, integrate, and evaluate Soldier as a System solutions.



Soldier Segment of the Model

Anthropometric and physiological elements included in the Soldier Segment of the model were obtained from Anatomy and Physiology references.

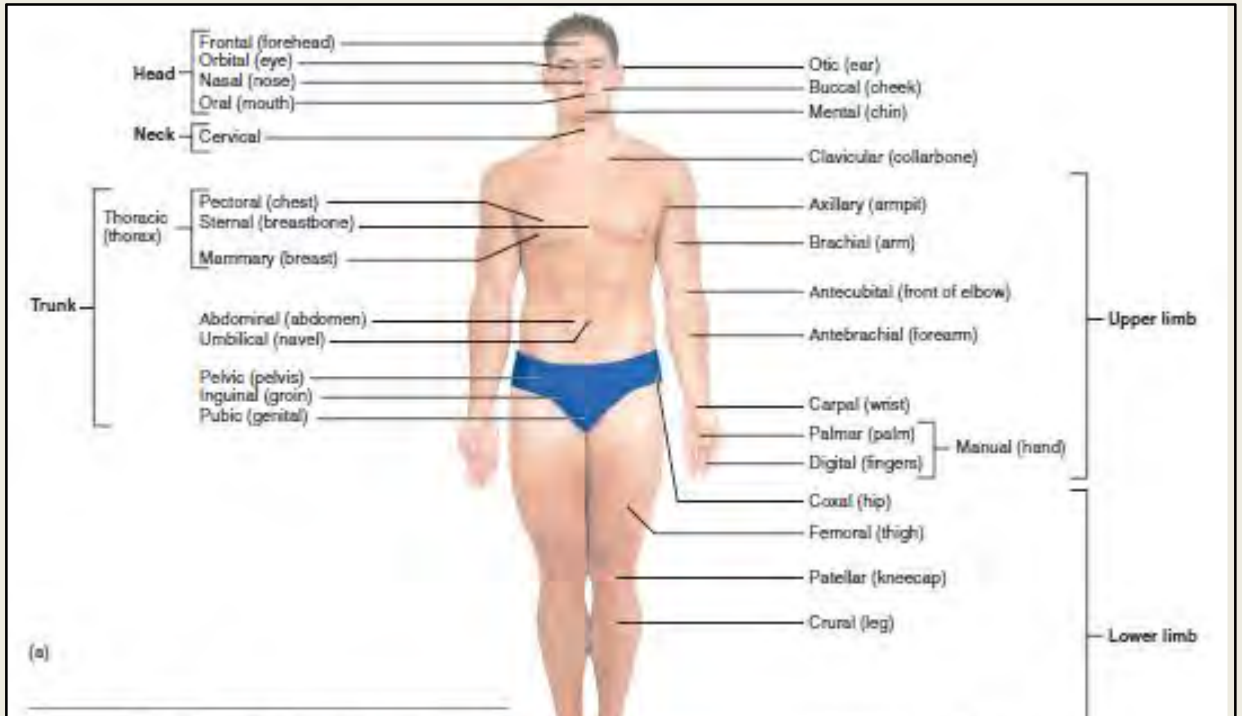


Figure 1.9 AP|R Body Parts and Regions
The anatomical and common (in parentheses) names are indicated for some parts and regions of the body. (a) Anterior view.

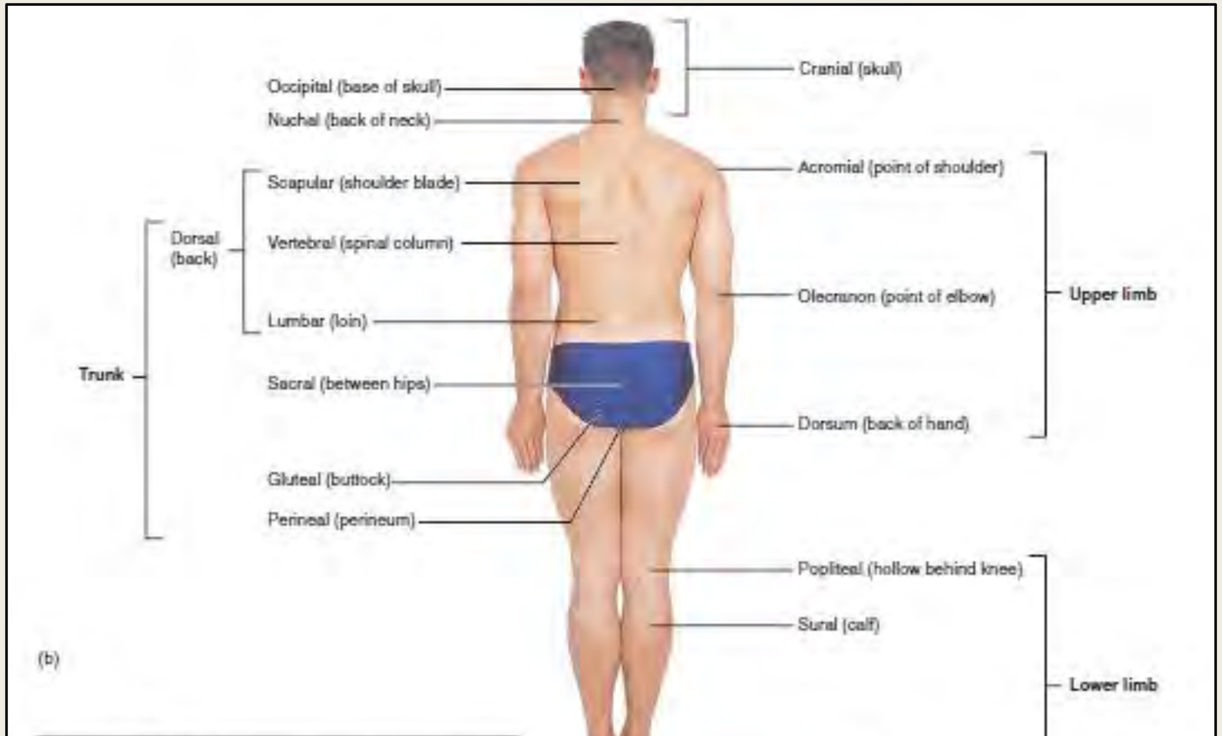


Figure 1.9 AP|R Body Parts and Regions *(continued)*
(b) Posterior view.

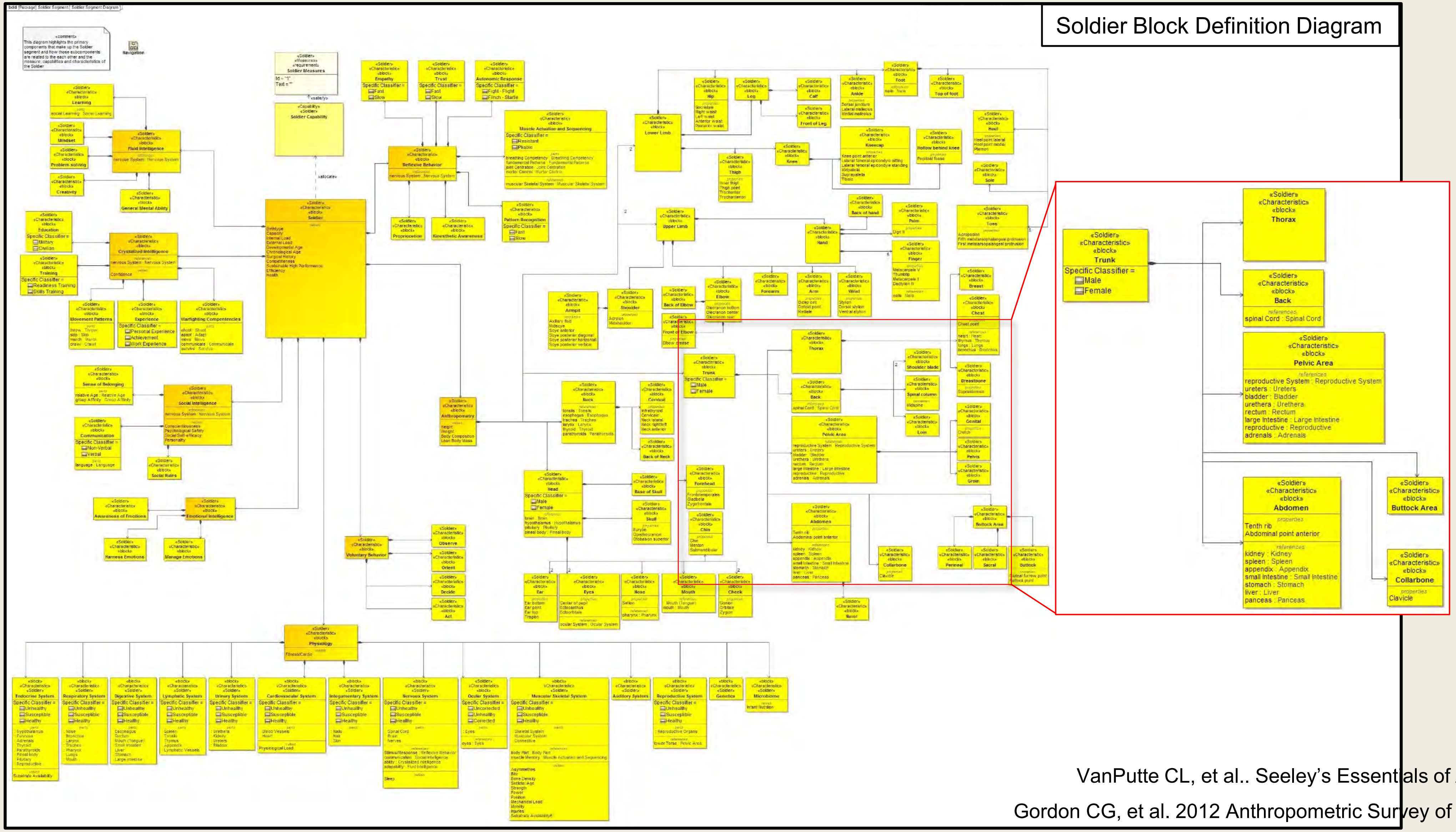
VanPutte CL, et al.. Seeley's Essentials of Anatomy and Physiology, 9th Ed. 2014.

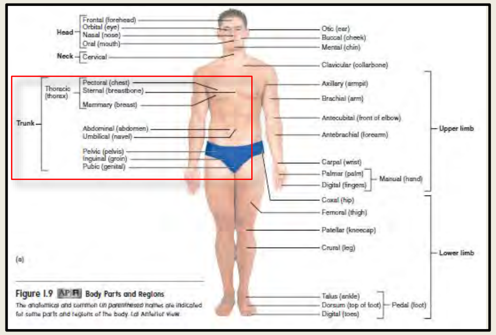
Gordon CG, et al. 2012 Anthropometric Survey of U.S. Army Personnel. NSRDEC. 2012.

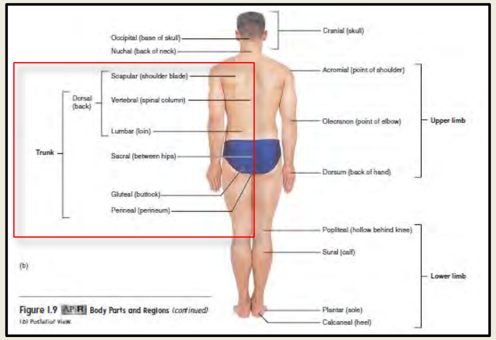
U.S. ARMY RDECOM

Soldier Segment of the Model

US ARMY NATICK SOLDIER RD&E CENTER · ARDEC







VanPutte CL, et al.. Seeley's Essentials of Anatomy and Physiology, 9th Ed. 2014.

Gordon CG, et al. 2012 Anthropometric Survey of U.S. Army Personnel. NSRDEC. 2012.

Soldier System Interaction Definition

List of Interactions for Target Engagement Operational Scenario

	Start Structure	End Structure (SOI)	Perspective from SOI	Function	Flow class	Basic Flow	Compliment	Candidate Name of Interaction
S-E	Buttstock	Shoulder	Human	Support, Stabilize	Material	Solid		Tactile/Human Stabilization
					Signal	Status	Tactile	
					Energy	Mechanical	Force	
	Shoulder	Buttstock	Equipment	Support, Secure	Material	Solid		
					Energy	Human	Force	
	Rifle Handguard	Hand	Human	Support, Stabilize	Material	Solid		Tactile/Human Stabilization
					Signal	Status	Tactle	
					Energy	Mechanical	Force	
	Hand	Rifle Handguard	Equipment	Support, Secure	Material	Solid		
					Energy	Human	Force	
	Rifle Grip	Hand	Human	Support, Stabilize	Material	Solid		Tactile/Human Stabilization
					Signal	Status	Tactle	
					Energy	Mechanical	Force	
	Hand	Rifle Grip	Equipment	Support, Secure	Material	Solid		
					Energy	Human	Force	
S-E	Rifle Handguard	Hand	Human	Support, Secure	Material	Solid		Tactile/Human Support
					Signal	Status	Tactle	
					Energy	Mechanical	Force	
	Hand	Rifle Handguard	Equipment	Support, Secure	Material	Solid		
					Energy	Human	Force	
	Rifle Grip	Hand	Human	Support, Secure	Material	Solid		Tactile/Human Support
					Signal	Status	Tactile	
					Energy	Mechanical	Force	
	Hand	Rifle Grip	Equipment	Support, Secure	Material	Solid		
					Energy	Human	Force	

Otto K and Wood K. Product Design: Techniques in Reverse Engineering and New Product Development, 1st Ed. 2000.

Raytheon

CYBER RESILIENT AND SECURE WEAPON SYSTEMS ACQUISITION / PROPOSAL DISCUSSION

Integrated Defense Systems

Holly Dunlap

October 2017

Raytheon

Perception, Expectations and Reality

Cyber Resilient and Secure Weapon System Acquisition

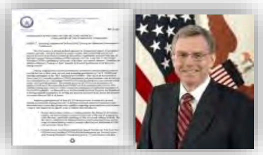
- National Strategy, Priorities and Big Picture Messaging
- DoD Cybersecurity Budget Review
- Current State RFP Analysis
- Acquisition RFP Guidance
- Channel the Energy and Contribute
- Recommendations
- Final Thoughts

Raytheon

DoD Policy and Strategy

Oct '10: Establishment and standup of U.S. Cyber Command

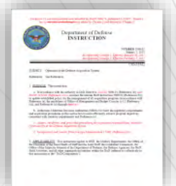
Feb '13: PPD-21, security and resilience of critical infrastructure against cyber threats



J. Michael Gilmore, Director, OT&E

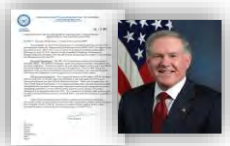
August 14: Directed Cybersecurity in OT&E

2015:
Multiple proposed bills to address information sharing between gov't and private sector



2017: DoD 5000.02 Encl 14, Cyber security in the Defense Acq Sys

2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017

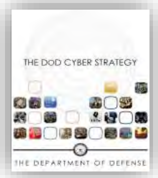


Frank Kendall
Deputy Under Secretary for AT&L

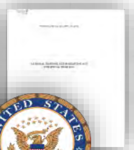
Jul '11: Memo outlining Program Protection Plan (PPP) for Cyber hardening of DoD Systems

Gen. Alexander, Commander USCYBERCOM

Mar '13: Public acknowledgement of Cyber warfare "teams" ready by 2015



Apr '15: DoD strategy expands network defense beyond their own systems and addresses synchronization of Cyber operations with kinetic effects



2016:
NDAA 16 Section 1647 Evaluation of Cyber Vulnerabilities

> *Improve weapons systems cybersecurity.* DoD will assess and initiate improvements to the cybersecurity of current and future weapons systems, doing so on the basis of operational requirements. For all future weapons systems that DoD will acquire or procure, DoD will mandate specific cybersecurity standards for weapons systems to meet.
>
> – *The DoD Cyber Strategy, April 2015*

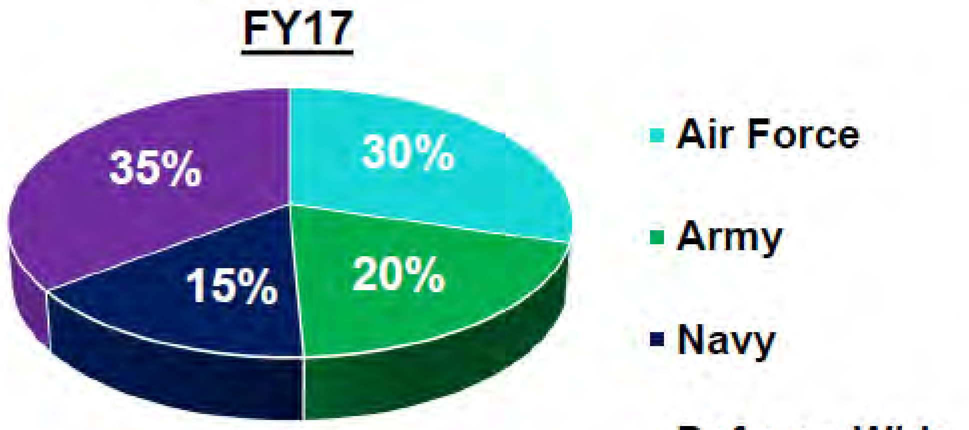
Policy is evolving, acquisition requirements need to incorporate policy requirements

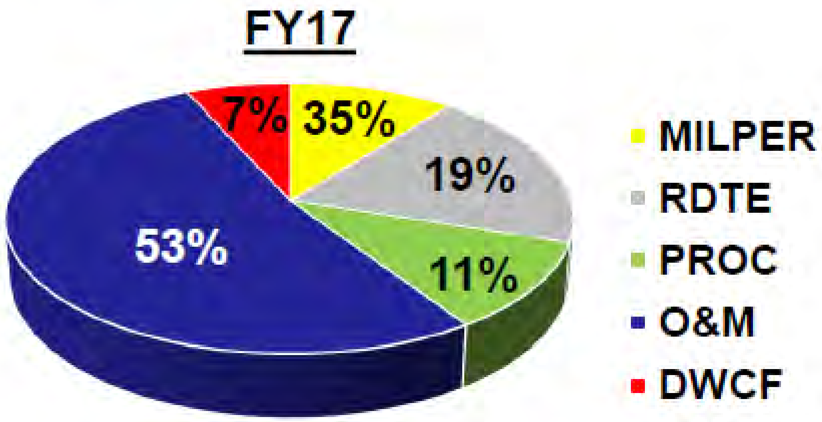
DoD FY17 PB Request for Cybersecurity Overall

Raytheon

($M)	FY16En	FY17	
Air Force	1,545.6	1,990.5	+28%
Army	945.1	1,329.6	+41%
Navy	950.2	1,038.2	+9%
Defense-Wide	2,300.8	2,375.4	+3%
Total	5,741.7	6,733.7	+17%

($M)	FY16 En	FY17	
MILPER	637.3	713.3	+12%
RDTE	1,062.9	1,299.1	+22%
PROC	587.7	725.2	+23%
O&M	2,992.0	3,545.1	+18%
DWCF	462.2	451.0	-2%





MILPER: Military Personnel
RDTE: Research, Development, Test and Evaluation
PROC: Procurement
O&M: Operations and Maintenance
DWCF: Defense Working Capital Fund

CYBERSECURITY BUDGET INCREASES AS THE PRIORITY INCREASES

2017
$2B
requested for cybersecurity procurement and RDT&E

Raytheon

A Look At Current State Proposal Requirements

Defense Platform/Embedded Program RFP Analysis

The analysis included 10 RFPs in 2016.

The following keywords were used to extract sections of the RFP Statement of Work and Sections L and M language.

Customers included:

- (3) Air Force — (1) United States; (1) direct commercial sale, (1) Foreign Military Sale
- (4) Navy — (2) United States; (2) direct commercial sale
- (3) Army — (3) United States

KEYWORDS USED:
cyber
cyber security
cybersecurity
cyber hardening
cyber defense
cyber protection
information assurance
IA
program protection
system security
security assessment
risk management framework
RMF
vulnerability analysis
survivability
resiliency
DIACAP
INFOSEC

Raytheon

RFP SOW Analysis Results Summary

Request for Proposal, Statement of Work (SOW) Analysis Results Summary

CYBER RESILIENCY AND SECURE SYSTEMS RELEVANT REQUIREMENTS – HOLISTIC PROGRAM PROTECTION										
							FMS	DCS	International	International
Program Protection	Navy #1	Navy #2	Army #1	Army #2	Army #3	AirForce #1	Air Force #2	Navy #3	International Customer #1	Navy #4
	x	x	x	x	x	x	x	x	x	x
• Program Protection Plan (PPP) development and implementation • Systems security Architecture • Software assurance • Secure coding • Information Assurance (IA) • Cyber hardening • Computer Network Defense (CND) • Embedded system security	Cybersecurity Plan	DFARS CDI	PPiP	Cybersecurity	Cybersecurity	Program Protection Plan	References System Security but really cybersecurity	Cyber resiliency (not specific words)	Resiliency	Cyber resiliency
			Critical Functional Analysis	PPiP	Anti-tamper	Cyber Resilient Architecture	PPiP	cybersecurity	System Security Architecture	Cyber security system
			Cybersecurity	SwA	Defense Exportability Features	Cybersecurity	Validation Plans		Security Management Plan (Emphasis on cybersecurity)	
			System Security Plan	Key Management		Software Assurance			Lifecycle considerations for security	
						Anti-tamper			Computer Network Defense	
						SCRM (Trusted Access Program Office, TAPO)			Cyber Hardening	
						Validation & Verification			Information Assurance	

How many cyber resiliency and system security relevant SOW requirements made the transition to Section L and Section M?

Section L and Section M

- Section L: Instructions, Conditions and Notices to Bidders
- Section M: Evaluation Factors and Rating Methodology

How many cyber resiliency and/or system security relevant SOW requirements made the transition to Section L and Section M?

ZERO

Opportunity for Improvement

- Flow and consistency
  - Seems like multiple authors
- Recommend broad coverage first then specific security specialties
  - Program protection
    - System security engineering
      - Including architecture and resiliency
    - Software assurance
    - Cybersecurity
    - Anti-tamper
    - Supply Chain risk management
    - General program security
- Detailed requirements should be included within each of the security specialties
- Presence of system security or holistic program protection within Sections L and M

Review of a Sample RFP

First-glance SOW outline looks promising:

Cybersecurity / System Security has a Presence!

Deeper Review

3.1.7 Security

3.1.7 SECURITY

The contractor shall ensure coverage, by a Facility Security Officer (FSO) and an Information Assurance Officer/Information System Security Officer (IAO/ISSO), at the contractor and deployment site. The contractor shall prepare and implement a Site Security Management Plan (SSMP) (CDRL A010). The contractor shall work with the site commander on coordination of facility access required by the contractor and its sub-contractors. The contractor shall provide the Government access to all existing security-related data and documentation.

3.1.7.1 INFORMATION SECURITY

The contractor shall ensure that cleared subcontractor facilities shall schedule and conduct annual Information Security Program Reviews (ISPRs) and self-inspections. Serious deficiencies at the subcontractor location shall be reported to the contractor ...

Deeper Review

3.1.7 Security

3.1.7.2 Program Protection

The contractor shall plan and implement an Acquisition System Protection program encompassing acquisition security, program protection, supply chain risk management and systems security engineering for this contract based upon the requisite Program Protection Plan (PPP) and threat documents provided by XXX. The contractor shall generate, update, maintain and implement a Program Protection Implementation Plan (PPIP) (CDRL A011) which will be a stand-alone document for this contract. The PPIP shall include compliance implementation planning provided PPP, DoDI 5200.39, DoDI 5200.44, DoD 5200.1-M, SI 538-02, DoDM 5200.01, DoDI 8500.01, DoD 5200.8-R, CJCSI 6510.01F, CJCSI 3210.01B, and CNSSP 11. The contractor shall provide inputs to and support Government security analyses, including system security analyses, the System Vulnerability Analysis (SVA), Operations Security (OPSEC) Plan, System Security Engineering (SSE) requirements analysis, and Cybersecurity/Computer Network Defense (CND) technical assessments. The contractor shall support government Protection Assessment Reviews (PAR), security audits and Program Protection Working Groups. The contractor shall develop Program Protection training plans and conduct contractor training of how to assess criticality of technologies and mitigate Critical Program Information (CPI) risks from known or postulated threats IAW government issued PPPs. The contractor shall conduct a CPI assessment. The contractor shall conduct annual self-assessments to evaluate program adherence to PPIP and processes (ADP 004).

Deeper Review

3.1.7 Security

3.1.7.2 Program Protection (cont.)

The contractor shall develop and implement security policy and procedures. The contractor shall provide self-assessment reports to the YYY program office and YYY Industrial Security Office no later than 30 days after the completion of the assessment. The contractor shall provide government updates on implementing the XXX SSE requirements the MMM ES. The contractor shall maintain weapon system security features using established System Security Engineering processes DoD 5200.1-M Acquisition Systems Protection Program, DoDI 5000.2, Defense Acquisition Guidebook, MIL-HDBK-1013/1A Design Guidelines for Physical Security of Facilities, DoDM 5200.01 Information Security Program, DoD 5200.08R Physical Security Program, Committee on National Security Systems Advisory Memorandum (CNSSAM) TEMPEST 1-13 RED/BLACK Installation Guidance, Committee on National Security Systems 387 (CNSS) Advisory Memorandum Tempest 01-02, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Common Criteria and National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11. The contractor shall develop SSE requirements, System Connection Authorization Requirements documents, and Security Accreditation Agreements documents. The contractor shall comply with security requirements IAW DoDI 8500.01 (Cybersecurity), DoDI 8510.01 (Risk Management Framework for DoD Information Technology), and the NSA Guide for Addressing Malicious Code Risk, and be accredited by the Authorizing Official (AO) prior to operation. The contractor shall provide a Technology Control Plan (TCP) for concurrence to MMM EIR, before submitting to Defense Security Services (DSS) for approval, within 90 days of contract award, if a TCP is required.

Deeper Review

Raytheon

3.1.7 Security

3.1.7.4 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

The contractor shall assist the government in conducting a Criticality Analysis IAW DoDI 5200.44 immediately following the Software/M&S PDR to identify XYZ mission critical functions and Information and Communications Technology (ICT) critical components of the ZZZ system elements as requested. The Prime contractor shall submit to and participate in unannounced government audits into their supply chain activities no more three times per year –unless unacceptable supply chain practices are identified by the Government. The contractor shall demonstrate 1.) Visibility into its supply chain for critical components and materials. 2.) Understanding of the risks to that supply chain

3.) Implementation or plans to implement risk mitigations to counter those risks documented in the PPIP.

For all subcontracts involving the procurement of Critical Components identified in the Government PPP, the Prime contractor shall flow down requirements for supply chain risk management detailed in section below. The Prime contractor shall ensure vulnerabilities and discrepancies identified by subcontractors and lower tier vendors are reported to the XXX Supply Chain Risk Management/Trusted Systems and Networks Integration Council.

The Prime contractor shall only procure logic bearing components identified on the Critical Components List from vendors accredited by the Defense Microelectronic Activity (DMEA) (http://www.dmea.osd.mil/trustedic.html) or request an exception in writing prior to procurement to the ZZZ COTR and YYY with a justification as to why the component could not be procured from an accredited DMEA supplier. The contractor shall continuously monitor the Program Critical Components List for impact of YYY SCRM Advisories, Government-Industry Data Exchange Program (GIDEP) Alerts, and similar information from other programs.

Deeper Review

Supply Chain Risk Management (cont)

3.1.7.4 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

The contractor shall prepare an SCRM Impact Statement (ADP 005) for each ZZZ SCRM Advisory for which a response is required containing the following:

a. ZZZ SCRM Advisory Number,
b. Points of Contact for Information,
c. Confirmation of the presence of the affected component,
d. System and subassemblies impacted,
e. Description of the function performed by the component,
f. Physical locations of the component,
g. Status of the component

Impact statements shall be submitted to the ZZZ SCRM Advisory Coordinator listed on the advisory. The contractor shall follow the response instructions listed on the advisory.

The provisions of this SOW shall be included in the solicitations and subcontracts for all suppliers, suitably modified to identify the security risks suppliers must address to ensure the protection of CPI and critical components within the supply chain.

Section M, Factor and Sub-factor Weighting

Raytheon

Evaluation Factors
Factor 1 (F1): Technical
Sub-factor TS1: Architecture and Design
Sub-factor TS2: Software Architecture and Development
Sub-factor TS3: Technology Maturity/Manufacturing Readiness
Factor 2 (F2): Management
Sub-factor MS1: Program Management
Sub-factor MS2: Schedule
Sub-factor MS3: Small Business Participation & Commitment
Factor 3 (F3): Past Performance

Table M-2-1 Non-Price Evaluation Factors/Sub-factors

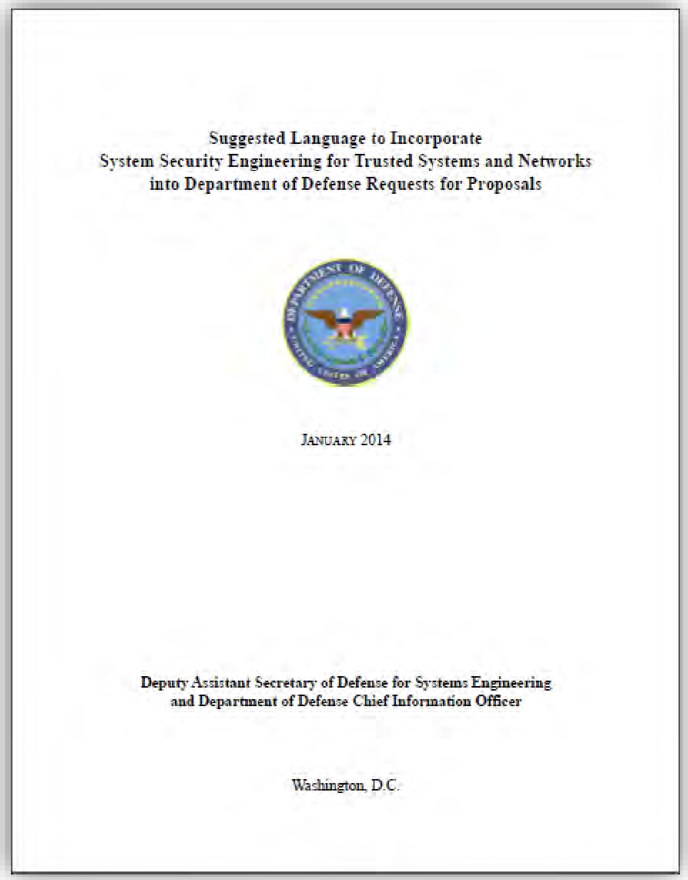
Increases in weight/importance

Security must be included within the evaluation criteria if you want anything related to System Security Engineering, Software Assurance, Cybersecurity, Security Relevant Supply Chain Risk Management, Cyber Resiliency, Cybersecurity Testing, Anti-tamper, etc., etc., etc.

Opportunity for Improvement

- Flow and consistency
  - Seems like multiple authors
- Recommend broad coverage first then specific security specialties
  - Program protection
    - System security engineering
      - Including architecture and resiliency
    - Software assurance
    - Cybersecurity
    - Anti-tamper
    - Supply Chain risk management
    - General program security
- Detailed requirements should be included within each of the security specialties
- Presence of system security or holistic program protection within Sections L and M

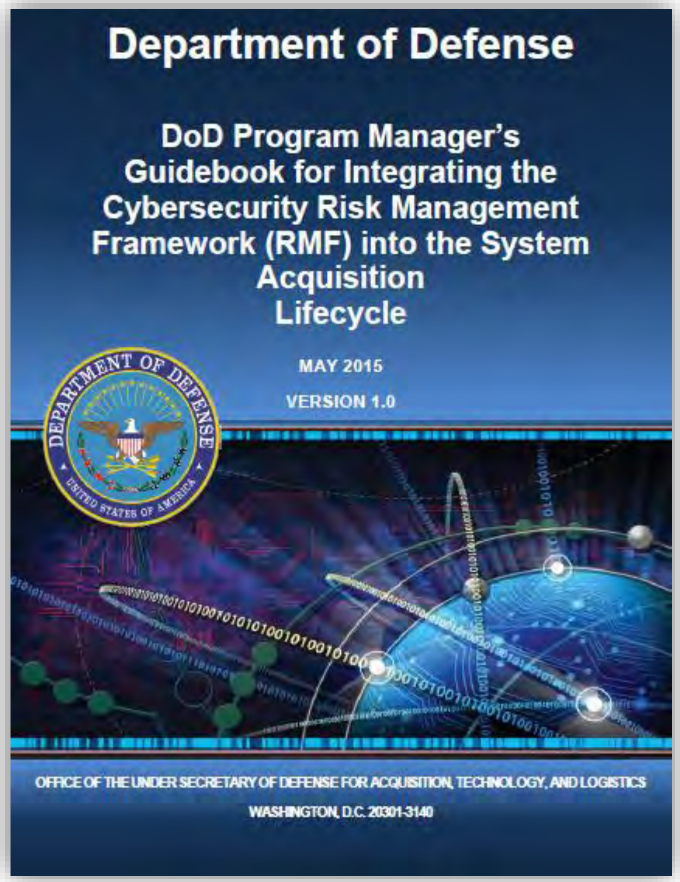
Sample of Existing Proposal Guidance


Suggested Language to Incorporate
System Security Engineering for Trusted Systems and Networks
into Department of Defense Requests for Proposals

JANUARY 2014

Deputy Assistant Secretary of Defense for Systems Engineering
and Department of Defense Chief Information Officer

Washington, D.C.

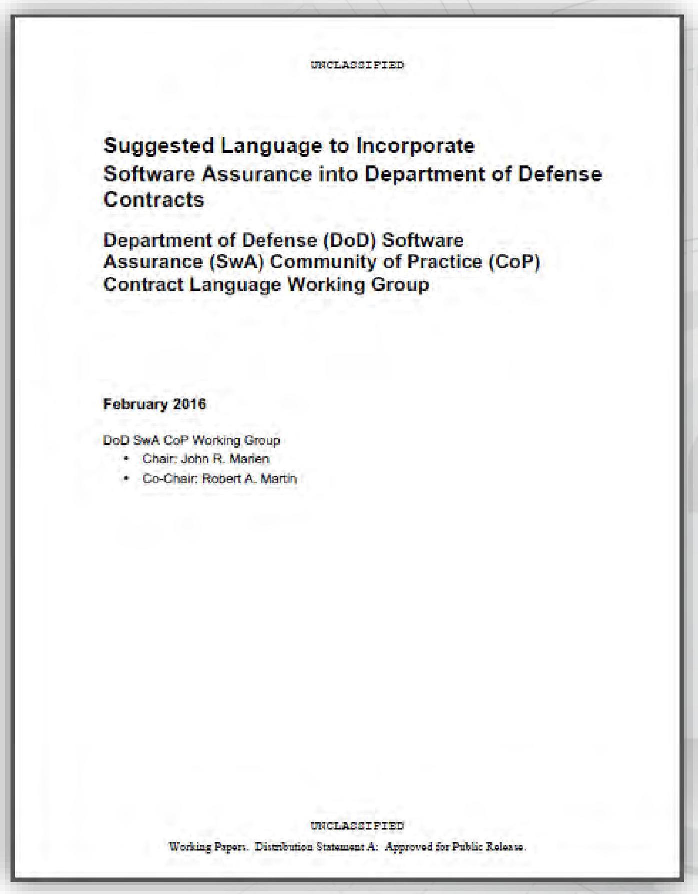

Department of Defense

DoD Program Manager's
Guidebook for Integrating the
Cybersecurity Risk Management
Framework (RMF) into the System
Acquisition
Lifecycle

MAY 2015

VERSION 1.0

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140


UNCLASSIFIED

Suggested Language to Incorporate
Software Assurance into Department of Defense
Contracts

Department of Defense (DoD) Software
Assurance (SwA) Community of Practice (CoP)
Contract Language Working Group

February 2016

DoD SwA CoP Working Group
- Chair: John R. Marien
- Co-Chair: Robert A. Martin

UNCLASSIFIED
Working Papers. Distribution Statement A: Approved for Public Release.

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html
Detailed excerpts in backup slides.

Channel the Energy and Contribute to the Solution

Raytheon

- There isn't a lack of acquisition proposal guidance
  - Too much guidance has led to similar results as a lack of guidance
  - Lots of well intentioned rice bowls contributing to perspective specific guidance
- We need a holistic integrated framework for program protection proposal guidance
- Start by developing a holistic program protection presence within Sections L and M
  - This outline can be the foundation to develop the details of the security specialty requirements across the life-cycle within the SOW
- The requirements details can be tailored per program
- We don't have a technology problem

Driving a holistic approach and consistency within Sections L and M could potentially be one of the most impactful actions this community could take

Proposed

Language for Sections L and M

Raytheon

- Goal is to ensure cyber resiliency and system security presence within every DoD platform and embedded system proposal

- Considerations:
  - Consistent with existing DoD policy
  - Agnostic to service or DoD customer
  - Agnostic to platform type
  - Flexibility to support legacy and “new start” programs
  - Concise language to minimize impact to proposal page counts
  - Tied to existing performance metrics and KPP

Raytheon

Consistent with DoD 5000.02

DoDI 5000.02, January 7, 2015, Change 2, 02/02/2017, 99 Enclosure 3

13. Program Protection

Program protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. Where a DoD **capability advantage** derives from a DoD-unique or **critical technology**, program protection **manages and controls the risk** that the enabling technology will be lost to an adversary. Where a DoD capability advantage derives from the integration of commercially available or custom-developed components, program protection **manages the risk that design vulnerabilities** or **supply chains will be exploited to destroy, modify, or exfiltrate critical data, degrade system performance, or decrease confidence** in a system. Program protection also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages.

Raytheon

Consistent with DoD 5000.02

DoDI 5000.02, January 7, 2015, Change 2, 02/02/2017, 99 Enclosure 3 (cont)

13. Program Protection

a. PPP. Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program.

b. Countermeasures. Program managers will describe in their PPP the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement. Countermeasures should include anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations in accordance with DoD Instruction 5200.39 (Reference (ai)), DoD Instruction 5200.44 (Reference (aj)), and DoD Instruction 8500.01 (Reference (x)). Program managers will submit the program's Cybersecurity Strategy as part of every PPP. Countermeasures should mitigate or remediate vulnerabilities throughout the product life cycle, including design, development, developmental and operational testing, operations, sustainment, and disposal.

PROPOSED

Acquisition Instructions to Industry

- Section L
  - Present the system security view of the platform architecture which enables system resiliency in a cyber contested environment
  - Present the critical mission thread analysis methodology which identifies the system mission critical functions and system mission critical components (hardware, software, and firmware) directly effecting KPPs.
  - Present the system security risk assessment methodology
  - Present the system security risk mitigation and countermeasure approach
  - Present the verification and validation approach to prove effectiveness of system security and system survivability in a cyber contested environment
  - Present how system security has been integrated into lifecycle considerations

PROPOSED

Acquisition Instructions to Industry

- Section M *(one-to-one mapping to section L)*
  - The proposal demonstrates that the system security view of the platform architecture provides sufficient details of the approach to support (future) assessments of cyber resiliency, system security, and system survivability to meet the KPPs while operating in a cyber contested environment
  - The proposal demonstrates that the critical mission thread analysis methodology directly contributes to the identification of system mission critical functions and system mission critical components (hardware, software and firmware) identification
  - The proposal demonstrates that the system security risk assessment methodology directly contributes to the system security risk mitigation approach
  - The proposal demonstrates the system security risk mitigation approach supports the decision making process to reduce the system security risks impacting KPPs
  - The proposal demonstrates that the verification and validation approach will provide assurance that the system security requirements have been meet
  - The proposal demonstrates that system security lifecycle considerations have been included in the overall system lifecycle plan

NDIA SSE Committee Review & Final Recommendation

NDIA

3.2 Request for Proposal (RFP) – Section L – Instructions, Conditions, & Notices to Offeror

Section L in the Request for Proposal (RFP) identifies the information the Government needs to accomplish the technical evaluation in accordance with the criteria established in Section M. RFP Sections L and M must be consistent with each other. Section L includes provisions and other information or instructions to guide contractors. SSE considerations are included in Section L as follows:

System Security Engineering

- Present the system security view of the platform architecture which enables system resiliency in a cyber contested environment
- Present the critical mission thread analysis methodology which identifies the system mission critical functions and system mission critical components (hardware, software, and firmware) directly effecting KPPs
- Present the system security risk assessment methodology
- Present the system security risk mitigation and countermeasure approach
- Present the verification and validation approach to prove effectiveness of system security and system survivability in a cyber contested environment

Present how system security has been integrated into lifecycle considerations

3.3 Request for Proposal (RFP) – Section M – Evaluation Factors for Award

Section M in the RFP provides comprehensive information to assist the Source Selection Evaluation Board (SSEB) in evaluating the contractor's understanding and capability to meet the requirements covered in the SOW. RFP Sections L and M must be consistent with each other (i.e. map one-to-one). SSE considerations are included in Section M as follows:

The Government will evaluate the proposed approach to SSE and assess the degree to which it will identify changing threats and the system's threat exposure, integrate SSE risk management with other SE process areas, and appropriately mitigate any threats. The evaluation will further focus on:

Factor 1 – Technical Capability: The Government will evaluate the proposed approach to SSE based on the contractor's understanding of the SSE requirements for <Insert SYSTEM NAME> as described in the SOW and initial PPIP. The evaluation will further focus on:

- The proposal demonstrates that the system security view of the platform architecture provides sufficient details of the approach to support (future) assessments of cyber resiliency, system security, and system survivability to meet the KPPs while operating in a cyber contested environment
- The proposal demonstrates that the critical mission thread analysis methodology directly contributes to the identification of system mission critical functions and system mission critical components (hardware, software and firmware) identification
- The proposal demonstrates that the system security risk assessment methodology directly contributes to the system security risk mitigation approach
- The proposal demonstrates the system security risk mitigation approach supports the decision making process to reduce the system security risks impacting KPPs
- The proposal demonstrates that the verification and validation approach will provide assurance that

NDIA SSE Committee Review & Final Recommendation

the system security requirements have been meet

- The proposal demonstrates that system security lifecycle considerations have been included in the overall system lifecycle plan

Factor 2 – Past Performance: The Government will evaluate the proposed approach based on relevant past performance experience in implementing and conducting SSE programs. The Government will evaluate the offeror on relevant past performance experience in implementing and conducting SSE programs. The Government will determine how such experience relates to the offeror's understanding of, and capability to meet, the SSE requirements covered in Section C – SOW as well as the contractor's demonstrated performance to implement SSE in similar projects:

- *Available past SSE performance.*
- Number of platforms and systems for which the contractor has integrated SSE (give only numbers).

Factor 3 – Cost/Price: The Government will evaluate the offeror on relevant past performance experience in implementing and conducting SSE programs. The Government will determine how such experience relates to the contractor's understanding of, and capability to meet, the SSE requirements covered in Section C – SOW as well as the offeror's demonstrated performance to implement SSE in similar projects:

- *Available past SSE performance.*

NDIA SSE Committee Review & Final Recommendation

NDIA

3.4 Request for Proposal (RFP) – Cost Volume - SSE Cost Estimate

The RFP – Cost Volume is prepared by the offeror and presents all costs, including the basis of estimate, implementation plan and schedule. The RFP cost estimate for SSE is based on the SSE requirements outlined in the PPP or other SE documentation that define SSE requirements. The program office provides the offeror with instructions regarding inclusion of SSE considerations in the Cost Volume as follows:

The offeror shall provide a complete detailed cost in the formal cost proposal and a CWBS for <Insert SYSTEM NAME> SSE engineering and architecture integration in the overall <Insert SYSTEM NAME> WBS. At a minimum, the contractor ***shall:***

- *Indicate/estimate the costs associated with SSE that exceed normal NISPOM costs.*
- *Indicate/estimate the design, engineering, development, testing, and other costs relative to SSE activities (e.g., CPI/CC identification, criticality analysis, vulnerability assessment, countermeasure development, counterfeit parts and firmware testing, etc.).*
- *Indicate/estimate all costs associated with an SSE measure to include: (i) the cost to acquire, develop, integrate, operate, and sustain the measure over the system life cycle; (ii) the cost as a measure of impact to system performance; (iii) the cost of documentation and training; and (iv) the cost of obtaining evidence and conducting analysis necessary for SSE-related requirements.*
- *Identify how the offeror will account for non-recurring engineering costs associated with SSE requirements.*
- *Describe the offeror's approach to using projected cost-benefit tradeoffs in SSE countermeasure selection.*

Final Thoughts

- Perception versus reality
- Terminology problem. I don't think this can be solved with more policy and guidance. This is a culture challenge.
  - System security
  - Cybersecurity
  - System security plan
  - Cybersecurity strategy
  - Holistic program protection
- Draft RFP is too late
  - Industry is shy to ask specific cyber/system security specific questions
- Need to identify who can drive consistency in standard proposal structure?
  - Is this something we can drive per Service (AF, Navy, Army, MDA)

Backup

Headquarters U.S. Air Force

Integrity - Service - Excellence

NDIA Systems Engineering Conference

Line of Action (LOA) 2 Action Plan

25 Oct 17

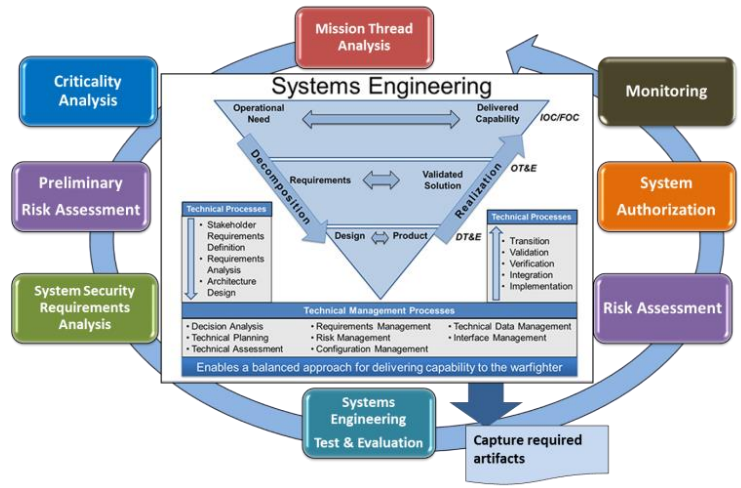
Dr. Ken Barker, SL
AFLCMC/EZ
DSN: 785-7213

LOA 2
Goal & Objectives

- **Goal: Efficiently and effectively incorporate Systems Security Engineering (SSE) into the Systems Engineering (SE) process in all phases of the Acquisition Lifecycle to increase cyber resilience in AF systems**
- **Team Members: AFLCMC, AFTC, SMC, NWC, AFMC, AFRL, SMEs**
- **Objectives**
  1. **Process Integration:** Integrate SSE into SE processes and deliverables
  2. **Process Assessment:** Develop metrics to measure SSE incorporation into SE processes and deliverables
  3. **Product V & V:** Develop system cyber test and evaluation methodology and capability across the lifecycle for all AF systems - aircraft, weapons, C4ISR, IT, Space, Nuclear

LOA 2
Integrate SSE into SE Processes

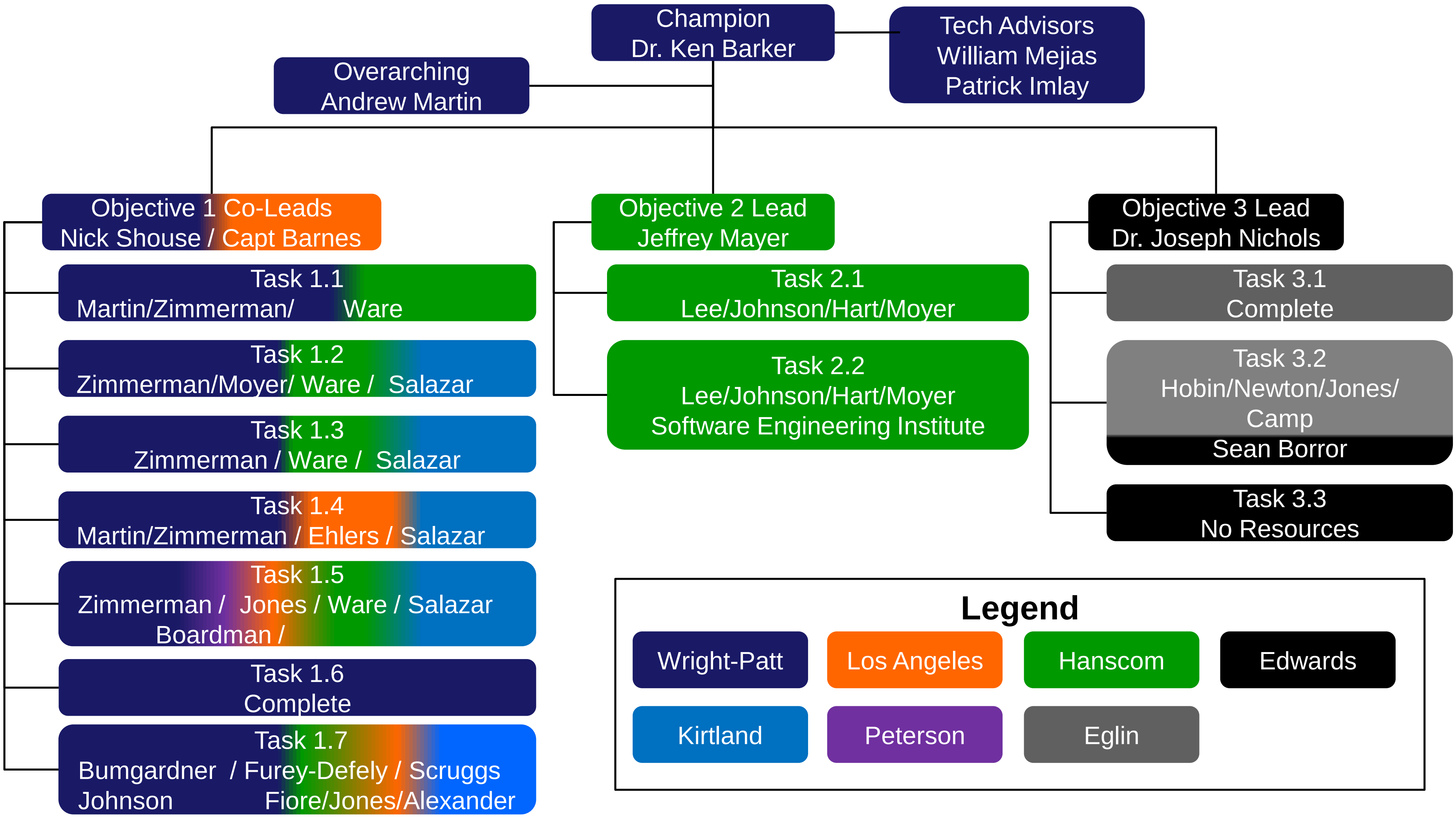
- **Status:**
  - Identified OPRs & formalized membership
  - Implementing Action Plan
  - Several process guides drafted/in coordination
  - SE Tech Review entry/exit criteria drafted
  - Cyber scorecard drafted; pilot apps under way
  - Cyber Test & Evaluation Study Completed



1

- **Near-term Way Ahead:**
  - Update existing guides based on feedback and evolving policy/regulations
  - Produce deliverables and work with Cyber Resiliency - Technical Advisory Council (CR-TAC) to disseminate/ institutionalize
  - Continue interfacing across LOAs, especially with the LOA 3 Cyber Resiliency Support Team (CRST)

LOA 2 Organization



Objective 1: Process Integration

- **Objective Description:** Integrate SSE principles into SE processes and deliverables
- **OPRs:**
  - Leads: Mr. Nick Shouse, AFLCMC/EZS;
    Capt Cameron Barnes, SMC/ENX
  - Reps from AFLCMC, SMC, AFNWC, AFMC, FFRDCs, Contractor SMEs

LOA 2 Input-Output

Input
- FAA
- NIST
- AO/CSAs
- LOA 6
- NDAA 1647
- CICC/CPT
- LOA 3

Processing
- LOA 2
- Task 1.2
- Task 1.7
- Task 3.2

Output
- System Requirements Document
- System Performance Specification
- Statement of Work tasks
- Required deliverables
- Etc.

LOA 2, Task 1.1

Establish executable process for CPI & CC ID

Task Description & Deliverables

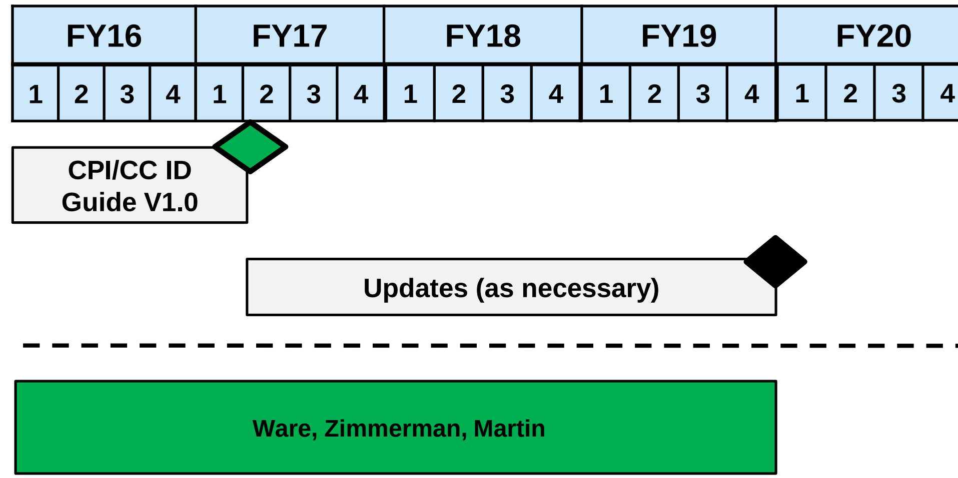
Description

- Provide process guidance that enables programs to accurately identify and obtain independent review and validation of CPI/CC.

Deliverables

- CPI and CC Identification Process Guide

Resource Loaded Schedule



Done Criteria

- Approval of CPI/CC Identification Process Guide by CR-TAC
- CPI/CC Identification Process Guide submitted for consideration to SAF/AQR for adoption as an Air Force Pamphlet (AFPAM) or referenced by AFPAM 63-113, Program Protection Planning for Life Cycle Management
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Analyze whether existing module of Program Protection course on CPI/CC ID is sufficient
- Accountability – Best practice to ensure correct implementation of DoDI 5200.39 and 5200.44
- Sustainment organization – Transition in FY19 or 20 to AFLCMC/EZSP and SMC/ENX for sustainment

LOA 2, Task 1.2

Define SSE & Integrate SSE into SE

Task Description & Deliverables

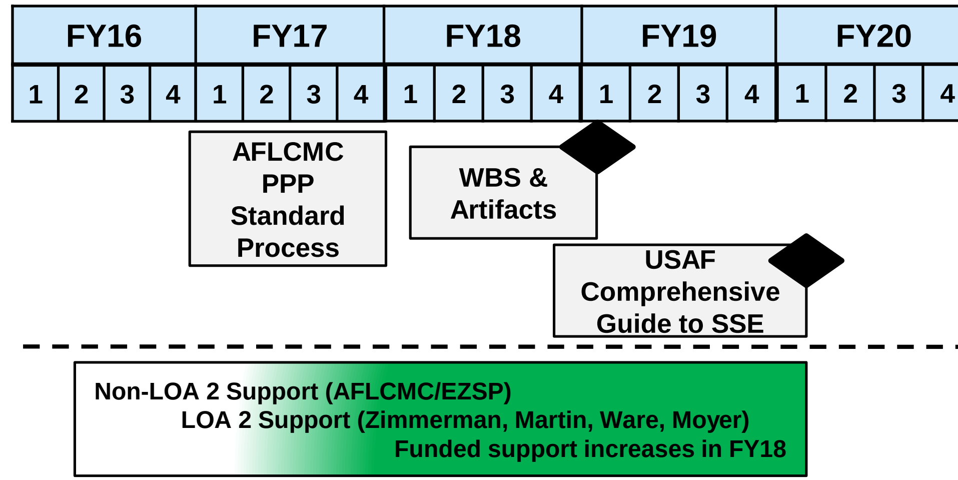
Description

- To provide understanding of SSE terms and concepts within a *Guide for Accomplishing Comprehensive SSE*

Deliverables

- Guide for Accomplishing Comprehensive SSE, including Program Work Breakdown Structure (WBS), artifacts, and templates

Resource Loaded Schedule



Done Criteria

- Approval of the Guide for Accomplishing Comprehensive SSE by CR-TAC
- Submitted to SAF/AQR for consideration as a replacement for the existing AFPAM 63-113 (*Program Protection Planning for Life Cycle Management*)
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Potentially add module to Program Protection course
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY20 to AFLCMC/EZSP and SMC/ENX for sustainment

LOA 2, Task 1.3

Establish executable process for System Security Risk Management

Task Description & Deliverables

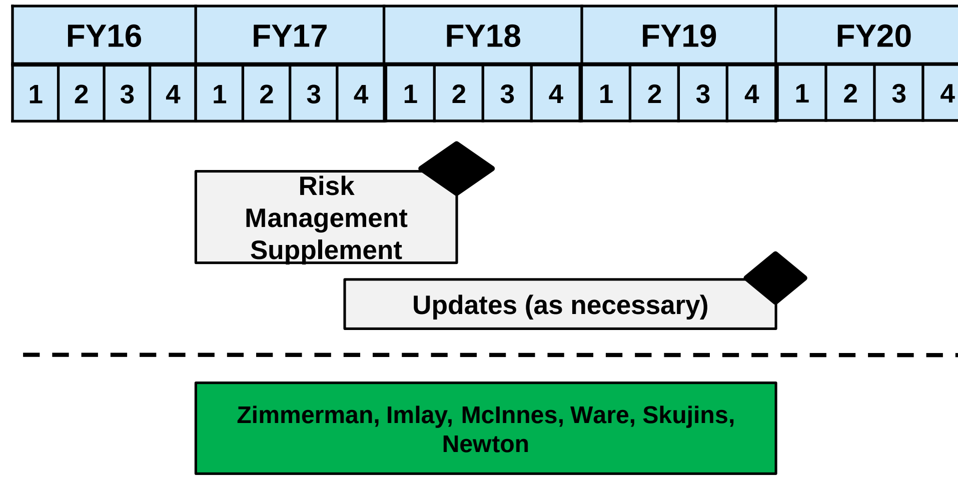
Description

- Provide one integrated system security risk management process that programs execute as part of their overarching risk management process, including the steps for risk planning, identifying, analyzing, handling, and monitoring.

Deliverables

- Risk Management Supplement to AFPAM 63-128, Integrated Life Cycle Management - Supplemental guide to integrate system security risk management

Resource Loaded Schedule



Done Criteria

- Approval of the Risk Management Supplement by the CR-TAC
- Submitted for consideration to SAF/AQR for update of the AFPAM 63-128, Integrated Life Cycle Management, to include system security risk management
- Supplement posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY19 or 20 to AFLCMC/EZAS and SMC/ENX for sustainment

LOA 2, Task 1.4

Develop and execute acquisition language guidance

Task Description & Deliverables

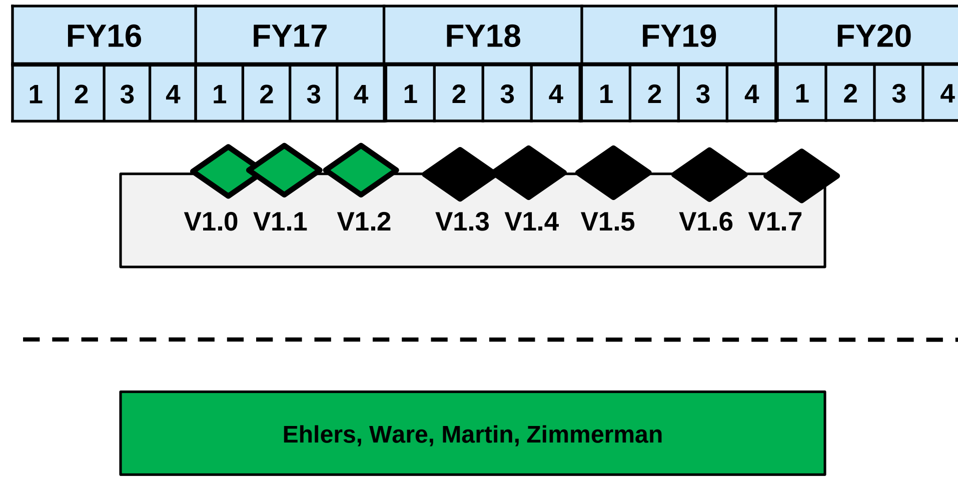
Description

- Provide SSE-focused guidance to program offices for use in various acquisition docs
  - Offers programs a common starting point

Deliverables

- USAF SSE Acquisition Guidebook – Iterative development with periodic publication of updated versions

Resource Loaded Schedule



Done Criteria

- Interim deliveries/updates made as new information becomes available from other Cyber Campaign Plan activities
- Approval of the Final USAF SSE Acquisition Guidebook by CR-TAC
- Guide posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, SSEs, and Contracts
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment

LOA 2, Task 1.5

Establish SETR SSE Entry & Exit Criteria

Task Description & Deliverables

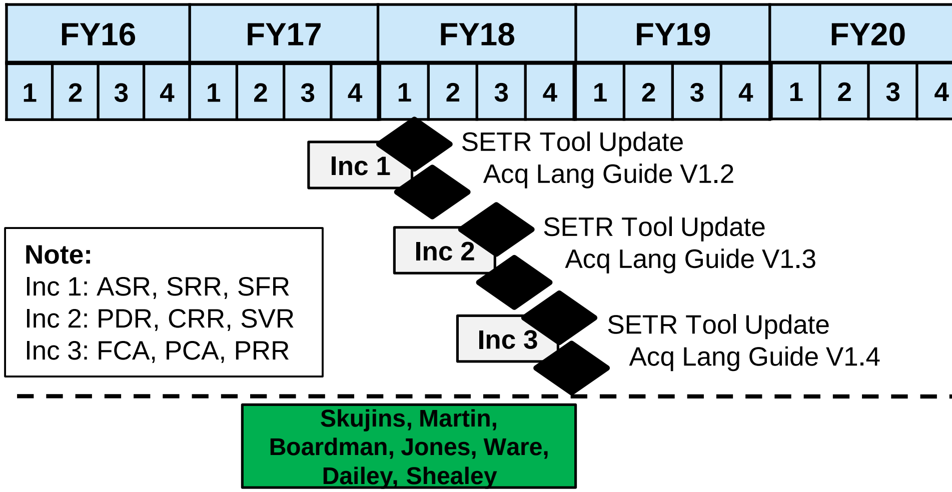
Description

- Establish SETR SSE entry/exit criteria that program offices across AFLCMC, SMC, and AFNWC can use to evaluate the design maturity of programs during various SETR activities.

Deliverables

- Updated SETR SSE Entry/Exit Criteria/Tasks outlined within the USAF SSE Acq Guidebook
- Updated SETR Toolset with SSE Entry/Exit Criteria

Resource Loaded Schedule



Done Criteria

- Final SETR Entry/Exit Criteria reviewed/approved by the CR-TAC
- Update of AFLCMC SETR Toolset with approval by AFLCMC/EZSI

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – TBD
- Accountability – Recommended to PEOs as a best practice
- Sustainment organization – Transition of SSE Acq Guidebook in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment. SETR Toolset will be continue to be maintained by AFLCMC/EZSI.

LOA 2, Task 1.6 (COMPLETE)

Provide recommended system security language for ICDs, CDDs, and CPDs

Task Description & Deliverables

Description

- Create guidance that enables program offices to interact with users and inform the development of weapon system requirements that account for SSE activities throughout the acquisition life cycle.

Deliverables

- Updated SSE Acquisition Guidebook identifying process owners; summaries of applicable requirements development processes; and sample ICD, CDD, and CPD requirements language

Resource Loaded Schedule

FY16				FY17				FY18				FY19				FY20			
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

SSE Acq Lang V1.1

Any updates part of Task 1.4

Imlay, Martin, Zimmerman, Moyer

Done Criteria

- Approval of USAF SSE Acquisition Guidebook v1.1 by the CR-TAC

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – See Task 1.4
- Accountability – See Task 1.4
- Sustainment organization – See Task 1.4

LOA 2, Task 1.7

Develop system and acquisition security requirements for programs

Task Description & Deliverables

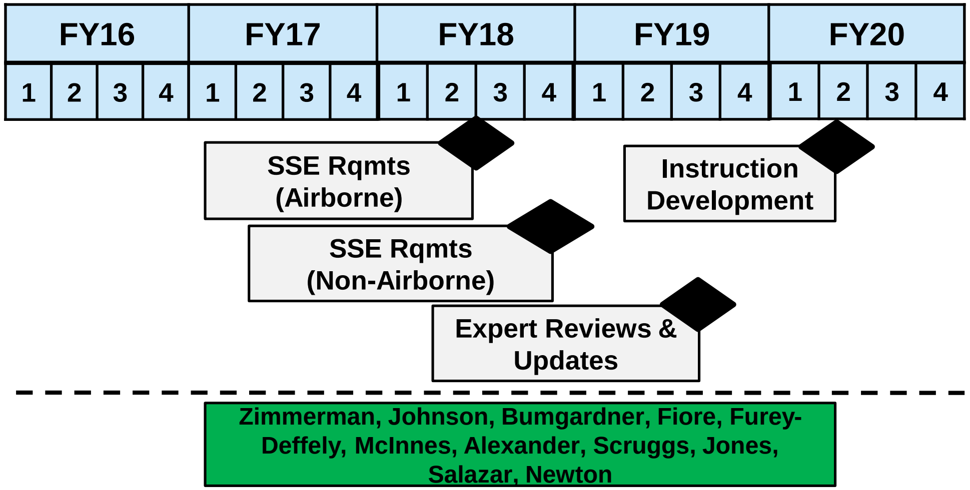
Description

- Develop a requirements construct modeled after the format used in (MIL-HDBK) 516C, that focuses on criterion, standards, methods of compliance (i.e., verification), and references.

Deliverables

- Traceable to NIST controls for reciprocity and audit purposes.
- Aligned with various domain frameworks
- An USAF-wide solution that includes areas of domain-agnostic requirements

Resource Loaded Schedule



Done Criteria

- Approval of the Final SSE Requirements Construct by CR-TAC
- Construct posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, especially PMs, SEs, and SSEs
- Training – Guidance/instruction on use of Construct
- Accountability – Potentially update Air Force Instruction 17-101 or other instruction
- Sustainment organization – Transition in FY20 to AFLCMC/EZSI and SMC/ENX for sustainment

Objective 2: Process Assessment

- **Objective Description:** Develop metrics to measure SSE incorporation into SE processes and deliverables
- **OPR:**
  - Lead: Mr. Jeff Mayer, AFLCMC/EZC
  - Representatives from AFLCMC, SMC, NWC, DOEs

LOA 2, Task 2.1

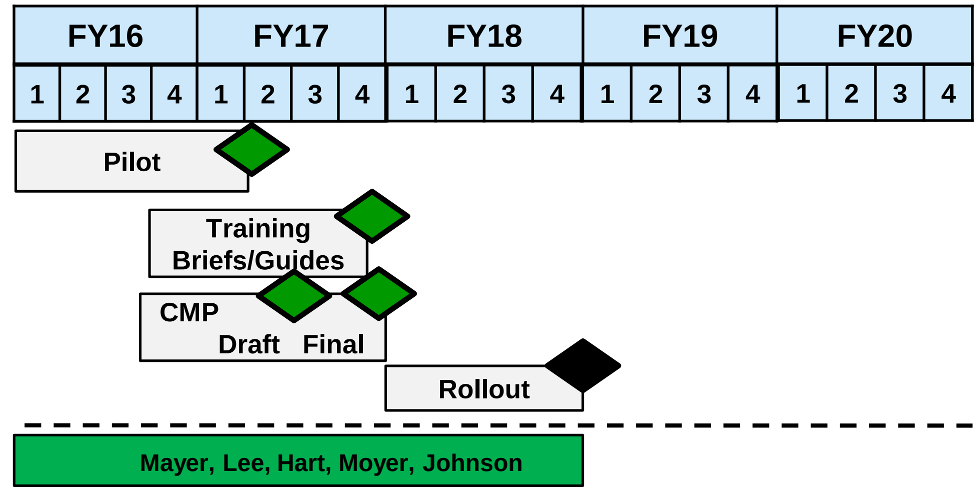
Develop a Cyber Health Scorecard to measure SSE process health within program offices

Task Description & Deliverables

Description
- Develop scorecard for program office use
  - Enable programs to evaluate quality of applied programmatic practices

Deliverables
- Final Enhanced Guidance
- Updated Overview and Training briefings
- Health Scorecard Configuration Management Plan
- Cyber Health Scorecard

Resource Loaded Schedule



Done Criteria

- Final Cyber/SSE Health Assessment reviewed/approved by the CR-TAC
- Guidance recommending use of tool sent by CROWS or SAF/AQR to PEOs
- PEO Enterprise Roll-up Capability integrated into tool
- Assessment posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, including PMs, System Program Directors, & PEOs
- Training – Narrated training briefs and enhanced guidance
- Accountability – Memorandum from SAF/AQR to PEOs encouraging use of assessment
- Sustainment organization – Potential transition in FY19 to AF SE Assessment Model (SEAM) and managed by AFMC/ENS and SMC/ENE

LOA 2, Task 2.2

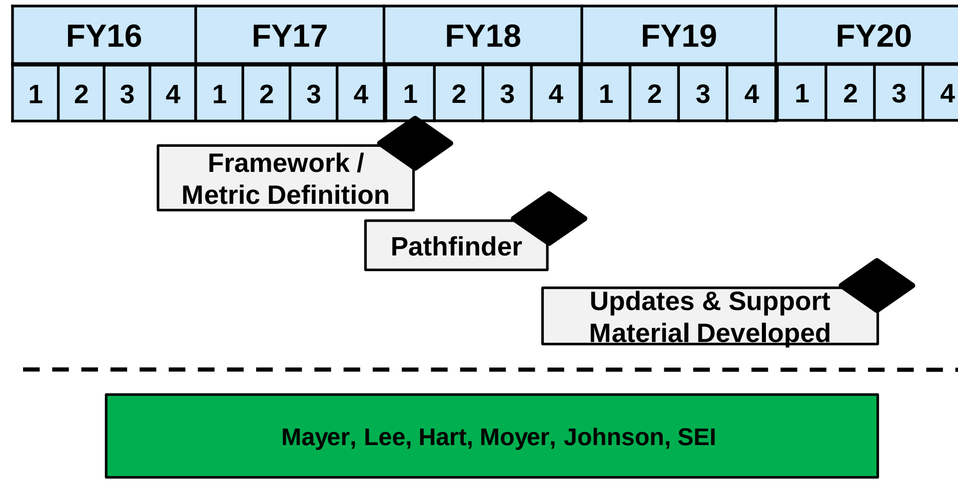
Develop methodologies & metrics to measure our systems' security and resiliency

Task Description & Deliverables

Description
- Form an AF-level Cybersecurity Metrics Framework
  - Allows capturing and summing metrics to provide system and/or platform level insight
  - Conduct pathfinders, refine metrics, and instantiate a collection tool & analysis method

Deliverables
- AF Cyber Metrics Framework

Resource Loaded Schedule



Done Criteria

- Final AF Cyber Metrics Framework reviewed/ approved by the CR-TAC
- Framework posted to site accessible by all acquisition center program offices

Institutionalization

- Targeted Audience – Acquisition center program office, including PMs, System Program Directors, & PEOs
- Training – TBD
- Accountability – TBD
- Sustainment organization – TBD

Objective 3: Product V&V

- **Objective Description:** Develop system cyber test and evaluation methodology and capability across the lifecycle for all AF systems - aircraft, weapons, C4ISR, IT, space, nuclear
- **OPR:**
  - Dr. Joe Nichols, AFTC/CZ
  - Reps from AF/TE, AFOTEC, AFMC, AFLCMC, SMC, NWC, AFRL, NASIC, DOEs

LOA 2, Task 3.1 (COMPLETE)

Monitor & provide Cyber T&E Study

Task Description & Deliverables

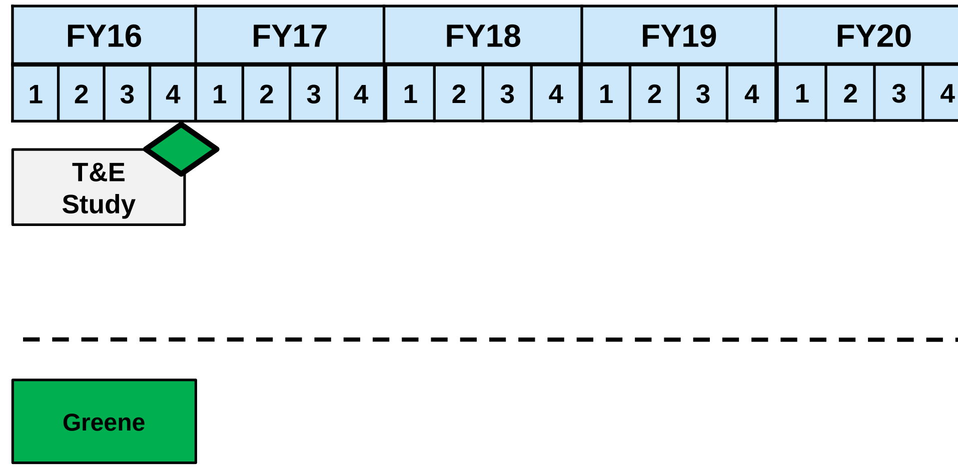
Description

- Complete Cybersecurity Test and Evaluation (CTE) Study under guidance of 46th Test Squadron
  - Identify environment, infrastructure, tools, methodology, manpower, & resources required

Deliverables

- Cyber T&E Study
  - Capability and infrastructure gaps
  - Process recommendations & investment map
  - Manpower study on required expertise and workforce requirement

Resource Loaded Schedule



Done Criteria

- Completion of the Cyber T&E Study to inform investment planning and task 3.2

Institutionalization

- The Cyber T&E Study is complete and maintained by the 46 TS. Analysis will be used to inform investment planning and task 3.2

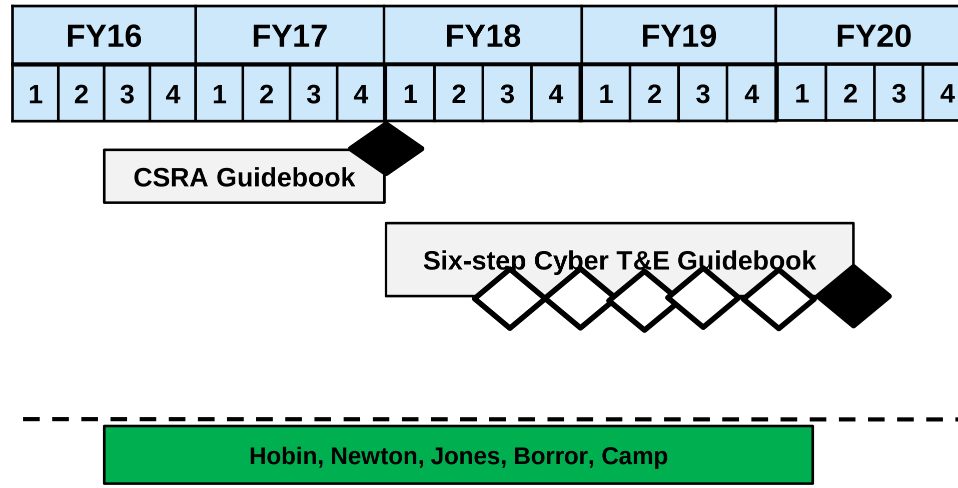
LOA 2, Task 3.2
Cyber Test Technique Development

Task Description & Deliverables

Description
- Develop cybersecurity test strategies, document best practices and lessons learned, and produce a cybersecurity test techniques handbook

Deliverables
- Cyber System Risk Assessment Guidebook
- Cyber T&E Guidebook

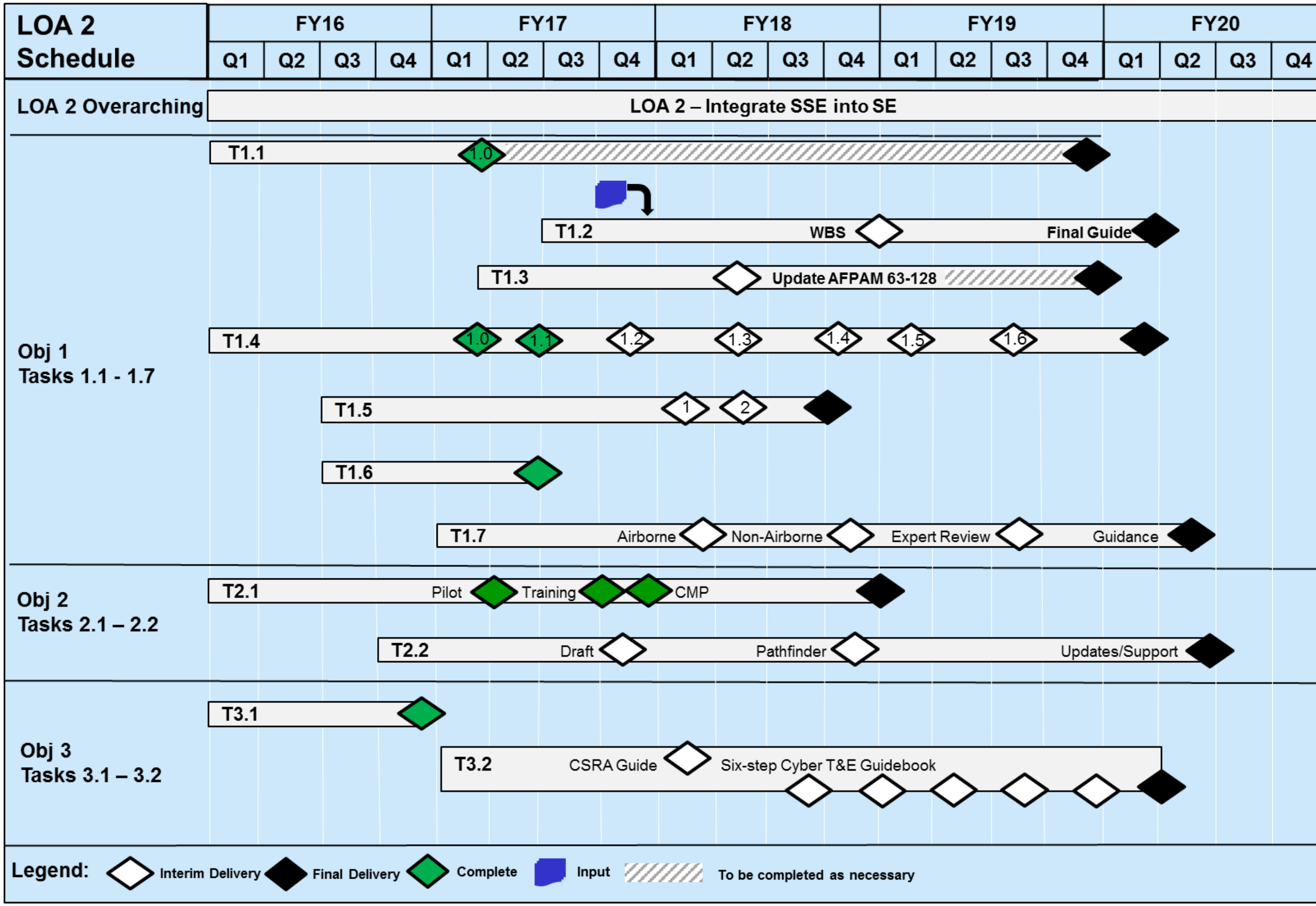
Resource Loaded Schedule



Done Criteria
- All guidebooks and methodology approved for use by Headquarters AF/T&E
  - 46 TS coordination and comment resolution completed
  - Internal LOA 2 coordination and comment resolution completed
  - Cross-LOA coordination and comment resolution completed

Institutionalization
- Targeted Audience – Acquisition center program office and Air Force Test Center, especially 46 TS
- Training – TBD
- Accountability – TBD
- Sustainment organization – Transition upon completion to the 46 TS for sustainment

Schedule


LOA 2 Schedule
FY16
FY17
FY18
FY19
FY20
Q1
Q2
Q3
Q4
LOA 2 Overarching
LOA 2 – Integrate SSE into SE
T1.1
1.0
T1.2
WBS
Final Guide
T1.3
Update AFPAM 63-128
T1.4
1.0
1.1
1.2
1.3
1.4
1.5
1.6
Obj 1
Tasks 1.1 - 1.7
T1.5
1
2
T1.6
T1.7
Airborne
Non-Airborne
Expert Review
Guidance
T2.1
Pilot
Training
CMP
Obj 2
Tasks 2.1 – 2.2
T2.2
Draft
Pathfinder
Updates/Support
T3.1
Obj 3
Tasks 3.1 – 3.2
T3.2
CSRA Guide
Six-step Cyber T&E Guidebook
Legend:
Interim Delivery
Final Delivery
Complete
Input
To be completed as necessary

Developing Requirements for Secure System Function

NDIA 20th Annual Systems Engineering Conference
October 23-26, 2017
Springfield VA

Michael McEvilley
Max Allway
Alvi Lim

The MITRE Corporation
Systems Engineering Technical Center
mcevilley@mitre.org
703.472.5409

Approved for Public Release; Distribution Unlimited. Case Number 17-3190

Basis for Effort

- **Integrating SSE into SE across multiple sponsor organizations and foci:**
  – AFLCMC/EZC Cyber Systems Engineering Division
  – Systems Mission Assurance Working Group (SMAWG)
  – PEO-BM process improvements to Anti-Tamper
  – Cyber Resiliency Steering Group (CRSG)
  – AF Cyber Campaign Plan

- **Recognition of the need for foundational requirements-oriented considerations informed by results of Program Protection pathfinders for CPI and CC identification**
  – Security requirements elicitation, analysis, and negotiation activities to identify, establish valuation of, and prioritize assets

Motivation for this Effort

- **Lack of foundational material in a form that is suitable to build application guidance for system security**
  - There is no security equivalent to MIL-STD-882E (2012), Department of Defense Standard Practice, System Safety
  - MIL-STD-1785 Systems Security Engineering (1989) was recast and remains validated as MIL-HDBK-1785 (1995/2014)
- **Computer security foundational materials date back to the 1970's – but have not been interpreted for "system context" application**
  - Ware, Anderson, Saltzer and derivative works
  - Developed to target "design for" and not "demonstrate compliance to" objectives

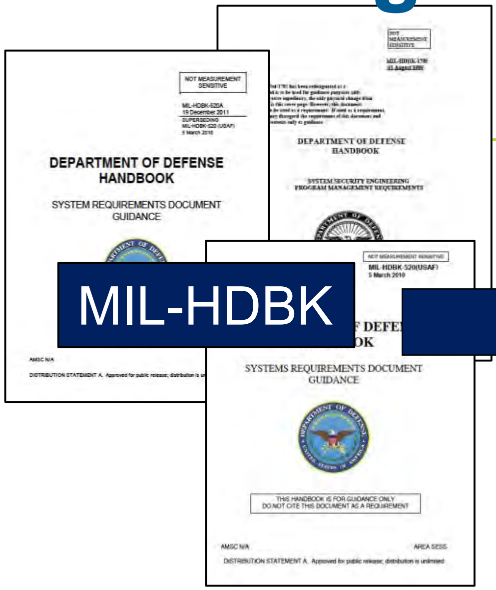
❖ **W. Ware**, et al, "Security Controls for Computer Systems," Report of the Defense Science Board Task Force on Computer Security, February 1970.

❖ **J. Anderson**, et al., "Computer Security Technology Planning Study," Technical Report ESD-TR-73- 51, Air Force Electronic Systems Division, Hanscom AFB, October 1972.

❖ **J. Saltzer**, M. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE, September 1975, 1278–1308.

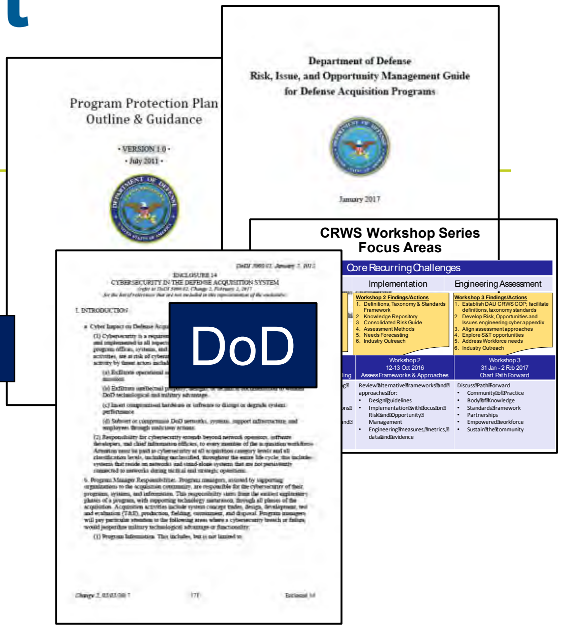
MITRE

Informing Aspects to the Effort



MIL-HDBK

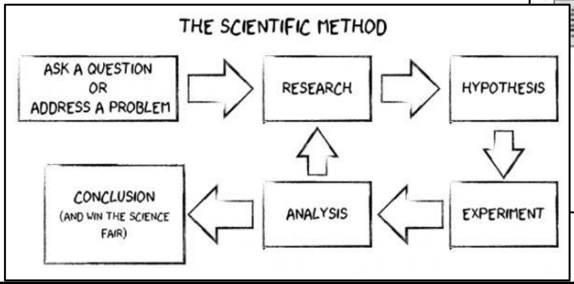
Developing Requirements for Secure System Function: Foundation, Method, and Supporting Considerations

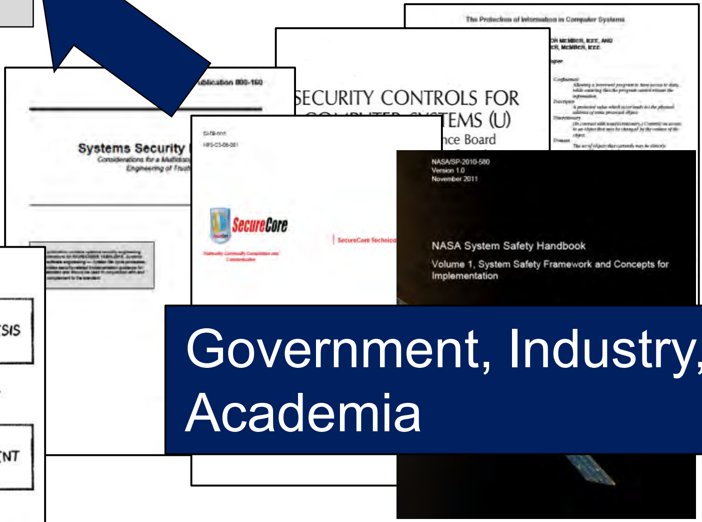


DoD

AF Support

- CPI Identification
- CC Identification
- Integrated CPI and CC Identification
- Program and SRD Analysis





Government, Industry, Academia

Comprehensive multidisciplinary and system-oriented considerations to incorporate security in Capability, Requirements, and Performance artifacts

MITRE

Discussion Topics

- **Section 1**
  – Challenges to engineering dependably secure systems
- **Section 2**
  – Concept and principle base
- **Section 3**
  – Method to drive requirements elicitation, analysis, negotiation
- **Section 4**
  – Viewpoint-driven considerations

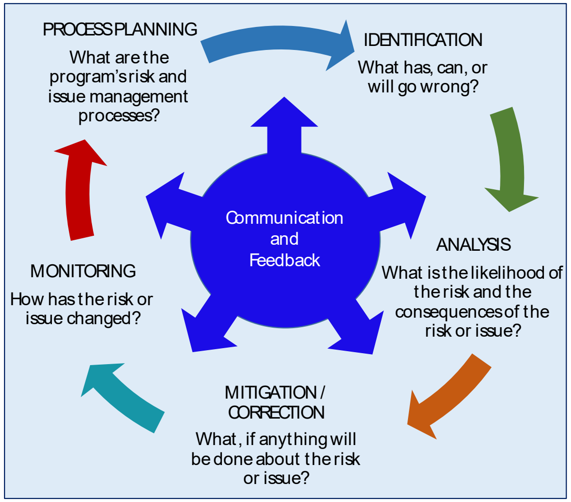
MITRE

Section 1 – Challenges

Challenges to the Effective Engineering of Dependably Secure Systems

- Absence of system perspective
- Accurately framing the problem
- Need for requirements-based risk management
- Level-of-Rigor (LoR) and evidence-based system security
- Dependably secure system function
- Uncertainty and the limits in understanding technology

Systems Engineering Need



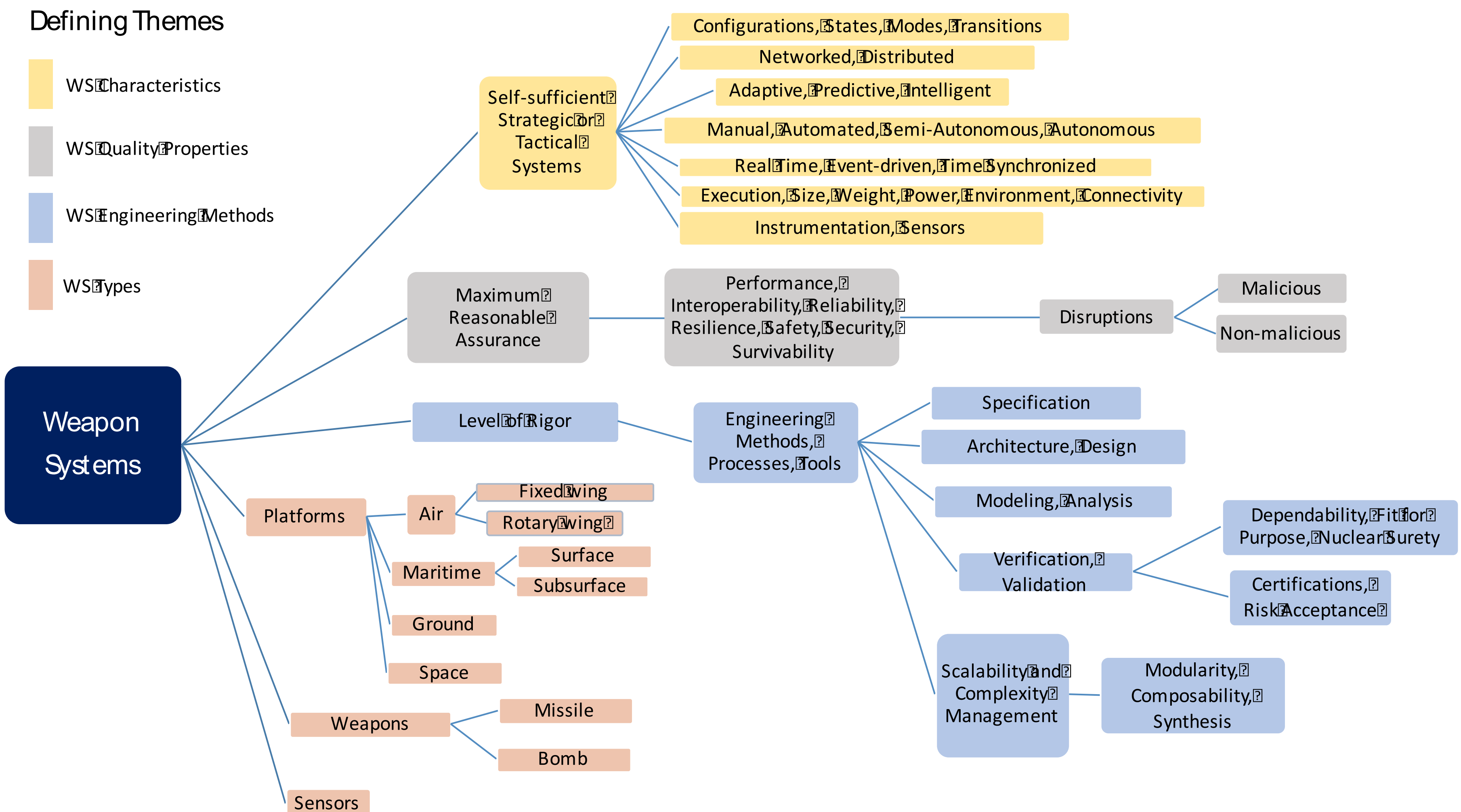
- Security of the Intended System Function
- Security Function of the System
- Security of Life Cycle Assets

While processes help, the quality and effectiveness of risk mitigation planning, judgement, "What we call 'requirements' determines a great deal – almost everything – about the risks we need to manage" ~ AT&L Memorandum, Jan 2017

Section 2 – Concept and Principle Base

Weapon Systems Characterization

Intentionally destructive delivery of lethal force

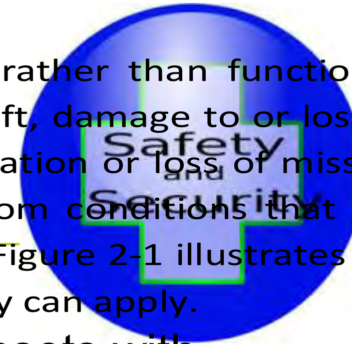


MITRE

interactions, as well as members of the general public.

Although this definition is broad, it focuses exclusively on physical, rather than functional, consequences. However, for systems such as non-recoverable spacecraft, damage to or loss of equipment may be meaningful only insofar as it translates into degradation or loss of mission objectives. Therefore, for the purposes of this handbook, freedom from conditions that can cause loss of mission (LOM) is also included in the definition of safety. Figure 2-1 illustrates the scope of potentially impacted populations to which the concept of safety can apply.

Security Working Definitions



Each adapted from NASA (NASA System Safety Handbook VOL1, 2011)

- **Security**
  - Freedom from those conditions that can cause loss of assets with unacceptable consequences
    - Stakeholder judgement
- **Secure System**
  - A system that for all states, modes, and transitions is deemed adequately secure
    - i.e., demonstrates "freedom from those conditions ..."
- **Adequate Security**
  - Meets the minimum tolerable level of security performance
  - Maximizes security performance relative to the impact of commitments that must be made and/or degradation of system performance

Figure 2-1. Impacted Populations within the Scope of Safety

Safety

Safety is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. In any given application, the specific scope of safety must be clearly defined by the stakeholders in terms of the entities to which it applies and the consequences against which it is assessed. For example, for non-reusable and/or non-recoverable systems, damage to or loss of equipment may be meaningful only insofar as it translates into degradation or loss of mission objectives.

Predominant Views of System Security

- **Security of the Intended System Function**
  - Security-driven constraints on all system functions
    - Avoid, eliminate, tolerate, forecast
      - defects, exposure, flaws, weaknesses

- **Security Function of the System**
  - Security functions that provide system protection capability
    - Mechanisms that constitute controls, countermeasures, features, inhibits, overrides, safeguards

- **Security of Life Cycle Assets**
  - Security for data, information, technology, methods, and other assets associated with the system throughout its life cycle

MITRE

Concept and Principle Coverage

- System, security, and adequate security
- Assets and reasoning about asset loss
- Secure system function
- Strategy for secure system function
- Risk, issue, and opportunity management

Ultimately – system security is about assets and the effect of their loss relative to the system-of-interest ands its enabling and supporting systems

Section 3 – Method

Generalized Security Requirements Elicitation, Analysis, Negotiation Method

T R A C E A B I L I T Y

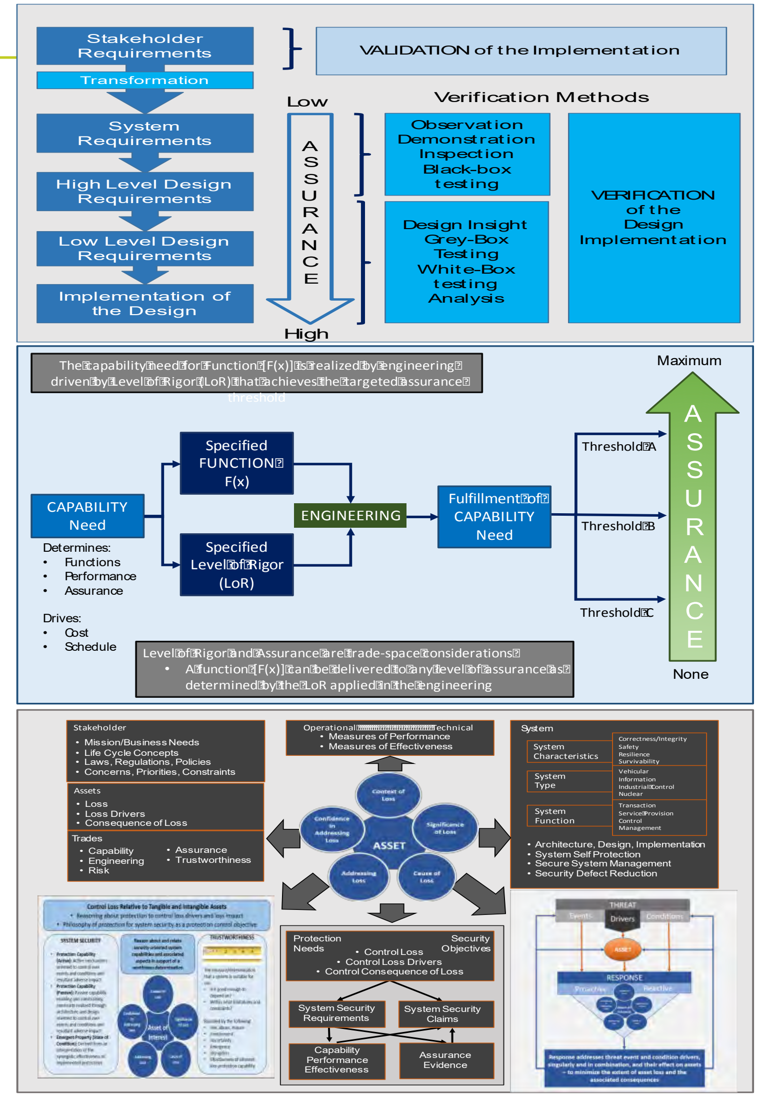
Determine Security Context
- Identify stakeholder roles, responsibilities and authorities
- Identify stakeholder, system and engineering objectives, constraints and concerns
- Define system life cycle concepts
- Record traceability between decision making authority, life cycle concepts and stakeholders objectives

Determine Asset Loss Consequences
- Identify stakeholder, system, and life cycle assets
- Establish valuation of assets and determine consequences of assets loss
- Rank and prioritize the assets based on criticality and precedence
- Record traceability between assets, associated loss consequences, valuation, and stakeholders

Assess Susceptibility to Adversity
- Account for certainty, emergence, speculation, and uncertainty
- Identify events and conditions that lead to assets loss consequences
- Determine tolerances for risk and loss
- Refine criticality and precedence ranking of assets and susceptibility to loss
- Record traceability between events and conditions, assets, and associated loss consequences

Define Security Objectives and Protection Needs
- Identify security objectives and success criteria
- Establish protection needs
- Record traceability between security objectives, success criteria, and protection needs for an asset, asset type, or asset class

Develop Security Requirements
- Develop security requirements at the appropriate level of granularity for security function and security-oriented constraints
- Define verification methods that includes level of rigor and level of assurance
- Record traceability between security requirements, and applicable sources
- Validate security requirements
- Record security requirements in a system requirements baseline



MITRE

Section 4 – Viewpoint Considerations

System Requirements "Viewpoints"

MIL-HDBK-520A – System Requirements Document (SRD) Guidance

A.3 System or Subsystem Requirements

A.3.1 Required states and modes

A.3.2 System or subsystem functional requirements

A.3.3 System external interface requirements

A.3.4 System internal interface requirements

A.3.5 System internal data requirements

A.3.6 Adaptation requirements

A.3.7 Environmental, Safety, and Operational Health (ESOH) requirements

A.3.8 Security and privacy requirements

A.3.9 System environment requirements

A.3.10 Computer resource requirements

A.3.11 System quality factors

A.3.12 Design and construction constraints

A.3.13 Personnel-related requirements

A.3.14 Training-related requirements

A.3.15 Logistics-related requirements

A.3.16 Other requirements

A.3.17 Packaging requirements

A.3.18 Statutory, regulatory, and certification requirements

A.3.19 Precedence and criticality of requirements

A.3.20 Demilitarization and disposal

A.4 VERIFICATION PROVISIONS

A.4.1 Verification methods

A.5 REQUIREMENTS TRACEABILITY

A.5.1 Traceability to capability document or system specification

A.5.2 Traceability to subsystems requirements

Although security requirements are explicitly called out in A.3.8, security-driven concerns regarding *Security of the Intended System Function* affect content throughout A.3, A.4, A.5

Revised Viewpoints

4. Secure System Function Requirements Considerations

4.1 System States and Modes
4.2 System Functions
4.3 Communication
4.4 System Interfaces
4.5 Design and Construction Constraints
4.6 Safety
4.7 System Environment
4.8 System Configuration and Adaptation
4.9 Computing
4.10 System Quality Factors
4.11 Maintenance
4.12 Logistics
4.13 Packaging, Labeling, and Handling
4.14 Personnel
4.15 Training
4.16 Statutory, Regulatory, and Certification
4.17 Retirement and Disposal
4.18 Priority and Criticality of Requirements
4.19 Other Requirements
4.20 Verification
4.21 Traceability

- **Each viewpoint provides a "lens" into the system to provide an explicit statement of a need to be met**
  - **Proactive**
  - **Reactive**
  - **Constraining**
- **The requirements for secure system function have two generic forms**
  - **Explicit function**
  - **Explicit constraint**

Conclusion

- **SSE and what it represents as a necessary part of SE remains an open-ended question**
  – We continue to evolve our thinking towards an optimal end state

- **Challenges remain and are primarily rooted in**
  – Absence of system-oriented security perspective
  – Viewing security through an operations, organizational, and IT lens
  – Insufficient leveraging from other disciplines

- **This work is oriented to closing the gap between SE and SSE with focus limited to requirements elicitation, analysis, and negotiation for secure system function**

MITRE

Future Work

- **Explicitly bring in resilience considerations**
- **Add depth to Section 4 viewpoint considerations**
- **Elaborate on the tasks in each of the activities presented in the Section 3 generalized method**
- **Explore other specialties and disciplines and incorporate their concepts, principles, and methods to more effectively achieve secure system function when operating in contested cyberspace**
  - System safety
  - Fault tolerance
  - Reliability

NDIA SE Conference 2017

NDIA Cyber Resilient & Secure Weapon Systems April 2017 Summit Highlights

Holly Dunlap
Raytheon
NDIA SSE Committee Chair
Holly.Dunlap@Raytheon.com

Event Purpose

NDIA Systems Engineering Division held a "Top SE Issues Workshop", August 2016

Cyber Resilient & Secure Weapon Systems was identified as a Top SE Issue

System survivability in a cyber contested operational mission environment is critical. We need to elevate the system security risk to the program risk register to ensure a security focus. We need well defined methods, processes, standards, metrics and measures, along with skilled professionals to integrate system security into our product development lifecycle.

*NDIA – National Defense Industrial Association

Summit Agenda

NDIA

Systems Engineering Cyber Resilient and Secure Weapon System Summit

Agenda

April 18 – 20, 2017
The MITRE Corporation, McLean, VA

NDIA

Tuesday, April 18, 2017

7:00 am – 8:00 am **Registration Check-in**

8:00 am – 8:15 am **Welcome**
- Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

8:15 am – 9:00 am **Keynote Address: OSD Systems Engineering**
- Ms. Kristen Baldwin, *Acting Deputy Assistant Secretary of Defense for Systems Engineering*

9:00 am – 9:45 am **Keynote Address: Air Force Perspective, Cyber Resiliency Office for Weapon Systems (CROWS)**
- Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*

9:45 am – 10:30 am **OSD Cyber Resilient Weapon Systems Workshop Series, Summary of Discoviries**
- Ms. Melinda Reed, *DASD (SE) Deputy Director Program Protection*

10:30 am – 10:45 am **Networking Break**

10:45 am – 11:15 am **Keynote Address: Air Force Perspective**
- Mr. Peter Kim, *Air Force Chief Information Security Officer*

11:15 am – 12:00 pm **Mission Assurance Through Integrated Cyber Defense**
- Col William Bryant, USAF, *SAF/A6 CIO*

12:00 pm – 1:00 pm **Lunch on Own (MITRE Cafeteria)**

1:00 pm – 2:45 pm **Industry Best Practices to Integrate Cyber Resiliency and Security into Standard Methods & Processes**
- Facilitated by: Mr. Eric Rickard, *Vice President, Cyber Futures – Platform Security, Booz Allen Hamilton*

2:45 pm – 3:15 pm **Networking Break**

3:15 pm – 4:00 pm **Strategic Systems of Systems and Mission Thread Analysis Discussion**
- Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*

4:00 pm – 4:30 pm **Cyber Resiliency Architecture Process for Weapon Systems**
- Ms. Suzanne Hassell, *Raytheon Company*

4:30 pm – 5:00 pm **Wrap-up and Close the Day**
- Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

Wednesday, April 19, 2017

8:00 am – 8:15 am **Welcome and Agenda Review**
- Ms. Holly Dunlap, *Event & NDIA System Security Engineering Chair*

8:15 am – 10:15 am **Services Perspective, Plans, Initiatives, Message to Industry**
- Army Presenter: Mr. Doug Wiltsie, Army SES, *Executive Director, SoSE&I*
- Navy Presenter: CAPT Albert Angel, USN, *Navy Cybersafe Director*

10:15 am – 10:30 am **Networking Break**

10:30 am – 11:15 am **High Assurance Cyber Military Systems (HACMS)**
- Mr. Ray Richards, *I2O Program Manager, DARPA*

11:15 am – 12:00 pm **Industry: Our Experience in Working with Government Customers on Cyber Resilient & Secure System**
- Facilitated by: Mr. Irby Thompson, *President Star Lab Corp.*

12:00 pm – 1:00 pm **Lunch on Own (MITRE Cafeteria)**

1:00 pm – 1:30 pm **Company's Approach to Creating One Voice to Government**
- Facilitated by: Rick Foster, *Lockheed Martin Corporation*

1:30 pm – 2:15 pm **Industry – Acquisition and Request for Proposal Discussion**
- Ms. Holly Dunlap, *Raytheon Company*

2:15 pm – 3:15 pm **Panel Discussion: In Working with Government Customers, What Does the Current State and Ideal Future State Look Like? What are Priority Gaps that Need to be Addressed?**
- Facilitated by: Mr. Neil Adams, *Principal Director Defense Systems, Draper*

3:15 pm – 3:45 pm **Networking Break**

3:45 pm – 4:15 pm **Explore Identifying Strategic Topics Where Enhanced Government and Industry Communication and Collaboration is Needed**
- Facilitated by: Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*

4:15 pm – 4:45 pm **Discuss Mechanisms to Enable Better Government and Industry Communication and Collaboration**
- Facilitated by: Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*

4:45 pm – 5:00 pm **Wrap-up and Close the Day**
- Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

NDIA

Thursday, April 20, 2017

8:00 am – 8:15 am **Welcome**
- Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

8:15 am – 8:45 am **2016 Government and Industry Cybersecurity Testing Collaboration Highlights**
- Dr. Robert Tamburello, *(Acting) Director, National Cyber Range*
- Mr. Joe Manas, *Raytheon Company, NDIA Test & Evaluation Division Chair*

8:45 am – 9:45 am **Panel Discussion: Cybersecurity Testing – How Do We Work Towards Producing the Right and Consistent Evidentiary Information to Enable Decision Making?**
- Facilitated by: Mr. Joe Manas, *Raytheon Company*

9:45 am – 10:15 am **Sustainment**
- Mr. Jonathan Kline, *CTO, Star Labs Corp.*

10:15 am – 10:30 am **Networking Break**

10:30 am – 11:00 am **Legacy Systems Lessons Learned**
- Mr. Bob Lozano, *Raytheon Company*

11:00 am – 12:00 pm **Safety Community Cyber Considerations: Government Perspective**
- Mr. Donald Hanline, *Safety Engineer, AMCOM*
- Ms. Myesha Dabney, *Safety Engineer, NOSSA*

12:00 pm – 1:00 pm **Lunch on Own (MITRE Cafeteria)**

1:00 pm – 1:45 pm **FY16 Section 1647, Cyber Resiliency Assessments**
- Dr. Mark Lukens, *Senior Analyst for Cyber Programs, Office of the Undersecretary of Defense, (AT&L)*

1:45 pm – 2:00 pm **DoD Risk, Issue, and Opportunity Management Guide**
Industry Thoughts on How to Integrate System Security and Cybersecurity
- Mr. Kevin Plyler, *General Dynamics*

2:00 pm – 2:30 pm **Cyber in Advanced Manufacturing**
- Ms. Kaye Ortiz, *Defined Business Solutions*

2:30 pm – 2:45 pm **Networking Break**

2:45 pm – 3:15 pm **Safeguarding Covered Defense Information: Government Perspective**
- Ms. Mary Thomas, *DPAP*
- Ms. Vicki Michetti, *CIO*

3:15 pm – 3:45 pm **Safeguarding Covered Defense Information: Industry Perspective**
- Mr. Jeff Dodson, *Global CISO VP Cybersecurity, BAE Systems*

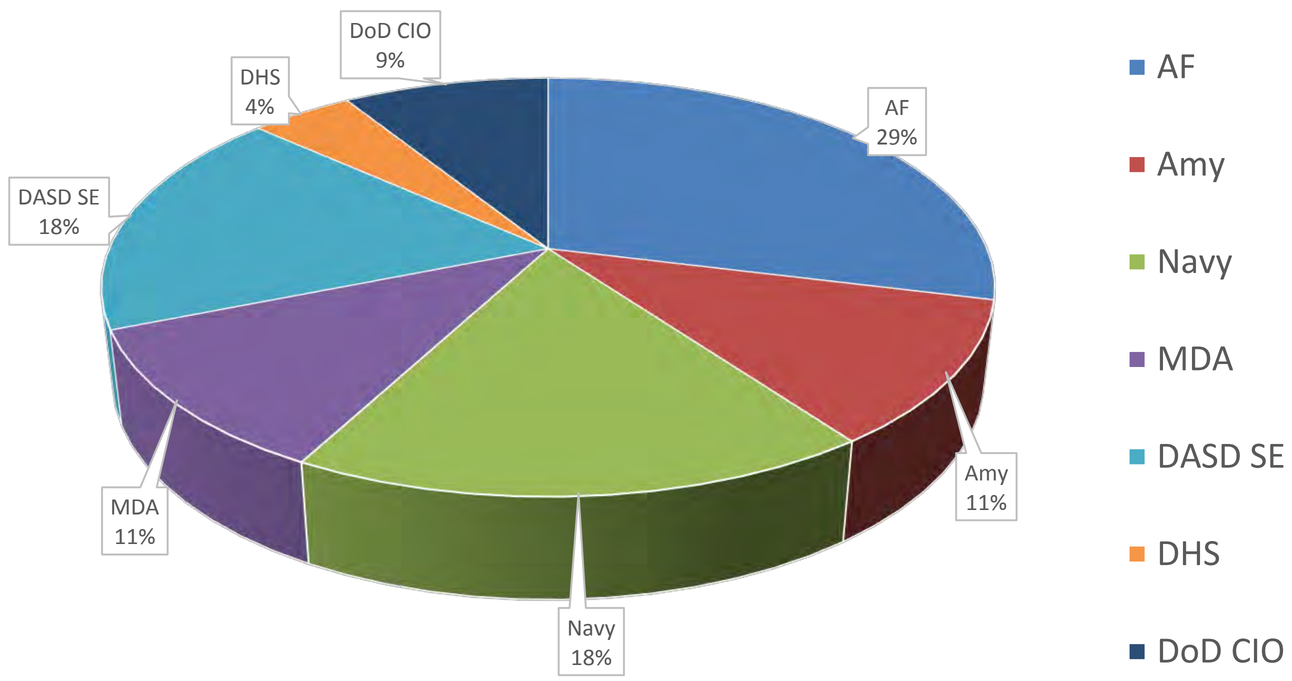
3:45 pm – 4:00 pm **Final Thoughts and Wrap-up**
- Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

The NDIA has a policy of strict compliance with federal and state antitrust laws. The antitrust laws prohibit competitors from engaging in actions that could result in an unreasonable restraint of trade. Consequently, NDIA members must avoid discussing certain topics when they are together – both at formal association membership, board, committee, and other meetings and in informal contacts with other industry members: prices, fees, rates, profit margins, or other terms or conditions of sale (including allowances, credit terms, and warranties); allocation of markets or customers or division of territories; or refusals to deal with or boycotts of suppliers, customers or other third parties, or topics that may lead participants not to deal with a particular supplier, customer or third party.

Who Attended

- **175 Attendees**
  - 33% Government
  - 67% Industry

Government Representation



Industry Representation

Raytheon	DBS
NGC	Electronic Warefare associates
MITRE	Ensility
BAE Systems	GTRI
Boeing	INL
Booz Allen	Innovative Defense Technologies
Draper	Riverside Research
BAH	SAIC
Lockheed	SEI
Star lab	SRI International
Aerospace Corporation	STR
General Dynamics	Synexxus
Rolls Royce	Tri Guard Risk Solutions
Textron	
US falcon	
Vencore	
ACET	
ARAR Technology	
BDA/DE	

What We Talked About

Word Cloud

"Cyber Resiliency" in all 27 Topics

27:
Cyber Resiliency

10:
Risk Based Analysis
Mission Thread Analysis
Architecture
Carbon Based Units
Taxonomy

8:
RFP Language
Legacy Systems
Techniques that Work
Culture

7:
Test and Evaluation
Compliance Checklist

6:
SE Responsibility

5:
SSE Role
Domain Expertise
Risk Management Framework
Bake-in
Measurement
Supply Chain
Sustainment

Key Take Away from Services & OSD

- **Affects everyone, responsibility of everyone**
- **SE responsibility to design and deliver systems that are resilient to cyber threat.** Transitioning from Network IT responsibility due to cyber association to SE responsibility to integrate security focus / risk management into the systems we design and deliver.
- **Over 70% of systems in sustainment, how is sustainment addressed**
- **Industry needs to stop promoting magic beans**
- **Acquisition guidance needs to transition to contracts**

- **Biggest challenge is the Carbon Based Units (People)**
- **Risk Management Framework Results**
  - Need to:
    - Improve risk focus instead of compliance & checklist focus
    - Domain expertise is imperative
    - Converge to eliminate duplication and conflicts
    - Test early & often.
  - Not identifying risks correctly, security is coming from IT backgrounds when the security is being applied to mission systems

Challenges from Government to Industry

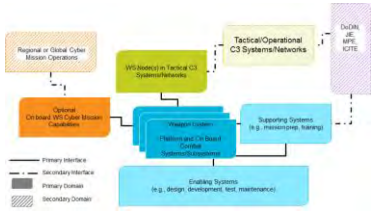
- **Government wants examples from Industry:**
  - Issues to learn from
  - Techniques that work
- **Need help from Industry:**
  - How to improve security with technology that doesn't require redesign
  - How to improve security quickly and efficiently
  - Increase customer confidence in the resiliency & security of the systems we deliver
- **Together we need to address:**
  - What does cyber resiliency look like?
  - How do we measure cyber resiliency?
  - How do we execute and implement cyber resiliency?

Additional key findings:

- Trying to do risk management in an policy/process environment. Need to develop use cases and test cyber system security risk management methods.
- Knowledge of how the system is designed is knowledge of where the risk is, Government does not always have that detail. Government does not fundamentally know how these systems work nor how they are being used. Need help from industry to better understand the system design & capabilities.
- We need to stop taking a reactive approach to our solution. Move away from threat based, b/c it's considered reactive. How do you get the "good" guys to look forward.

Design Patterns, Standards and Methods

What system elements or properties do we acquire?



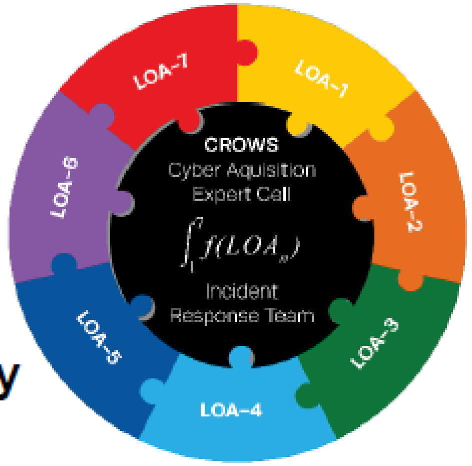
Allocate cybersecurity requirements to the system architecture and design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:

1. **Manages access** to, and use of the system and system resources;
2. Is **configured to minimize exposure** of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment;
3. Is structured to **protect** and **preserve system functions** or resources, e.g., through segmentation, separation, isolation, or partitioning;
4. **Monitors, detects** and **responds** to security anomalies;
5. **Maintains priority system functions** under adverse conditions; and
6. **Interfaces with DoD Information Network** or other external security services.

Draft DTM 118 "Cybersecurity in the Defense Acquisition System" establishes a threshold for what to address

AF CyberCampaign Plan: WeaponSystem Focus

- 7 Lines of Action (LOAs)
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: "Bake-In" Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support



People, Processes, & Products

- Cyber Squadron Initiatives
- Test & Evaluation (infrastructure & capability growth)
- Industrial Control Systems/SCADA cyber protection measures

Ensure mission success in a cyber contested environment

Industry Themes for Government

- **Policy is mudding the waters**
  - Lots of guidance & standards.
- **Number of Authorities**
  - Unclear of all the relevant & related authorities
  - How many authorities? Who do we listen to and take direction from?
  - Inconsistency in direction
- **Controls and Requirements**
  - Taxonomy
  - Need to be founded and traced to real world scenarios.
- **Challenge Assumptions**
  - Understanding of the CONOPS and how the system is protected throughout the lifecycle.
- **We need to understand the priorities & protection boundaries.**
- **Priorities need to be reflected in RFP and incentivized**

Key Take Aways

- **Focus on mission assurance & not compliance.**
- **Must understand how systems function and the CONOPS**
- **Security must be integrated within Systems Engineering & throughout the system lifecycle**
- **Trace controls (“counter-measure”) to specific real-world attack**
- **Cybersecurity testing needs a more structured & integrated approach**
  - Not based on test till the money runs out.
  - How do we produce evidence that provides increased confidence in the system?
- **Need government support to include system security as part of proposals (Section L & M)**

Key Take Aways

- **Need to collaborate to work smarter.**
  - Both Government & Industry want to work together.
- **Everyone is learning. Need to provide customers with risk, cost, performance based trade options.**
- **Mission thread analysis – move from information assurance to mission assurance**
  - Deliver mission assurance through resiliency
  - Assume the attacker is already in the systems.
- **How do we create design standards as enablers and not restrainers?**
- **Post cyber event often results in refining and defining roles & responsibilities and (re)organizational structure. Communication and process are a common theme.**
- **Convergence (integration) before divergence.**
  - Policy, standards, guidance

Specific Actionable Opportunities

- **DoD Risk, Issue, and Opportunity Management Guide**
  - Cybersecurity, Opportunity to shape.
- **Safety Community**
  - JOINT SERVICES-SOFTWARE SAFETY AUTHORITIES
  - Investigate Cyber Considerations - Joint Weapons Software System Safety Process
- **Systems Engineering Research Center (SERC)**
  - University of Virginia
  - Resilience research efforts, analytically-based decision-support tools
  - Seeking industry partnership to test methods and tools
  - Peter A. Beling
Associate Professor and Interim Chair
Department of Systems and Information Engineering
University of Virginia
434-982-2066
beling@virginia.edu

20th Annual Systems Engineering Meeting

23-26 October 2017

HSI Best Practice Standard

Patrick M. Fly
The Boeing Company

Stephen C. Merriman
SCMerriman Consulting LLC

Background

- **1984:** NATO DRG Workshop on Applications of Systems Ergonomics to Weapon System Development
- **1986:** US Army establishes MANPRINT program.
- **2003:** DoD requires HSI on major system acquisition programs (DODD 5000.01/DODI 5000.02)
- **2005:** DoD establishes Joint HSI Working Group
- **2005-2007:** Development of HSI Program Plan DID (DI-HFAC-81743)
- **2007:** USAF establishes AFHSIO for policy, advocacy and oversight
- **2008:** DOD establishes Joint HSI Steering Committee
- **2008-2011:** Development of HSI Report DID (DI-HFAC-81833)
- **2010:** DoD, USAF and US Navy release/update HSI Management Plans
- **2012:** DoD establishes HSI Standard Working Group
- **2016-Present:** SAE International Leads Development of HSI Standard

Background

- OSD and Service HSI efforts have largely focused on “in-house” (Government) activities.
- Only one Service has a current HSI implementing regulation (AR 602-2).
- The SAE International G-45 Human Systems Integration committee has focused on developing and improving DoD and industry HFE and HSI requirements since 1976.
- SAE International was selected in 2016 to lead development of a new industry HSI Standard.
- Development of a new HSI Best Practice Standard is a challenge due to its complexity and the short development schedule requested by DoD.

Why Do This?

- DODD 5000.01 and DODI 5000.02 require the Services to “plan for and implement HSI beginning early in the acquisition process and through the product life cycle.”
- We have an HSI Program Plan DID…
- We Have an HSI Report DID…
- Everyone “Knows” We Should “do HSI” on Acquisition Programs….

But…..

- Application of HSI in contracts is uneven…
- Lots of people think HSI is HFE….
- Most times, a full HSI program is not contracted for…
- Sometimes an HSI Plan is required, but execution is not….

Approach

- Build on HFE, Safety and Training domains; they already have documented standards.
- Force Protection, Manpower, Personnel, and Habitability domains have neither DoD nor industry standards….So, the SAE committee documented task assumptions for the domains that have no documented standards.
- The standard is divided into two major sections;
  - Informational, describing HSI, its domains, and activities
  - Guidance, specifying those HSI activities that "shall" or "should" be conducted on system acquisition programs

Standard Organization

1. Forward
2. Background
3. Terms and Definitions
4. General Requirements (HSI and Domain Overviews)
5. Detailed Requirements – HSI Process (see next slide)
6. Notes
7. Appendices

Organization (Section 5)

- Human Systems Integration Process
- Program Initiation
- Pre-Milestone B Activities
- HSI Program Advocacy and Coordination
- HSI Tradeoffs
- Requirement Refinement, Decomposition and Flow-Down
- HSI in Subcontracting
- System Architecture Support
- Risk Issue and Opportunity Identification and Management
- HSI Analysis
- Preliminary and Detailed Design and Procedure Support
- HSI Requirement Verification
- HSI in Sustainment
- HSI Documentation and Product Handoffs
- Management and Customer Coordination, Progress Reporting
- HSI Quality Control

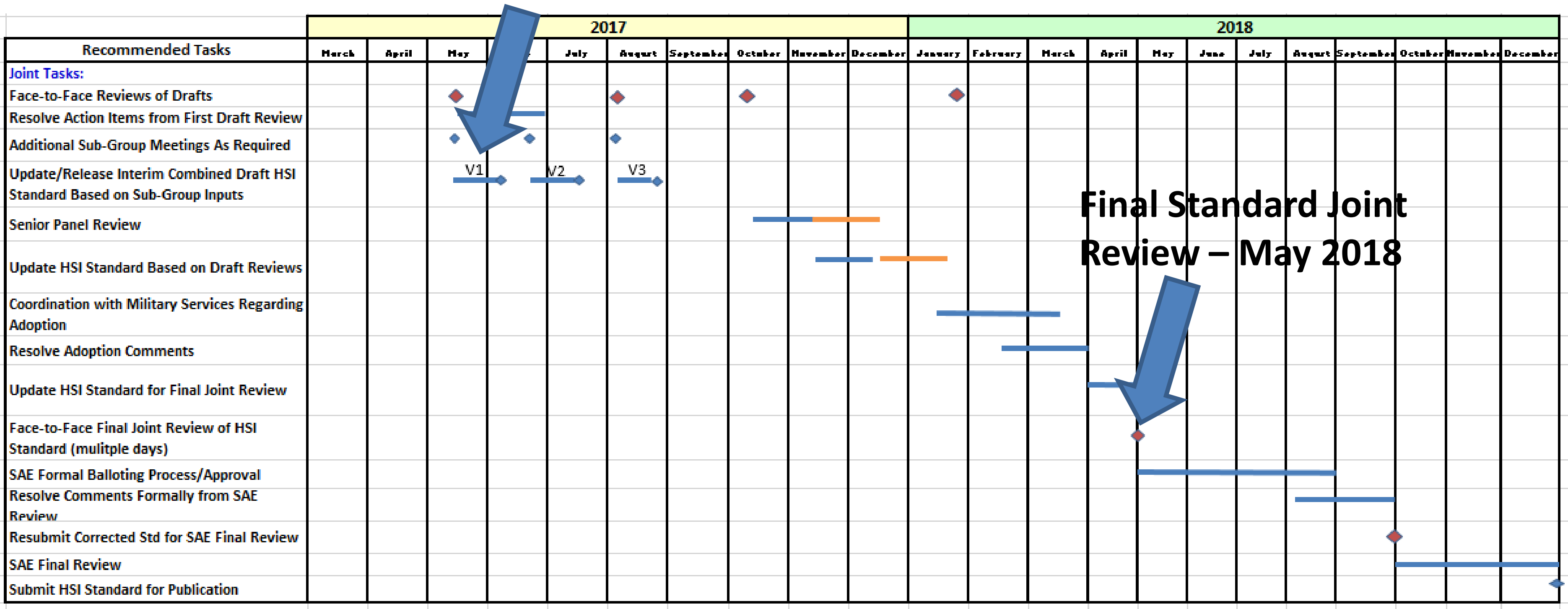
Organization (Section 5)

- Human Systems Integration Process
- Program Initiation
- Pre-Milestone B Activities
- HSI Program Advocacy and Coordination
- HSI Tradeoffs
- Requirement Refinement, Decomposition and Flow-Down
- HSI in Subcontracting
- System Architecture Support
- Risk Issue and Opportunity Identification and Management
- HSI Analysis
- Preliminary and Detailed Design and Procedure Support
- HSI Requirement Verification
- HSI in Sustainment
- HSI Documentation and Product Handoffs
- Management and Customer Coordination, Progress Reporting
- HSI Quality Control

Questions?
Additions?

Development Schedule

First Standard Review- May 2017



Challenges

- Many different and interesting topics to address!
- Not many contractor HSI Leads, experienced with leading “full HSI” programs (all domains)
- Not many contractor SMEs experienced in Manpower, Personnel, Habitability, Force Protection and Survivability
- A two-year standard development schedule is desired by DoD.

Current Status

- First full-draft standard was reviewed on May 22, 2017. A few areas still need some work…
- 95% solution by August, 2017 face-to-face G-45 meeting in Marietta, GA.
- Assessment by a Senior Review Group is scheduled for November, 2017.
- Final standard should be ready for SAE balloting and DoD adoption review by April, 2018.
- Companion DoD Handbook is expected soon thereafter….

Significance of HSI Standard

- The DoD (and other Federal Agencies) will have a contractible standard for HSI on major system acquisition contracts (15 years after DoD established the HSI requirement!)
- This standard builds upon, and is consistent with, existing DOD Policy and HSI DIDs.

Still to be Done

- Author Domain standards for Manpower, Personnel, Habitability and Force Protection and Survivability domains!
- DoD monitor HSI Standard Implementation, Effectiveness, Cost, and Benefits…. once the standard has been adopted.

Questions/Comments?

Please contact:

Stephen C. Merriman, scmerriman@tx.rr.com, 214-533-9052 (Cell)

OR (for SAE/Administrative Questions)

Sonal Khunti, Aerospace Standards Specialist

1 York Street, London, UK W1U 6PA

Office +44 (0) 207 034 1251

Mobile +44 (0) 7590184521

Email skhunti@sae.org

Web Site: www.sae.org

And Remember!

Systems of Systems Engineering Technical Approaches as Applied to Mission Engineering

Dr. Judith Dahmann
Dr. Aleksandra Markina-Khusid
Janna Kamenetsky
Laura Antul
Ryan Jacobs

Approved for public release. Distribution unlimited 17-3712-15

Topics

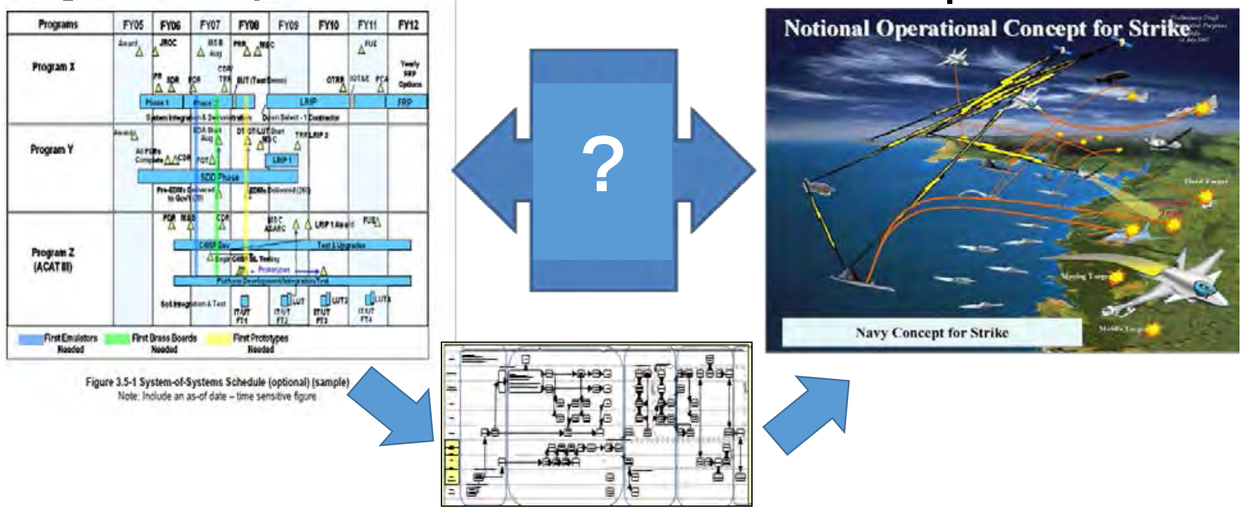
- **Mission engineering (ME)**
- **The relationship between system of systems engineering (SoSE) and ME**
- **Particular challenges of SoSE applied to missions**
- **Some SoSE technical approaches which address these challenges**

Mission Engineering Challenge

- Systems are acquired to meet user needs in a mission context
- Mission operations are supported by sets of systems (or systems of systems) which work together to achieve mission objectives
- Systems supporting each role in a mission (i.e. kill chain) will vary over the course of the operation and be used for multiple missions

System Acquisition

Operations



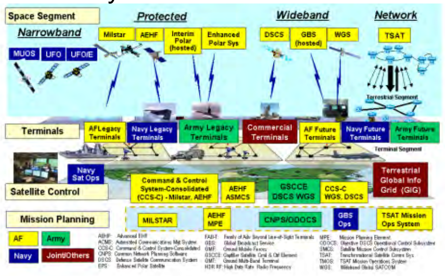
Mission/SoS Architecture/Engineering

Mission Engineering is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects

Defense Acquisition Guide Ch 3

Systems of Systems in Defense

Military Satellite Communications



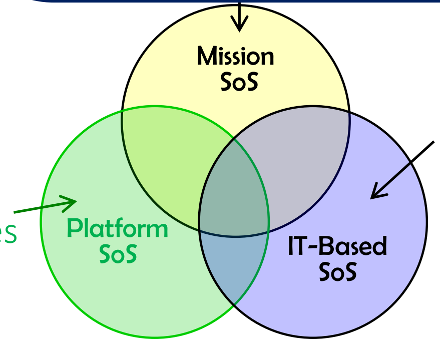
Missions

Sets of systems working together to provide a broader capability or mission

Tactical Vehicle

Platforms

A military platform (e.g. ship, aircraft, satellite, ground vehicle) equipped with independent systems (e.g. sensor, weapons, communications) needed to meet platform objectives



Operations Center

Information Technology

Networked information systems to support operations within or across platforms or systems to meet mission or capability objectives

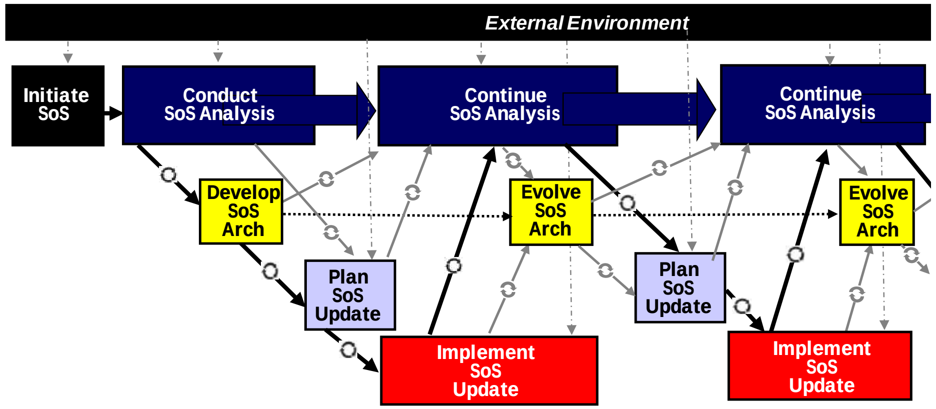
Considerations in mission SoS

- **Mission environment**
  - Mission context - variable physical environments, threats and non-material elements - critical in driving SoS for missions
- **Composition**
  - Execution of missions is based on the employment of the set of systems available and appropriate for the mission environment
  - Performance needs of a system in the Mission SoS may vary depending on the performance of other systems in the SoS (‘AKA ‘Float and Flow’)
- **Mission ‘webs’ versus ‘threads’**
  - While there may be a logical sequence of actions for a mission, in practice there are sets of systems which support missions under different situations

MITRE

SoSE Wave Model Applied to ME

Define the mission including mission threads and mission context (*Includes mission objectives, CONOPs, scenarios, key functionality, threat*)	Conduct SoS Analysis
Identify current systems supporting the mission and how they are employed (*How are we implementing the mission today?*)	
Assess mission performance to assess how well current systems work together meet mission objectives	
Identify gaps from a mission effectiveness perspective and fault isolate the source of gaps	
Identify and assess options for improving the mission effectiveness (*Including changes in how the systems are employed as well as new or different systems, systems updates and non-material considerations*)	Develop SoS Architecture
Guide systems acquisitions, from requirements through implementation to test and maintenance to assure effective mission execution	Plan SoS Update
Conduct mission level integration and test	Implement SoS Updates
Monitor mission effectiveness with changes in mission context, scenarios and threat capabilities	

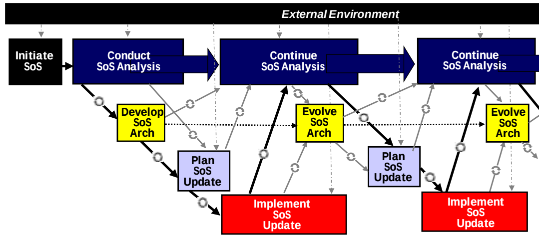


Like other SoS, SoS for missions

- Are ***not 'designed'*** top down, green field systems
- ***Evolve over time*** based on changing capability needs and systems
- Engineering follows the an **evolutionary** '***wave***' process versus traditional system 'V'

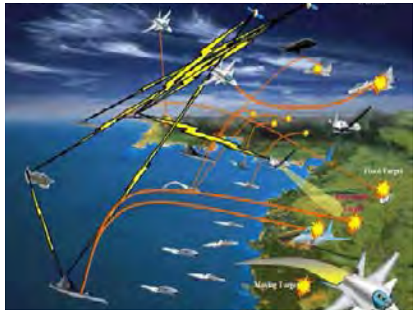
MITRE

Mission Engineering
SoSE Engineering to Meet Mission Objectives



Baseline current SoS Against **Mission Objectives**
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Evaluate options and **trades across the SoS** to improve or sustain mission performance
- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces



Implement changes in systems, integrate and test updated SoS **mission capability**

Negotiate with systems to make changes to support **mission performance** improvement
- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

MITRE

Key Activities in ME Process

A key starting point for ME is understanding current state of mission

- Operational mission objectives and CONOPS (mission threads)
- Current and planned systems
- Identifying critical, priority mission gaps

Technical assessment of options and trades

- Fault isolating sources of gaps
- Assessing alternative approaches to addressing capability gaps

Baseline current SoS Against **Mission Objectives**
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Evaluate options and **trades across the SoS** to improve or sustain mission performance
- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces

Implement changes in systems, integrate and test updated SoS **mission capability**

Negotiate with systems to make changes to support **mission performance** improvement
- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

Tracking implementation, integration and test

- Given independence of systems and development schedules

Planning and funding coordinated changes in systems

- ‘Capability package’ which cross systems owners and development schedules

Key Activities in ME Process

A key starting point for ME is understanding current state of mission

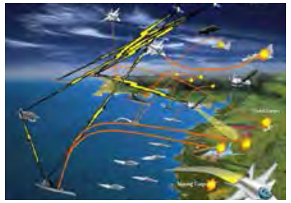
– Operational mission objectives and CONOPS (mission threads)
– Current and planned systems
– Identifying critical, priority mission gaps

Technical assessment of options and trades

– Fault isolating sources of gaps
– Assessing alternative approaches to addressing capability gaps

Baseline current SoS Against **Mission Objectives**
- Assess end-to-end performance of SoS to implement mission **effects/kill chain**
- Identify **gaps**

Evaluate options and **trades across the SoS** to improve or sustain mission performance
- New TTP for the SoS
- Reconfiguration of SoS
- New/upgraded systems
- New system interfaces



Implement changes in systems, integrate and test updated SoS **mission capability**

Negotiate with systems to make changes to support **mission performance** improvement
- Plan **coordinated capability package** for mission improvement
- Coordinate technical, program and budget plans

Tracking implementation, integration and test

– Given independence of systems and development schedules

Planning and funding coordinated changes in systems

– 'Capability package' which cross systems owners and development schedules

MITRE

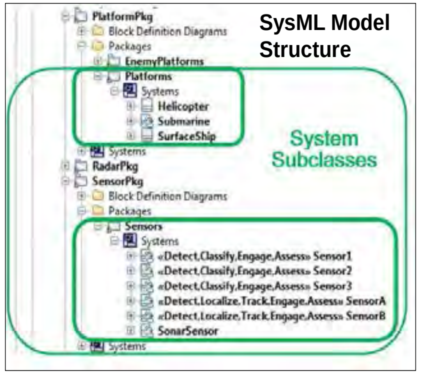
SoSE Technical Approaches to Address ME

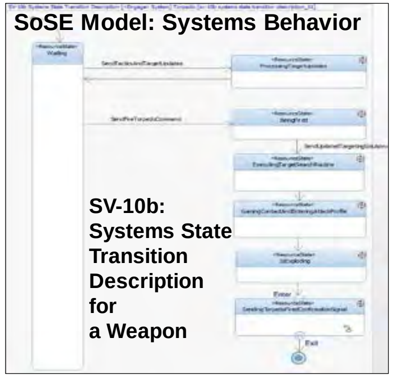
Technical assessment of options and trades
- Fault isolating sources of gaps
- Assessing alternative approaches to addressing capability gaps

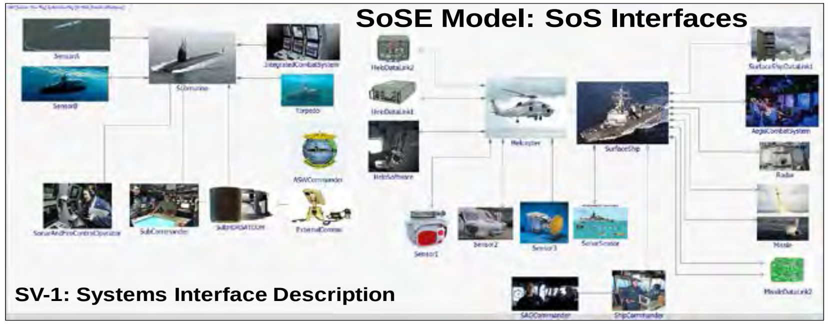
- **Mission environment**
- **Composition**
- **Mission ‘web’**

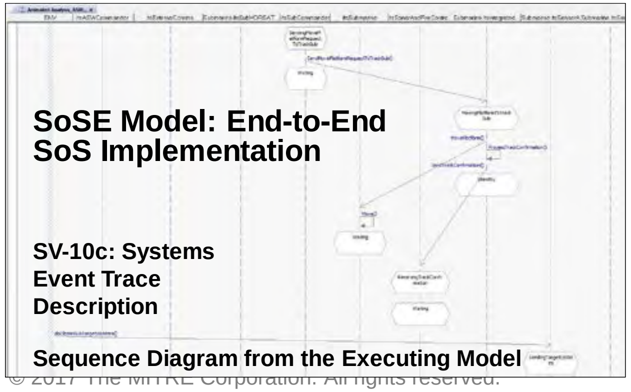
- **Scalable model-based approaches to SoS architecture representation**
- **Analytic approaches to SoS architecture assessment**
- **Assessing impacts of SoS architecture changes on operational mission outcomes**

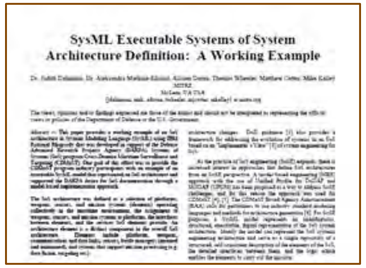
Model-Based SoSE



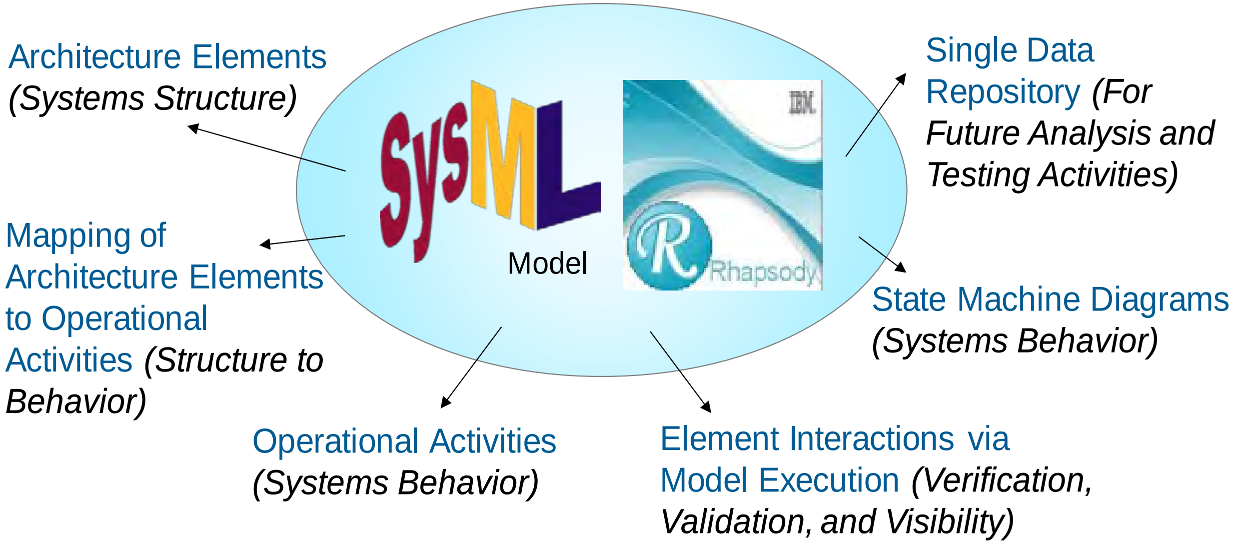







SysML Executable Systems of System Architecture Definition: A Working Example

- **For SoSE purposes, SysML model represents an unambiguous, structured, executable, digital representation of the SoS system architecture**



“SysML Executable Systems of Systems Architecture Definition: A Working Example”

IEEE International Systems Conference
http://2017.ieeesyscon.org/

MITRE

Model-Based SoSE

Why is this important for mission engineering?

- The systems composed into an SoS architecture to support a mission are typically drawn from a **variety of specialty areas** (sensors, weapons, platforms, communications) and **diverse organizations** which bring **various perspectives** to the mission
  - ***Specificity*** provided by models can help avoid misunderstandings about system behavior, system interactions/interfaces (*Have I addressed all the needed interfaces to execute the end to end sequence of actions? Value of executable)*
- A model allows for representation of the complexity of the interrelations among systems in the mission, reflecting the variety of paths in the '***mission web***'
- It is important to have a ***commonly understood representation*** providing both the mission engineer and the constituent systems engineers a cross cutting integrated view across the systems and how they are expected to be employed in a mission context
  - Value of ***standards***-based modeling approaches

Sequence Diagram from the Executing Model

http://2017.ieeesyscon.org/

Scalable Model-Based SoSE

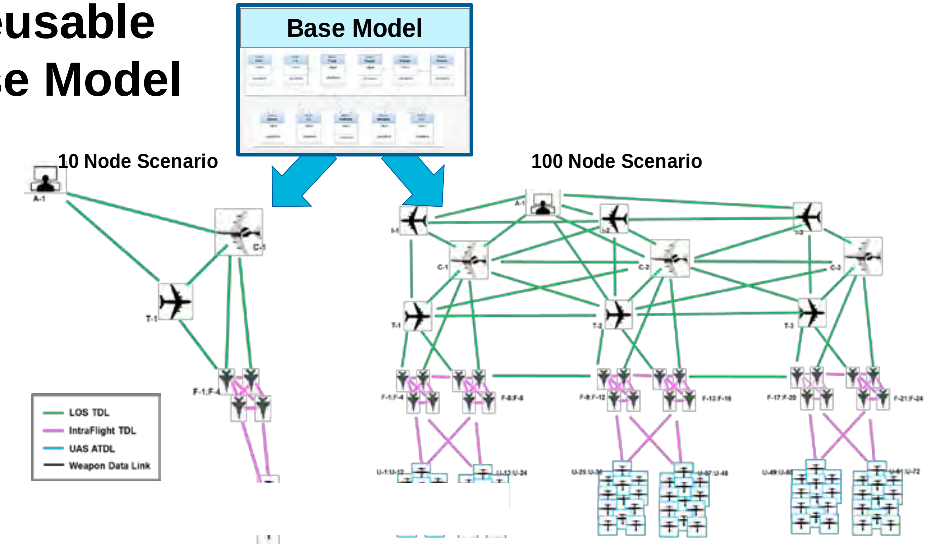
See NDIA paper XYZ for technical details

- **A key enabler of model-based SoSE is the ability to efficiently develop large complex SoS architecture model**

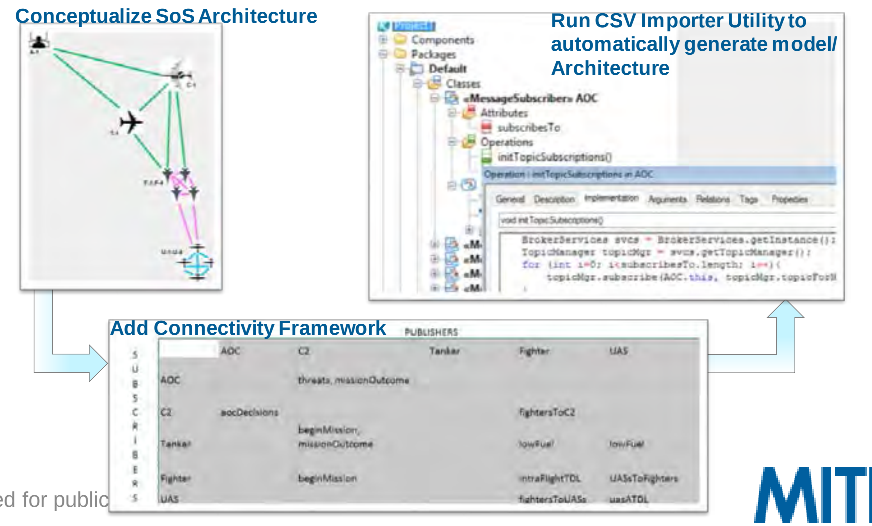
The effort required to build SoS architecture models can be reduced by starting the modeling process with a reusable **base model template**, independently of the architecture size

Tools can facilitate integration of SoS connectivity information into MBE tools, tightening the coupling between subject matter experts (SMEs), software engineers, and analysts -- comma separated variable (CSV) **importer tool**

Reusable Base Model



CSV Importer

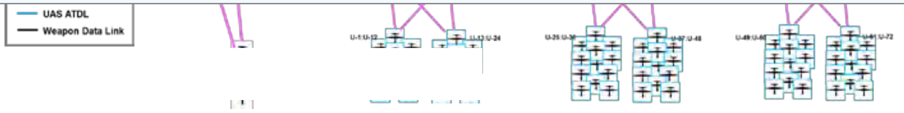


Scalable Model-Based SoSE

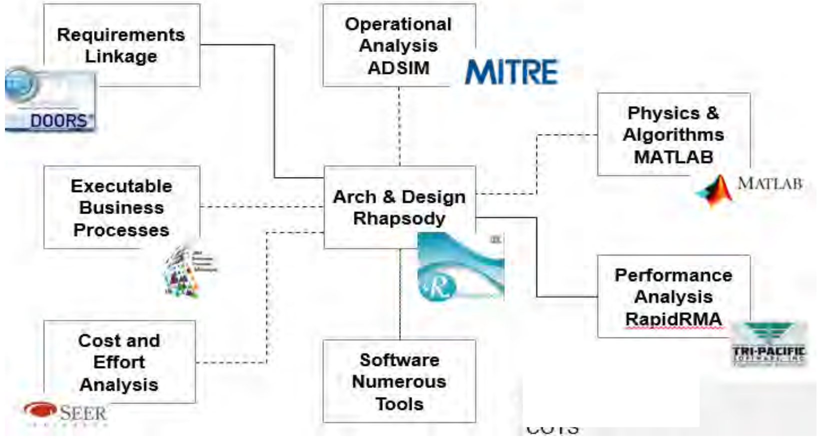
See NDIA paper 19804 for technical details

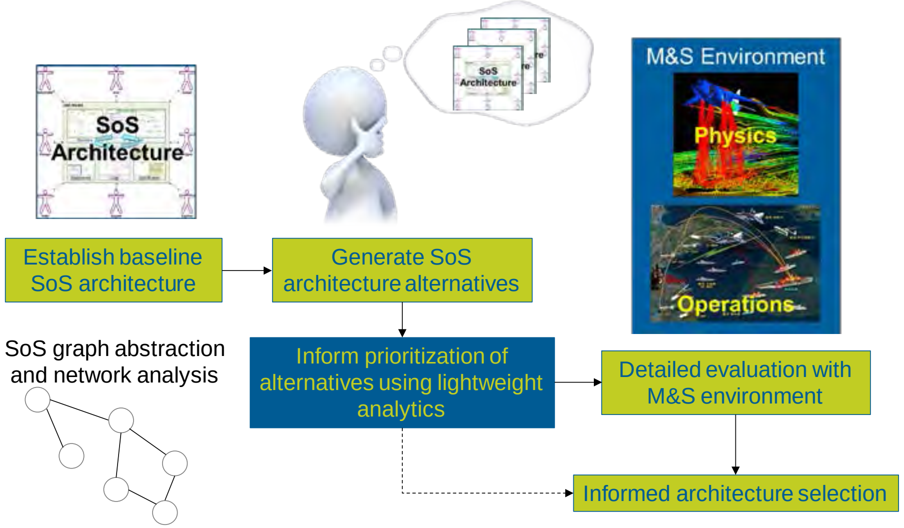
Why is this important for mission engineering?

- Missions can be large and comprise many systems, and the time required to develop a model framework for each mission architecture can raise the ***cost of entry*** for use of models to support mission engineering
- Gathering the ***needed data*** to understand the current state of a large mission can be difficult given the diversity of knowledgeable mission stakeholders.
  - Providing ***intuitive tools*** to allow stakeholders to share knowledge in a way familiar to them can build confidence and speed knowledge gathering
  - Automated transform ***directly into a model*** again lowers the cost of entry for large mission architecture, and reduces likelihood of errors or misunderstandings



Analytic Approaches to SoS Architecture Assessment (1 of 2)



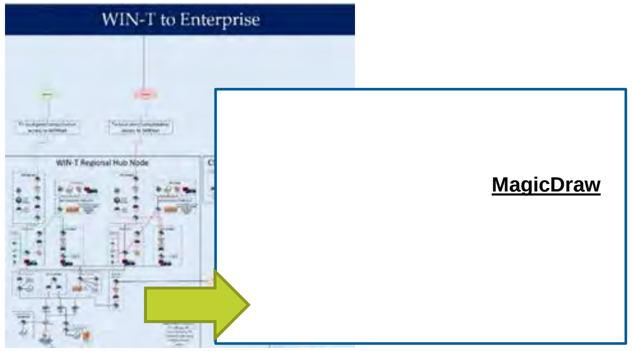


- **Representing SoS architecture in a model opens the options for analysis**
  - Interfacing a SoS model with other tools to assess performance, cost, other aspects of the SoS, provides a shared representation of the architectures for analysis from different perspectives
  - Developing approaches to assess alternative architectures is a challenge for the perspective of scalability
  - How do you identify viable options for more detailed analysis when there is such a large trade space?

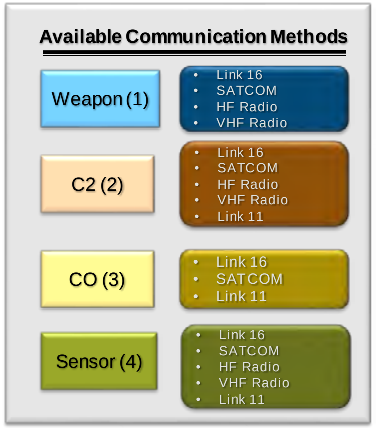
MITRE

Analytic Approaches to SoS Architecture Assessment (2 of 2)

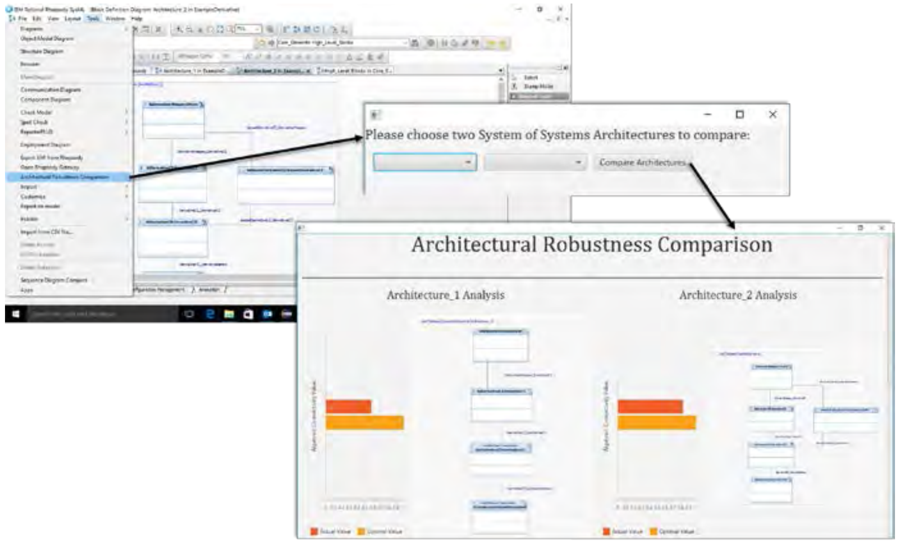
Thread Simulation



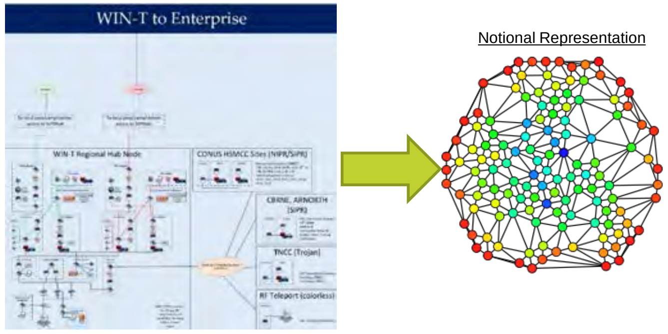
Identify Patterns and Inform Mitigation Strategies



- **Use of architecture data in a graph theoretic analysis**



Graph Theoretic Approach



	VHF Radio		HF Radio		Link 11			Link 16				SATCOM			
VHF Radio	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0
	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0
HF Radio	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0
	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0
Link 11	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0
	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0
	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1
Link 16	1	0	1	0	0	0	0	0	1	0	0	1	0	0	0
	0	1	0	1	1	0	0	1	0	1	0	0	1	0	0
	0	0	0	0	0	1	0	0	1	0	1	0	0	1	0
	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1
SATCOM	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0
	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0
	0	0	0	0	0	1	0	0	0	1	0	0	1	0	1
	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0

VHF Radio | Link 16 | Link 11 | HF Radio | SATCOM

Identify vulnerable assets within the Army Network Architecture

See NDIA paper 19802 for technical details

MITRE

Analytic Approaches to SoS Architecture Assessment

Thread Simulation

Why is this important for mission engineering?

- Scale and complexity of missions require trades across multiple metrics and many solution options
- Lightweight analytic tools leverage architecture data to enable an initial quantification of mission impacts due to architecture changes
- This initial analysis can be used to filter out undesirable architecture options prior to investing resources to assess options with more detailed modeling and simulation tools

Identify vulnerable assets within the Army Network Architecture

Approved for public release. Distribution unlimited 17-3712-15

Linking SoS Architecture to Operational Outcomes

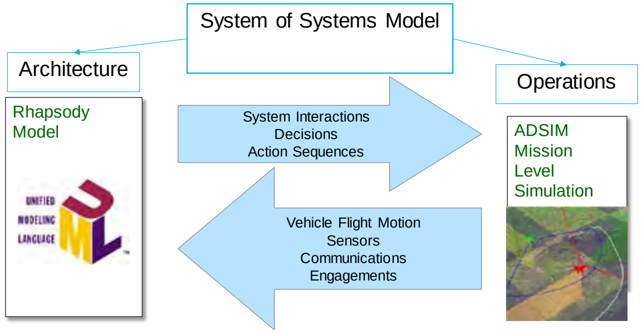
- **Effectiveness of SoS for missions is based on mission outcomes**
  – SE analysis of SoS for missions addresses the technical feasibility of the SoS options
  – Analyzing alternative SoS architectures or specific SoS compositions also needs to consider the impact on mission outcomes, typically addressed in operational simulations or test environments
  – This includes ***developing automated interfaces between architecture models and operational simulations***, allowing for analysis of the effectiveness of the SoS in representation scenarios, following proposed concepts of employment
  – Examples include Rhapsody to ADSIM, more recently to AFSIM

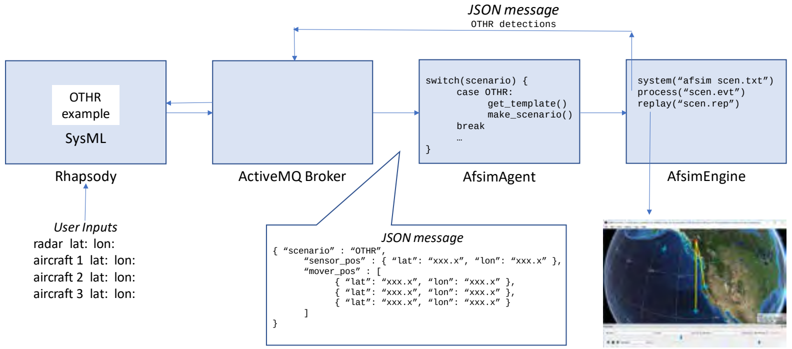

Battle Control System of Systems (SoS) Engineering Analysis

August 2016

NDIA 19th Annual Systems Engineering Conference

http://www.ndia.org/meetings/7870/Pages/default.aspx





Linking SoS Architecture to Operational Outcomes

Why is this important for mission engineering?

- Mission engineering is all about achieving user operational capability
- Ensuring technical feasibility is an important prerequisite – it is key that systems work together as planned based on engineering across the systems supporting the mission
- But it is key that the mission SoS composition is fit for purpose in the mission environment – physical, threat, etc. – and when executed leads to the expected mission outcomes under anticipated conditions
- Mission SoS architectures can be complex, and it can be time consuming and error prone to have to manually instantiate these in today's operational simulations
- Automating this facilitates the conduct of the analysis of the mission effect or proposed or alternative SoS compositions, and it allows operators and commanders to see the proposed composition in their operation context

Summary

- Mission engineering is an application of SoSE with specific driving characteristics
- As SoSE technical approaches and tools evolve, they provide valuable capabilities to enable technically based approaches to addressing mission engineering challenges

Abstract

In the US Department of Defense there is increased interest in **mission engineering - the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.** The Components have implemented mission engineering in areas where there is a critical interest in achieving mission capability such as ballistic missile defense or naval mission areas, and there is growing interest in addressing a broad set of mission areas through the implementation of mission integration management - the coordination all the programmatic elements - matching funding, schedules, technical improvements, resources (technical staff, development and test infrastructure, M&S etc.) across the relevant mission systems and supporting systems to develop, test, and field a phased set of mission capabilities. **One element of this is engineering of the systems of systems supporting the mission area.**

This presentation outlines the **key activities** involved in mission engineering and describes **opportunities for application of systems of systems engineering technical approaches** to these activities to provide the engineering base for mission integration and mission management. In particular, mission engineering often emphasizes the definition of the key activities need to execute the mission in the form of **mission threads or kill/effects chains and assessing gaps in mission performance.** Less attention has been paid to the various **patterns of mission activities and the engineering required to identify and assess alternatives to addressing the gaps and engineering the SoS to implement the preferred approach**. Drawing on work within the MITRE Systems Engineering Technical Center's model based engineering center, this presentation will present approaches to developing, representing and evaluating systems of systems architectures using model based methods and evaluating SoS configurations to address the functional needs of the mission which provide a set of approaches to supporting mission engineering.

Mission Integration Management NDAA 2017 Section 855

Mr. Robert Gold

Director, Engineering Enterprise
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

NDAA FY17 Section 855 (1 of 3)

(National Defense Authorization Act for Fiscal Year 2017)

Mission Integration Management (MIM) Legislation

SEC. 855. MISSION INTEGRATION MANAGEMENT.

(a) IN GENERAL.—The Secretary of Defense shall establish mission integration management activities for each mission area specified in subsection (b).

(b) COVERED MISSION AREAS.—The mission areas specified in this subsection are mission areas that involve multiple Armed Forces and multiple programs and, at a minimum, include the following:

(1) Close air support.
(2) Air defense and offensive and defensive counter-air.
(3) Interdiction.
(4) Intelligence, surveillance, and reconnaissance.
(5) Any other overlapping mission area of significance, as jointly designated by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff for purposes of this subsection.

(c) QUALIFICATIONS.—Mission integration management activities shall be performed by qualified personnel from the acquisition and operational communities.

(d) RESPONSIBILITIES.—The mission integration management activities for a mission area under this section shall include—

(1) development of technical infrastructure for engineering, analysis, and test, including data, modeling, analytic tools, and simulations;
(2) the conduct of tests, demonstrations, exercises, and focused experiments for compelling challenges and opportunities;
(3) overseeing the implementation of section 2446c of title 10, United States Code;
(4) sponsoring and overseeing research on and development of (including tests and demonstrations) automated tools for composing systems of systems on demand;
(5) developing mission-based inputs for the requirements process, assessment of concepts, prototypes, design options, budgeting and resource allocation, and program and portfolio management; and
(6) coordinating with commanders of the combatant commands on the development of concepts of operation and operational plans.

Four recommended mission areas with options for additional areas

Six 'Responsibility' areas

https://www.congress.gov/114/crpt/hrpt840/CRPT-114hrpt840.pdf

NDAA FY17 Section 855 (2 of 3)

(e) SCOPE.—The mission integration management activities for a mission area under this subsection shall extend to the supporting elements for the mission area, such as communications, command and control, electronic warfare, and intelligence.

(f) FUNDING.—There is authorized to be made available annually such amounts as the Secretary of Defense determines appropriate from the Rapid Prototyping Fund established under section 804(d) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2302 note) for mission integration management activities listed in subsection (d).

(g) STRATEGY.—The Secretary of Defense shall submit to the congressional defense committees, at the same time as the budget for the Department of Defense for fiscal year 2018 is submitted to Congress pursuant to section 1105 of title 31, United States Code, a strategy for mission integration management, including a resourcing strategy for mission integration managers to carry out the responsibilities specified in this section.

855 Scope, Funding, and Strategy

NDAA FY17 Section 855 (3 of 3)

10 USC 2446c is

- Put in place by the Acquisition Agility Act (NDAA FY17 Sections 805-809)
- A tasking to acquisition programs to employ a Modular Open Systems Approach and Prototyping
- MIM responsibility (d)(3) in Section 855 regarding Management of Interfaces (e.g. overseeing implementation of Section 805)

"§ 2446c. Requirements relating to availability of major system interfaces and support for modular open system approach

"The Secretary of each military department shall—

"(1) coordinate with the other military departments, the defense agencies, defense and other private sector entities, national standards-setting organizations, and, when appropriate, with elements of the intelligence community with respect to the specification, identification, development, and maintenance of major system interfaces and standards for use in major system platforms, where practicable;

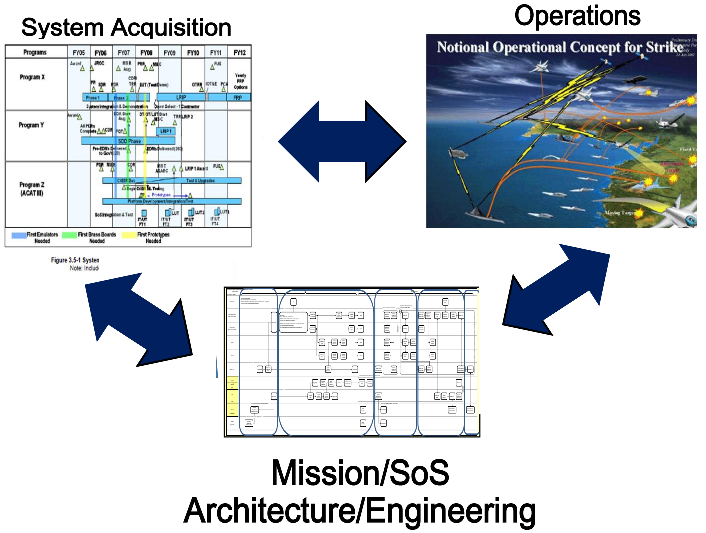
"(2) ensure that major system interfaces incorporate commercial standards and other widely supported consensus-based standards that are validated, published, and maintained by recognized standards organizations to the maximum extent practicable;

"(3) ensure that sufficient systems engineering and development expertise and resources are available to support the use of a modular open system approach in requirements development and acquisition program planning;

"(4) ensure that necessary planning, programming, and budgeting resources are provided to specify, identify, develop, and sustain the modular open system approach, associated major system interfaces, systems integration, and any additional program activities necessary to sustain innovation and interoperability; and

"(5) ensure that adequate training in the use of a modular open system approach is provided to members of the requirements and acquisition workforce.".

Mission Engineering (ME)



Mission Engineering is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects

- **Mission engineering treats the end-to-end-mission as the 'system'**
- **Individual systems are components of the larger mission 'system'**
- **Systems engineering is applied to the systems of systems (SoS) supporting operational mission outcomes**
- **Mission engineering goes beyond data exchange among systems to address cross cutting functions, end to end control and trades across systems**
- **Technical trades exist at multiple levels; not just within individual systems or components**
- **Well-engineered composable mission architectures foster resilience, adaptability and rapid insertion of new technologies**

Impacts of ME on the DoD Enterprise

- **Defines mission outcomes to identify and frame the correct problem**
- **Develops an accepted end state for mission success with defined mission success factors to drive the performance requirements for individual systems**
- **Aligns the affected stakeholders – Users, Operators, Acquirers, Testers, Sustainers – with the desired mission and capability outcomes**
- **Develops an assessment framework to measure progress toward mission accomplishment through end-to-end system integration of test & evaluation of mission threads**

ME Is Not the Same as SE

- **Meta-Functions exist across the SoS**
- **Situational Awareness and Command/Control are more complex due to multiple ways to accomplish mission – must evolve alongside military Concept of Operations (CONOPs)**
- **Technology issues aren't always obvious**
- **Resiliency and mission hardening requirements must be collectively assessed**
- **Testing will be expensive if not unaffordable**
- **Resource management techniques don't scale – Engineers, development/test facilities etc.**
- **Emergent behaviors difficult to anticipate or assess**
- **Synchronization of budgets and implementation is difficult at best**

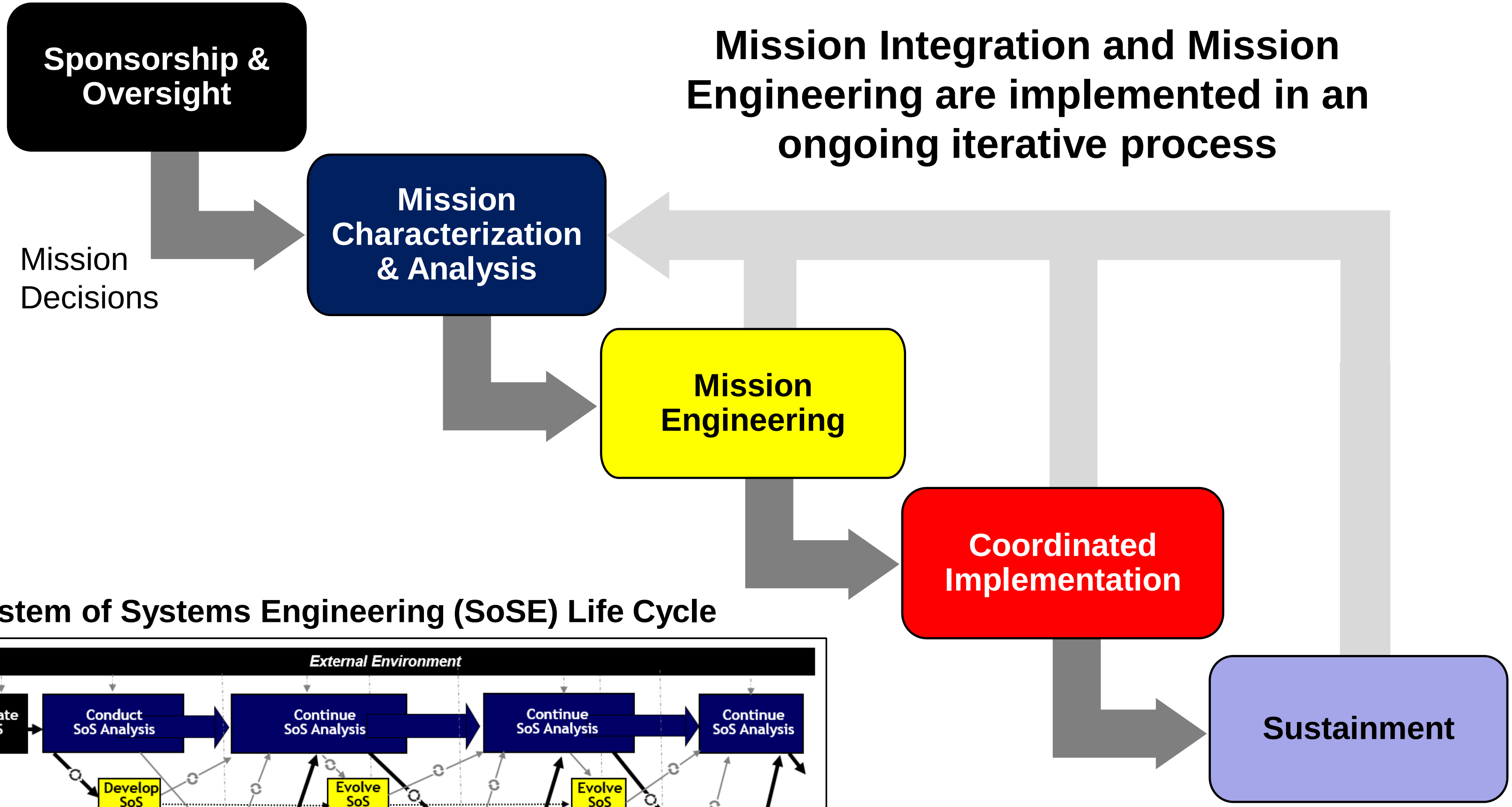
Challenges Faced Today (1 of 2)

- **Limited corporate/leadership demand for ME**
- **Lack of integration of ME considerations and results into Systems Engineering Technical Reviews (SETRs), Milestone reviews, resourcing decisions**
- **Cost/benefit of conducting mission engineering and analysis**
- **Large scope and complexity of missions**
  - Cross multiple portfolios and organizations
  - Multiple complex, system interdependencies
- **Lack of dedicated ME resources (funding, people, tools, data)**
  - Availability and development of ME skills
  - Development of effective ME processes and practice
- **Methods, tools and data (next page)**

Challenges Faced Today (2 of 2)

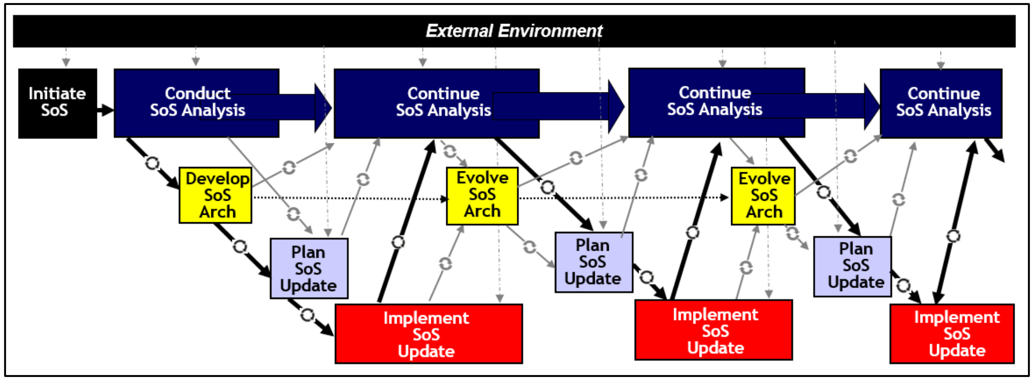
- **Methods, tools and data**
  - Challenges of developing integrated analysis capabilities that bridge engineering and mission effects
    - Limits on the available analysis methods to address complexity and dynamics
    - Difficult to link changes in systems or SoS engineering models with impacts on missions in operational or mission simulations
    - Tools address only subset of issues, making complex analysis and engineering trades manpower intensive and time consuming, are difficult to use together
  - Need for data on missions, systems, interfaces, interactions and interdependencies
    - Very distributed, maintained in various forms by different organizations
    - Focus on specific system needs and don't address interdependencies and interactions
    - Even when available, can be hard to locate or access
    - Current system models are developed for different purposes which can challenge their effective use in addressing mission level issues

MIM Key Activities



Mission Integration and Mission Engineering are implemented in an ongoing iterative process

System of Systems Engineering (SoSE) Life Cycle



Source: Defense Acquisition Guidebook, Chapter 3 Systems Engineering, Section 3.1.2 Systems of Systems (https://shortcut.dau.mil/DAG/CH3)

MIM Joint Mission Patterns

General reusable solutions of Joint Mission patterns.
Descriptions of formalized best practices.

Joint Mission Designation: ***Delegated to a Service***

Service already handling scope or well within their scope

Joint Mission Analysis: ***Service-Led Engineering***

USD(AT&L) & Joint Staff help set joint mission context

Service does everything below that context, including managing requirements and acquisition

Joint Mission Analysis: ***Joint Engineering***

USD(AT&L) & Joint Staff facilitate system engineering and architecture

Programs support development of mission capability fielding packages

Joint Mission Agency: ***Priority and Scope Merits Separate Agency***

Critical, joint mission area

Largely independent

Oversight & Context | Mission Eng & Analysis | Program Execution

Outcomes of ME and MIM

- **Planning, Programming, Budgeting, and Execution (PPBE) informed by gaps created by dis-investment decisions or unfunded mission critical components**
- **Cross-cutting capabilities performing as required or desired**
  - Development and engineering synchronized
  - Fielding expectations documented and promulgated
  - Sustaining activities prepared to support fielding
- **Stakeholders of capabilities are identified with greater potential to:**
  - Improve coordination of management actions
  - Resolve or avoid system conflicts
- **Opportunity for much greater and more effective savings when trades & analyses are performed at a mission or portfolio level**

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Mr. Robert Gold

ODASD, Systems Engineering

703-695-3155

robert.a.gold4.civ@mail.mil

NDIA

Booz | Allen | Hamilton

ACQUISITION SYSTEM INTEROPERABILITY CONSIDERATIONS

National Defense Industrial Association (NDIA)
Systems Engineering Conference

John J. Daly

Booz Allen Hamilton
daly_john@bah.com

OCTOBER, 25, 2017

AGENDA

- Introduction
- Systems and Software Engineering – System Life Cycle Processes
- SE Life Cycle Processes Interoperability Considerations
- Drivers to Increased Interoperability Emphasis
- NDIA 2107 AAA - Modular Open System Approach
- MBSE and Acquisition
- Wrap Up

INTRODUCTION

- Acquisition Reform efforts cancelled tens of thousands of military specifications and standards
  - There is a move to more non-governmental standards
  - There is a move to more profiles of acceptable standards, than mandated singular standards “There can be only one!”
  - Interoperability between some kinds of standards (e.g. data) is easier with current technology
  - There is increased appreciation that standards lag innovative technology
- An adoption of the ISO/IEC/IEEE8 15288, Systems and Software Engineering–System Life Cycle Processes was made by the DoD
- The NDAA 2107 Acquisition Agility Act (AAA) requires DoD acquisition to react more quickly and “agilely” to technology, Threat, and Mission changes using a Modular Open System Approach (MOSA)
- Open Architectures are being widely adopted in the DoD

These are all enablers of increased Interoperability

SYSTEMS AND SOFTWARE ENGINEERING
SYSTEM LIFE CYCLE PROCESSES

- **Acquisition reform efforts cancelled tens of thousands of military specifications and standards**
  - DoD Components expressed a need for SE-related standards to put on contract
  - Analysis was conducted to determine areas where new standards are needed
- **DoD adopted the voluntary consensus standard ISO/IEC/IEEE8 15288, *Systems and Software Engineering–System Life Cycle Processes,* for use in DoD acquisition.**
  - The standard establishes a common process framework for describing the life cycle of man-made systems and defines a set of SE processes and associated terminology typical for the full system life cycle - including conception, development, production, utilization, support, and retirement.
- **Two new DoD SE-focused Non-Government Standards (NGS) were developed and adopted by DoD as companion standards to ISO/IEC/IEEE8 15288**
  1) IEEE 15288.1, IEEE *Standard for Application of Systems Engineering on Defense Programs*; Issued May 15, 2015; adopted for use by DoD June 5, 2015
  2) IEEE 15288.2, IEEE *Standard for Technical Reviews and Audits on Defense Programs*; Issued May 15, 2015; adopted for use by DoD June 5, 2015

They define DoD requirements for SE processes, technical reviews, and audits

THE 15288 AND COMPANION STANDARDS

- **Provide guidance for definition, control, and improvement of the organization or project's system life cycle processes**
- **Address man-made systems that may be configured with one or more of the following elements: hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities… *(Pretty much everything!)***
- **IEEE 15288.1, IEEE *Standard for Application of Systems Engineering on Defense Programs*; expands on the SE life cycle processes with <u>additional detail specific to DoD acquisition projects</u>**
- **IEEE 15288.2, *Standard for Technical Reviews and Audits on Defense Programs,* provides detailed definition, requirements, and evaluation criteria for the technical reviews and audits <u>associated with DoD acquisition projects</u>**
- **NDIA, in collaboration with DoD representatives, drafted guidance for utilizing 15288.1 and 15288.2 on contracts.**
  - incorporated *in DoD Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs* April 2017; http://www.acq.osd.mil/se/pg/guidance.html

15288 SE LIFE CYCLE PROCESSES

Establishes a common framework for describing the life cycle of man-made systems and defines a set of processes and associated terminology from an engineering viewpoint

Agreement Processes / Organizational Project-Enabling Processes	Technical Management Processes	Technical Processes
Agreement Processes • Acquisition • Supply **Organizational Project-Enabling Processes** • Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Reference: **ISO/IEC/IEEE 15288, "Systems and Software Engineering System Life Cycle Processes"**

15288 SE LIFE CYCLE PROCESSES

- **Stress the importance of SE within the scope of the overall acquisition**
- **Define the acquirer's expectations, generally expressed in requirements, for a supplier's SE processes (outcomes, activities, and/or outputs) and technical reviews and audits**
- **Levy requirements on the supplier, via the contract, to perform effective SE**
- **Ensure the supplier's SE efforts are appropriately funded and resourced**
- **Ensure a means for the supplier to demonstrate compliance with those requirements**

"The 15288 Standards provide one method to define the acquirer's expectations and requirements for the supplier's performance of SE processes and technical reviews and audits. Thoughtful and proper use of these standards can enhance communication and understanding between the acquirer and supplier throughout the solicitation process and contract execution."

Reference: DoD Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs April 2017; http://www.acq.osd.mil/se/pg/guidance.html

SE LIFE CYCLE PROCESSES
INTEROPERABILITY CONSIDERATIONS

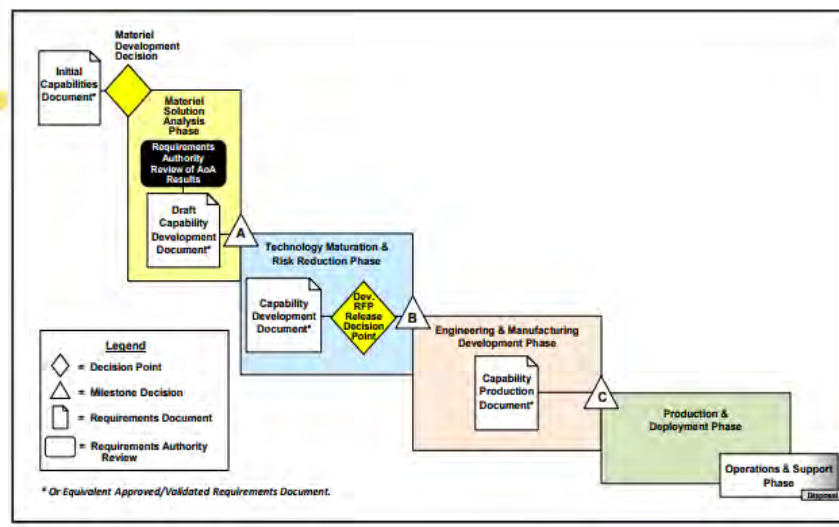
- **Implementation of these SE System Life Cycle Processes involves interoperability consideration (both planned and unplanned) in engineering system capabilities where:**
  - Where the system function depends on data from external sources
  - Where the system functions cross system boundaries – distributed functionality
  - Where a the system needs an internal modular approach to accommodate technology basic system requirement (mission/threat) change within the Systems lifecycle.
  - Where system design and development, as well as performance in the system's functional role as a DoD capability, depend on that system's ability to interoperate with other systems to perform both planned, and unplanned missions.
- **An important consideration is anticipated or unanticipated interoperability**

Performing effective SE across the system life-cycle involves direct and indirect consideration of interoperability across technical, physical, stakeholder, acquisition, and mission (functional) domains.

ANTICIPATED INTEROPERABILITY

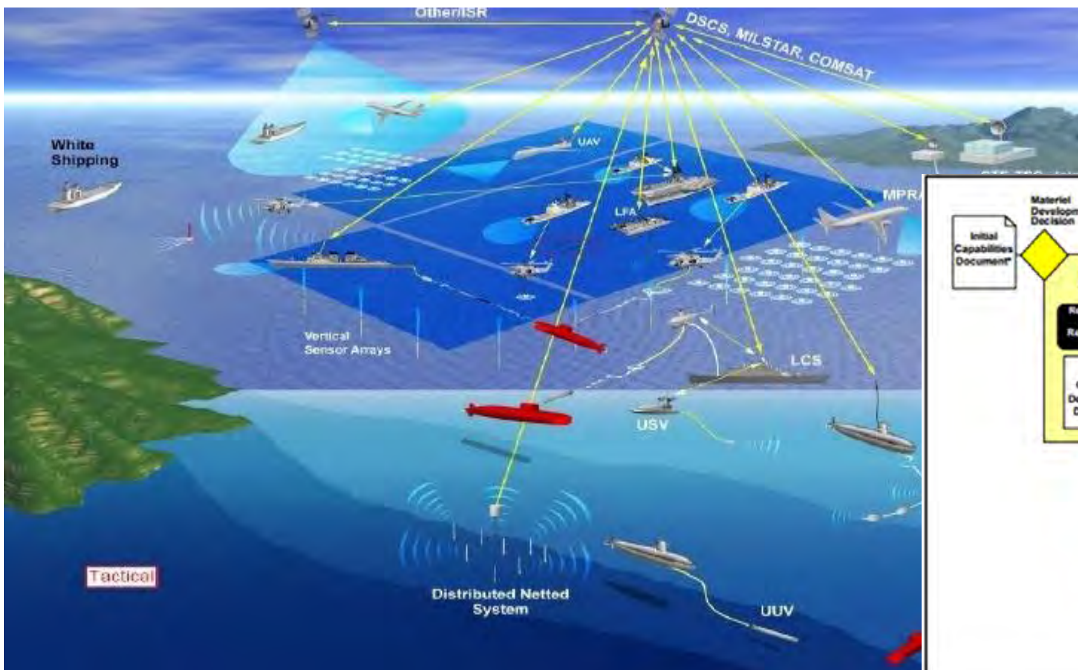
- **Requirements to interoperate are well known and stable**
- **Need to interoperate is part of basic requirement set**
- **Technology and function/mission are on same time scales and predictable**
- **Acquisition life cycle is linear in traditional model**

e.g. LVCAR Distributed training

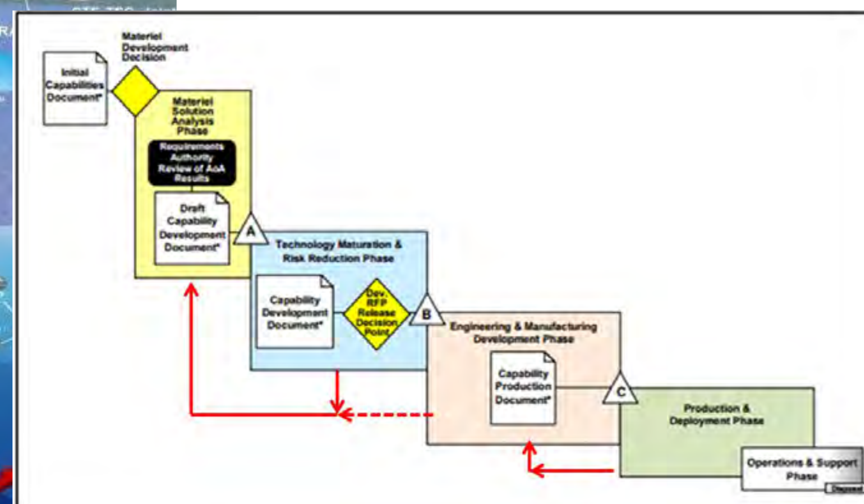


UNANTICIPATED INTEROPERABILITY

- Interoperability needs develop during acquisition
- Very hard /impossible to define *up-front* in traditional acquisition model
- Other systems/missions desire to leverage system capability
- Technology and function/mission change, often on differing time scales and unpredictably
- Acquisition life cycle requires feedback loops to accommodate evolving requirements and disparate time scales of technology and mission



e.g. C4ISR network



DRIVERS TO INCREASED INTEROPERABILITY EMPHASIS

- **15288 Systems Engineering Life Cycle Processes -** *requiring increased rigor in and contracting accountability for robust SE across entire lifecycle*
- **NDAA 2017 DoD Acquisition Agility Act (AAA) -** *Sec. 805. Modular Open System Approach In Development Of Major Weapon Systems*
- **Joint Staff changes to JCIDS -** *ongoing revisions (e.g. "IT Box"; Incremental CDD's…)*
- **Rapid Technology change -** *accelerated timelines, especially in certain areas: (e.g. battery technology)*
- **Unanticipated Threat/Mission change -** (e.g Asia-Pacific rebalance)
- **Ubiquitous data availability -** *new uses in current capabilities (e.g. geospatial implementation)*
- **Focus beyond data interoperability -** *to functional interoperability*

NDAA 2107 AAA MODULAR OPEN SYSTEM APPROACH (MOSA)

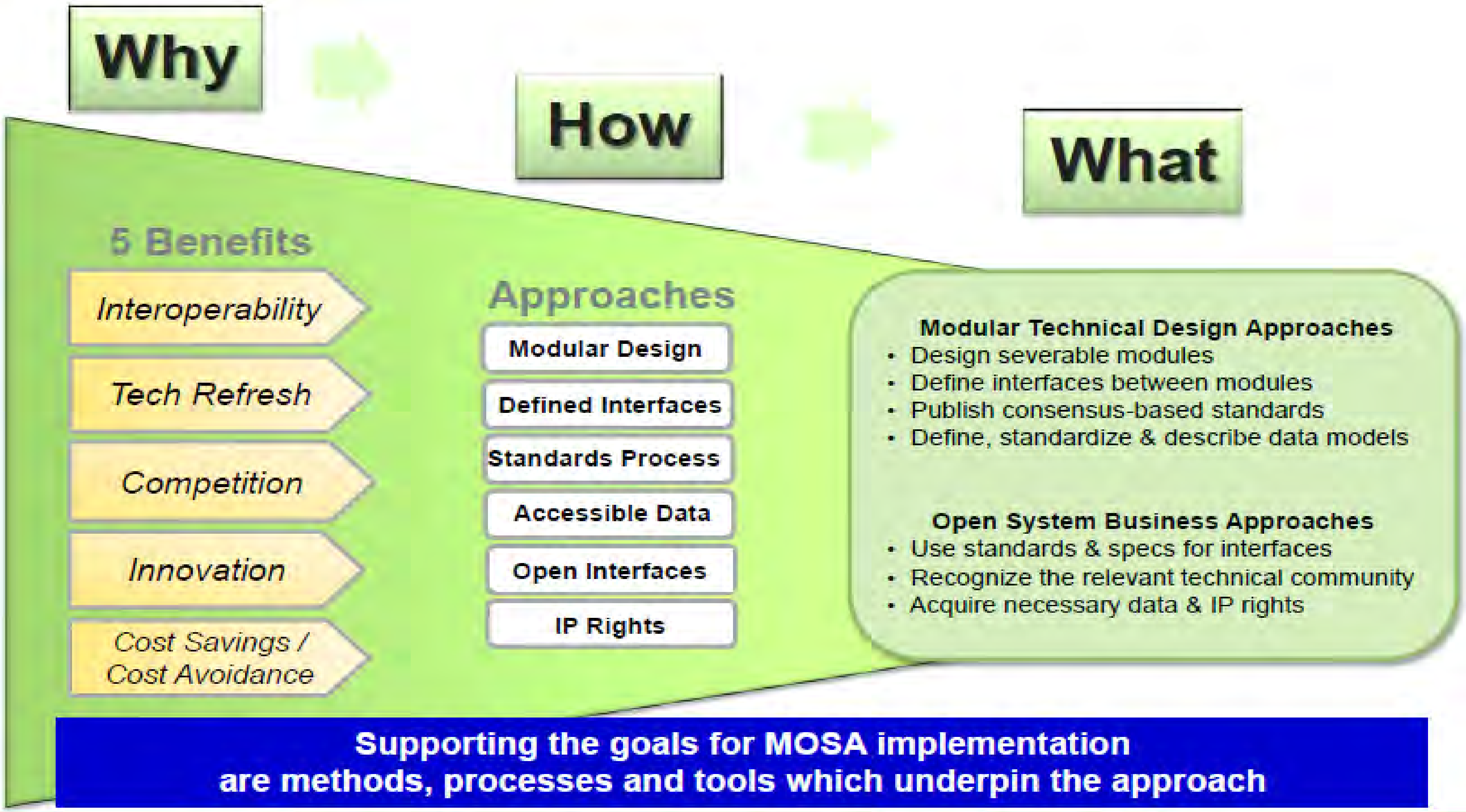
- **SEC. 805. MODULAR OPEN SYSTEM APPROACH IN DEVELOPMENT OF MAJOR WEAPON SYSTEMS.**
  - § 2446a. **Requirement for modular open system approach in major defense acquisition programs** *A major defense acquisition program that receives Milestone A or Milestone B approval after January 1, 2019, shall be designed and developed, to the maximum extent practicable, with a modular open system approach to enable incremental development and enhance competition, innovation, and interoperability.*
  - § 2446b. **Requirement to address modular open system approach in program capabilities development and acquisition weapon system design** *In Program Capability Documents; Analysis Of Alternatives; Acquisition Strategy; Request For Proposals*
  - '§ 2446c. **Requirements relating to availability of major system interfaces and support for modular open system approach**: *"for each major defense acquisition program that receives Milestone B approval after January 1, 2019, a brief summary description of the key elements of the modular open system approach as defined in section 2446a of this title or, if a modular open system approach was not used, the rationale for not using such an approach"*

NDAA 2107 AAA
BENEFITS OF MOSA

"2446a.(b).(1).(C) uses a system architecture that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation while yielding—

"(i) significant cost savings or avoidance;
"(ii) schedule reduction;
"(iii) opportunities for technical upgrades;
"(iv) increased interoperability, including system of systems interoperability and mission integration; or
"(v) other benefits during the sustainment phase of a major weapon system; and…"

MOSA APPROACHES



Reference: "Using the 5 Benefits of a Modular Open Systems Approach (MOSA) to Choose Enablers"; Philomena Zimmerman; NDIA SE Conference, October 26, 2016

MODULAR OPEN SYSTEM APPROACH
AN ENABLER OF INTEROPERABILITY?

Among other benefits, a **modular approach can enable interoperability** in areas where implemented:

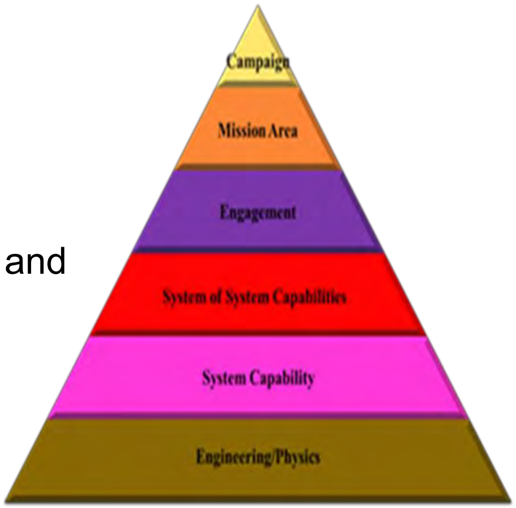
- **Implies architecture and interfaces are published and well known -** *Open Architecture Approach?*
- **Allows for Anticipated/Unanticipated interoperability**
- **Component modularization enables tech refresh/evolution, as well as interoperability with other components –** *internal and external*
- **Physical systems modularity and interoperability a key new acquisition emphasis** *e.g Virginia class SSN/LCS ships*
- **Enables more rapid response in system acquisition to new threats -** *e.g. EW systems*
- **Extent of modularity is driven by many other factors -** *cost, performance, complexity etc…*

- ***How much is enough?***
- ***How is modularization for another capability's interoperability needs paid for?***
- ***How do missions put a "marker" on systems for interoperability in their mission area?***

OPPORTUNITY

To implement MOSA and other changes to the Acquisition System to accommodate Complexity/ Technology/Threat/Interoperability what new Systems Engineering processes can we utilize?

- System Engineering in general, and as practiced by DoD is changing and new tools, techniques, and types of analysis are sought for the more complex systems, and systems of systems of today
- Engineers are very familiar with the use of software modeling frameworks and tools to solve complex engineering problems, these are used in every facet of design and production by manufacturers - Why not government Aquisition and oversight?
- Many modeling and architecture tools exist for data parsing and interoperability between stages of acquisition:
  - Data set interoperability is easier **"up the modeling pyramid"** from development level activities to oversight (higher to lower fidelity)
  - This enables looking at "**Top-Level" capability mission performance** for refining/updating requirements, and accommodating system changes and trade-off's due to threat/technology/mission evolution and change



Model-Based System Engineering (MBSE) is a methodology and tools (often part of architecture tools) to help us manage complexity, modularization, and enhance interoperability

MODEL BASED SYSTEMS ENGINEERING (MBSE)

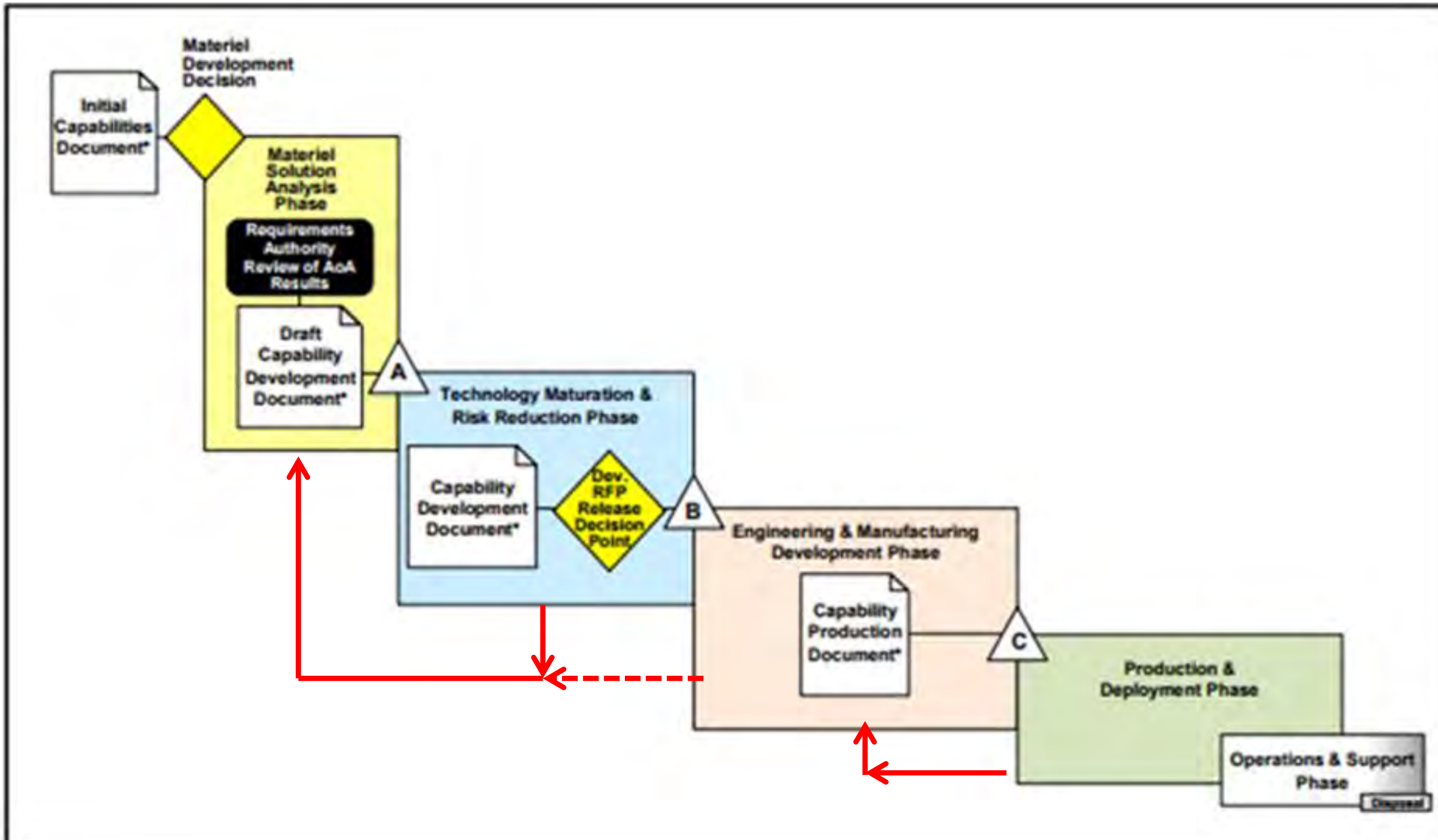
HELP WITH INTERNAL SYSTEM ACQUISITION INTEROPERABILITY ?

- **MBSE provides a method to organize data to function / purpose over a program's lifecycle – it *could be a robust Systems Engineering Process in supporting 15288 implementation***
  - It can be used in an acquisition program to organize cost, schedule, and performance data in a structured way amenable to software tools for analysis/display/decision making
  - An MBSE approach is inherently robust and contains the data required to model the process:
    - Requires a structure that organizes a process with often disparate data into an organized entity
    - Has the prerequisite digital structure to support modeling capability performance
- **MBSE can be used to help objectively model an acquisition programs capability in performance terms and *address trade-offs on modularity***
- **MBSE can model an acquisition programs capability and *interoperability between it and mission partner capabilities* to optimize them**
- **MBSE can enable End-to-End modeling and simulation and provide clarity on requirements and insight on trades between both functional and performance requirements; and provide insight on interoperability gaps and needs**

If we view an acquisition lifecycle as a process, with many sub processes also "model-able".. then the use of a scalable conceptual framework (MBSE) to organize data and model it is attractive

Questions/Discussion

ACQUISITION "MID-COURSE GUIDANCE"



STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

An Approach to Verification of Complex Systems

NDIA Systems Engineering Conference
26 October 2017

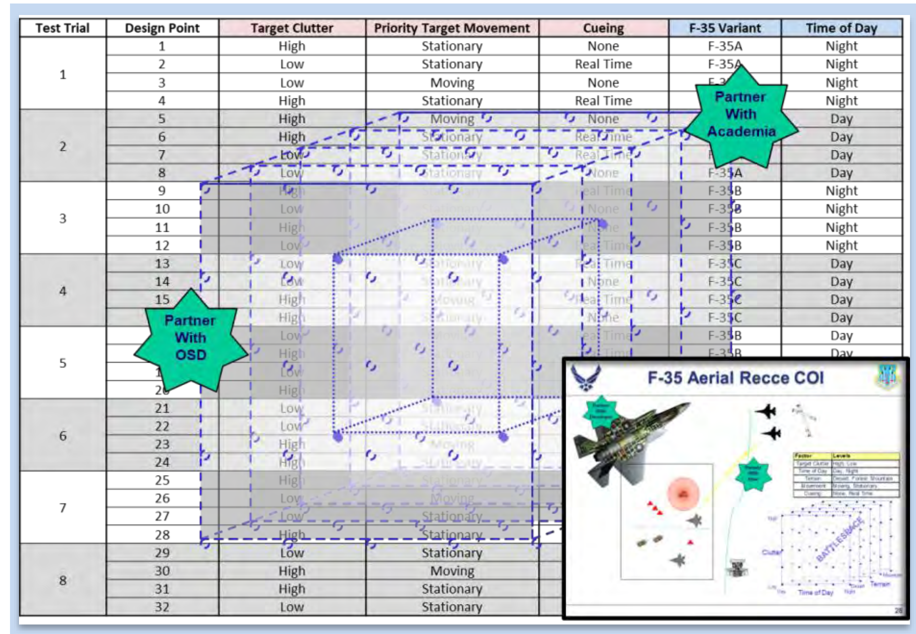
Dr. Wilson N. Felder
Industry Professor, and Director, SERC Doctoral Fellows Program
School of Systems and Enterprises

Topics

- Complexity awareness
- Elements of Adaptive V&V
- Importance of partnerships
- Action Plan

Complexity Awareness

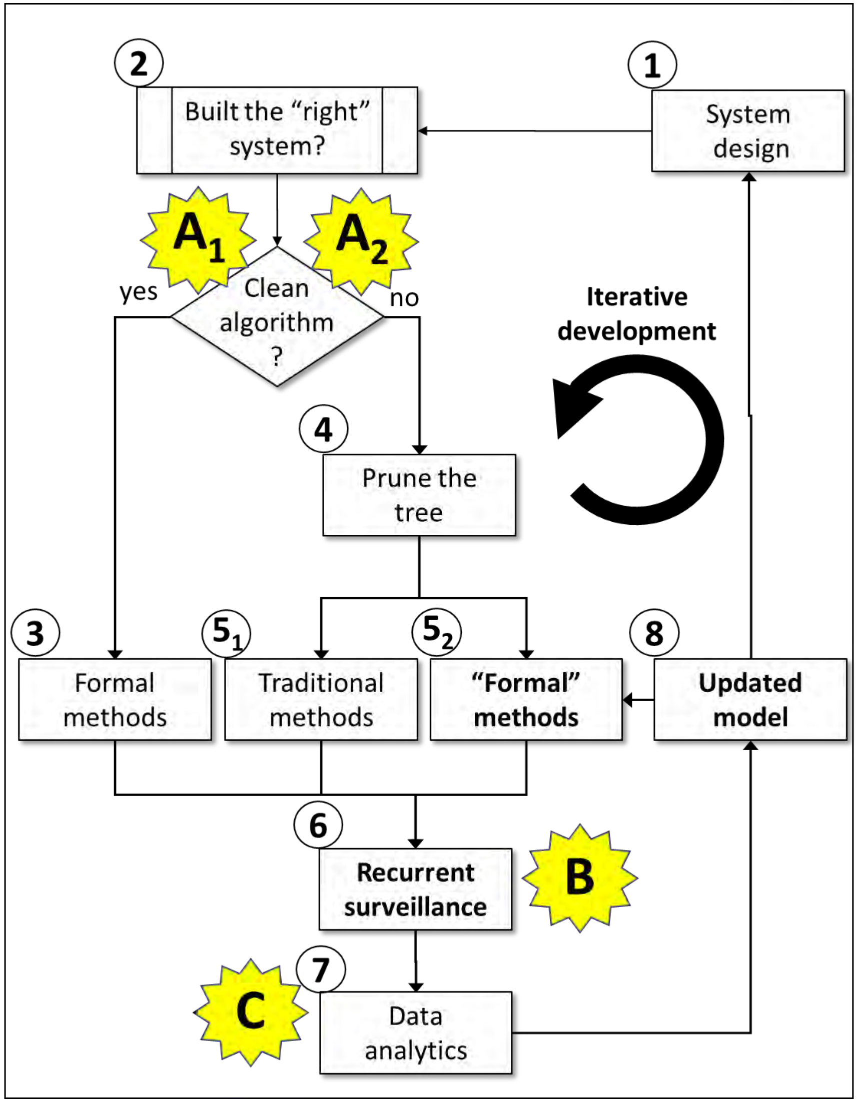
- Too many system states
- **Don't have enough** bandwidth to cover them all
- Fat tailed probabilities
- Dynamic, asynchronous, ad hoc exchange of digital data among constituents
- Surprises



AFOTEC concept of "hypercube" test matrix

A working model

- How do we deal with the problem of complexity (perhaps unrecognized complexity)?
- **Here's one possible approach…**



Elements of Adaptive V&V

Life Cycle Governance

Have testers verify the "glossy brochure" for the system

Adaptive V&V Tools	Life cycle stages				
	Research	Design	Development	Test	Operations
Life Cycle Governance					
MBE					
Agile					
Formal Methods					
Recurrent Surveillance					

Shifting left and right

Adaptive V&V

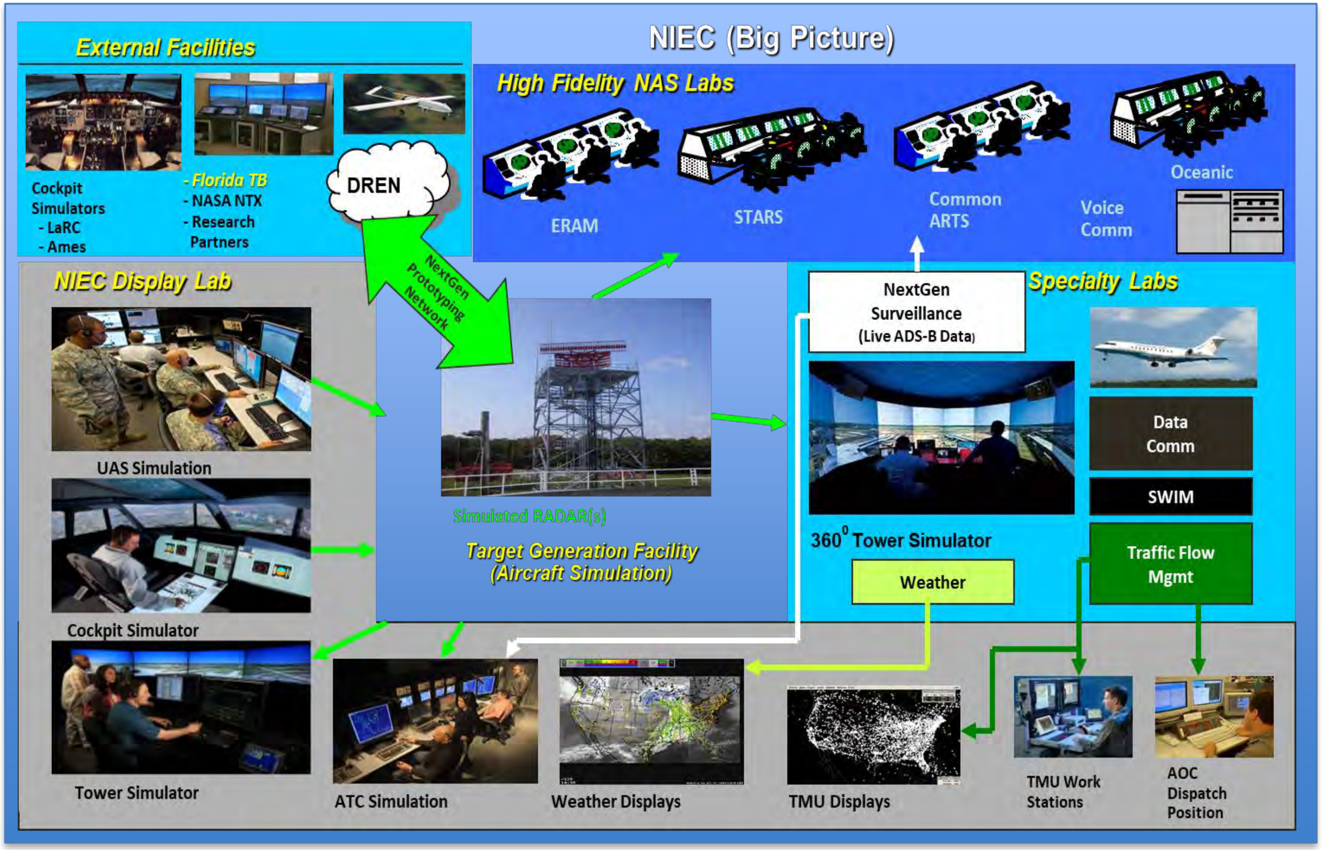
Deploy the basic capability, then add functionality over time

Data Analytics during operations reveal latent defects

Iterative Development

- Not just, or even exactly, agile methods
- More the application of agile principles to government acquisitions
- **See Barry Boehm's recent book**
- Example from FAA TFM program
  - 6 month "sprints"
  - R&D/development/test/operational facilities co-located

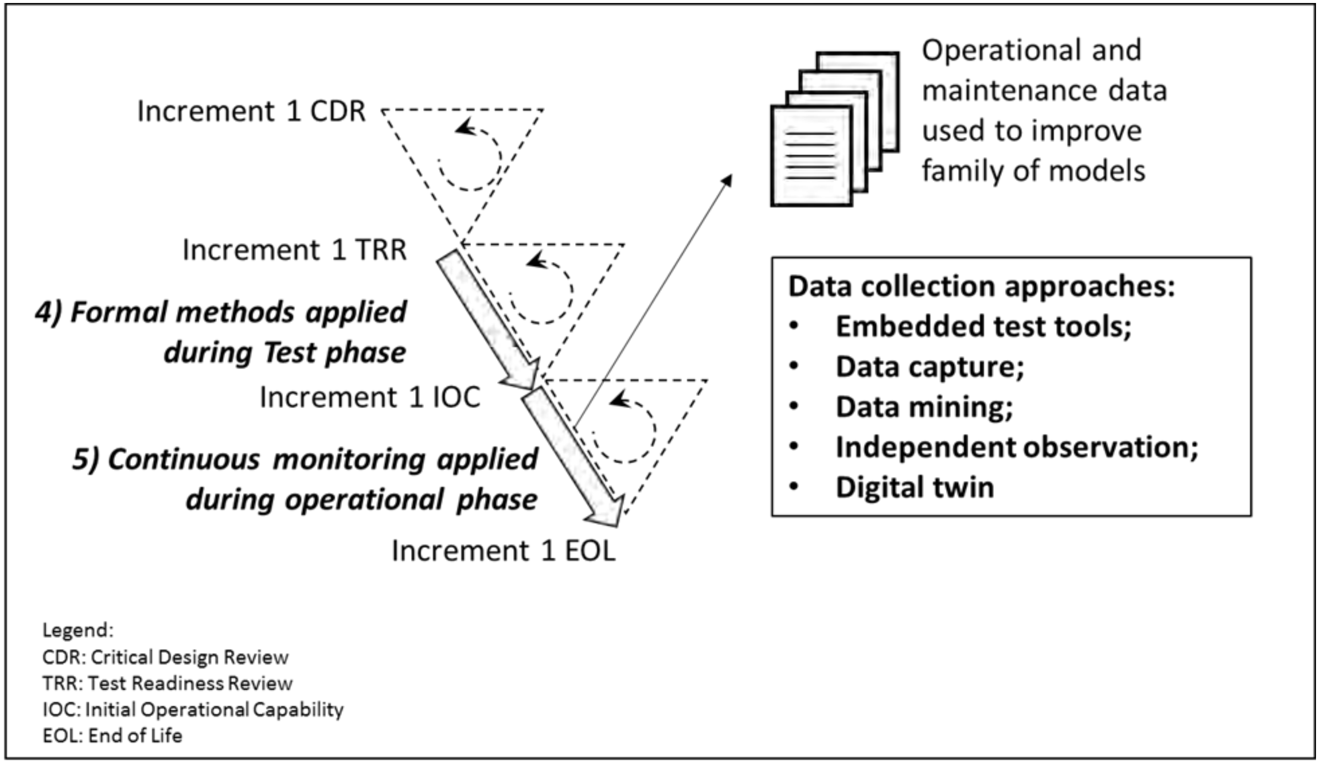
Model Based Engineering



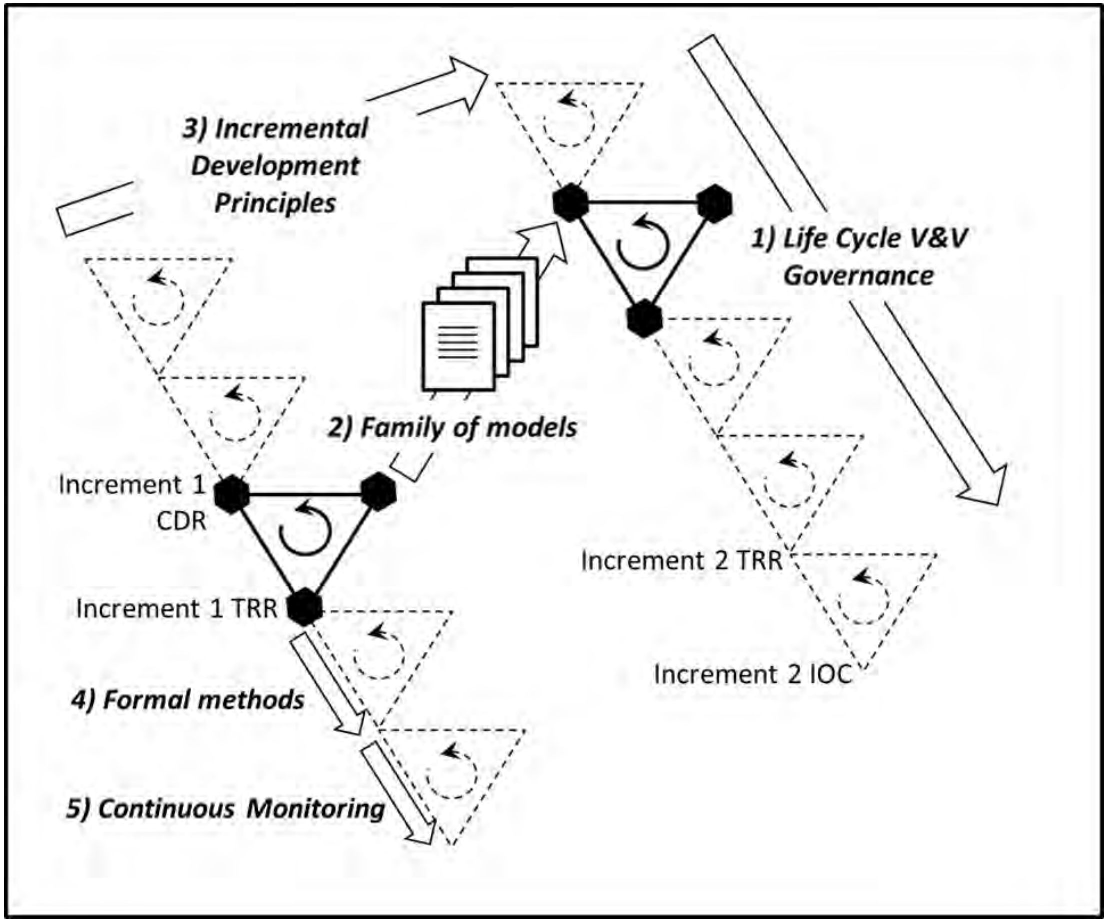
The FAA's NIEC/TGF complex *IS* the MBE core for the NAS!

NIEC – NextGen Integration and Evaluation Center
TGF – Target Generation Facility
MBE – Model Based Engineering
NAS – National Airspace System

Formal Methods and Recurrent Surveillance

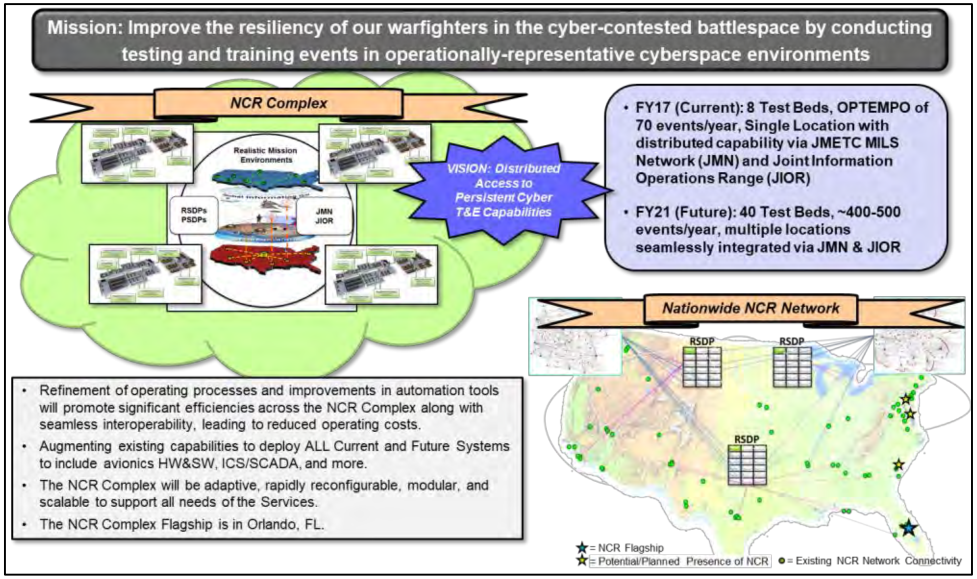


Summary:
The Adaptive V&V Framework



Importance of Joint/Interagency/ Whole-of-Government Solutions

- Share best practices
- Make use of best-in-class facilities and capabilities
- Partner across agencies
- Also within agency across stage gates!



Action Plan

- **Use policy changes to drive V&V "to the left" and also "to the right"**
- Formalize flexible iterative development practices in acquisition regulations
- Advocate for national policy reform permitting use of real portfolio management
- Standardized models (from a data definition point of view) so **that they can be used to communicate from "later stages of an earlier iteration, to earlier stages of a later iteration."**
- Formalize the use of recurrent surveillance tools to catch the inevitable but unpredictable emergent behaviors.

Questions and Discussion

Contact Information

Dr. Wilson N. Felder

(240) 204-1145

Stevens Institute of Technology

wfelder@stevens.edu

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Review of Best Practices for Technical Leadership Development

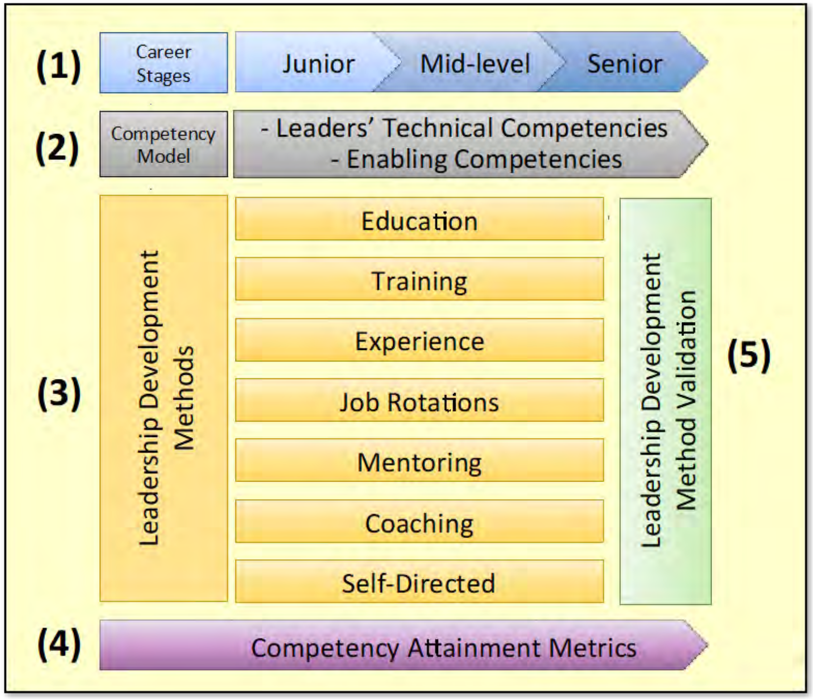
NDIA Systems Engineering Conference
26 October 2017

Dr. Wilson N. Felder
Industry Professor, and Director, SERC Doctoral Fellows Program
School of Systems and Enterprises

Review of Best Practices for Technical Leadership Development from Organizational Benchmarking

Context

- Part of SERC Technical Leadership Research Topic
- Co-sponsored by DAU and DASD(SE)
  - Developed a technical leadership development framework
  - Defined three career levels
  - Vetted a set of 24 competencies



Conducted a set of organizational benchmarking visits

Methodology

- Identified organizations with "best-in-class" reputations for technical leadership development
- Conducted benchmarking visits with each
- Interviewed one or more SME managers familiar with the organization's approach to technical leadership development
- Structured, competency based interview protocol
- Open-ended discussion

Organizations

- U.S. Navy Quality Management
- ONR
- U.S. Navy Strategic Systems Program
- NAVSEA
- Sandia
- Raytheon Missile Systems
- NASA Marshall Space Flight Center
- DAU Southeast Region
- U.S. Army ARDEC
- Lockheed-Martin
- Gulfstream
- Accenture
- Missile Defense Agency

Caveats

- Not a human subject study, so no personal data were collected
- Observations by/opinions of SMEs at organizational level within agency/company
- Not for attribution at any level
- Results were incorporated in the TLDF study

Synopsis of Best Practices Found

- Local tailoring
- Emerging leader ownership of process execution
- Evidence based metrics
- HR/line organization/project organization collaborated as equal partners
- Other observations:
  - Starts before first day of work
  - Continuous across career stages
  - All used many methods to impart competencies

Local Tailoring

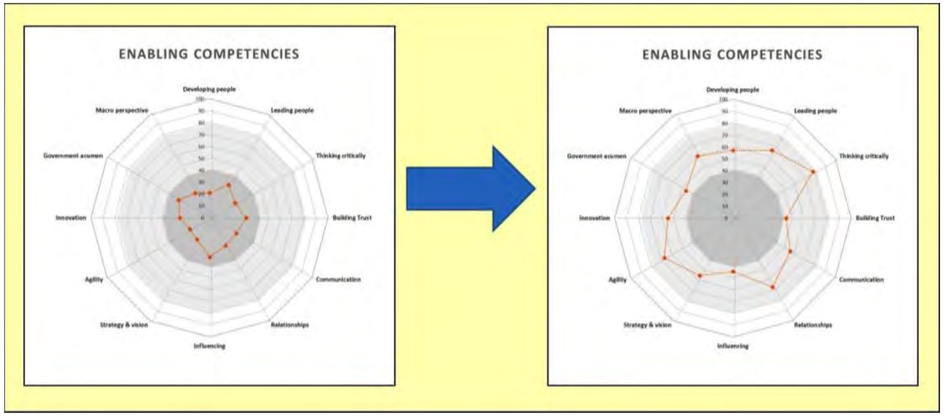
- Tailored geographically
- Tailored organizationally

Emerging Leader Ownership of Process Execution

- Tools are provided to emerging leaders to track and manage their own competency attainment
- Workshops and group meetings to cement progress and maintain commitment

Metrics from Evidence Based Competency Achievements

- Competency attainment plotted on spider/radar charts by participant
- Evidence from tangible achievements noted



- 360° Feedback provides quality assessment of claim
- Process separate from performance assessment and is not used to make salary decisions

HR/Line/Project Collaboration

- Support for leadership development is from executive leadership level
- HR, functional management, and project management all provide support and encouragement as a team
- In some cases, these three entities collaborate in assigning emerging leaders to developmental positions

Additional Features

- Application of multiple development methods
- Continuous development across career stages
- Starts before day one
  - "Making the offer sticky"

Acknowledgments

The RT-149 team:
Dr. Wilson Felder, PI
Dr. Steve Yang, Co-PI
Dr. Katherine Duliba
Dr. Mike Pennotti
Jeffrey Mo

References

Felder, Wilson N., Steve Yang, Michael Pennotti, Katherine Duliba, and Cheuk Mo. “Leadership Development Framework for the Technical Acquisition Workforce.” Technical Report. Hoboken, NJ: Systems Engineering Research Center, October 25, 2016.

Duliba, Katherine, and Wilson N. Felder. “Strengthening Systems Engineering Leadership Curricula Using Competency-Based Assessment.” In *15th Annual Conference on Systems Engineering Research*, 1–10. Redondo Beach, CA, 2017.

Duliba, Katherine A., Cheuk Y. Mo, Michael Pennotti, Steve Yang, and Wilson N. Felder. “A Technical Leadership Development Framework for Systems Engineers.” In *14th Annual Conference on Systems Engineering Research*. Huntsville, AL, 2016.

1870

STEVENS

INSTITUTE of TECHNOLOGY

THE INNOVATION UNIVERSITY®

stevens.edu

Contact Information

Dr. Wilson N. Felder

(240) 204-1145

Stevens Institute of Technology

wfelder@stevens.edu

Beyond Technical Interoperability

Net Centric Operations
Context for the Interoperability *& Net Centric Operations* Track
@ 2017 NDIA SE Conference
October 2017

Jack Zavin
Chair
I/NCO Track
jack.e.zavin.civ@mail.mil
(703) 614-7945

AGENDA

- Describe Interoperability and related matters
- Describe Net Enabled Operations

Describe Interoperability and related matters

Achieving Interoperability :
A perpetual motion machine

<u>Interoperability:</u>
The ability to operate in synergy in the execution of assigned tasks.

Interoperability is more than just the technical exchange of information

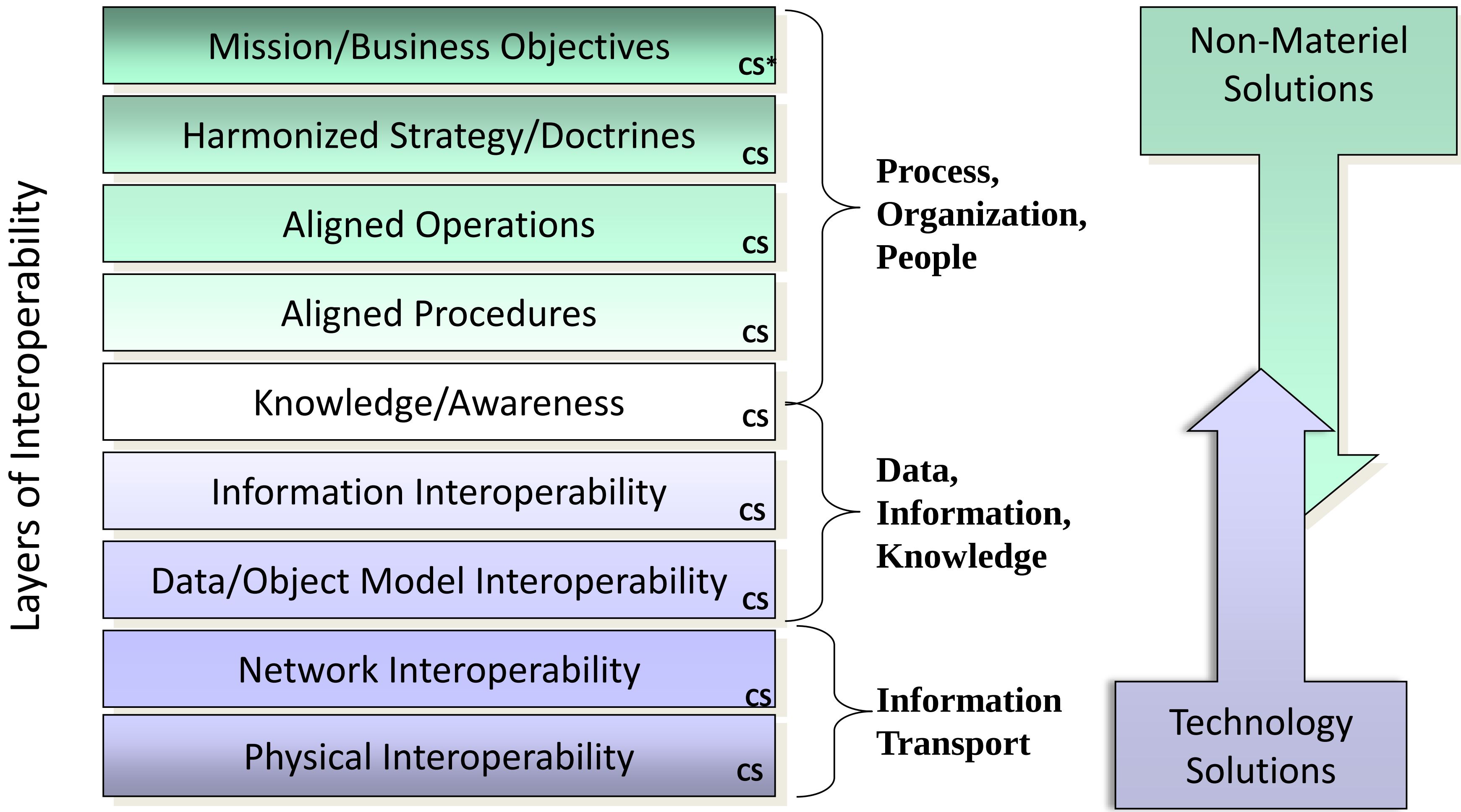
Solutions Sets must cover Process, Organization, People, Information, and Materiel across the range of DoD operations

Interoperability must be balanced & synchronized with Cyber Security.

<u>Cybersecurity:</u>
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

<u>Information Assurance:</u>
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

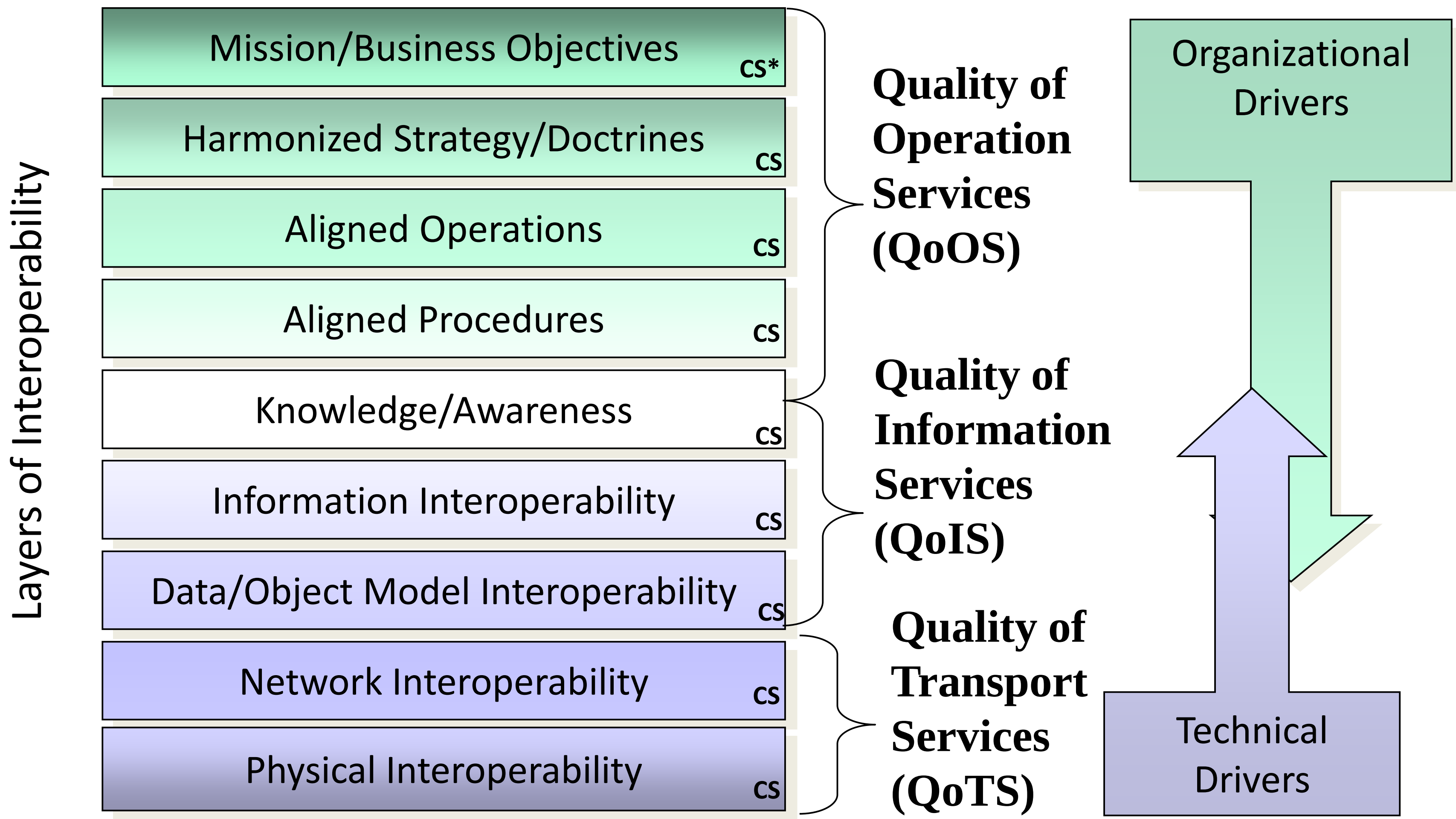
Interoperability Model:
A composite of Materiel & Non-materiel solutions



CS = Cyber Security [formerly Information Assurance]

Adapted from "Beyond Technical Interoperability – Introducing a Reference Model for Measure of Merit for Coalition Interoperability'. Dr. Andreas Tolk, VMASC, ODU. 8th CCRTS , NDU , June 2003

Interoperability Model & QoS



CS = Cyber Security [formerly Information Assurance]

Adapted from "Beyond Technical Interoperability – Introducing a Reference Model for Measure of Merit for Coalition Interoperability'. Dr. Andreas Tolk, VMASC, ODU. 8th CCRTS , NDU , June 2003

End-to-End Quality of Service

End-to-End Quality of Service =

Quality of Operation Services + **Quality of** Information **Services** + Quality of Transport Services

Key Needs:
- Mission or business objectives
- Harmonized strategy or doctrines
- Aligned operations
- Aligned procedures
  - Knowledge/awareness of actions by people and processes

Key Metrics:
- Urgency:
  - Timeliness
- Priority:
  - Degree of cooperation
- Cyber Security (CS)
  - Fluidity of response
  - Clarity of understanding
  - Ubiquity or extent of influence
  - Accuracy

Key Needs:
- Discoverability & availability
- Transport interoperability
- Data/object model interoperability

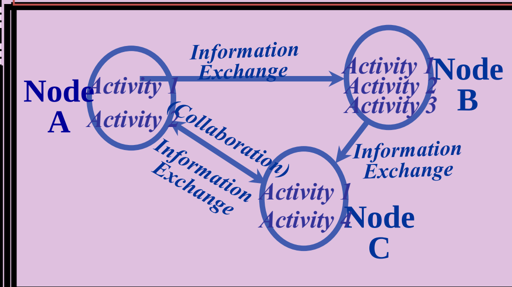
Key Metrics:
- Urgency:
  - Data/topic latency, service response time, application timeliness
- Priority:
  - Precedence of user requests, data, and services
- Cyber Security (CS)
  - Data Trust: integrity & availability, fault tolerance, accessibility
  - Security: data confidentiality, authentication, non-repudiation

Key Needs:
- Network interoperability
- Physical interoperability

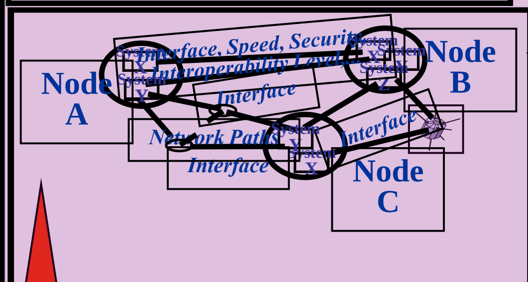
Key Metrics:
- Urgency:
  - Transport lag or delay, jitter, packet loss, packet errors
- Priority:
  - Class of service, differentiated service, precedence, preemption, guaranteed service
- Cyber Security (CS):
  - Data Trust: Availability, Connectivity (fixed, mobile)
  - Security: encryption, intrusion detection, authentication, authorization, access control

The A Word & Components

All Viewpoint (The content & terminology/definitions)



The Operational Viewpoint **describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission or business objective.**



The Systems Viewpoint **describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational view.**

- **Information Format & Content**
- **Information Transport**
- **Information Processing**
- **Information Assurance**
- **User interface**

The Standards Viewpoint **describes the profile of rules, standards, and conventions governing systems implementation.**

Functional & Organizational

"AS-IS" & "T0-BE(s)"

Non-Materiel Solutions

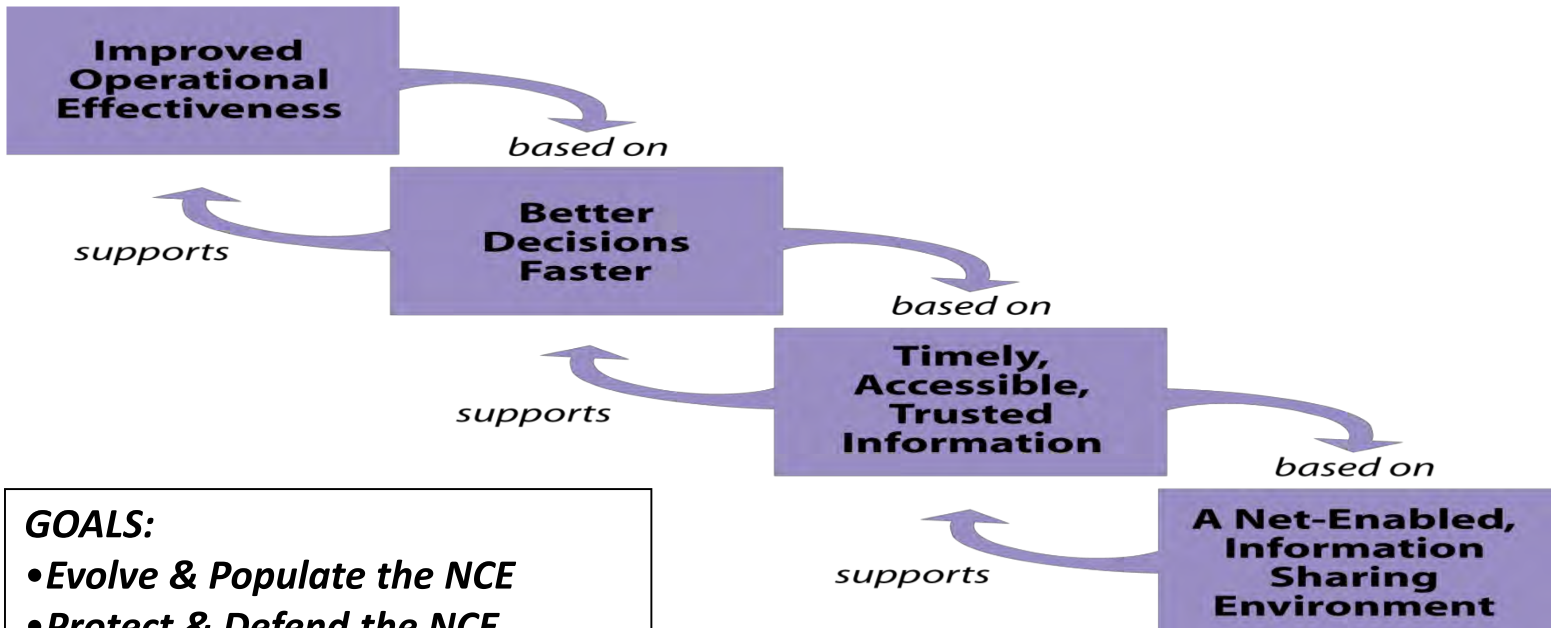
Information Technology Standards Registry

Keep this equation balanced: OV = SV + Non-Materiel

Net Enabled Operations

Net Centric Environment (NCE): Objective, Goals & Description

Objective: ***A*****ll users, whether known or unanticipated, are able to easily discover, access, trust, and use the data/information that supports their mission objectives unconstrained by their location or time of day.**

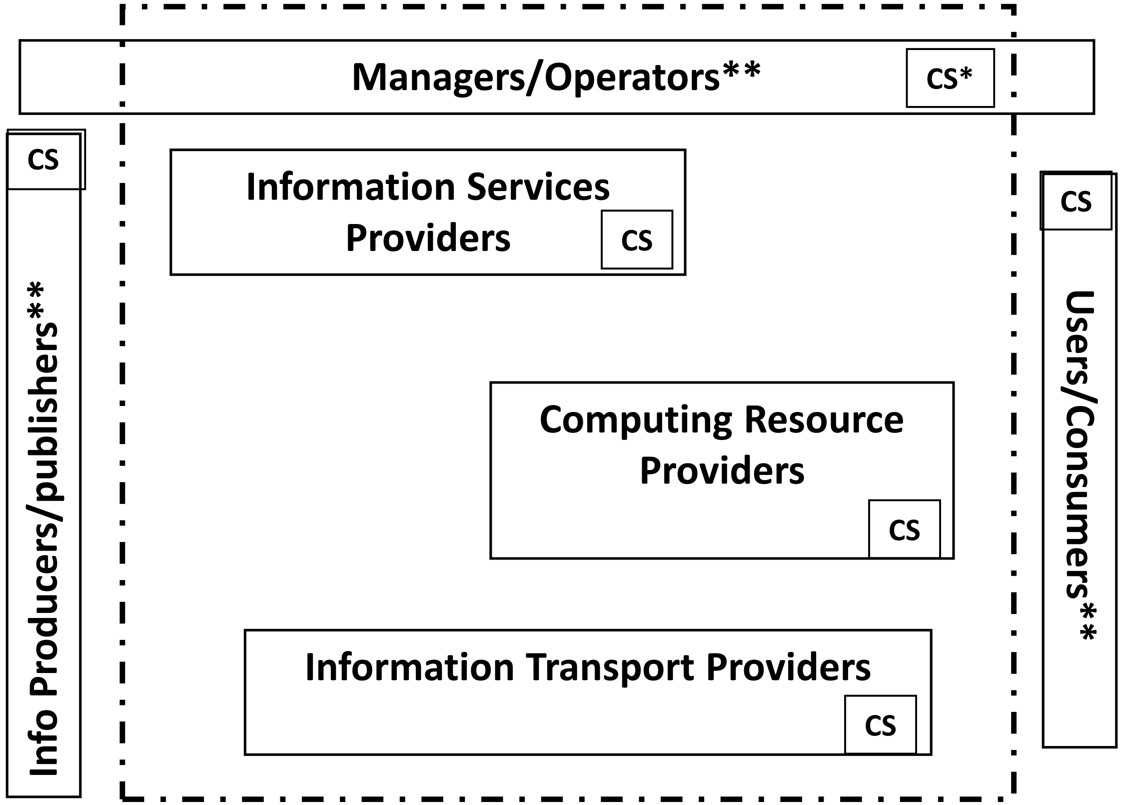


GOALS:

- ***Evolve & Populate the NCE***
- ***Protect & Defend the NCE***
- **Manage & Operate the NCE**

The NCE is implemented with evolving balanced & synchronized sets of Process, Organization, People, Information & Materiel (POPIM) Solutions.

Net Centric Environment: Functional Performers

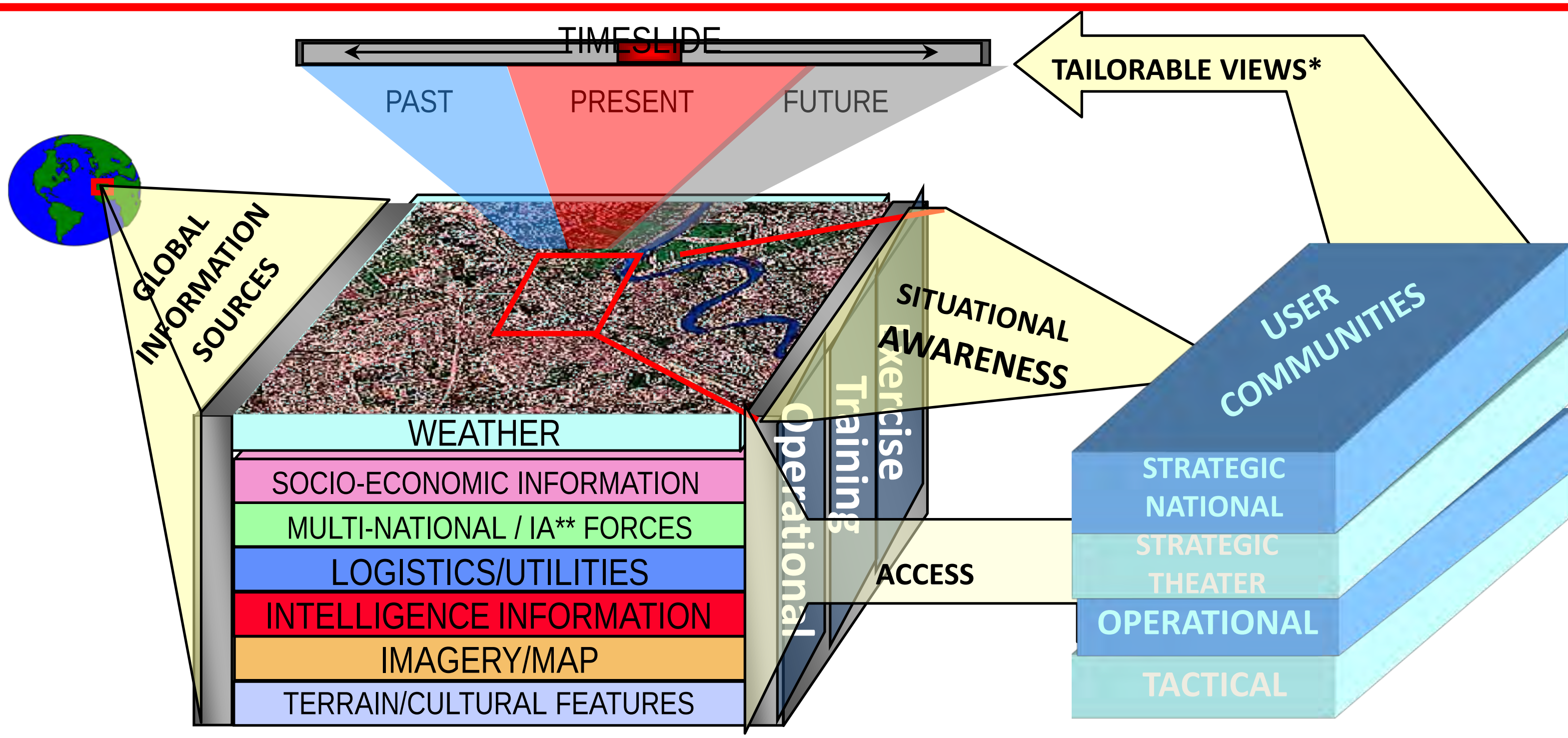


- *Behavior and relationship characteristics include: Quality of Service; Quality of Protection; Addressing; Tagging of content & roles/Identities;*
- *Information Forms include voice, video, images, text, graphics….*

** CS = Cyber Security*

*** Includes Software Applications whether hosted locally or by a computing resource provider.*

Situational Awareness in a Net Centric Environment



<u>Situational awareness</u> is tailored*, timely, comprehensive, and accurate knowledge of the battlespace (or area of interest) that provides the Warfighter (Commander/Decisionmaker) a consistent view of all militarily relevant information on friendly (blue) and adversary (red) forces, non-combatants (gray personnel), and the battlespace (or area of interest).

(Notes: *"User Defined Operational Picture": ** IA=Inter-Agency)

Net Centric Attributes

Attribute	Description
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g. precedence, preemption) .
Secure & available information transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation. Includes encryption for data at rest.
Post in parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g. raw, analyzed, archived).
Smart pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g. discovery). User Defined Operational Picture vice Common Operational Picture.
Information/Data centric	Information/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on “desktop” or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user’s role, identity & technical capability.
Quality of Transport service	Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

QUESTIONS?

Definitions of Functional Performers (1 0f 2)

<u>Computing Resource Provider:</u>
A capability that can respond to a request from a user or another service to store, process, manage, and control data or information (shared and/or distributed) through an external interface.

<u>Information Service Provider:</u>
A capability that can respond to a request from a user or another service to provide a specific functionality, such as the ability to post, discover, access, process and display hosted information and data (including positioning, navigation, and timing services) across an "enterprise" based on established data standards.

<u>Information Provider (i.e., Producer or Publisher):</u>
A capability that produces information and data, based on established data standards, and provides that information and data using any of a number of distribution methods, which include bilateral distribution to known users, broadcast, and publish/post or subscribe/pull models, for use in accomplishing a mission.

Definitions of Functional Performers (2 0f 2)

Manager/Operator:
A capability that provides the ability to monitor, manage, control, protect, and configure information transport, information services, and the underlying computing resources that provide end-user services, as well as connectivity to "enterprise" application services.

User/Consumer:
A capability that utilizes or consumes information transport, computing resources, or information services to perform its intended function.

Information Transport Provider:
A capability that provides the ability to transport information and services via assured end-to-end connectivity across the operational environment.

Idaho National Laboratory “Defense Acquisition System” System of Systems Engineering

Abstract ID: #19736

For:
NDIA
20th Annual Systems Engineering Conference
23-26 October 2017

Prepared by:
Idaho National Laboratory (INL)
Larry Dean Harding
Systems Engineering

Idaho National Laboratory

INL Systems Analyses & Engineering Contacts

Mitchell Kerman
Division Director
(208) 526-3631
mitchell.kerman@inl.gov

Ron Klingler
Department Manager
(208) 526-0183
ron.klingler@inl.gov

NDIA Presenter

Larry Harding
Systems Engineer
(208) 526-6111
dean.harding@inl.gov

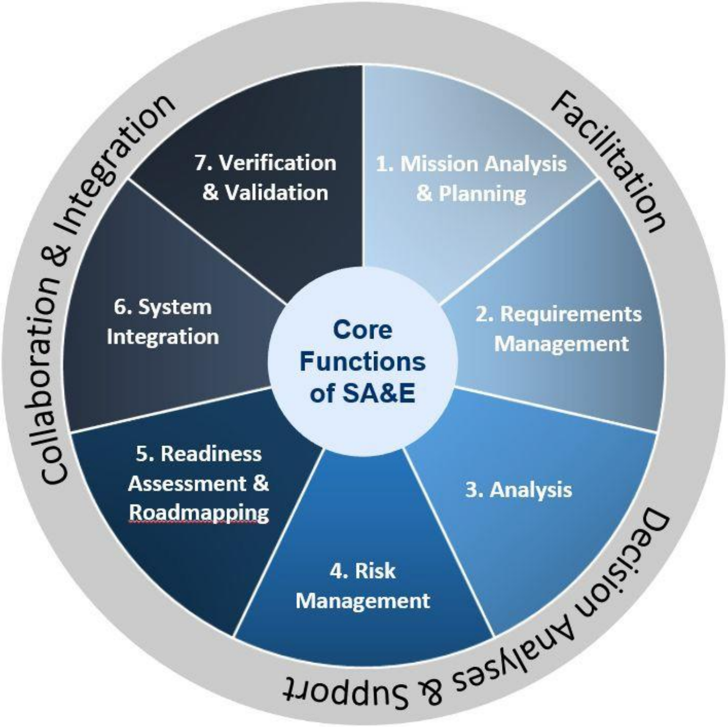
John Collins
Group Lead for
Energy & Environment Projects
(208) 526-3372
john.collins@inl.gov

Jody Henley
Group Lead for
Nuclear Projects
(208) 526-1979
jody.henley@inl.gov

Shyam Nair
Group Lead for
Process & Data Sciences
(208) 526-3071
shyam.nair@inl.gov

INL Systems Analyses & Engineering Web Page
https://systemsengineering.inl.gov

Core Functions –
INL Systems Analyses & Engineering



1

- Concise Problem Definition
- Understanding Important Customer Needs
- Concise System/Project Boundaries
- Strategic Planning & Baselines
- "Concept" of Operations
- Stakeholder Buy-in
- Acquisition Strategy
- White Papers

2

- Technical, Functional, and Operational Analysis
- Requirements Elicitation, Clarification, Derivation, and Tracking
- Traceability, Change Control, and Impact Analysis
- Requirements Verification and Validation Planning

3

- Analysis of Alternatives
- Decision Metrics
- Organization Analysis & Visualization of Complex and Big Data
- Uncertainty Analysis & Probabilistic Risk Assessment
- Risk-informed Decision-making
- Integration of Viable Solutions
- Chemical Process Engineering & Analysis
- Chemical Process Control
- Computational Fluid Dynamics

4

- Risk Identification and Tracking
- Justification for Funding Contingency
- Risk Handling Strategy
- Risk Reduction Plan
- Risk-informed Path Forward

5

- Technology Maturity Analysis
- Technology Development Roadmap/Path Forward
- Roadblock Identification & Mitigation
- System Assessments (e.g., Energy Systems)

6

- Program & Project Integration
- Laboratory-wide R&D Integration
- Laboratories/Industries/ Universities Integration
- Integration of System Elements
- Systems of Systems Analyses

7

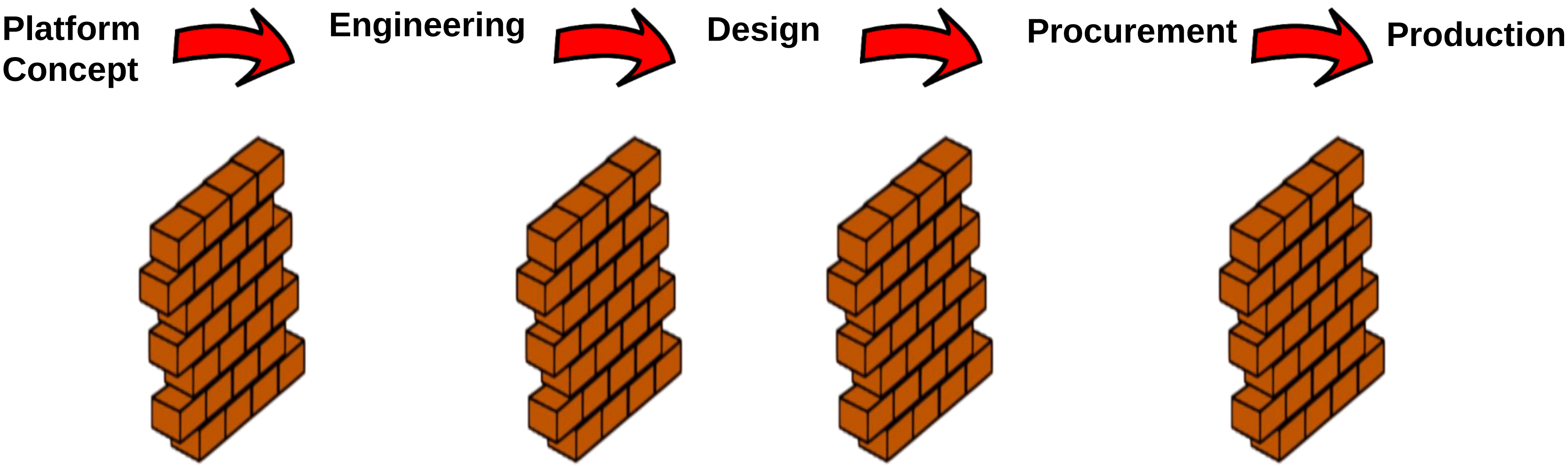
- Verification of System Performance and Functionality
- Validation of System Specification and Design Parameters
- Test Planning and Implementation

INL/MIS-17-42149

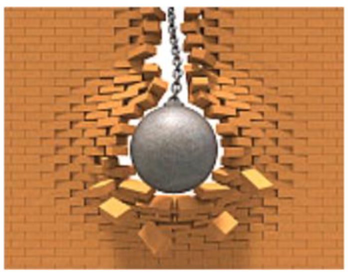
“Defense Acquisition System” System of Systems Engineering

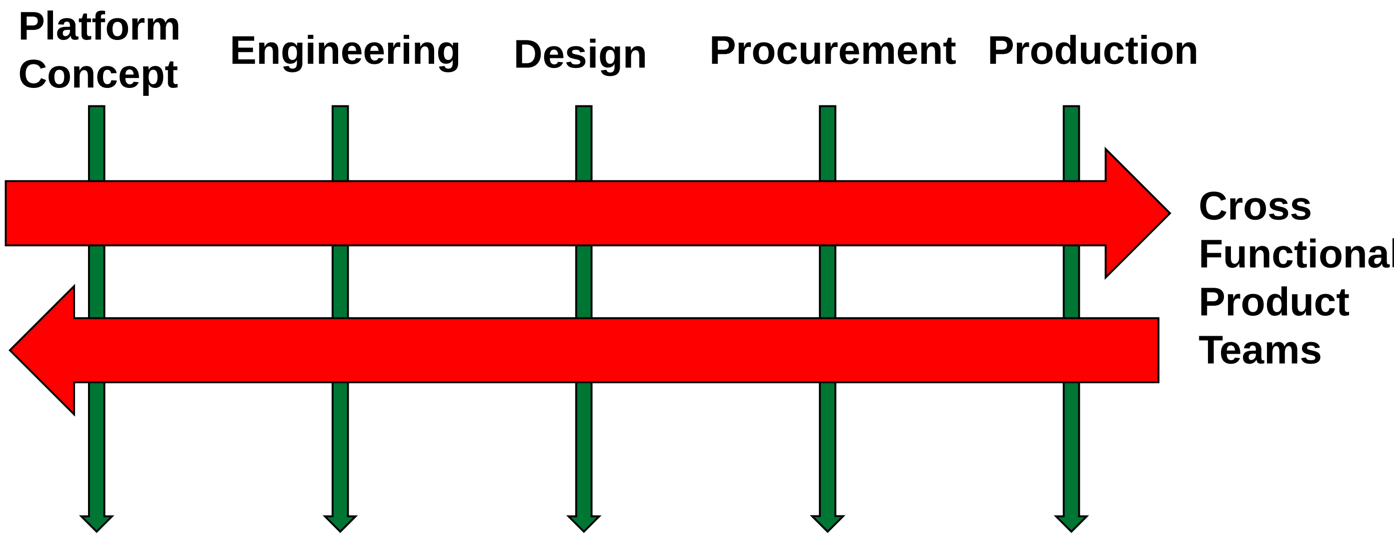
The Defense Acquisition System is a Joint Services process with the primary function to develop and provide DoD military capabilities. Because all branches of the military use this common system, by nature it is a very complex and lengthy process. The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System, is composed of three major lanes of authority: (1) The Defense Acquisition System; (2) Joint Capabilities Integration & Development System (JCIDS); and (3) Planning, Programming, Budgeting & Execution Process. The purpose of this presentation is to introduce the Idaho National Laboratory’s (INL) seven step process and a holistic approach of systems integration techniques directed at these three lanes of authority.

Chrysler's Mini Van Platform



Chrysler's Mini Van Platform



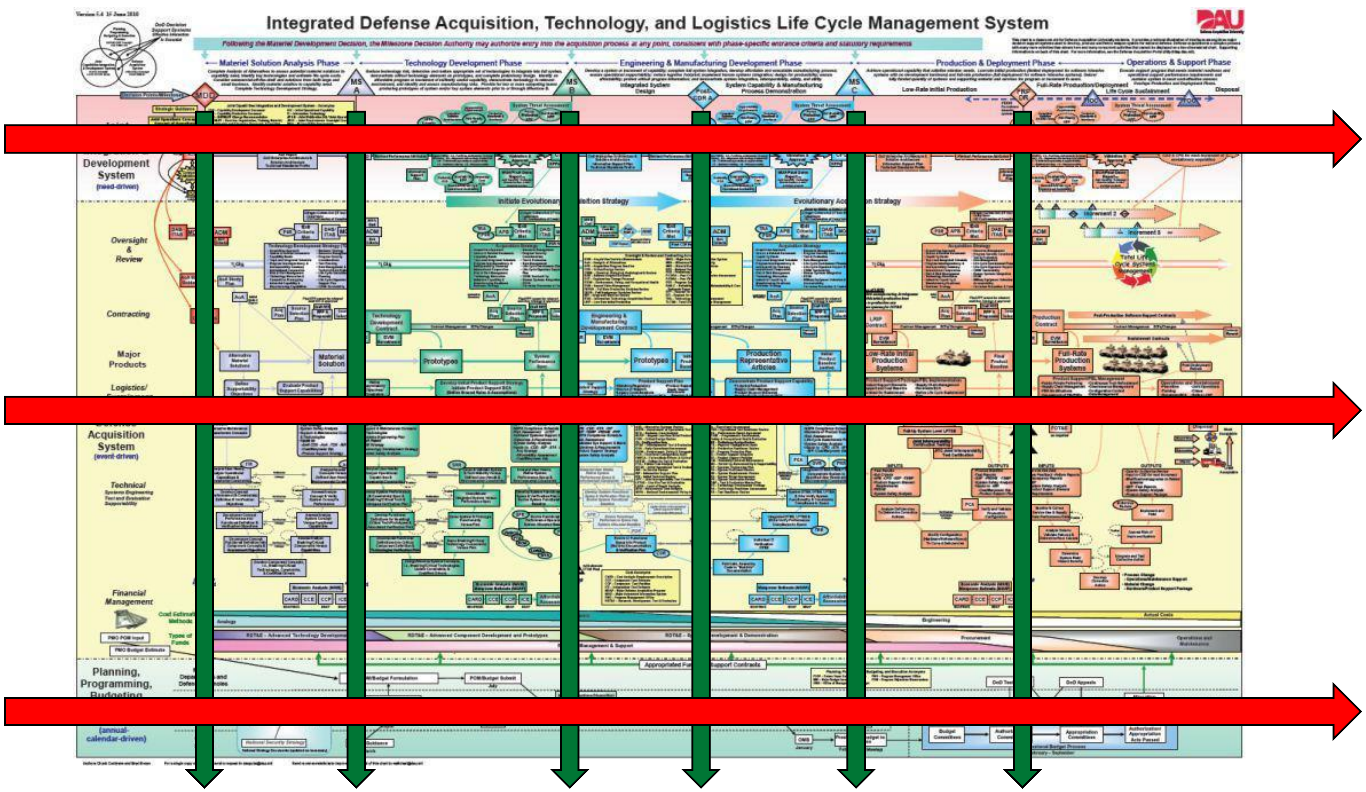


Keiretsu

Enhanced Communications and Coordination
Improve Efficiency
Applicable to Several Vehicle Platforms

INL/MIS-17-42149

INL Seven Step Integration Methods



JCIDS

Defense Acquisition System

Planning, Programming, Budgeting & Execution

Analysis of Alternatives

Requirements Definition and Derivation

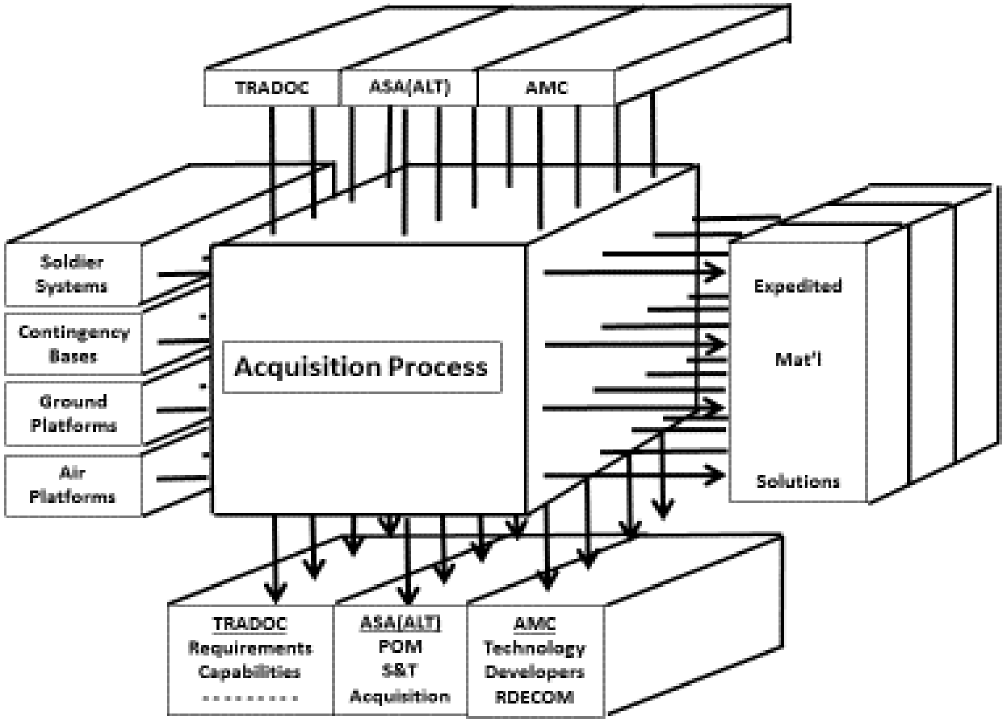
Risk Management

Technology Readiness Assessments

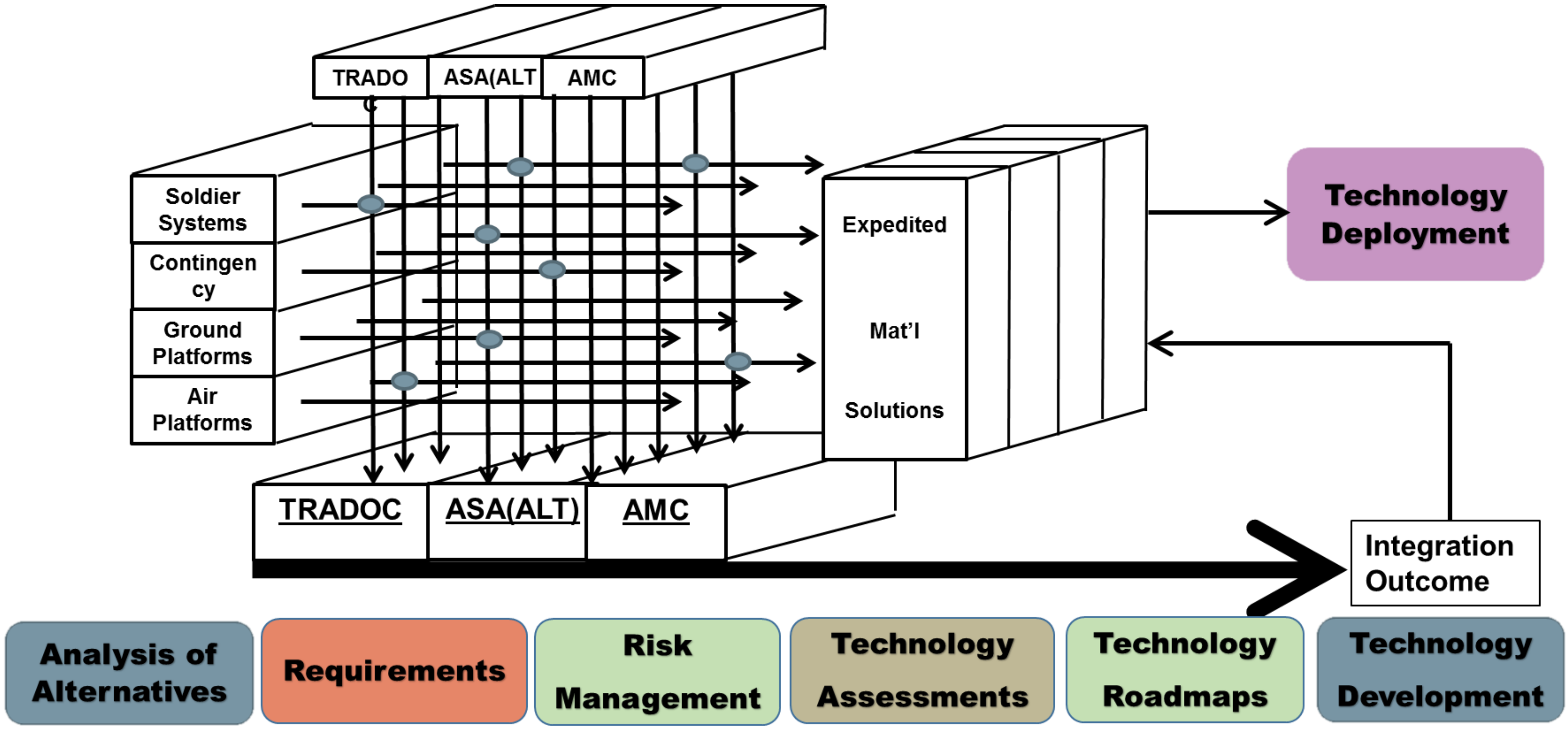
Technology Development Roadmaps

Technology Development

Deployment



TRADOC
ASA(ALT)
AMC
Soldier Systems
Contingency Bases
Ground Platforms
Air Platforms
Acquisition Process
Expedited
Mat'l
Solutions
TRADOC
Requirements
Capabilities
ASA(ALT)
POM
S&T
Acquisition
AMC
Technology
Developers
RDECOM



TRADOC
ASA(ALT
AMC
Soldier Systems
Contingency
Ground Platforms
Air Platforms
Expedited
Mat'l
Solutions
Technology Deployment
TRADOC
ASA(ALT)
AMC
Integration Outcome
Analysis of Alternatives
Requirements
Risk Management
Technology Assessments
Technology Roadmaps
Technology Development

Assess Technology Maturity

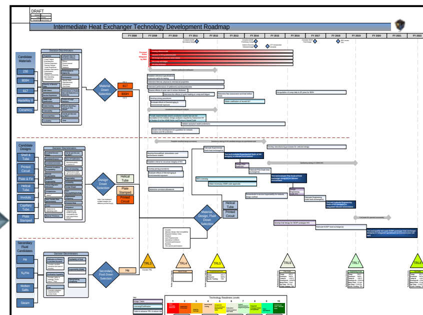
NGNP Area System	Min TRL
NGNP	3
Nuclear Heat Supply System (NHSS)	4
Reactor Pressure Vessel	4
Reactor Vessel Internals	4
Reactor Core and Core Structure	4
Fuel Elements	4
Reserve Shutdown System	5
Reactivity Control System	4
Core Conditioning System	4
Reactor Cavity Cooling System	4
Heat Transfer System (HTS)	3
Circulators	5
Intermediate Heat Exchanger	3
Cross Vessel Piping	4
High Temperature Valves - Flapper	6
High Temperature Valves - Iso, Relief	4
Power Conversion System (PCS)	4
Steam Generator	4
Balance of Plant (BOP)	3
Fuel Handling System - Prismatic	4
Fuel Handling System - Pebble Bed	5
Instrumentation & Control	3

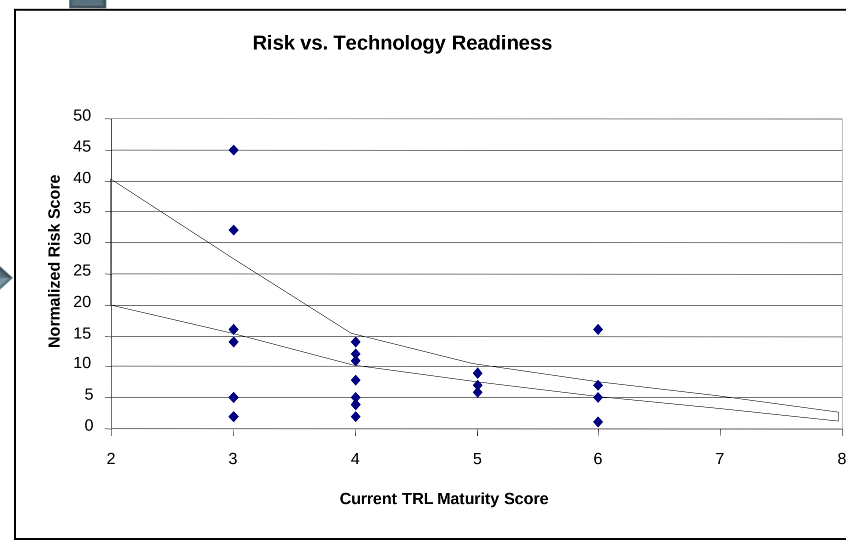
- **Select Systems, Structures, Components**
- **Rate Technology Readiness Level**

Advance TRLs & Reduce Risk

- **Develop Risk Register**
- **Systematically Reduce Risk**
- **Execute to Risk – Work – off Metric**

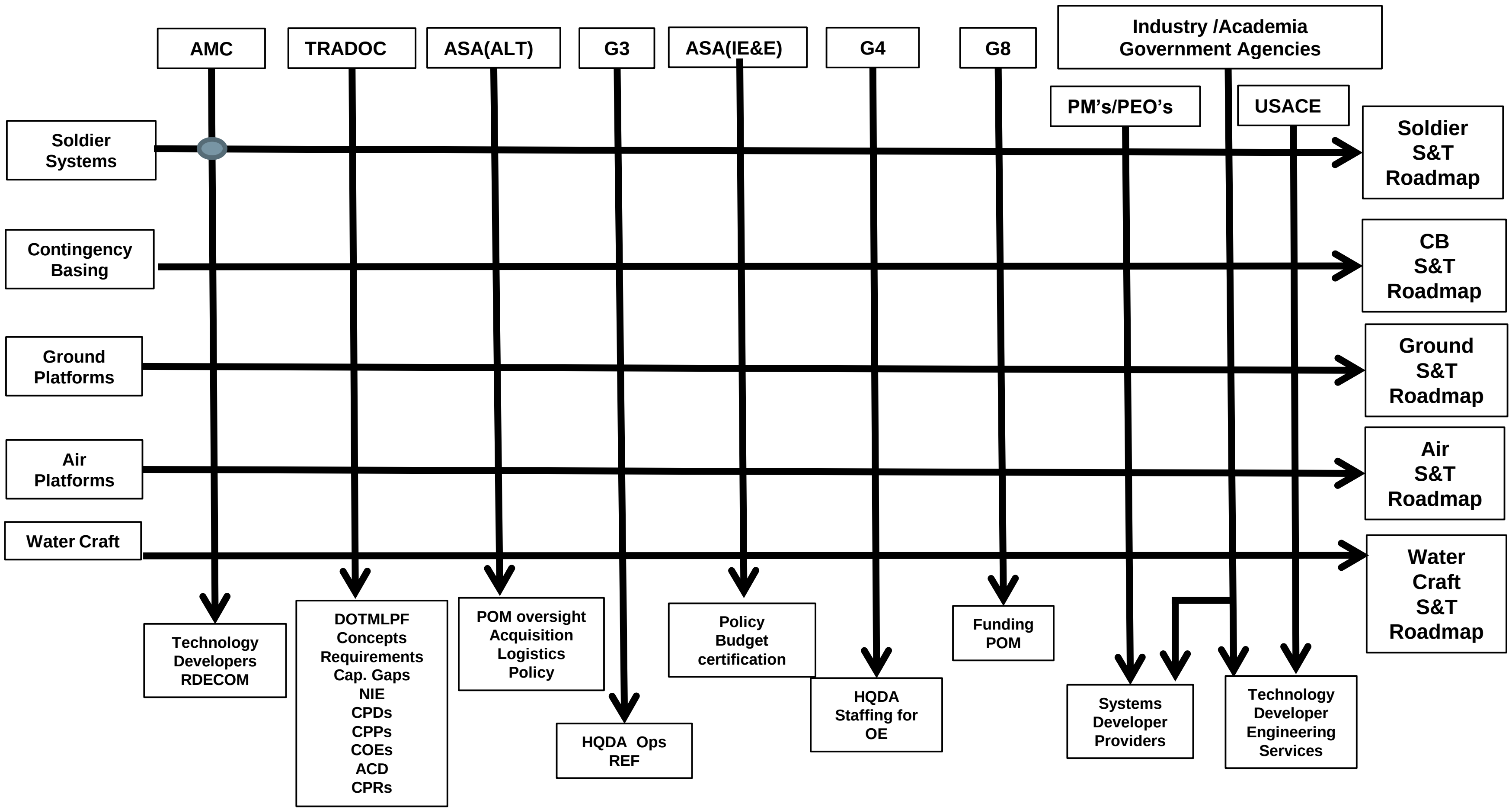
Build the Roadmap & Define Path Forward

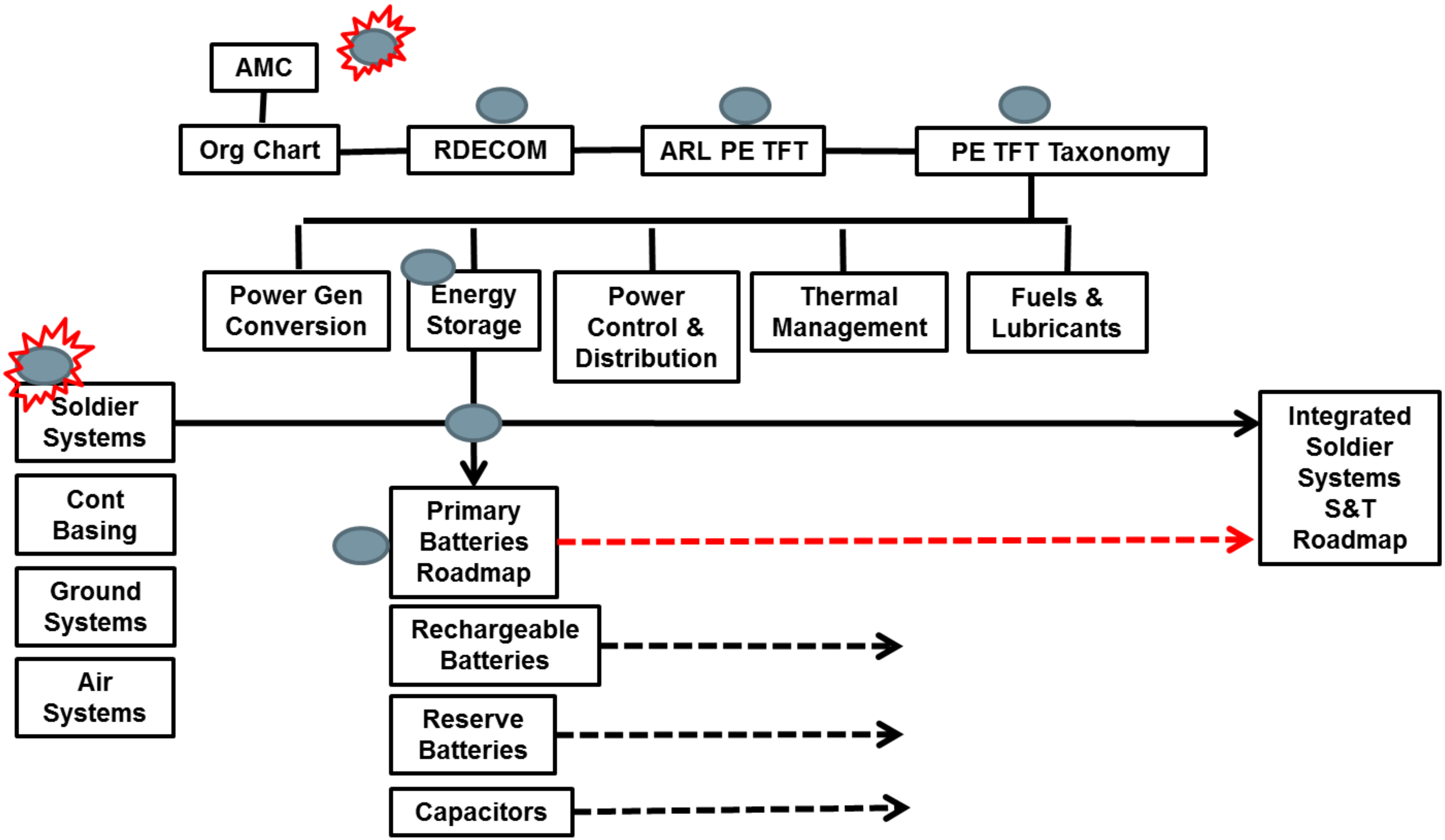




Execute the Roadmap & Refine Path Forward

- **Develop Technology Maturation Steps**
- **Define Decision Points**
- **Establish Performance Metrics**


AMC
TRADOC
ASA(ALT)
G3
ASA(IE&E)
G4
G8
Industry /Academia Government Agencies
PM's/PEO's
USACE
Soldier Systems
Contingency Basing
Ground Platforms
Air Platforms
Water Craft
Soldier S&T Roadmap
CB S&T Roadmap
Ground S&T Roadmap
Air S&T Roadmap
Water Craft S&T Roadmap
Technology Developers RDECOM
DOTMLPF Concepts Requirements Cap. Gaps NIE CPDs CPPs COEs ACD CPRs
POM oversight Acquisition Logistics Policy
HQDA Ops REF
Policy Budget certification
HQDA Staffing for OE
Funding POM
Systems Developer Providers
Technology Developer Engineering Services


AMC
Org Chart
RDECOM
ARL PE TFT
PE TFT Taxonomy
Power Gen Conversion
Energy Storage
Power Control & Distribution
Thermal Management
Fuels & Lubricants
Soldier Systems
Cont Basing
Ground Systems
Air Systems
Primary Batteries Roadmap
Rechargeable Batteries
Reserve Batteries
Capacitors
Integrated Soldier Systems S&T Roadmap

“Defense Acquisition System” System of Systems Engineering

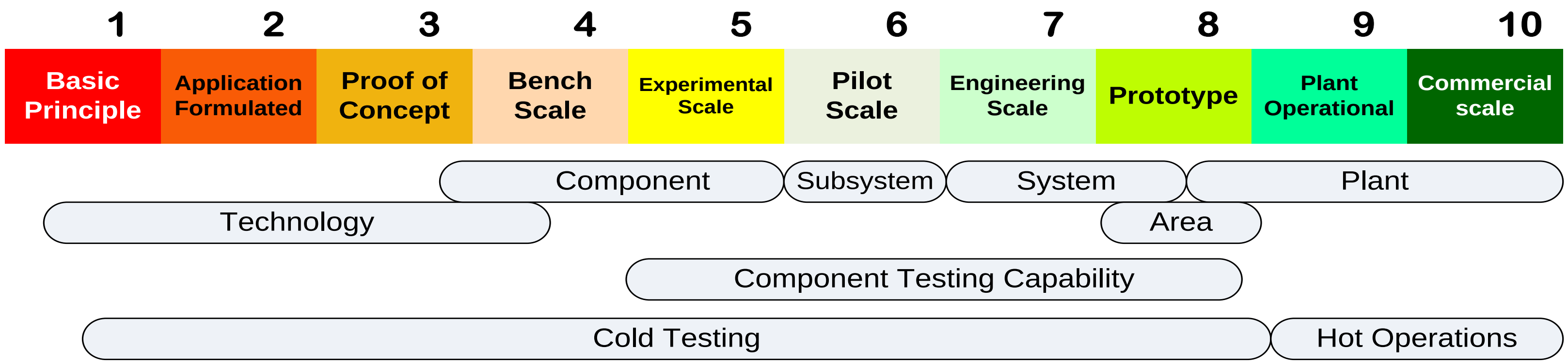
In general there are several hundred relationship nodes that are embedded in the Acquisition Process that presents numerous stopping points due to analysis, reviews, and approvals and in some cases contention due to stove pipe lines of authority and friction between organizations.

The construct provides three dimensional integration and applies the INL seven step integration methods to create technology roadmaps and expedited material solutions that could be directly applied to the Defense Acquisition Process and the JCIDS process.

- Early Development Planning
- Architecture
- Interoperability & Systems Integration
- Systems-of-Systems Systems Engineering
- Systems Engineering Effectiveness

Backup Slides

Technology Readiness Levels



Technology Readiness Assessment

The structures, systems, and components (SSC) comprising the Defense Acquisition Process are synthesized and evaluated through a Technology Readiness Assessment and assigned Technology Readiness Levels (TRL) based on technical maturity. For lower TRLs, assessments typically occur at an individual technology or component level. To mature the technology or component, integrated testing or modeling must occur at increasingly larger scales, with integrated components, and in increasingly relevant environments, thus achieving higher TRL ratings as the project progresses. A validated TRL baseline is established for the proposed physical design and is periodically reassessed throughout the project life cycle. Validated TRLs provide project management one measure of the level of technological risk encountered by the project.

Technology Development Roadmaps

With the baseline TRLs in place, technology development roadmaps (TDRMs) can then be generated to define the decision discriminators, forecast down selection timeframes, and focus project research and development and engineering tasks on increasing levels of technical maturity. TDRMs provide the required structure and are the primary means to systematically perform risk-informed decision making, quantify uncertainty, down select technologies, and mature technologies in a cost-effective and timely manner. Tasks include modeling, testing, bench-scale demonstrations, pilot-scale demonstrations, and full integrated prototype demonstrations. TDRMs for critical SSC are developed to:

- Set the project vision for technology maturation and risk resolution
- Identify the key selection discriminators and drive uncertainty reduction to inform technology and design down selection
- Ensure technology readiness is demonstrated through testing, modeling, simulations, piloting, and prototyping
- Provide early identification and resolution of technical risks
- Avoid late project technical challenges, which manifest themselves as cost overruns and schedule delays

Risk-Informed Project Readiness Assessment

The tasks needed to mature the technologies, as documented in the TDRMs, also reduce the technical project risk. Technical and programmatic risks including political decisions, social acceptance, and market demand are reviewed and risk handling strategies developed to reduce the probability of the risk event and lessen its damage should the event occur. While advancing project readiness, and engineering design. The resulting RISK-Informed Project Readiness Assessment serves to:

- Identify the tasks that provide the most efficient risk resolution
- Provide a path forward for reducing risk over the life of the project
- Link risk to project schedule and integrated priority list
- Integrate multiple stakeholders viewpoints into risk-informed path forward
- Provide a “Risk Work-off Metric” for the project to track risk to acceptable levels

Questions?

Larry Harding
Systems Engineer
(208) 526-6111
dean.harding@inl.gov

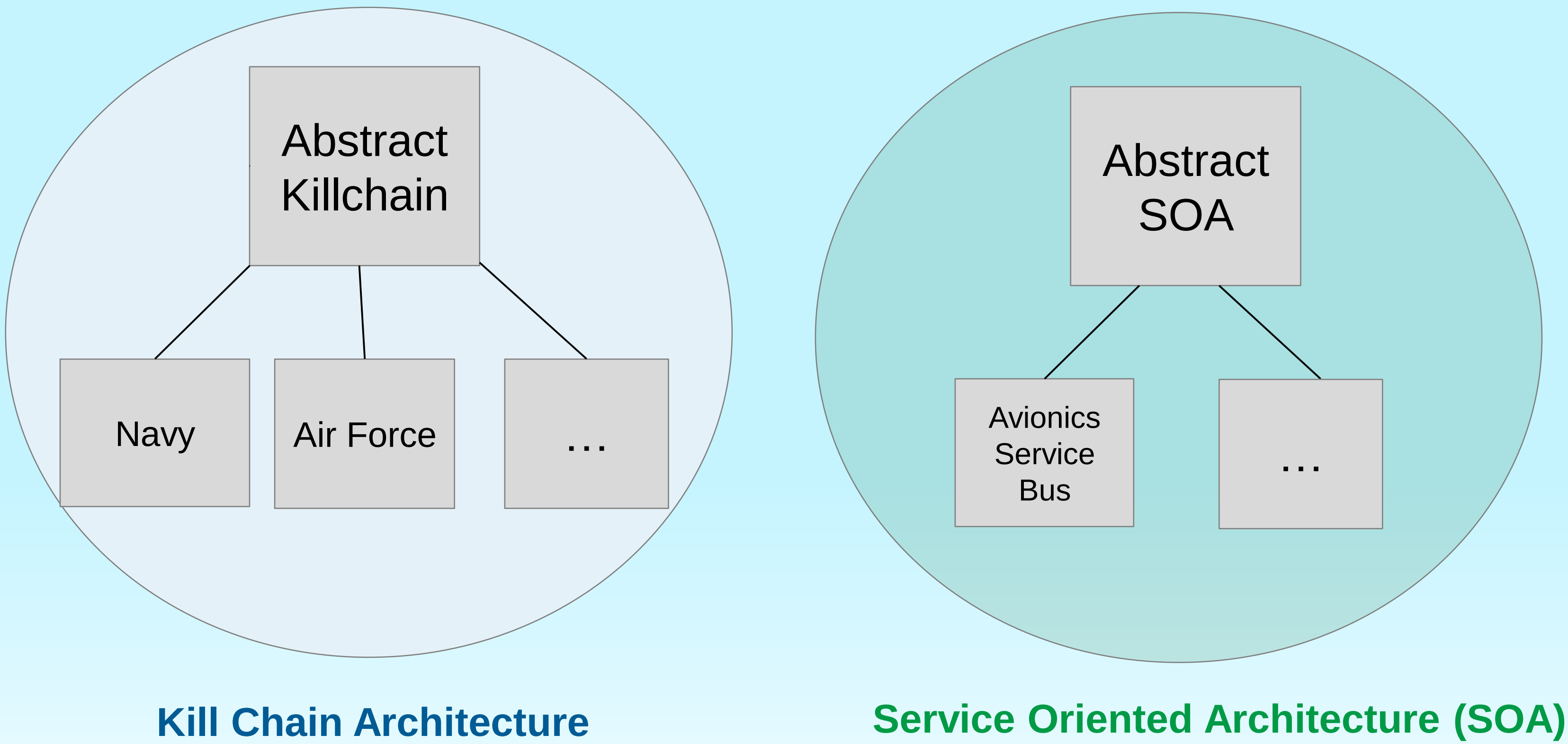
Scaling Model-Based System Engineering Practices for System of Systems Applications: Software Methods

October 2017

Janna Kamenetsky jannak@mitre.org
Laura Antul lantul@mitre.org
Dr. Aleksandra Markina-Khusid amk@mitre.org
Matt Cotter mjcotter@mitre.org
Dr. Judith Dahmann jdahmann@mitre.org

NDIA 20th Annual Systems Engineering Conference
http://www.ndia.org/events/2017/10/23/20th-systems-engineering-conference

Technical Approach: Inheritable Architectures



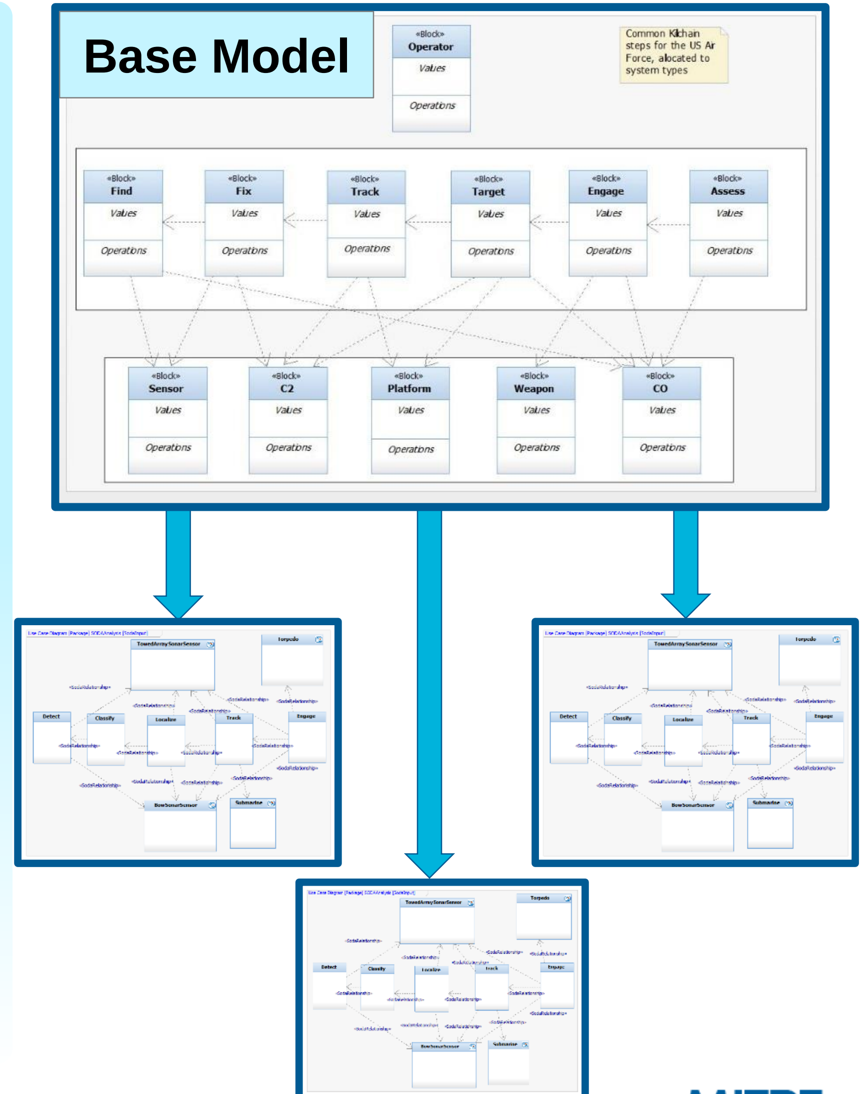
Enables Model Re-use corresponding to different architecture patterns

MITRE

Base Model Architecture

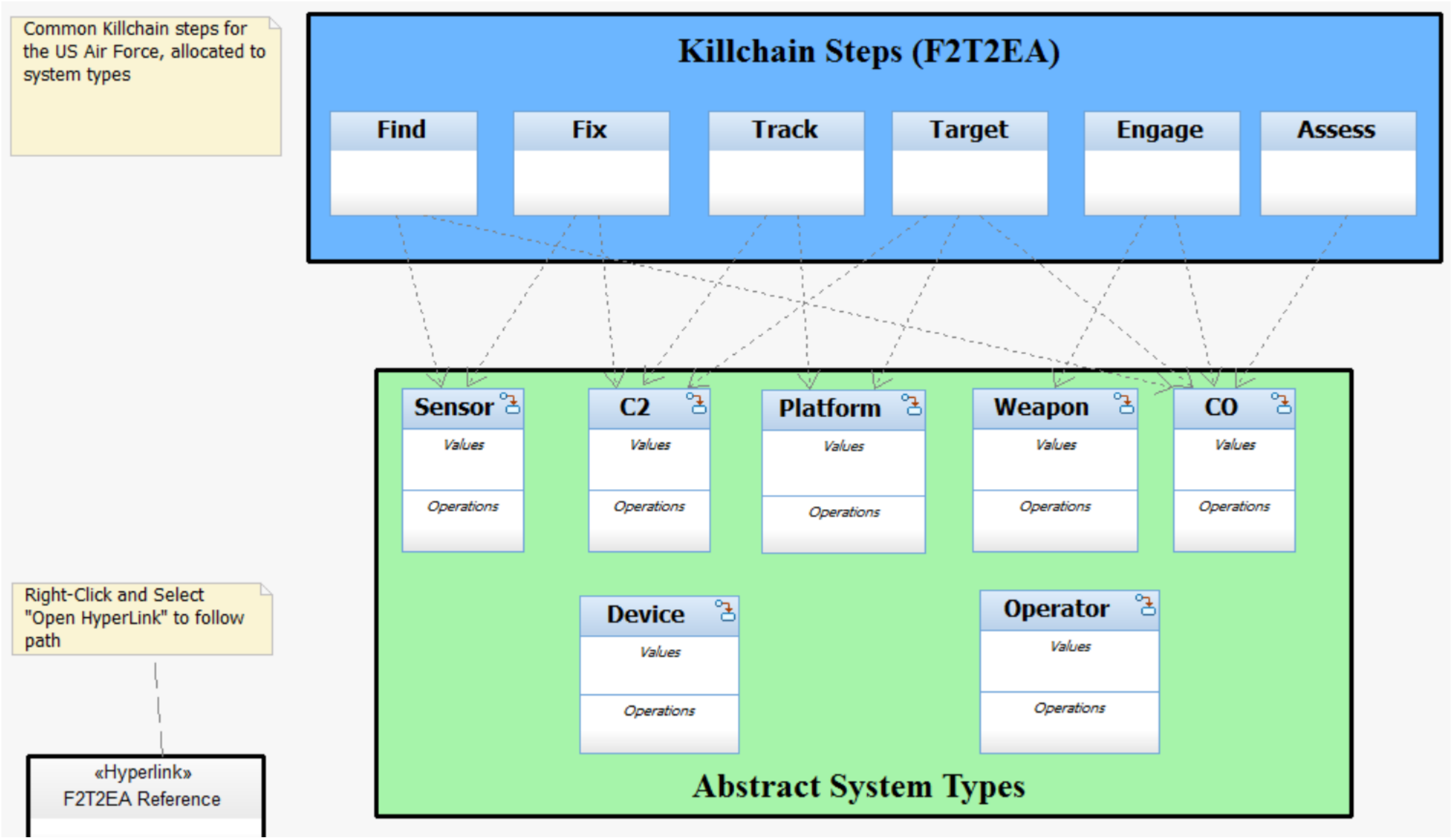
- **Base/Derivative Model Framework**
  - **Base Model captures key functional SoS architecture**
  - **Derivative model represent domain-specific behavior**

- **This approach helps:**
  - **Accelerate domain model development via Base Model reuse**
  - **Rapidly evaluate different options utilizing predefined stereotypes and analysis engines**
  - **Iterative design to continuously refine common SoS functions**

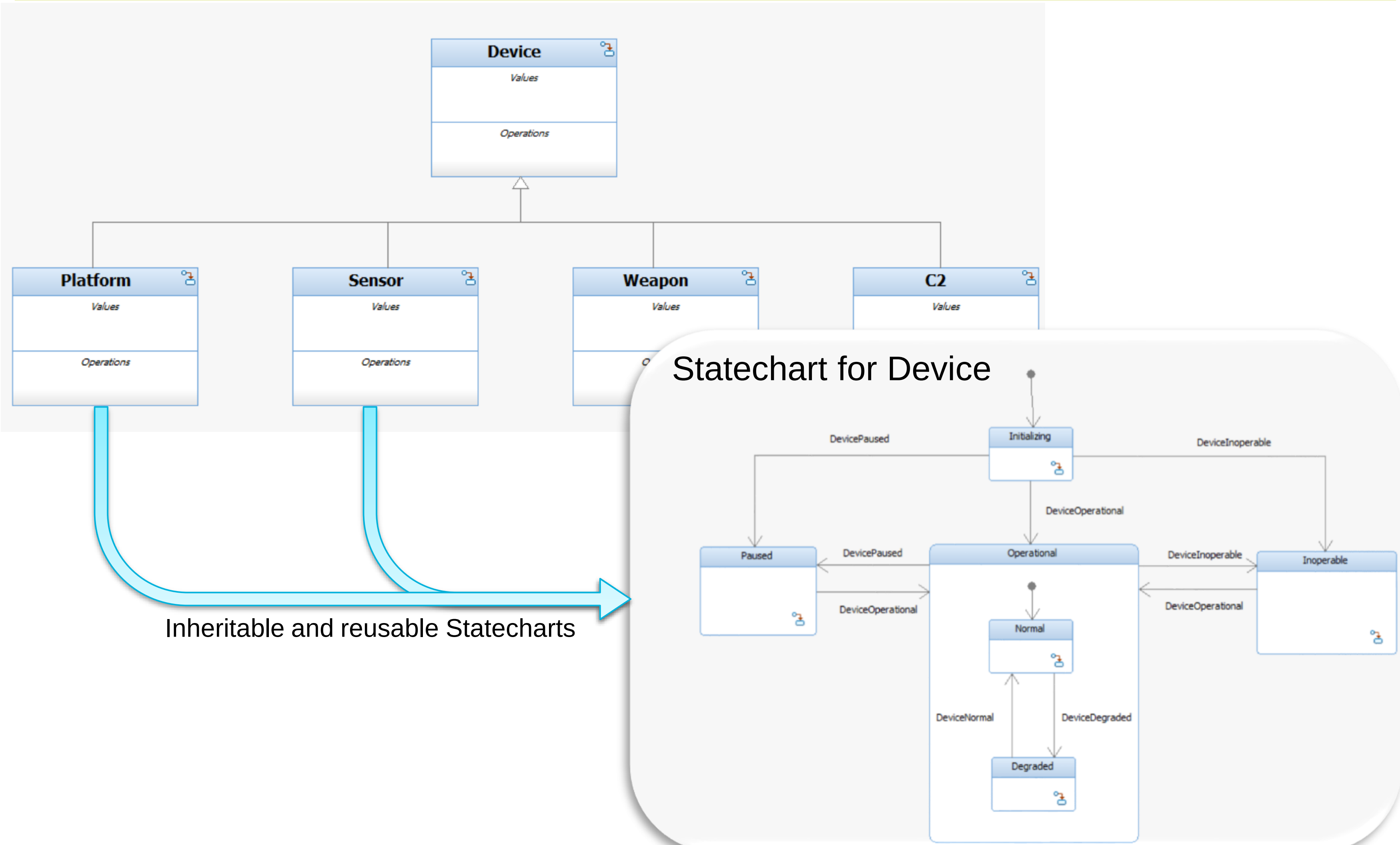


MITRE

Base Model: High Level Structure



Base Model: Inheritance Structure

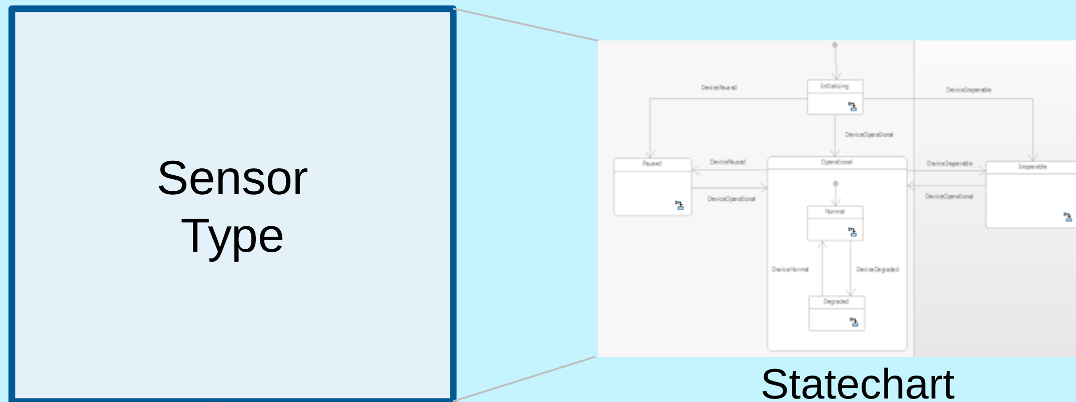


MITRE

BASE Model: Inheritable Types

BASE

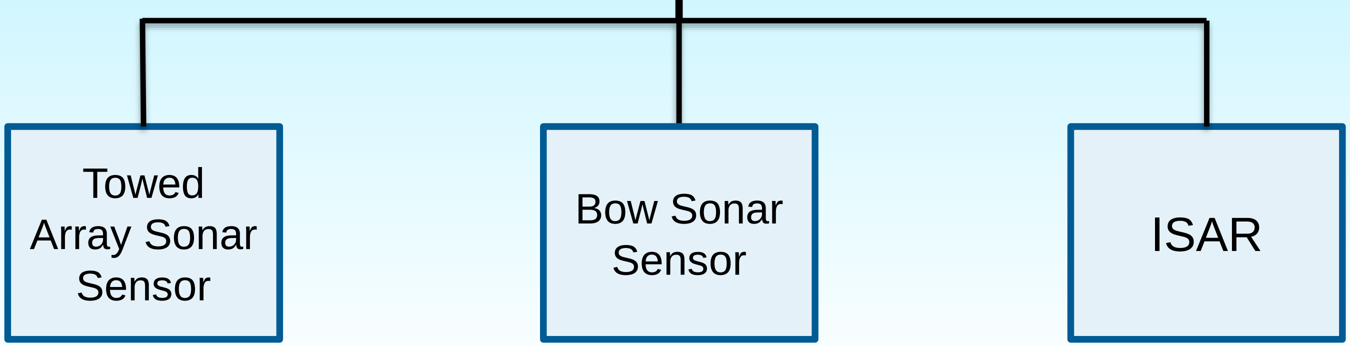
- <u>Operations (i.e. functions)</u>
  - processSignals()
- <u>Attributes (i.e. metrics)</u>
  - MaxRange



Statechart

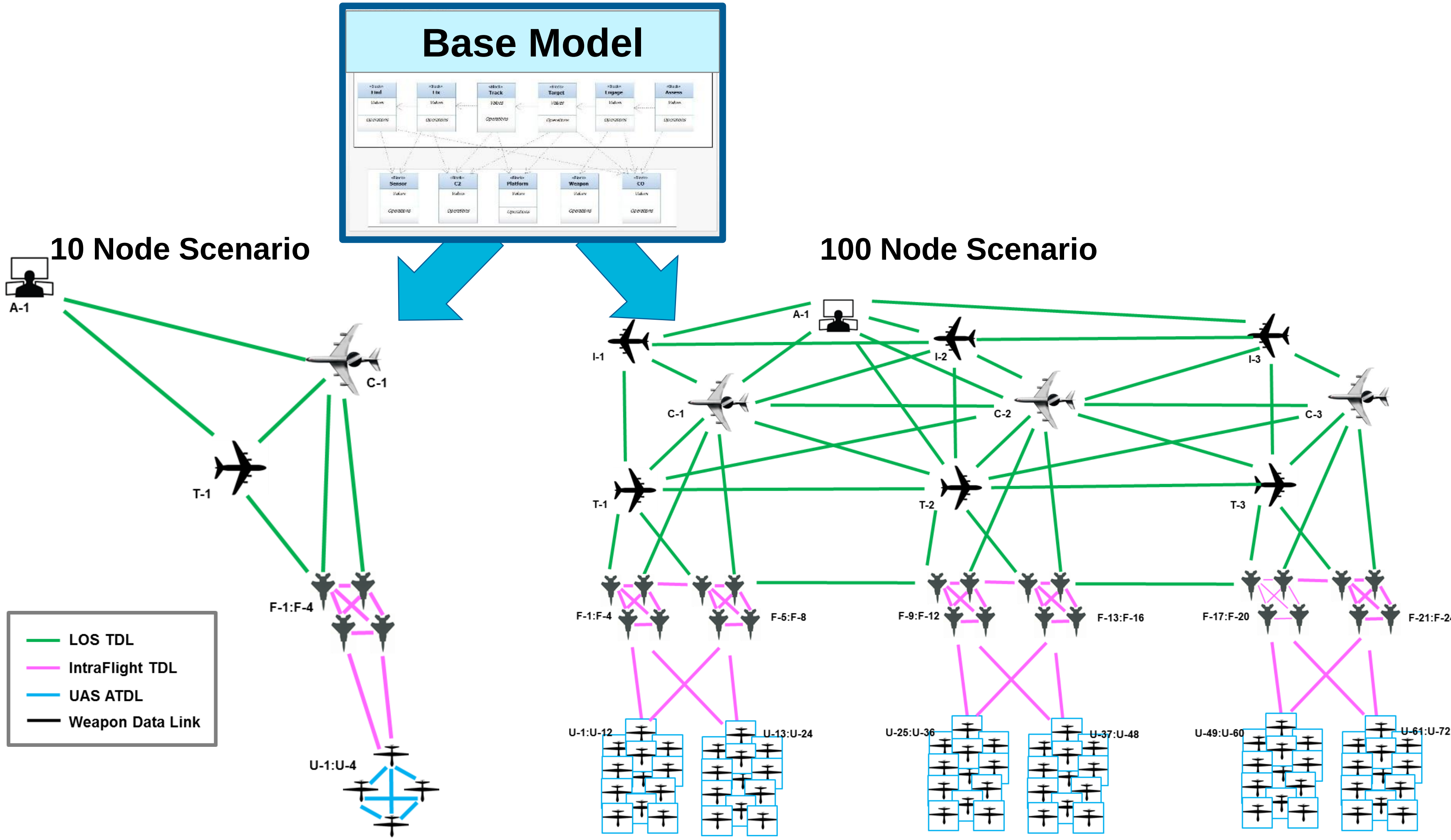
DERIVATIVE

(e.g. CDMaST)



MITRE

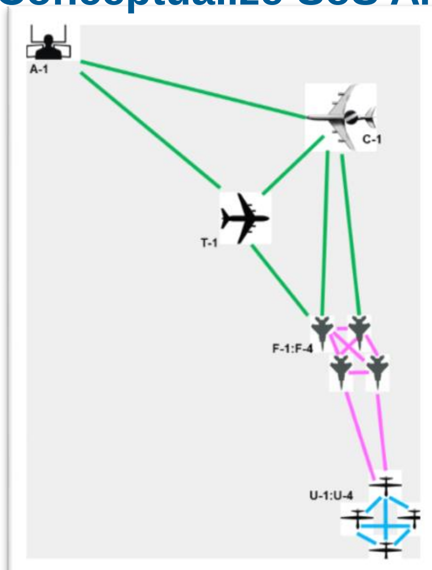
Base Model CSV Importer



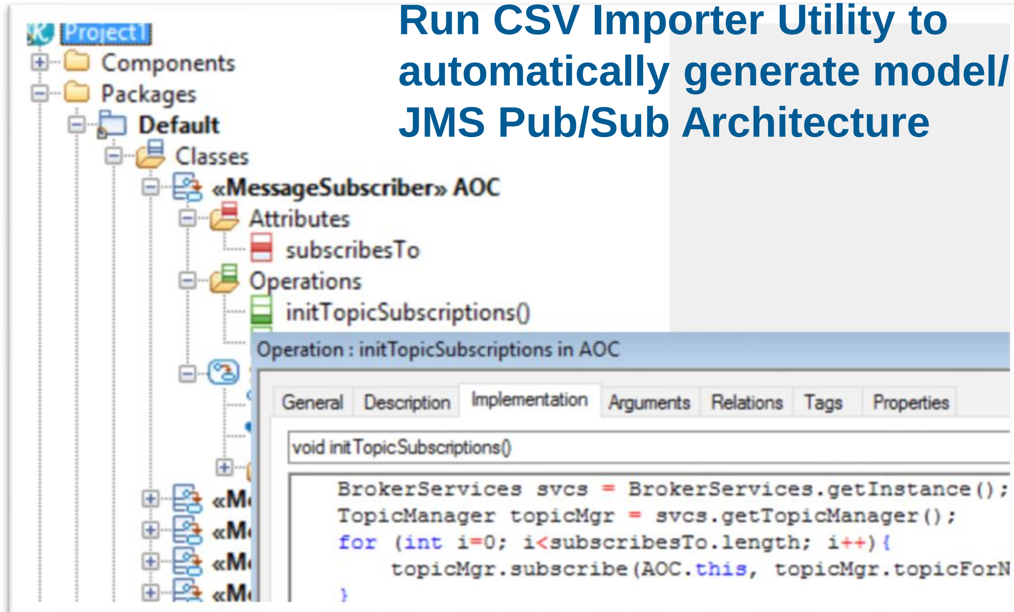
MBE Utility to reduce development effort associated with modeling large SoS complex networks

CSV Importer Utility

Conceptualize SoS Architecture



Run CSV Importer Utility to automatically generate model/ JMS Pub/Sub Architecture



Add Connectivity Framework

PUBLISHERS

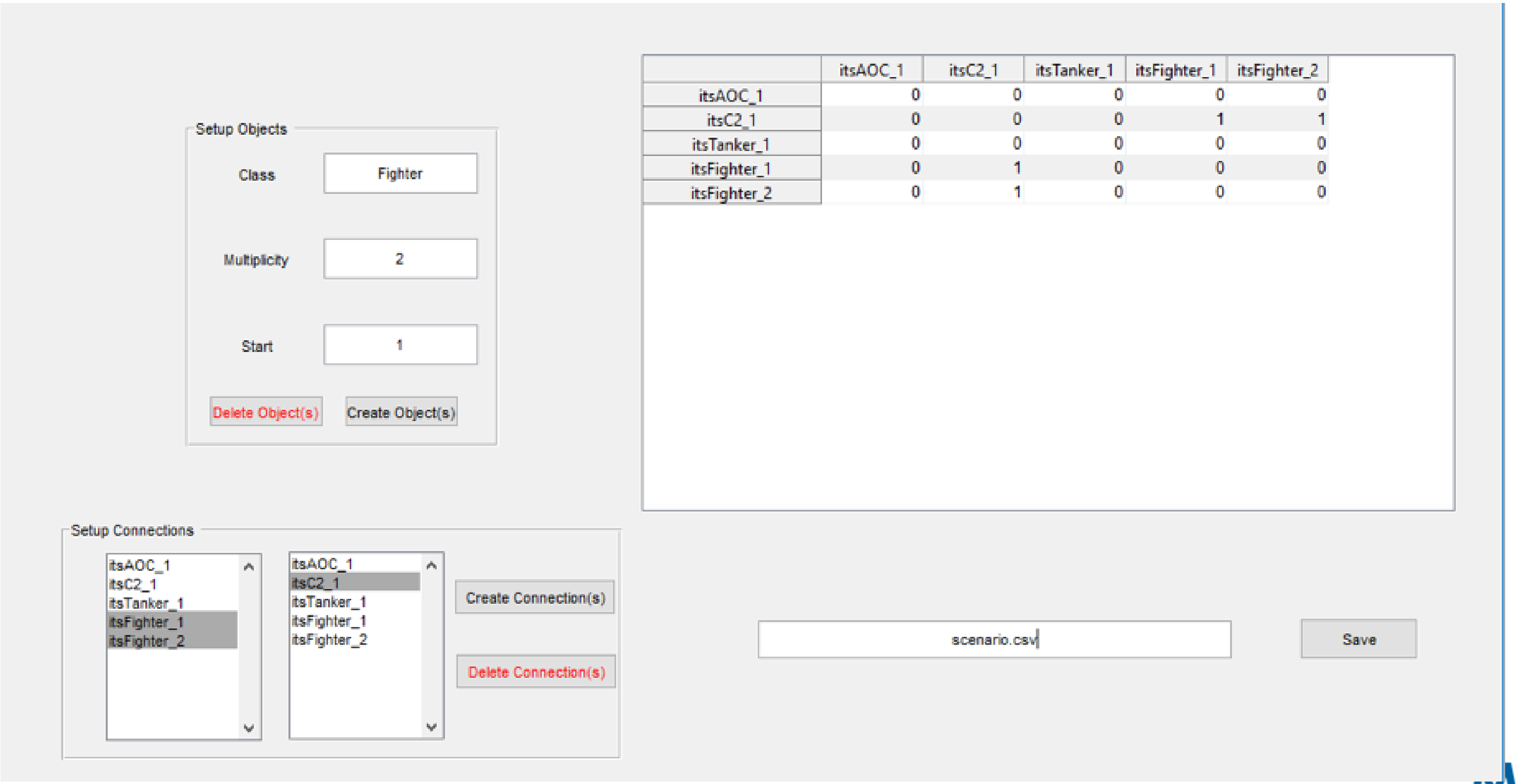
SUBSCRIBERS

	AOC	C2	Tanker	Fighter	UAS
AOC		threats, missionOutcome			
C2	aocDecisions			fightersToC2	
Tanker		beginMission, missionOutcome		lowFuel	lowFuel
Fighter		beginMission		intraFlightTDL	UASsToFighters
UAS				fightersToUASs	uasATDL

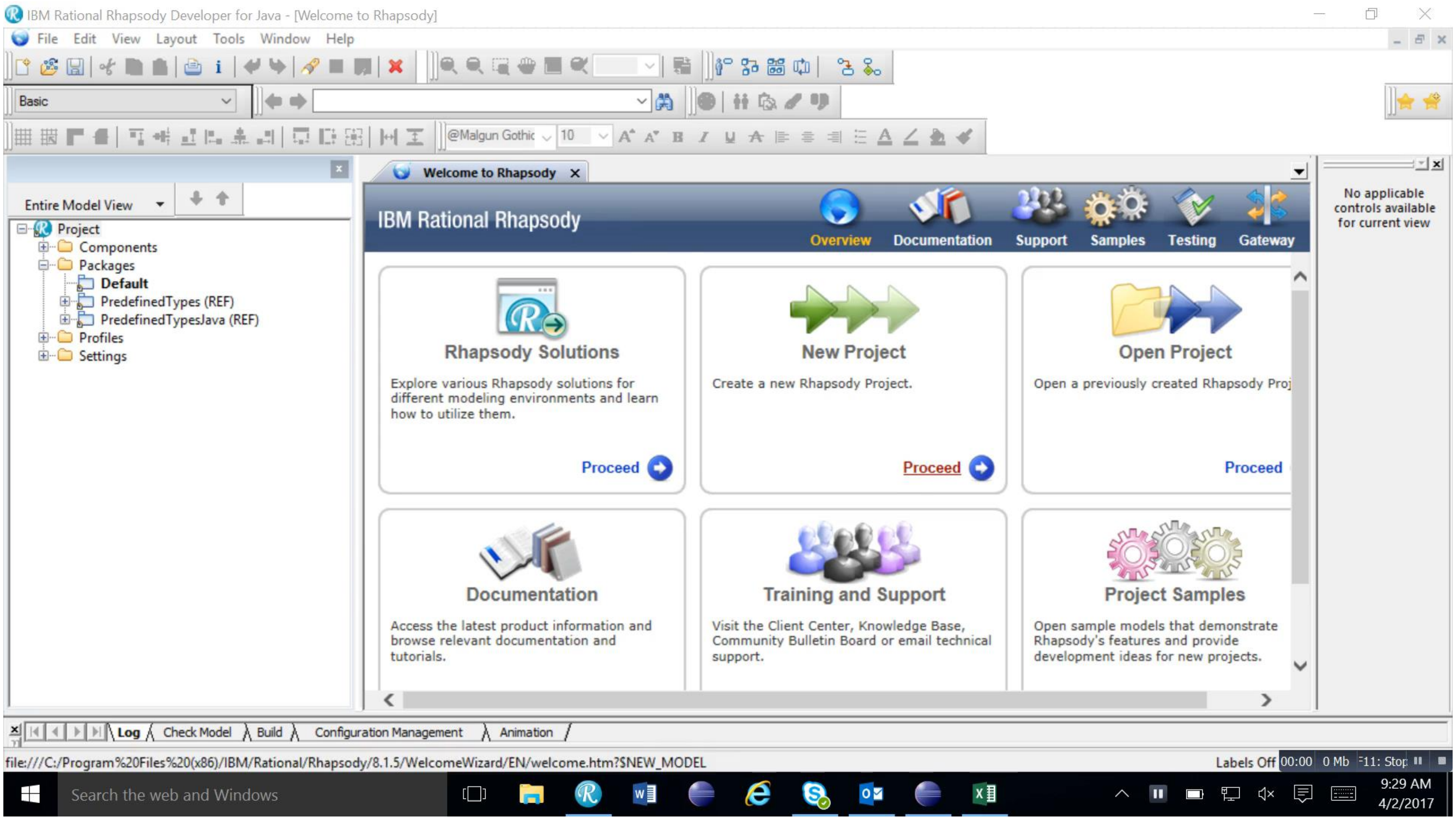
MITRE

Base Model GUI

- A MATLAB GUI has been built to simplify the process of populating a connectivity matrix
- The tool outputs a CSV file that can then be imported into the architecture model



Demonstration



Q2 Metrics – Experiments

- **Qualitative**
  – Experiment 1: Give the base model to MITRE employees to use on their projects as they see fit. Collect feedback.
    - Likes, dislikes, pain points, time savings estimates, description of use case, experience level
    - Time Cost: 30 min interview
- **Quantitative**
  – Experiment 2: Give MITRE employees a sample coms network and have them create it by hand and by using the CSV importer
    - Networks of different sizes
    - Measure time to complete exercise
    - Time Cost: Approx. 45 min per data point
  – Experiment 3: Randomized control trial with ~20 new interns
    - Group A: Create reference model from scratch
    - Group B: Create reference model using base model

Metrics – Experiment 1 Results

- **Project 1:**
  - 3 reviewers
  - Not adopted

- **Feedback:**
  - "…This base model would be a great reference, e.g., utilizing the package structure framework used, with the inheritable architectures and the focus on reuse."
  - "…We expect to draw ideas from it as we build our own model."
  - "We intend to focus more on activity diagrams than state charts."
  - "Our project is not in the context of the Air Force, so we would have to change the block and activity names."
  - "Overall it is not a good fit for [our project]."

- **Project 2:**
  - 1 reviewer
  - Adopted

- **Feedback:**
  - Qualitative

    Base Model state charts look too "in-depth", "specific", need to take a closer look to see if they will work for my use case. But if they work, "that would be awesome", it will save tons of time.
  - Pseudo - Quantitative

    Estimated time savings of 40 hours on work completed so far.
  - Update

    Base Model has proven a good fit for project and has been used extensively.

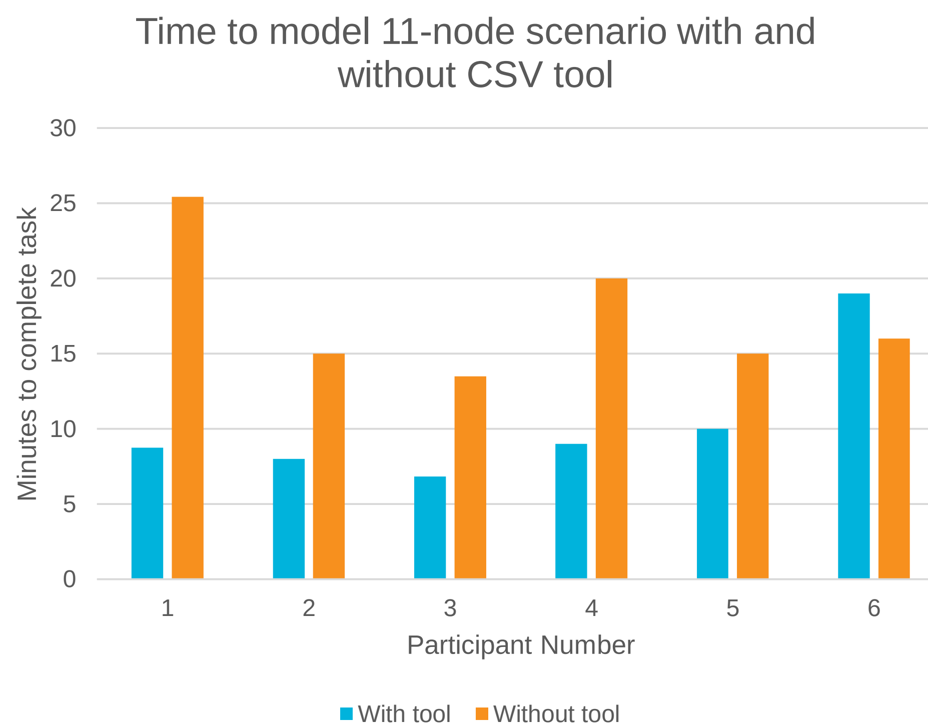
Metrics – Experiment 2 Results

<u>The Scenario</u>

This is a hypothetical Air Force kill-chain scenario consisting of 1 ground control station (AOC), 1 air command and control (C2), 4 Fighter Jets, 4 Unmanned Aircraft Systems (UASs), and 1 Tanker.

- AOC needs to be able to communicate with C2, since C2 alerts AOC when there is a threat and then gets its orders from the ground.
- C2 also needs to be able to communicate with all fighters and the Tanker during the mission.
- Also, all fighters and UASs need to be able to communicate with the Tanker, since they'll occasionally need to refuel during flight.
- Every fighter needs to be able to communicate with every other fighter, and
- every UAS needs to be able to communicate with every other UAS.
- Moreover, every fighter should be able to communicate with every UAS, and vice versa.

You may assume all communication channels are bi-directional (any communication matrix you set up should be symmetric with respect to rows and columns).



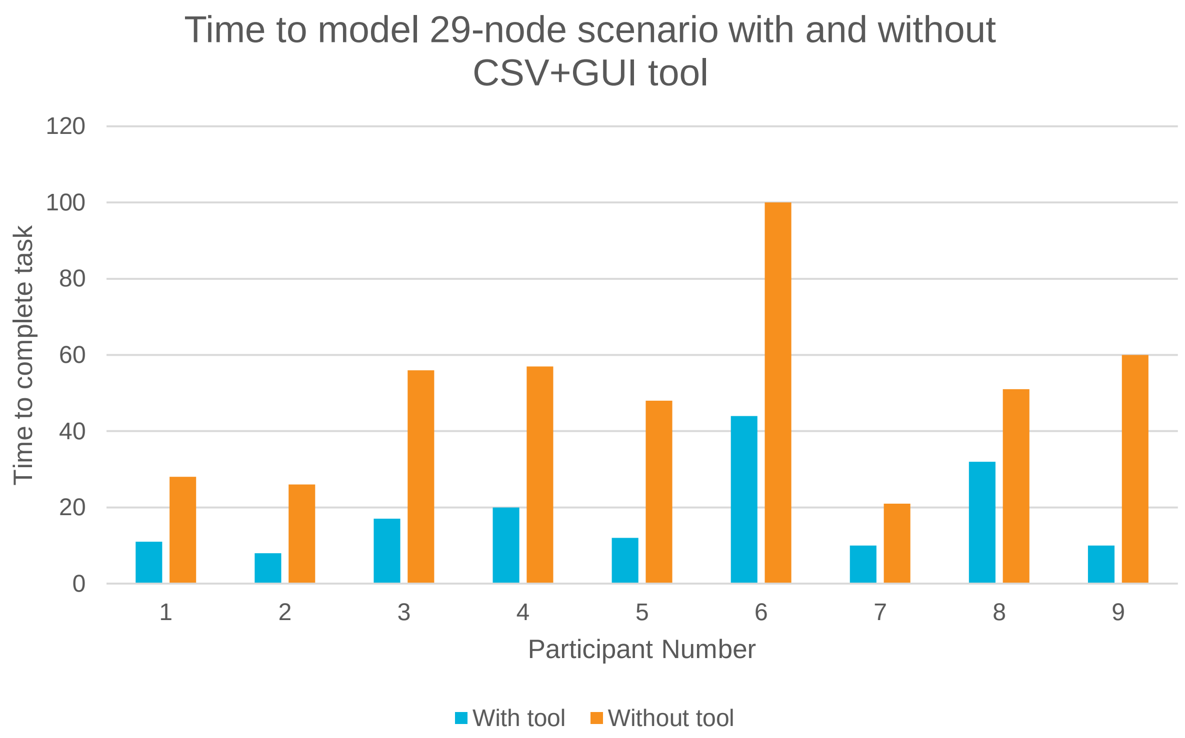
Time savings

Mean: 39%

Standard Dev: 12%

MITRE

Metrics – Experiment 2 Results



Time savings

Mean: 63%

Standard Dev: 14%

Average mistakes

Without tool: 9.2

With tool: 0.8

Defense System of Systems Gap Analysis

Abstract ID: #19757

For:
NDIA
20th Annual Systems Engineering Conference
23-26 October 2017

Prepared by:
Idaho National Laboratory (INL)
Christopher A. Dieckmann, ESEP
Systems Engineering Lead for National and Homeland Security Projects

INL Systems Analyses & Engineering Contacts

Mitchell Kerman
Division Director
(208) 526-3631
mitchell.kerman@inl.gov

Ron Klingler
Department Manager
(208) 526-0183
ron.klingler@inl.gov

NDIA Presenter

Chris Dieckmann
Group Lead for
National & Homeland
Security Projects
(208) 526-5986
chris.dieckmann@inl.gov

John Collins
Group Lead for
Energy & Environment
Projects
(208) 526-3372
john.collins@inl.gov

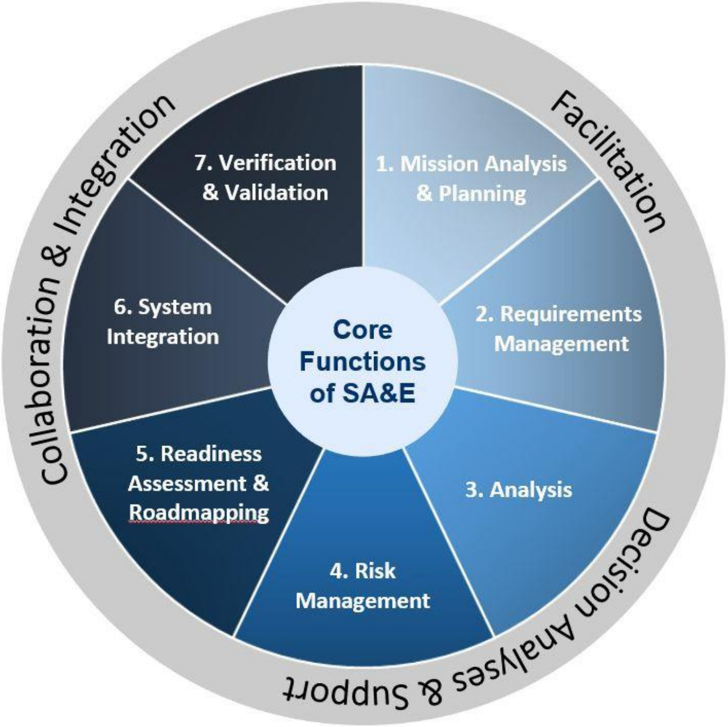
Jody Henley
Group Lead for
Nuclear Projects
(208) 526-1979
jody.henley@inl.gov

Shyam Nair
Group Lead for
Process & Data Sciences
(208) 526-3071
shyam.nair@inl.gov

INL Systems Analyses &
Engineering Web Page
https://systemsengineering.inl.gov

INL/CON-17-42210

Core Functions –
INL Systems Analyses & Engineering



1

- Concise Problem Definition
- Understanding Important Customer Needs
- Concise System/Project Boundaries
- Strategic Planning & Baselines
- "Concept" of Operations
- Stakeholder Buy-in
- Acquisition Strategy
- White Papers

2

- Technical, Functional, and Operational Analysis
- Requirements Elicitation, Clarification, Derivation, and Tracking
- Traceability, Change Control, and Impact Analysis
- Requirements Verification and Validation Planning

3

- Analysis of Alternatives
- Decision Metrics
- Organization Analysis & Visualization of Complex and Big Data
- Uncertainty Analysis & Probabilistic Risk Assessment
- Risk-informed Decision-making
- Integration of Viable Solutions
- Chemical Process Engineering & Analysis
- Chemical Process Control
- Computational Fluid Dynamics

4

- Risk Identification and Tracking
- Justification for Funding Contingency
- Risk Handling Strategy
- Risk Reduction Plan
- Risk-informed Path Forward

5

- Technology Maturity Analysis
- Technology Development Roadmap/Path Forward
- Roadblock Identification & Mitigation
- System Assessments (e.g., Energy Systems)

6

- Program & Project Integration
- Laboratory-wide R&D Integration
- Laboratories/Industries/ Universities Integration
- Integration of System Elements
- Systems of Systems Analyses

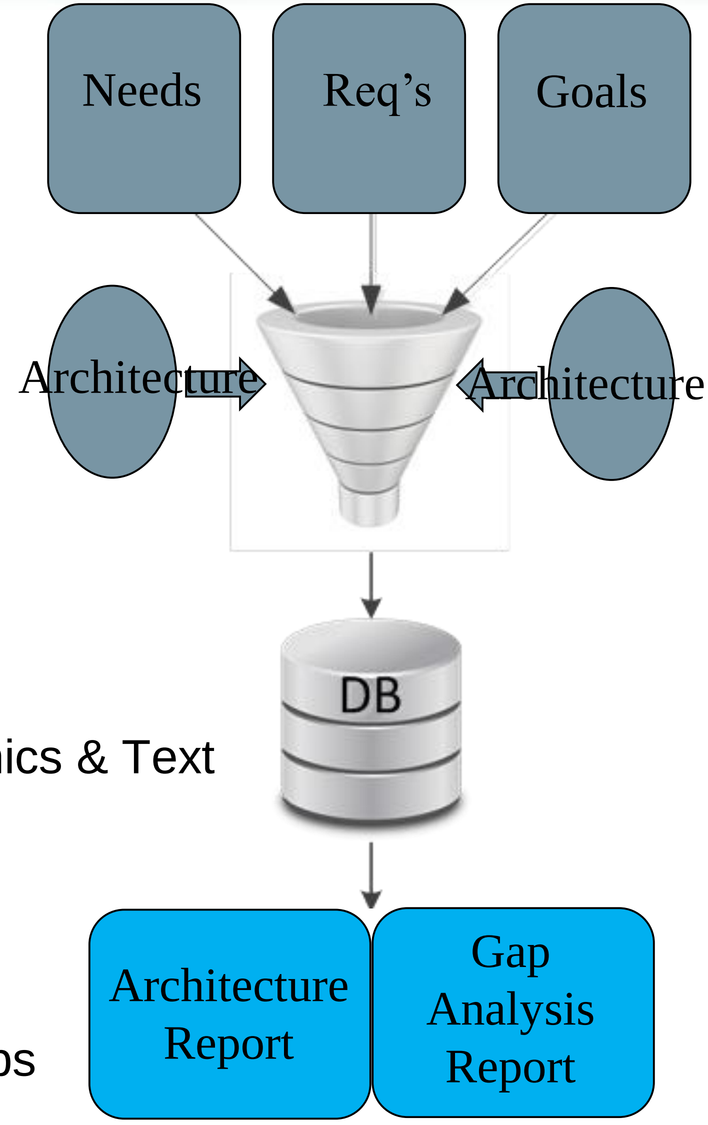
7

- Verification of System Performance and Functionality
- Validation of System Specification and Design Parameters
- Test Planning and Implementation

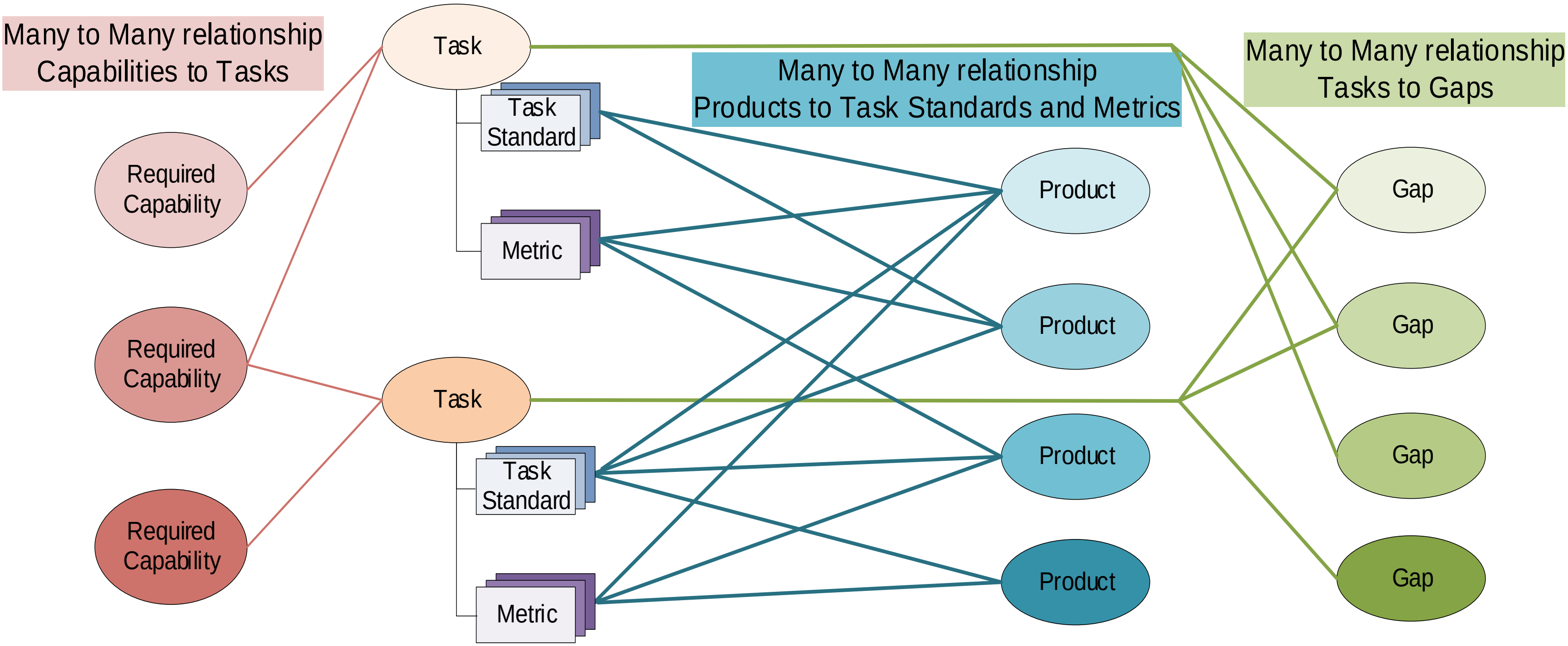
INL/CON-17-42210

INL Gap Analysis Data Gathering

- Gather Needs and Goals (Capabilities)
  - Review & Filter Documents
  - Interviews
- Analysis
  - Architecture Artifacts
  - Filter by Relevant Architecture
  - Map Capabilities to Needs & Goals
- Reporting
  - Architecture Report
    - Documents Architectural Artifacts
    - Provides Common Baseline in Graphics & Text
    - Supports Further Analysis
  - Gap Analysis Report
    - Needs & Goals, Potential Coverage
    - Implementation Gaps
    - Enterprise Capabilities, Potential Gaps



INL Gap Analysis Approach



- Capabilities are linked to Tasks
- Tasks are linked to Task Standards & Metrics
- Many Task Standards are shared among Tasks
- Many Metrics are shared among Tasks

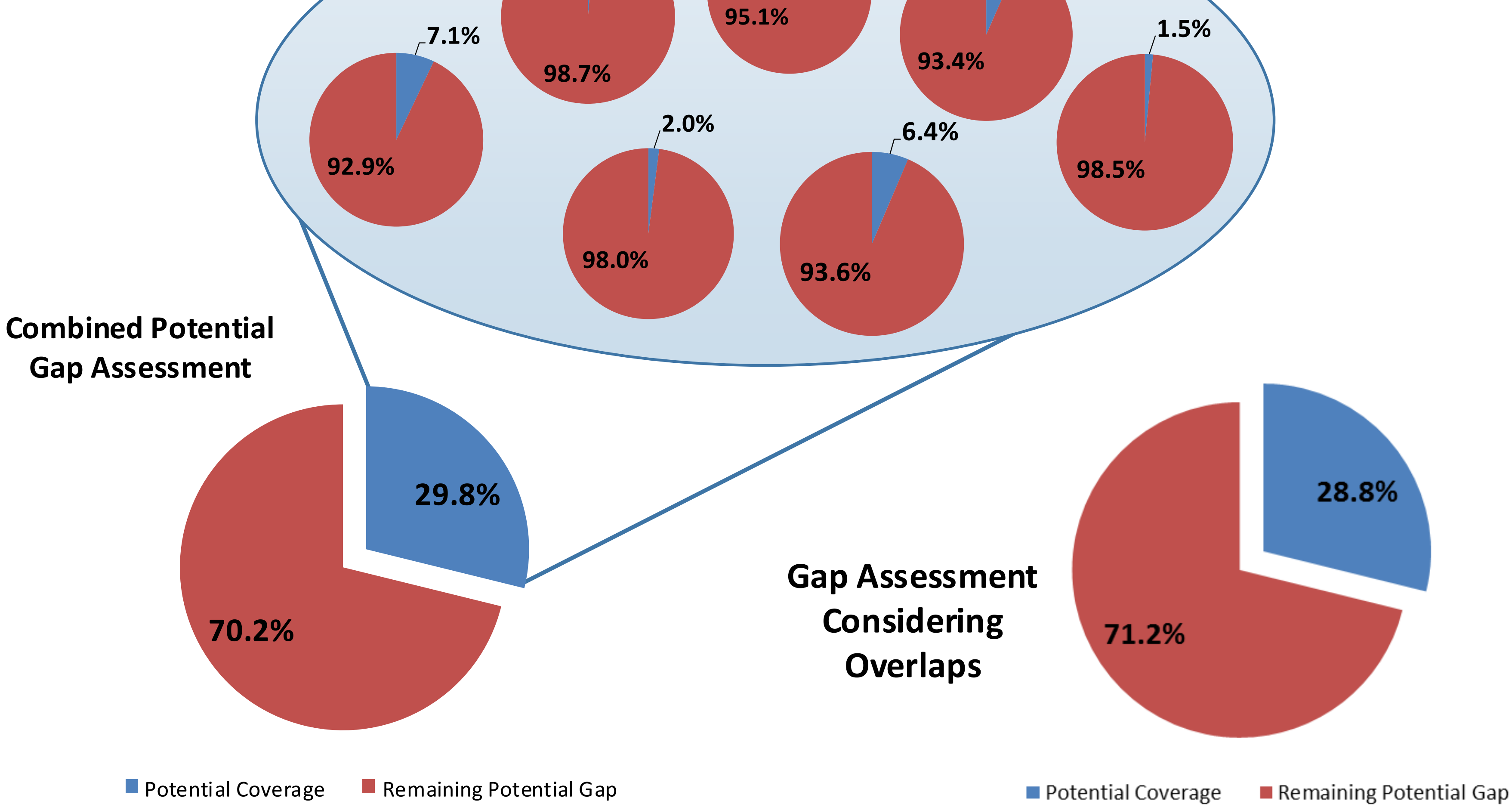
- Task Standards & Metrics evaluated as Met / Not Met by Products
- Task Standard & Metric evaluations roll up to Tasks
- Task evaluations roll up to Gap Closure Percentages

Shared Task Standards & Metrics Shrink Problem Space

INL/CON-17-42210

Gap Analysis Results

Numerical Sum of Gap Closure is larger than combined Gap Closure because of Capability Overlap



Capability Use by Location Field View

Contrast this Field View with the Acquisition HQ View on following slide

Legend:

Permission Level
- Admin
- User
- Unknown

Current Usage
- Using, no issues
- Using, with configuration (HW/SW) issues
- Deployed, not using
- Not Deployed
- Unkown

			Tool / Capability 1		Tool / Capability 2		Tool / Capability 3		Tool / Capability 4		Tool / Capability 5		Tool / Capability 6		Tool / Capability 7	
	Location	Planned / Assessed	Permission Level	Current Usage	Permission Level	Current Usage	Permission Level	Current Usage	Permission Level	Current Usage	Permission Level	Current Usage	Permission Level	Current Usage	Permission Level	Current Usage
CONUS	Location1	Planned														
	Location2	Planned														
	Location3	Planned														
	Location4	Planned														
	Location5	Assessed														
	Location6	Planned														
	Location7	Assessed														
	Location8	Planned														
	Location9	Planned														
	Location10	Planned														
	Location11	Planned														
	Location12	Planned														
OCONUS 1	Location13	Planned														
	Location14	Planned														
	Location15	Planned														
	Location16	Planned														
	Location17	Assessed														
OCONUS 2	Location18	Assessed														
	Location19	Assessed														
	Location20	Planned														
	Location21	Planned														
OCONUS 3	Location22	Assessed														
	Location23	Assessed														
	Location24	Planned														
	Location25	Assessed														
	Location26	Assessed														
	Location27	Assessed														
OCONUS 4	Location28	Assessed														
	Location29	Assessed														

Idaho National Laboratory

Capabilities Purchased and Deployed

Capability	Purchased Capabilities	Deployed Capabilities	Capability	Purchased Capabilities	Deployed Capabilities	Capability	Purchased Capabilities	Deployed Capabilities
Tool / Capability 1			***Tool / Capability 3***			***Tool / Capability 6***		
Tool Module / Sub-Capability 1	X	X	Tool Module / Sub-Capability 1	X		Tool Module / Sub-Capability 1	X	X
Tool Module / Sub-Capability 2	X	X	Tool Module / Sub-Capability 2	X	X	Tool Module / Sub-Capability 2	X	X
Tool Module / Sub-Capability 3	X	X	Tool Module / Sub-Capability 3	X	X	Tool Module / Sub-Capability 3	X	X
Tool Module / Sub-Capability 4		X	Tool Module / Sub-Capability 4	X	X	Tool Module / Sub-Capability 4	X	X
Tool Module / Sub-Capability 5	X	X	Tool Module / Sub-Capability 5	X	X	Tool Module / Sub-Capability 5	X	X
Tool Module / Sub-Capability 6	X	X	Tool Module / Sub-Capability 6	X	X	Tool Module / Sub-Capability 6	X	
Tool Module / Sub-Capability 7	X	X	Tool Module / Sub-Capability 7	X	X	Tool Module / Sub-Capability 7	X	
Tool Module / Sub-Capability 8	X	X	Tool Module / Sub-Capability 8	X	X	Tool Module / Sub-Capability 8	X	
Tool Module / Sub-Capability 9	X	X	Tool Module / Sub-Capability 9	X	X	Tool Module / Sub-Capability 9	X	
Tool Module / Sub-Capability 10	X	X	Tool Module / Sub-Capability 10	X	X	Tool Module / Sub-Capability 10	X	
Tool Module / Sub-Capability 11	X	X	Tool Module / Sub-Capability 11	X	X	***Tool / Capability 7***		
Tool Module / Sub-Capability 12	X	X	***Tool / Capability 4***			Tool Module / Sub-Capability 1	X	X
Tool Module / Sub-Capability 13	X	X	Tool Module / Sub-Capability 1	X	X	Tool Module / Sub-Capability 2	X	X
Tool Module / Sub-Capability 14	X	X	Tool Module / Sub-Capability 2	X	X	Tool Module / Sub-Capability 3	X	X
Tool Module / Sub-Capability 15	X	X	Tool Module / Sub-Capability 3	X	X	Tool Module / Sub-Capability 4	X	X
Tool Module / Sub-Capability 16	X	X	Tool Module / Sub-Capability 4	X	X	Tool Module / Sub-Capability 5	X	
Tool Module / Sub-Capability 17	X	X	Tool Module / Sub-Capability 5	X	X	Tool Module / Sub-Capability 6	X	X
Tool / Capability 2			***Tool / Capability 5***			Tool Module / Sub-Capability 7	X	X
Tool Module / Sub-Capability 1	X	X	Tool Module / Sub-Capability 1	X	X	Tool Module / Sub-Capability 8	X	X
Tool Module / Sub-Capability 2	X	X						
Tool Module / Sub-Capability 3	X	X						

Contrast this View with the Field View on prior slide

Acquisition HQ View

INL/CON-17-42210

Operational Impacts

Legend
• Issue Summary
❖ Impact Statement
➢ Solution Summary

- Capabilities are stove-piped vs. integrated
  - ❖ Reduced interoperability, duplication of capability, and tool proliferation
  - ➢ Implement a System Engineer / Architect to integrate systems / investments
- Training not tailored, timely, or recurring
  - ❖ Covered ancillary features and provided too early (>1 year ahead of tool)
  - ➢ Provide persistently available, feature and location specific training
- Capabilities deployed without direction or expectations for use
  - ❖ Multiple local adaptations and assumptions about Acquisition HQ intent
  - ➢ Deploy standardized tools with approved CONOPS, roles & responsibilities
- Capabilities only partially deployed or partially implemented at sites
  - ❖ Insufficient/EOL hardware, licensing, limited permissions limit capabilities
  - ➢ Synch HW investments with SW and socialize roles & responsibilities
- Requirements are not allocated to the Capabilities
  - ❖ Capabilities are added without verification or validation
  - ➢ Derive and validate requirements and verify Capabilities meet requirements

INL/CON-17-42210

Questions?

Chris Dieckmann
Group Lead for
National & Homeland Security Projects
(208) 526-5986
chris.dieckmann@inl.gov

Model Based Systems of Systems Engineering

Fran McCafferty
Principal Systems Engineer
fmccafferty@vitechcorp.com

System of Systems v System of Subsystems

…**The major distinction between systems as elements of an SoS and subsystems as elements of a system is therefore that the SoS comprises elements (systems) that are optimised for their own purposes before joining the SoS, whereas the system comprises elements (subsystems) that are optimised for the system's purpose (not necessarily their own).** …

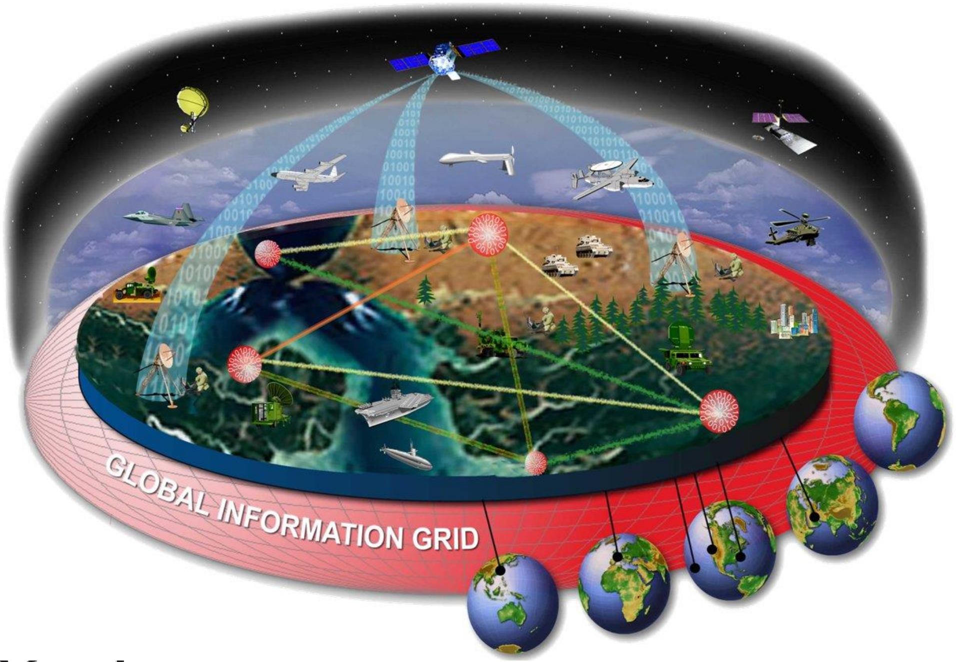
- Faulconbridge, Ian; Ryan, Michael. Introduction to Systems Engineering (Kindle Locations 268-277). Argos Press Pty Ltd. Kindle Edition.

System of Systems vs. System of Subsystems

Both comprise elements that are interconnected, *but:*

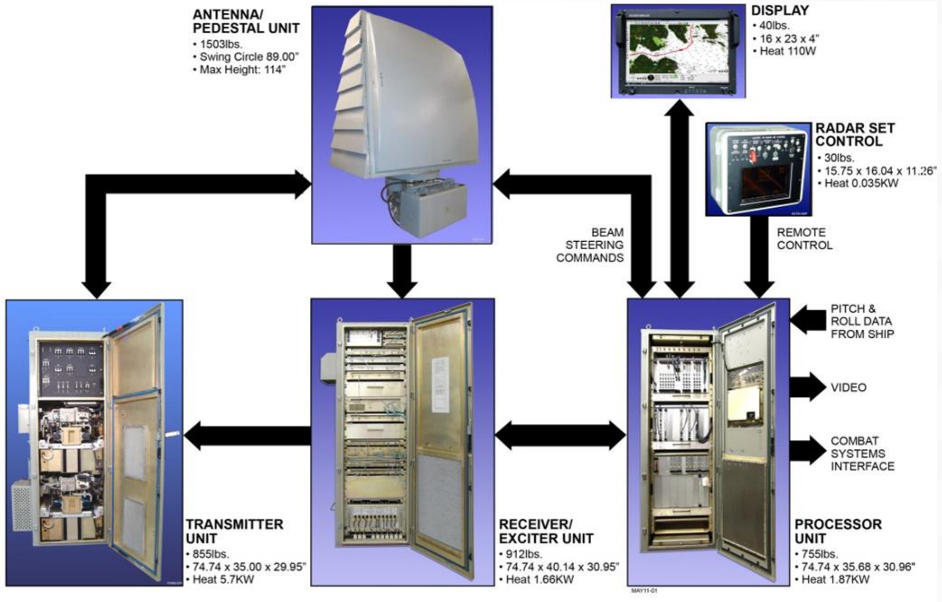
System of Systems

- Elements are systems in their own right, managerially and operationally independent
- Elements have been optimized for their own purpose



System of Subsystems

- Not independent
- Only exist to serve the parent system
- Invariably sub-optimal



What's your definition of a system?

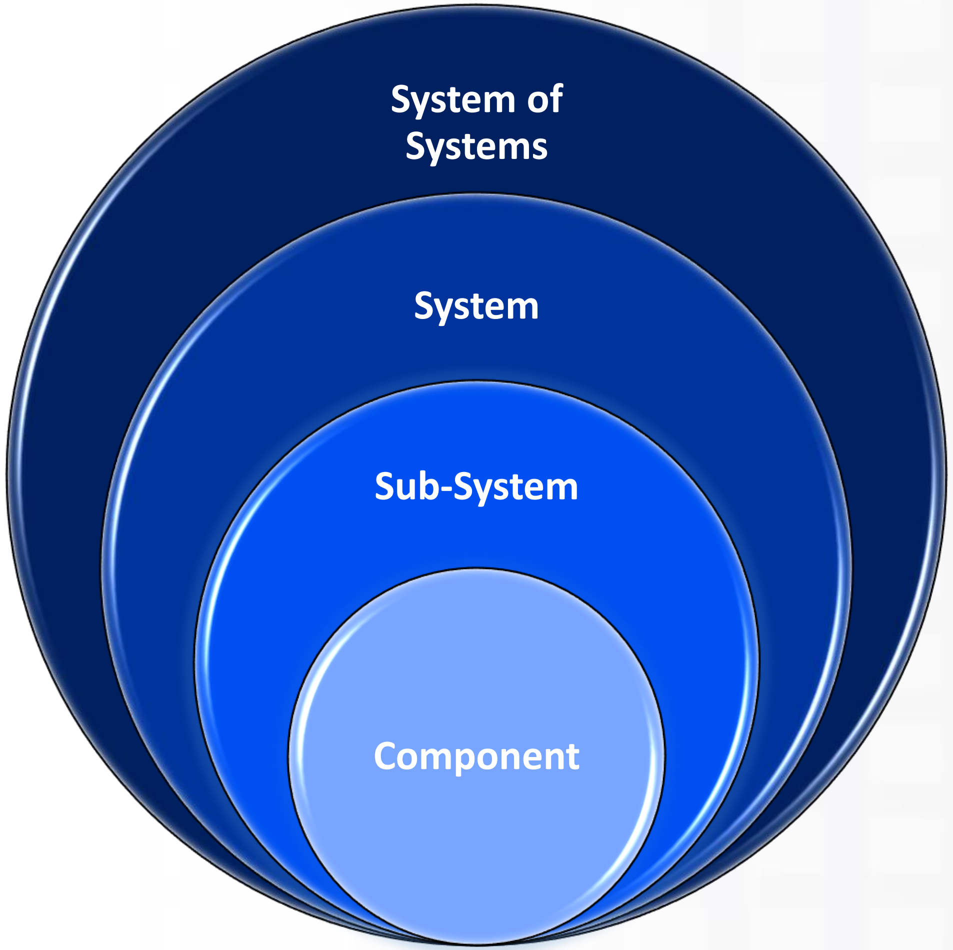
Fundamental Concepts

A System:

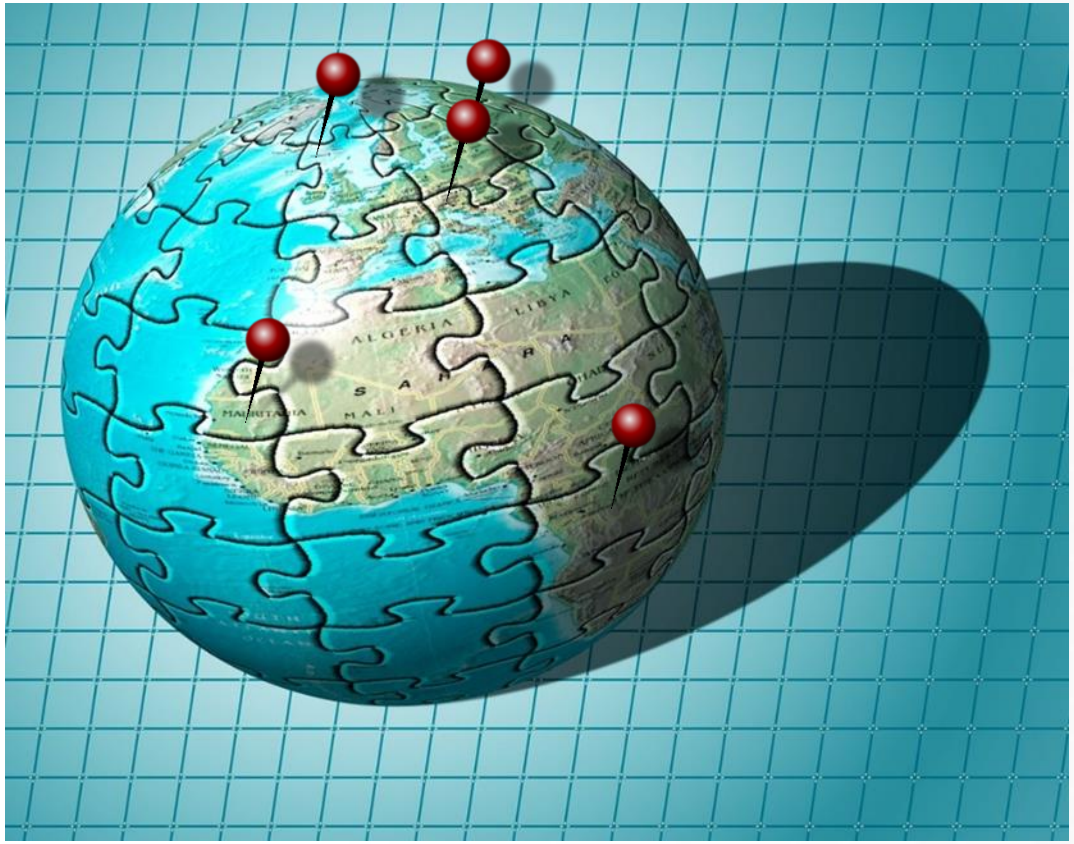
- Performs a function, transforming inputs to outputs
- Is a collection of interacting components with a common goal

A Subsystem:

- Can be considered a system
- Therefore, the analysis and specification of a system is hierarchical and iterative
  - System
  - Subsystem
  - Component
  - . . .



System of Systems



Multiple Cooperating Systems

- Multiple and often geographically distributed organizations
- Multiple design teams

Single Large System

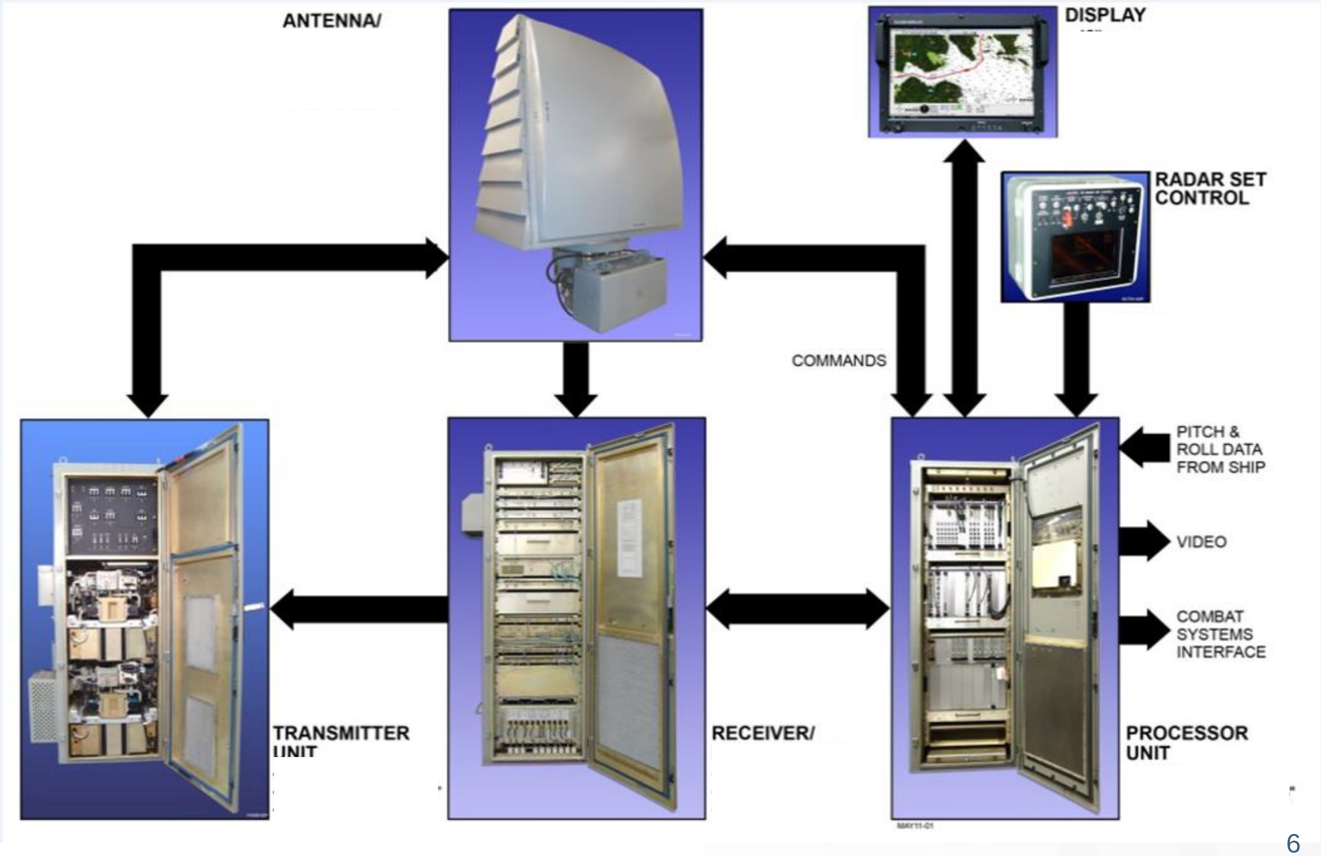
- What was it optimized for?
  - Cost
  - Schedule
  - Legacy technology
- System partition basis
  - Functionality
  - Geography
  - Organization expertise

Example: Radar
Air and Surface Search Radar – Restoration Program

How does a program office support a critical system for extended periods of time from a maintenance and upgrade perspective?

What are the options?

- **Replace the entire system**
    - Design from scratch
    - Implement an existing system
- **Maintain the existing system**
    - Replace broken/failed components
    - Perform capability upgrades



What are the options?

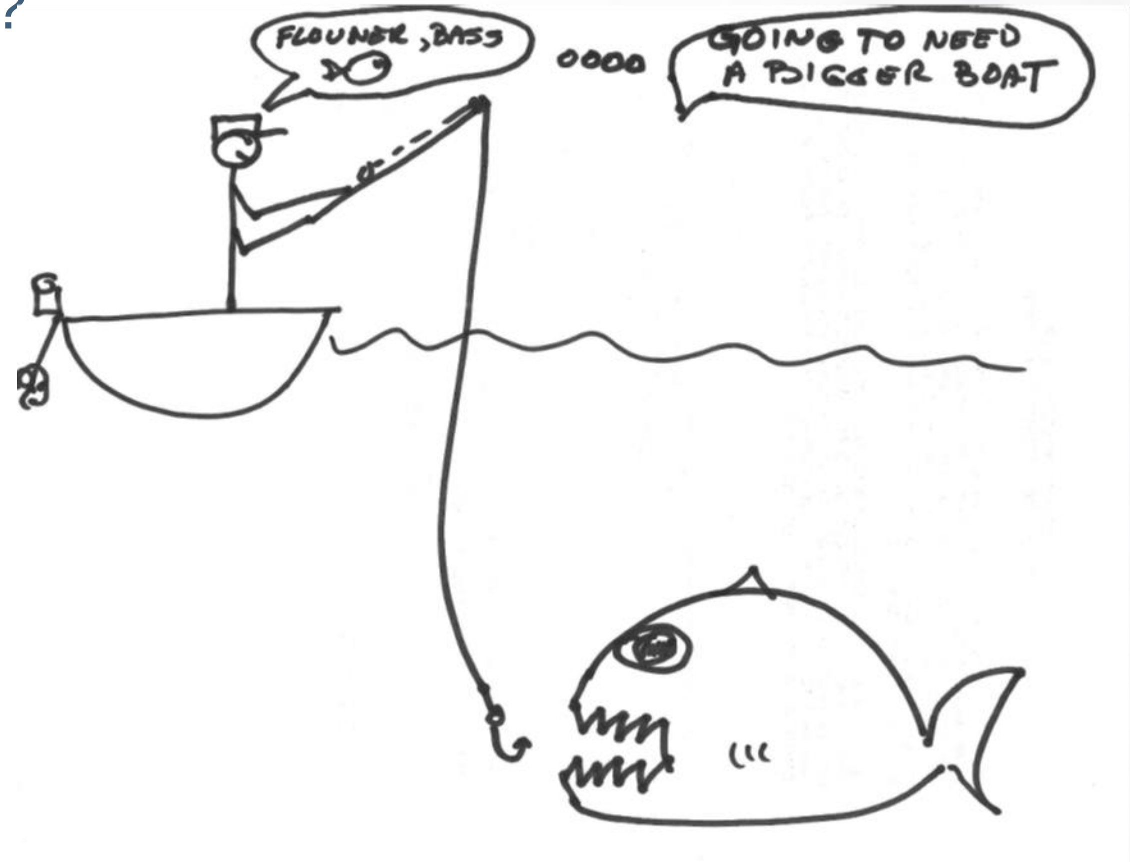
Options	Issues
Replace the entire system	
- Design from scratch	- cost, schedule, integration
- Implement an existing system	- cost, schedule, integration, capability
Maintain the existing system	
- Replace broken/failed components	- are parts available, can parts be made
- Perform capability upgrades	- do you get all of the benefits

Mission Engineering
System of Systems Engineering

Our world is far from static, so what do we do?

Do we need to evolve? Probably.

- Do we understand the problem?
- Can we afford to evolve?
- How much evolution can we stand?



Vitech

System of Systems US Navy Restoration Example

Single Large System

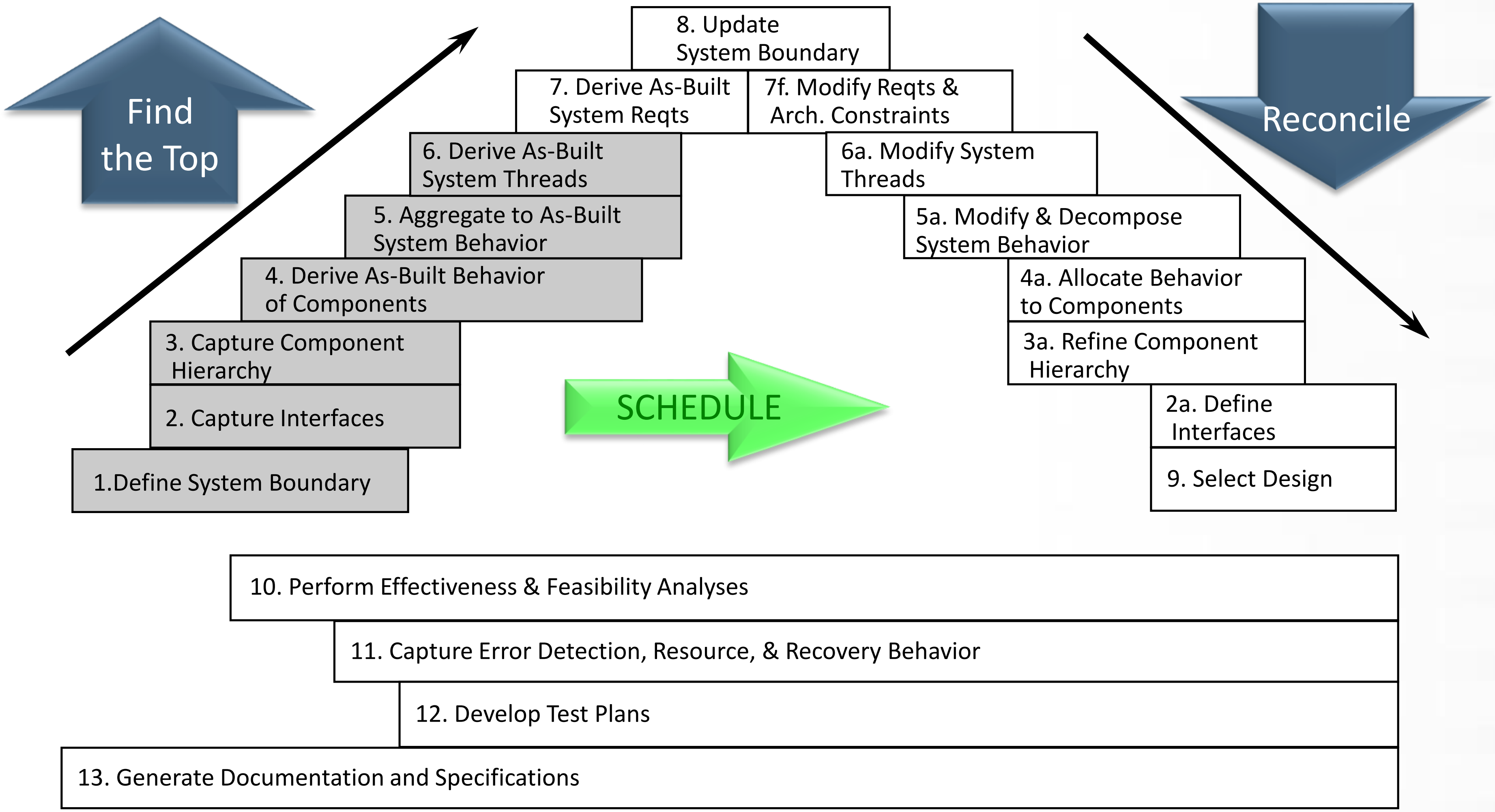
What was it optimized for?

- Cost
- Schedule
- Legacy technology

System partition basis

- Functionality
- Geography
- Organization expertise

MBSE Activities Timeline + Reverse Engineering



So what do you do?

What is in the scope of the project, and who says so?

- **Clearly define the boundaries**
  - Ensure the subsystems are fully defined from a capability, physical characteristics, and most importantly, know the interfaces.
  - Interface definition means knowing what information traverses the subsystem boundary.
  - What are the physical, logical, and functional characteristics?
- **Manage the complexity**
  - What changes?
  - How do we know?

Answer: Systems engineer it, model it!

Vitech

So what do you do?

If we reverse engineer the existing system, we know the critical capabilities and constraints.

- Capture the legacy requirements
- Model
  - Physical Architecture
  - Behavior – functions, information, control, and timing
  - Interfaces
  - Links
  - Constraints

Now we know the baseline.

Answer: Systems engineer it, model it!

Vitech

Do the analysis

Ask

- What does the upgraded system have to do?
- How do we partition?
- At what level do we want to compete acquisition?

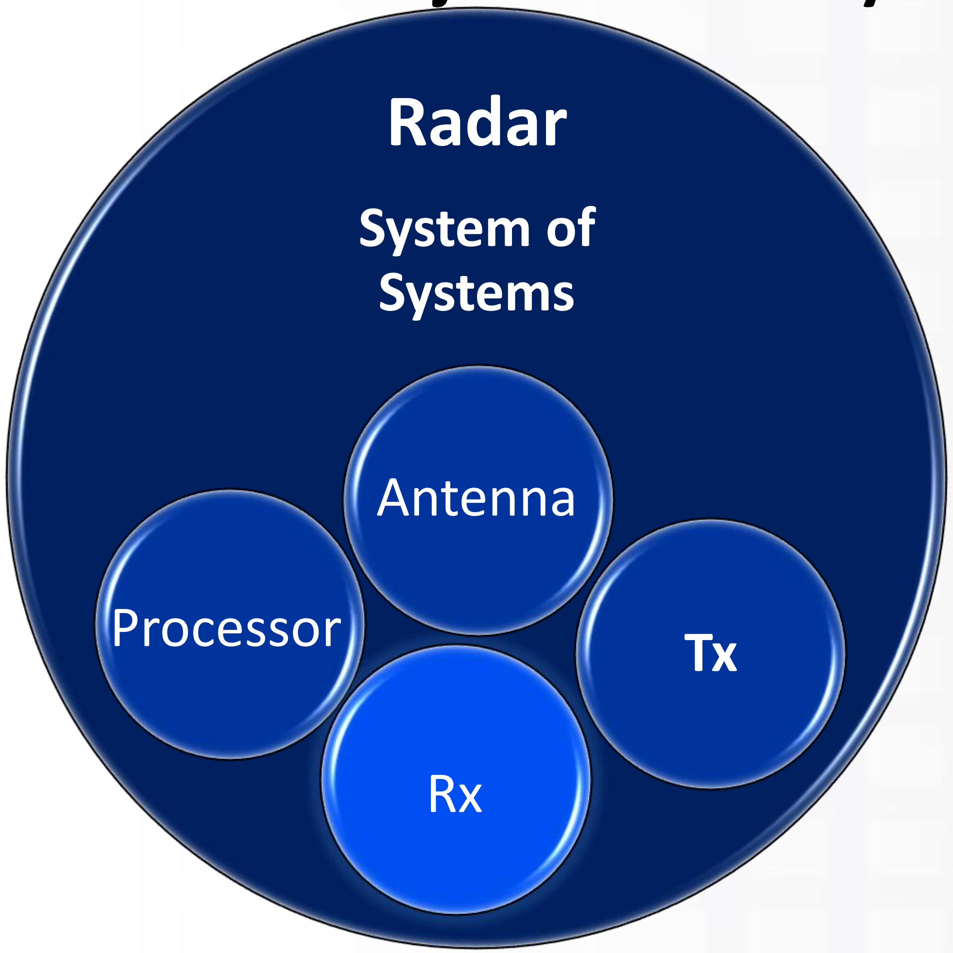
Apply Model Based Systems Engineering

Multi-Project Roadmap

- Partitions
  - Rx
  - Tx
  - Rx
  - Antenna
- **Why**, and **benefits** v. Mega Project
  - Strata, just boundary not down to nth layer,
  - thin model,
  - black box,
  - white box,
  - Integration Perspective,
  - contractual boundaries,
  - defining lower level

  - ….Let's have a look

Projects Hierarchy



Model the Requirements

Use what you have in SSS, IRS, ICD

SSS

- 3.2 System requirements
- 3.7 Major subsystems requirements

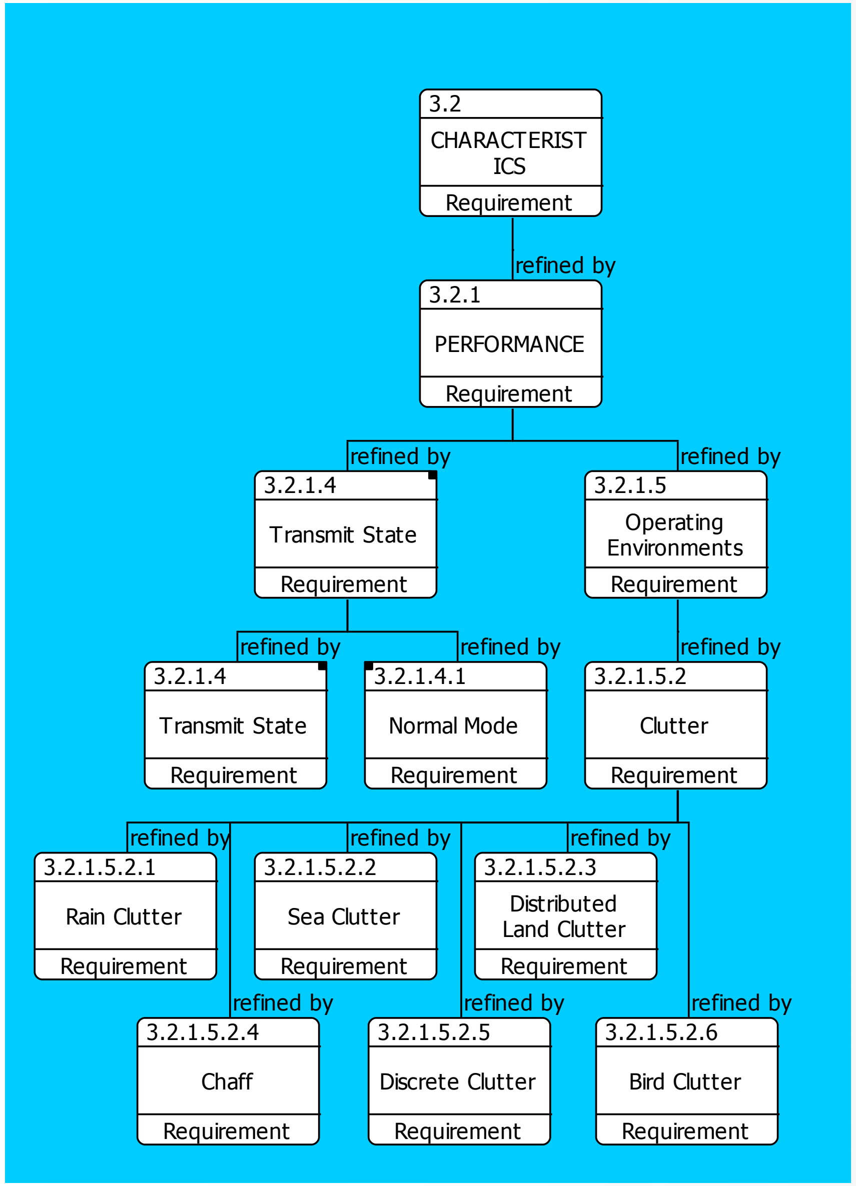


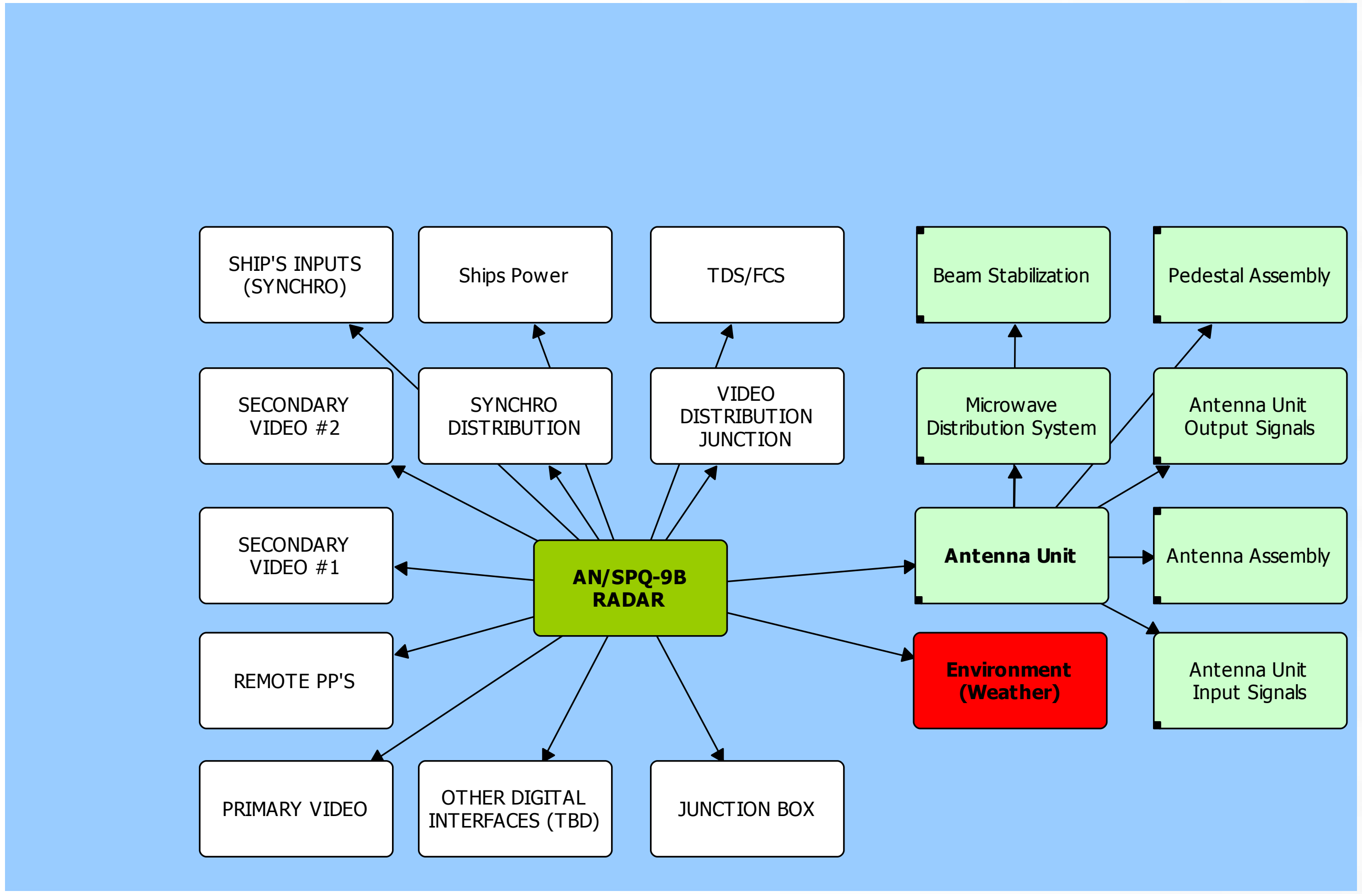
Diagram: CORE-generated requirements hierarchy diagram

Model the Architecture Using Components, Establish Interfaces/Links

Use what you have in SSS, IRS, ICD

<u>SSS</u>

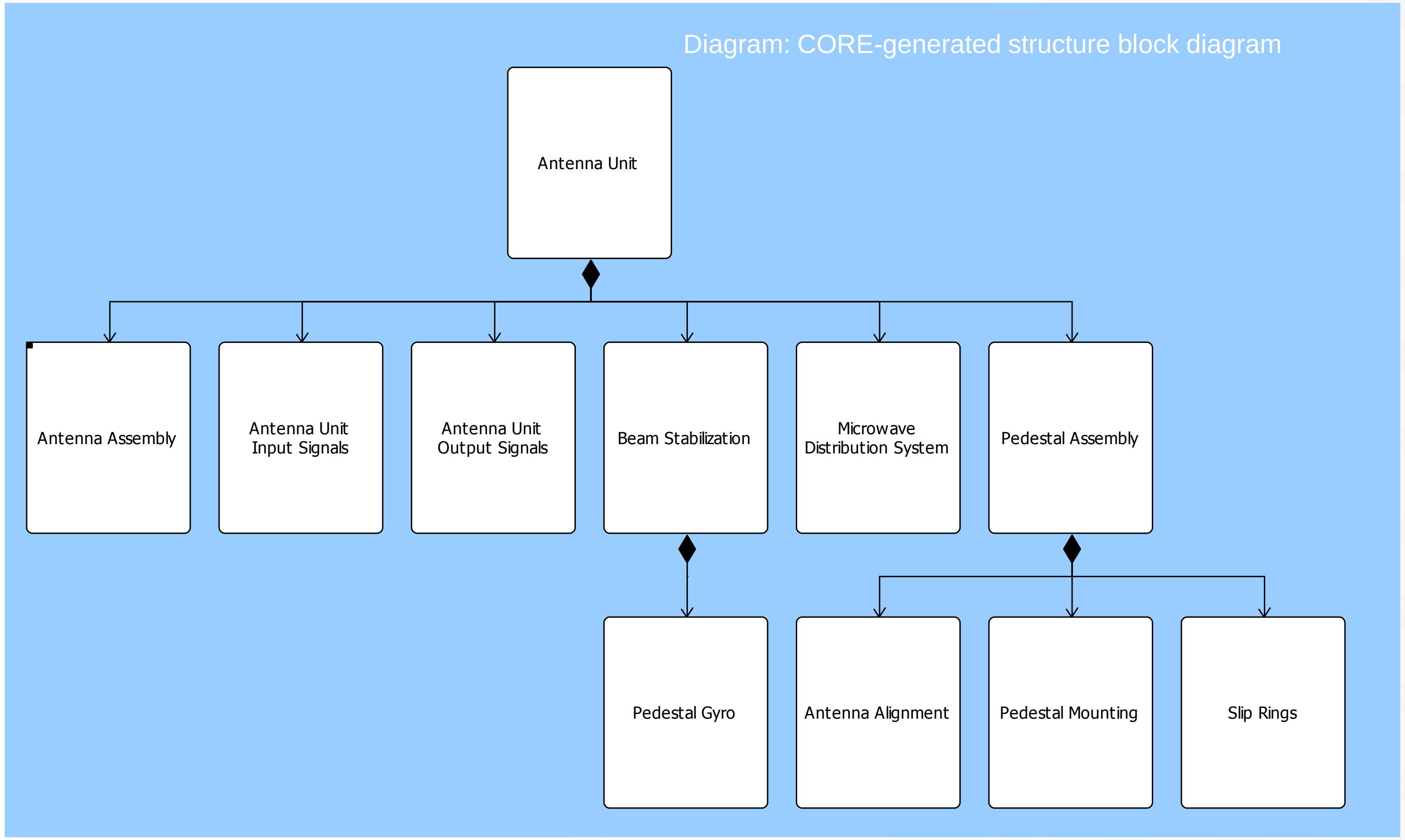
- 3.2 System requirements
- 3.7 Major subsystems requirements



Vitech

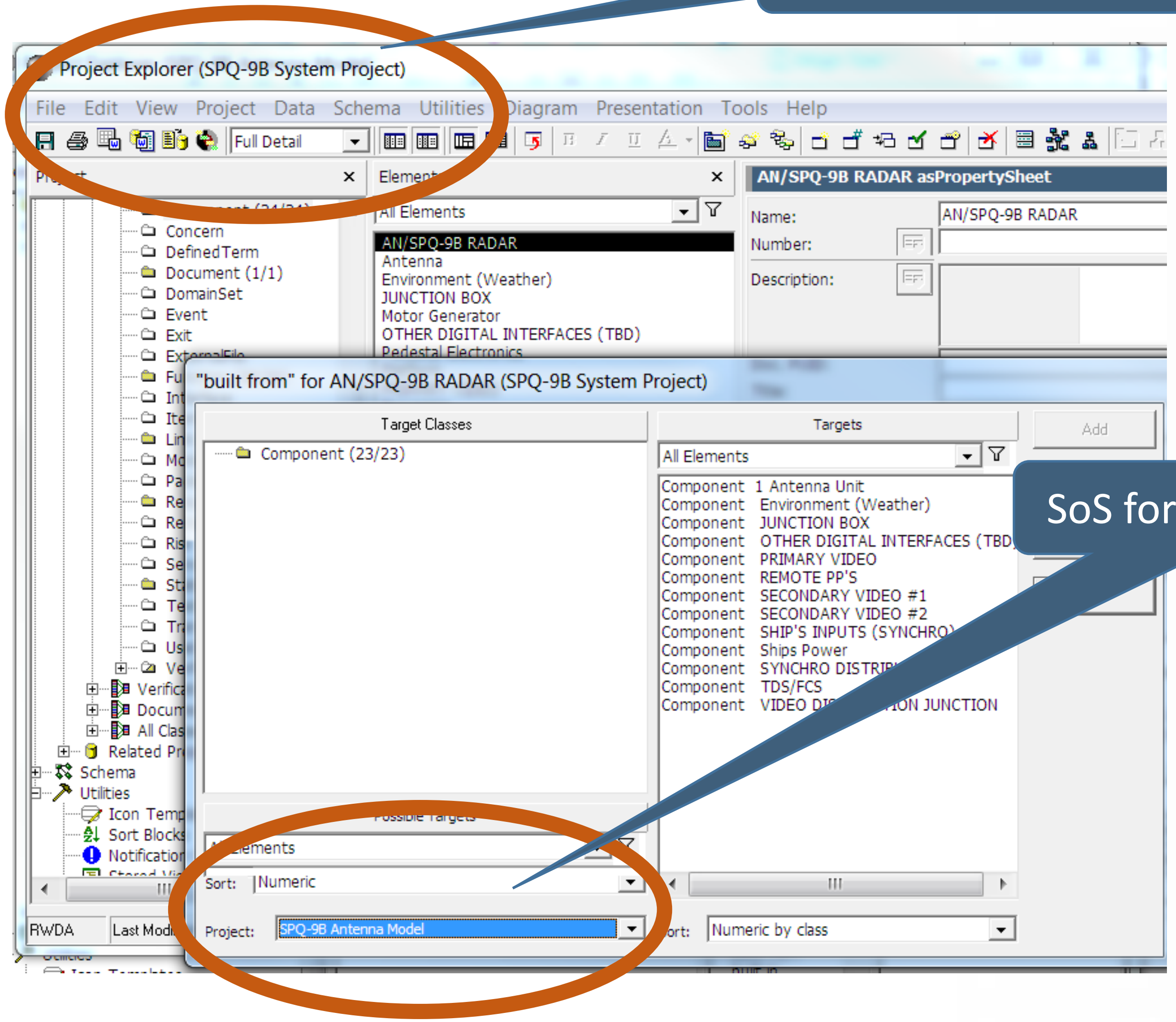
Antenna– Project

- Separate projects – maintains system context and subsystem boundaries.
- Link projects through components.
- Use “built from” relationship.
- Recall, a context function, is automatically generated, + can also be a decomposition of the radar.



Create Multiple Projects

System Project



SoS for Antenna Unit

Tiered Projects

Separate projects

- Maintains system context
- Identifies subsystem boundaries

Link projects through components

- Use “built from” relationship
- Recall, a context function, is automatically generated, + can also be a decomposition of the radar.

Specifications linked to specific project

- System Specification
- Antenna Unit– Subsystem Spec (SSS, or in the old days, B Spec)
  - Allows for the Antenna Unit to be easily severable,
  - Supports subsystem level acquisition strategies,
  - Provides context for technology insertion / and sustainment

Summary

- System of Systems and Mission Engineering similarities.
- Separate but linked projects provide context and linkage.
- Independent projects enable clearly understandable subsystems.
  - Higher fidelity of requirements, traceable but not overwhelming
  - Clear interfaces between subsystems
  - Physical hierarchy shows transition from one design/support group to another
- Promotes separation of concerns, while maintaining traceability and consistency
- PMO Support
  - Enables PMO to generate RFP from models
  - Radar Restoration is considering requiring a model as part of proposal package

For more information:

Vitech website: http://www.vitechcorp.com/
Blog: http://community.vitechcorp.com/home/
Presenter: fmccafferty@vitechcorp.com
540.951.3322 x304 or 856.217.9963

We invite your comments and questions.

THANK YOU!

U.S. Joint Staff J6
Deputy Directorate
for
Cyber and C4 Integration
(DD C5I)

Enhancing Joint and Coalition Interoperability

25 October 2017

Scott Shephard
Coalition Interoperability Division

J6 Strategic Direction

Joint Staff J6 will assist CJCS in providing best military advice while advancing cyber defense, C2 systems capabilities, and Joint and Coalition interoperability required by Joint Force to preserve nation's security

CJCS Joint Force Priorities

- Improve Joint Warfighting
- Restore Joint Readiness
- Develop Leaders for JF Next

DJ6 Intent

- Support CJCS and SecDef priorities
- Support, enable and advocate for C4 and Cyber Joint Warfighter capabilities
- Joint Staff CIO

NMS Themes

- 4+1 Actors
- Maintain our competitive advantage
- Allies and partners are critical to our success
- Joint Force must be globally integrated

Cyber Defense Line of Effort (LOE)

Lines of Operation:

1 Strengthen the defensibility of key DoD cyber terrain
2 Increase the abilities of cyber maneuver and fixed cyber defense forces
3 Enhance dedicated DoDIN cyber defenses
4 Develop cyber-focused strategies, plans and assessments

C2 Systems Capabilities LOE

Lines of Operation:

1 Identify and validate Joint and Component C2 capability requirements
2 Identify C2 capability gaps and assess risk
3 Enable and inform C2 operational priorities

Joint / Coalition Interoperability LOE

Lines of Operation:

1 Lead Joint Information Environment (JIE) implementation
2 Lead Mission Partner Environment (MPE) implementation
3 Define / develop / inform joint, allied & coalition interoperability standards
4 Conduct and synchronize capability demonstrations and assessments

Chief Information Officer Responsibilities LOE

Lines of Operation:

1 Establish and manage an IT Portfolio Management process for TJS
2 Develop Mission Networks / CJCS Controlled Activities Cyber Security Program
3 Implement Special Access Programs Security Controls
4 Execute Residual / Retained Joint Staff Support

End State

- Ready and resilient C4 and Cyber-enabled Joint Force capable of operating with:
  - Allies
  - Coalition Partners
  - Interagency
- Synchronization of our Lines of Effort, operation and activities across the C4 / Cyber environment in which the Joint Force Operates
- Robust JS CIO management and oversight roles, responsibilities and processes that support and enable our JS mission networks

"Wildly Important Goals"

Achieve Globally Integrated Capabilities

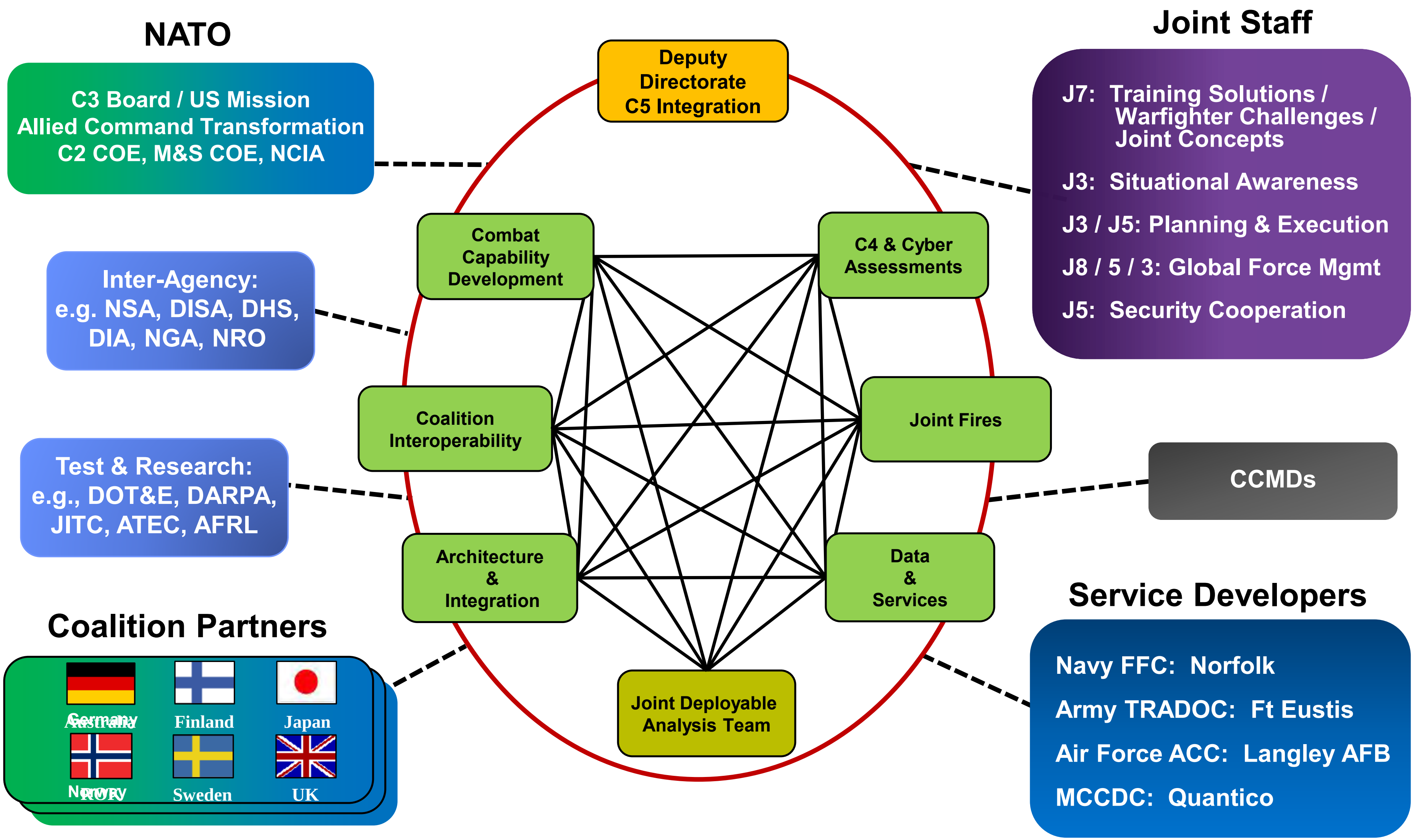
Develop Mature, Integrated Cyber Capabilities

Achieve Operational Interoperability

Achieve Sustained Coalition Interoperability Assurance and Validation (CIAV) in support of CCMDs

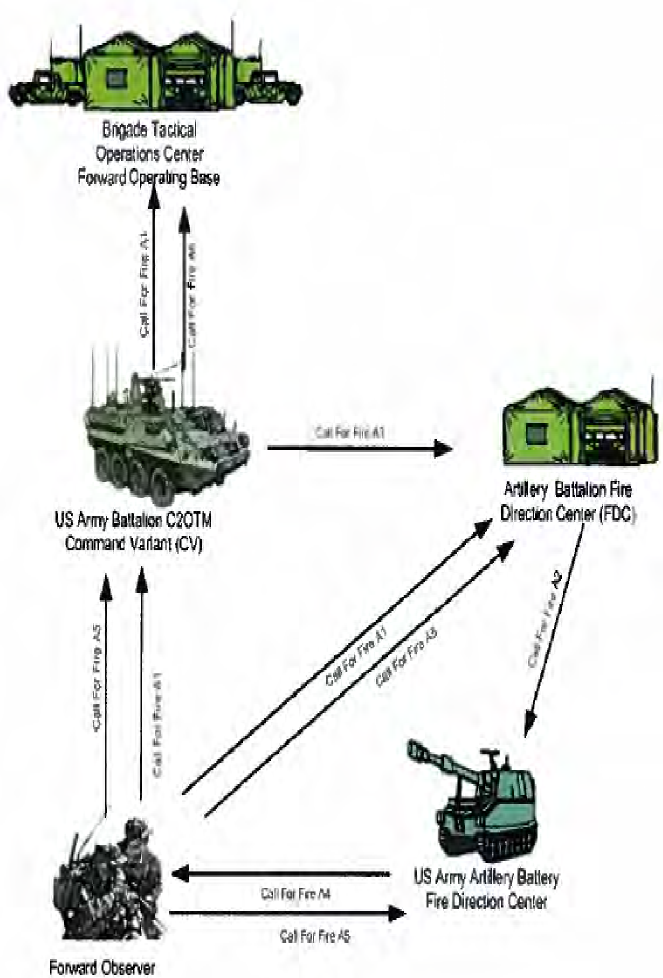
Note: All goals inclusive of Joint, Inter-Agency and Coalition partners

Interdependencies



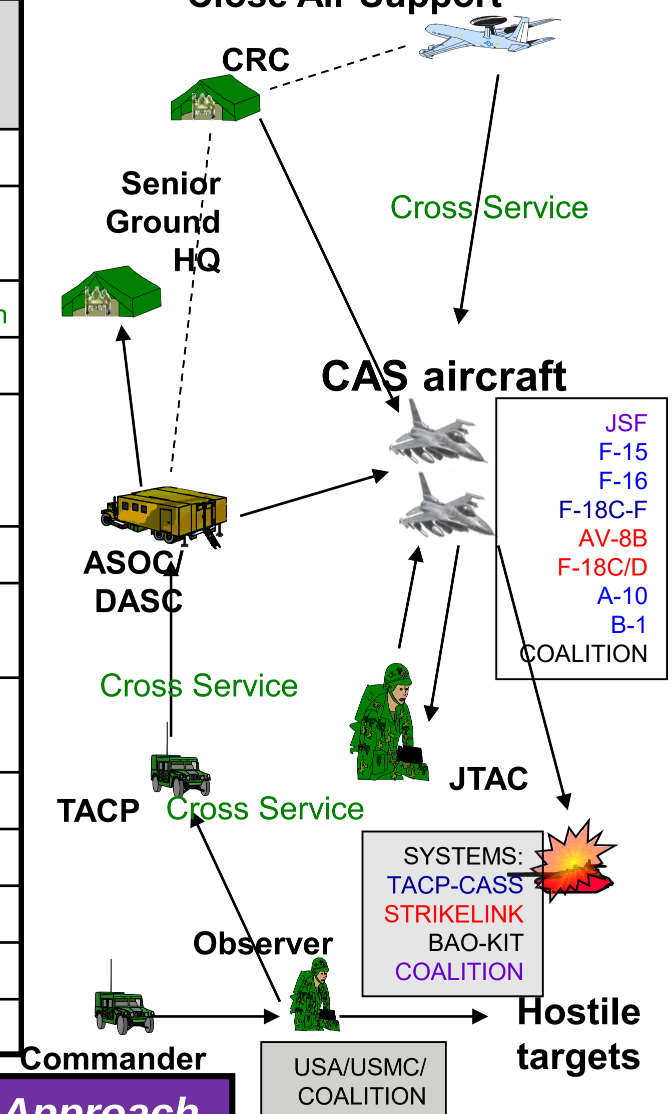
Joint and Coalition Mission Threads

Service-Specific
Call for Fires



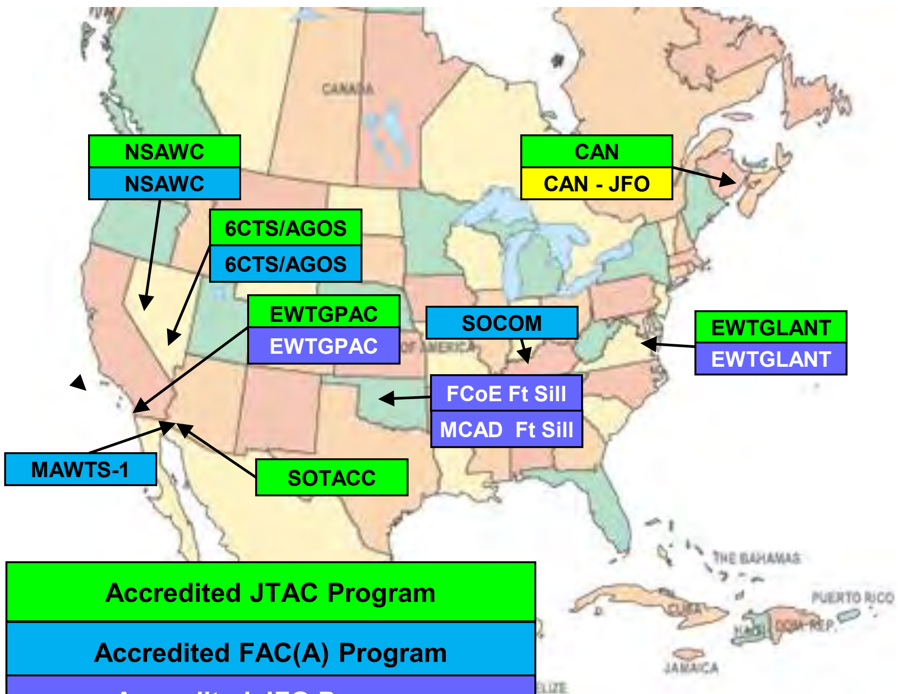
Mission Event No.	Description
1	Unit detects target
2	Commander decides to request CAS
3	Unit notified TACP < 3min
4	TACP passes request to ASOC
5	ASOC coordinates with senior ground HQs which approve request
6	ASOC assigns on-call aircraft
7	CRC send aircraft to contact point (CP)
8	AWACS passes critical updates to aircraft > 95% Acrcy
9	JTAC briefs aircraft < 2 min
10	Aircraft depart initial point (IP)
11	JTAC controls CAS aircraft
12	Bombs on target > 98.9 % PK
13	Assessment

Joint / Coalition
Close Air Support

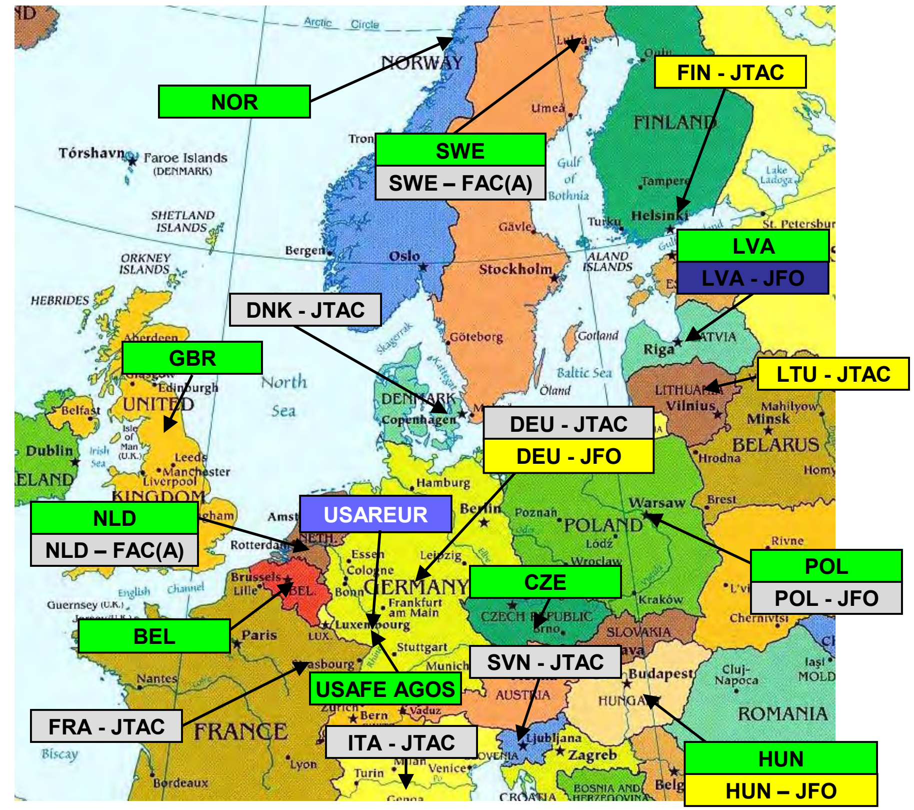


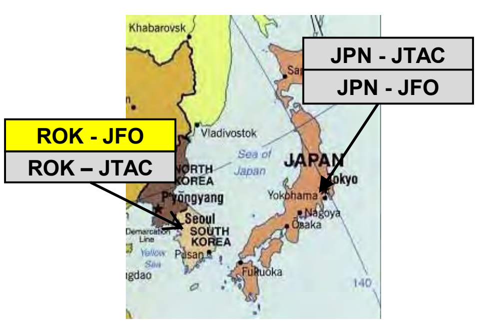
Service-Centric to Enterprise-Centric Approach

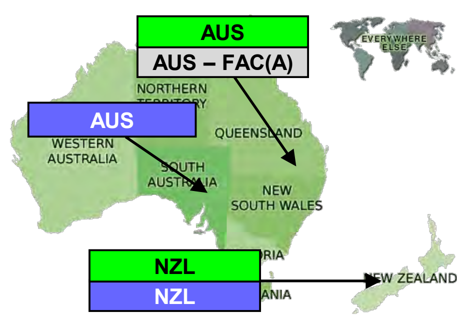
JTAC, FAC(A) and JFO MOA
Accredited Schoolhouses / Programs / Engagement



- Accredited JTAC Program
- Accredited FAC(A) Program
- Accredited JFO Program
- MOA Signatory – Accreditation Pending
- Talks in Progress







BOLD QUEST 16.2 Threads

Coalition ISR

- Joint and coalition partnership to share intelligence from multiple ground and air sources
- Drive operations and target engagement across multiple initiatives and throughout a common scenario

Joint Fire Support

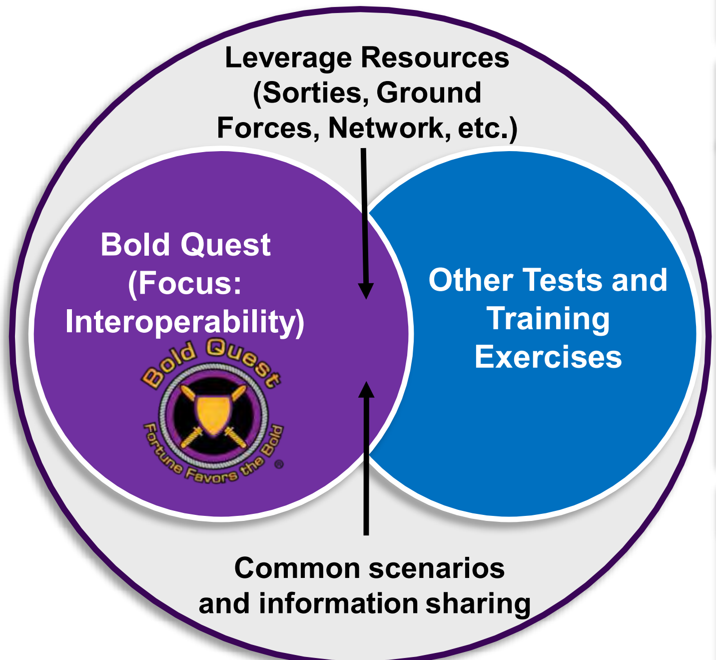
- Joint and coalition digital interoperability end-to-end from JFO / JTAC to CJTF
- Multiple nations participating with distinct system types exercising extensive cross-service and cross-nation threads
- JFOs from multiple nations demonstrating digital interoperability in a live fire event

Integrated Air and Missile Defense

- Exercising engagement authority and procedures in a robust BLUFOR / OPFOR, live and simulated sorties
- Air-air; surface-air; air-surface engagements in a complex air and surface environment

Live/Virtual Environment

- Coalition JTAC / JFO and Aircrew in distributed virtual sim (CONUS / OCONUS), with Air Support Operations Center (ASOC) and ISR support



Digitally Aided Close Air Support

- Digital interoperability among joint terminal attack controllers (JTAC), aircrew and C2 nodes
- Multiple nations with several JTACs, conventional and SOF, per nation
- Concurrent credit toward individual JTAC annual sustainment training

Friendly Force Tracking and Ground-Air Situational Awareness

- Demonstrating shared SA between US and Coalition hand-held FFT systems
- Developing NATO Interoperability standards with multiple nations and NATO HQ
- Provide ground tracks to fixed wing aircrew conducting CAS for SA and fratricide avoidance

Cyber

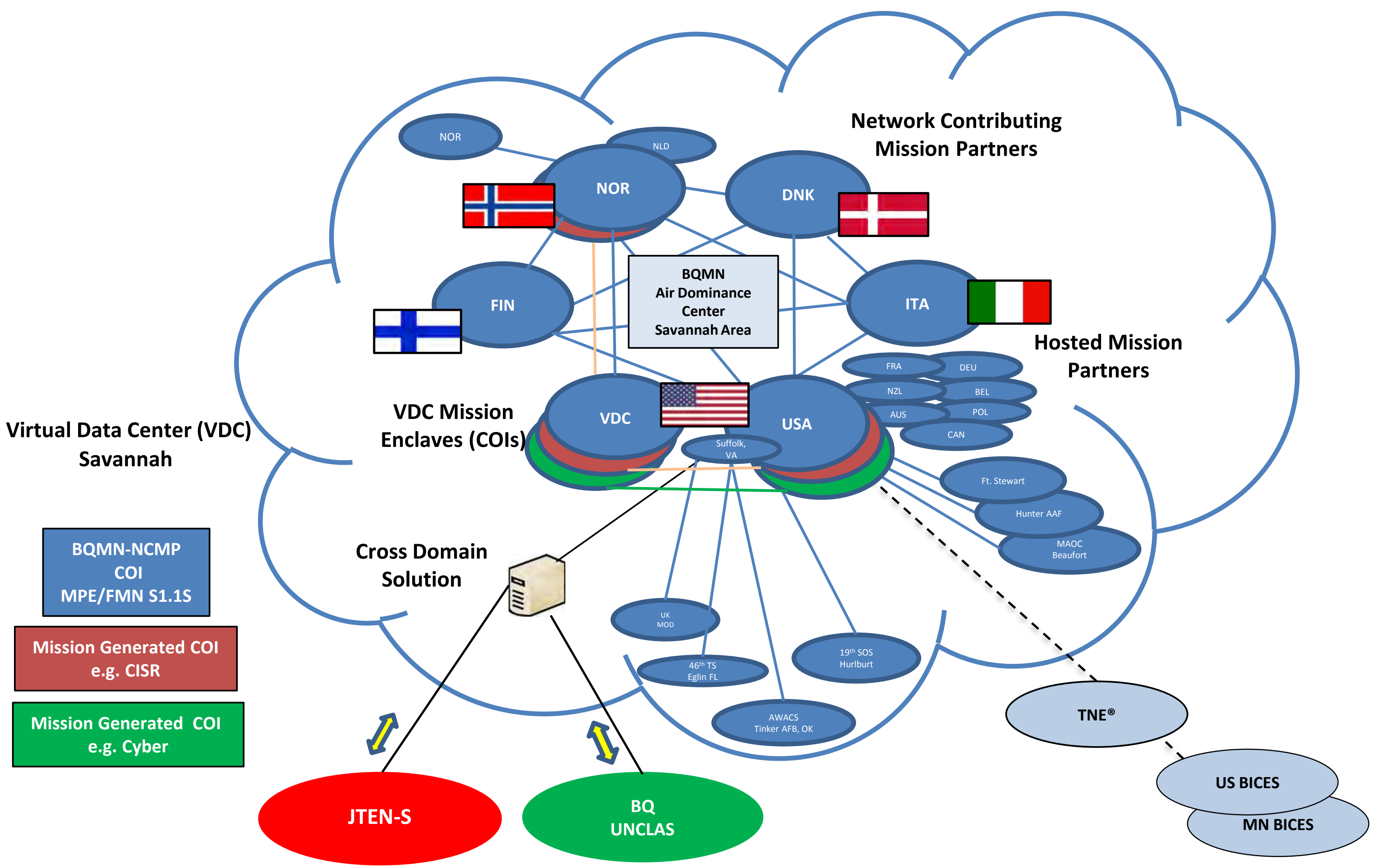
New in BQ16.2

- Stand-up multi-national cyber cell
- Conduct cooperative vulnerability assessment
- Cyber OPFOR effects

Coalition Network (Federated Mission Networking)

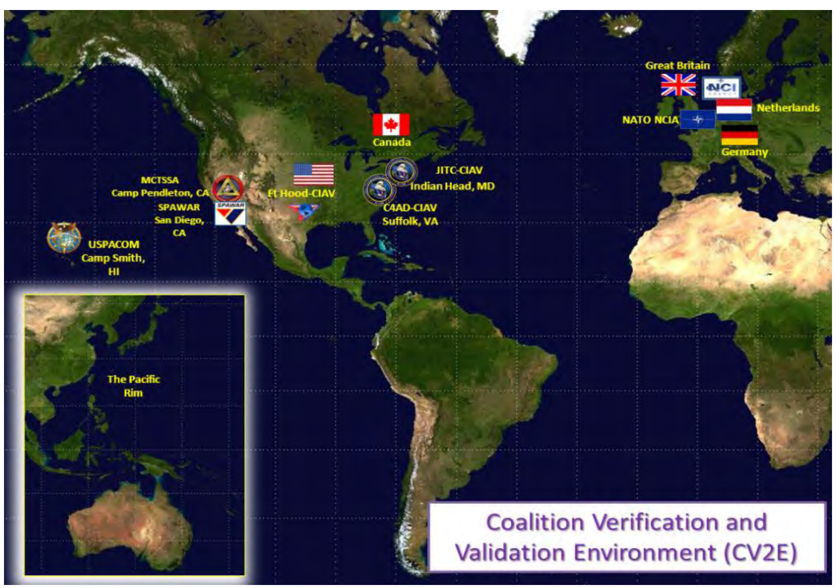
- Federated environment encompassing national networks / systems
- Each nation follows their own national policies and operates their own mission command systems and core services for collaboration
- Guided by collaboratively developed Joining, Membership and Exit Instructions (JMEI)

BOLD QUEST 16.2 Mission Network (11 Oct-3 Nov 2016)



Coalition Interoperability Assurance and Validation (CIAV)

- **Resolves mission-based interoperability problems BEFORE new systems and software are fielded**
- **Desk Top Analysis (DTA) methodology assesses end-to-end information exchange across DOTmLPF-P (solutions not always technical)**
- **Validates Coalition Mission Threads (CMTs) and Coalition Tactics, Techniques, and Procedures (CTTPs)**



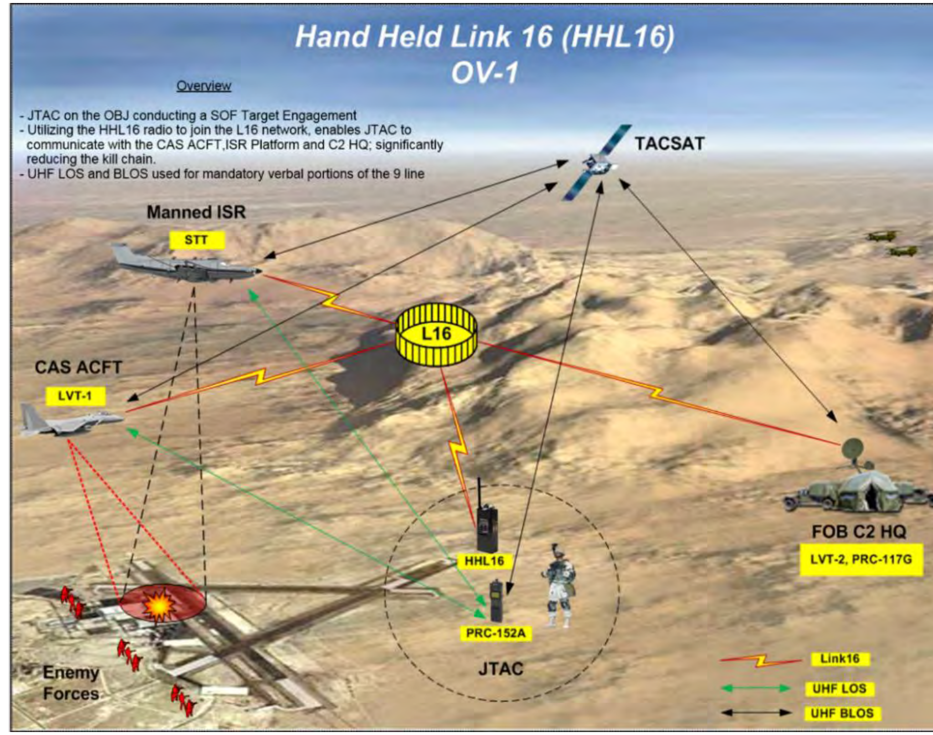
- **Coalition Test and Evaluation Environment (CTE2) replicates Afghanistan Mission Network (AMN) and systems**
- **Coalition Verification and Validation Environment (CV2E) simulates Mission Partner Environment (MPE) / Federated Mission Networking (FMN) systems**

DDC5I now leads U.S. CIAV

Technology Integration Example: Hand-Held Link 16 (HHL-16)

USSOCOM / C5AD project and JCTD project to integrate, assess, and rapidly field a handheld tactical datalink radio

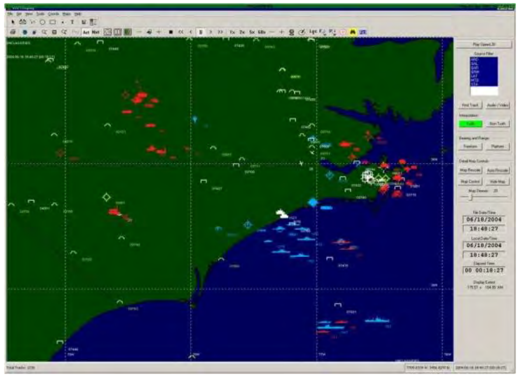
- Connects dismounted Joint Terminal Attack Controllers (JTACs) directly into LINK 16 network to digitally call for fire
- Provide all nodes with accurate situational awareness in joint integrated air and ground common operational picture
- Prevents fratricide and minimizes collateral damage
- Enables command and control in degraded RF environments
- Enables US and coalition forces to leverage worldwide L-16 capabilities of 50+ nations



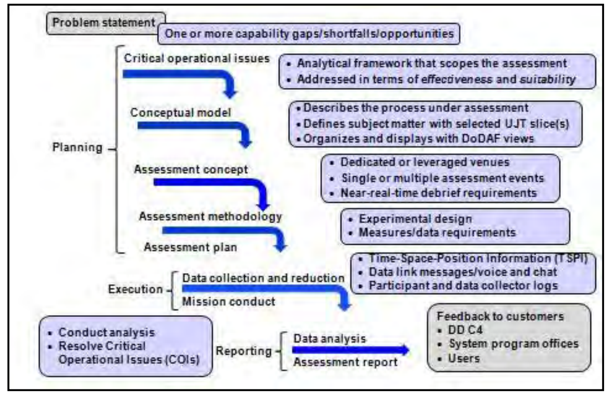
HHL-16 deployment began in FY 17

Technical Capabilities

Visual Analysis and Mission Monitoring Tool

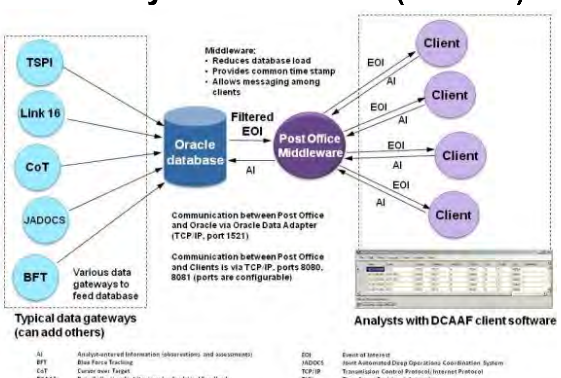


JDAT Capability Assessment Process



Deployable Technical Operations Center

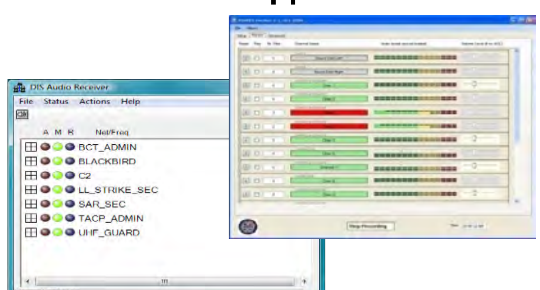
Data Collection Architecture for Analytical Feedback (DCAAF)



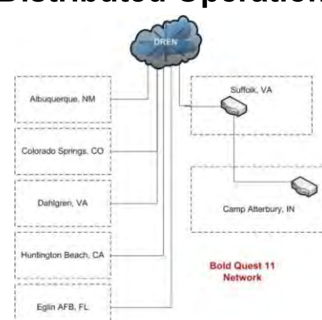
Delivering decision-quality recommendations from combatant command, multinational, and Service venues

Communications Assets

Software Applications



Distributed Operations



Joint and Coalition Interoperability Enablers

Interoperability built in, not added on

Coalition interoperability as a requirement

Policy that supports coalition information exchange

Leverage community of interest initiatives

Leverage interoperability forums

Common standards, standardized implementation

"Coordinated" acquisition across Services and nations

Machine-to-machine ideal but not required

Tactics, techniques and procedures

Training is key: "Train like we will operate"

Contact Information:

Scott Shephard
U.S. Joint Staff J6
757-836-0632
scott.s.shephard.civ@mail.mil

DoD Digital Engineering Strategy

Ms. Philomena Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

Digital Engineering Overview

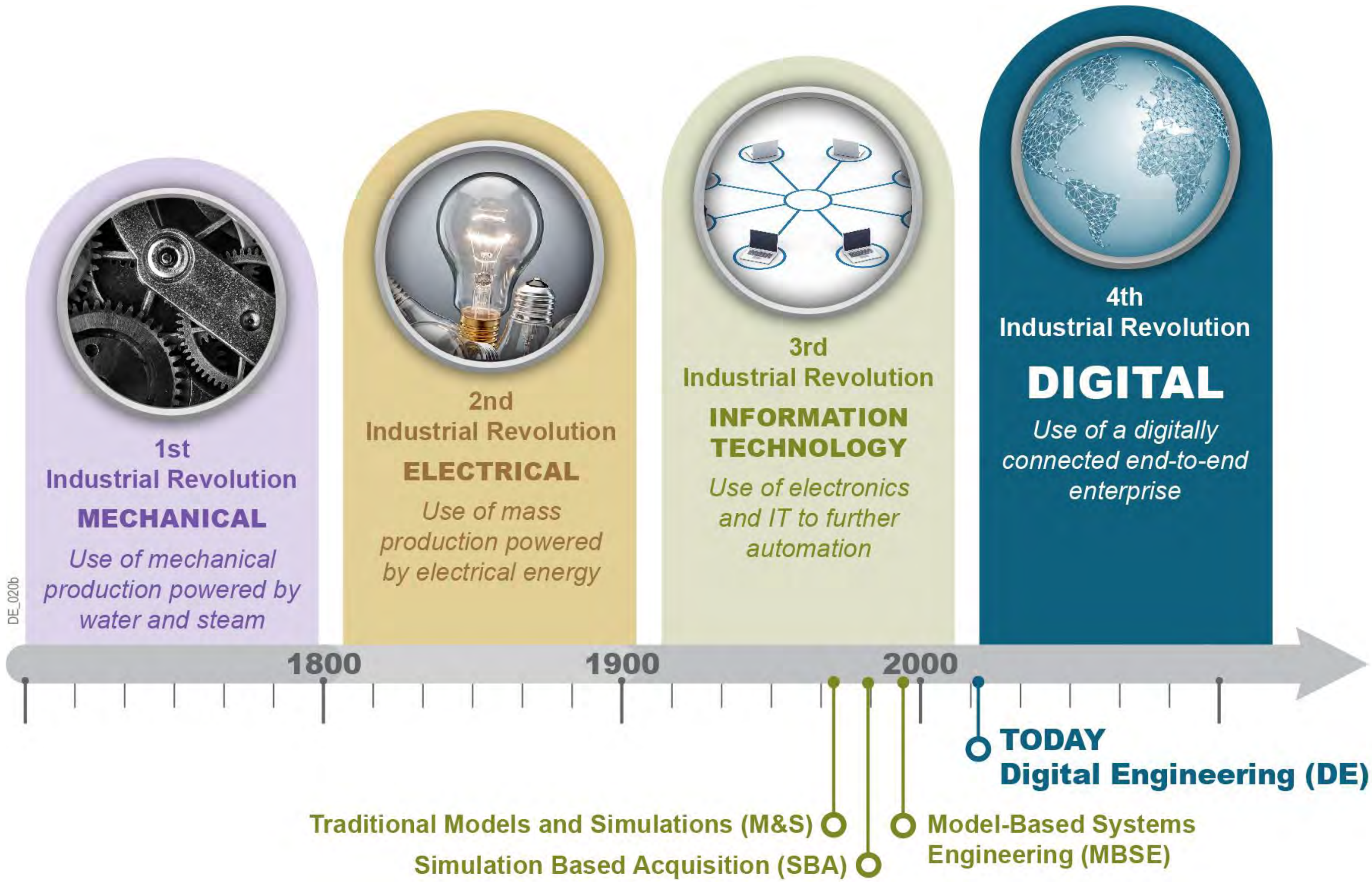
- **Background**
  - Dynamic operational and threat environments
  - Growth in system complexity and risks
  - Linear acquisition process that lacks agility
  - Cost overruns and delayed delivery of capabilities to the warfighter
  - Current practices can't keep pace with innovation and technology advancements

Digital Engineering: An integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.

- **Need**
  - Outpace rapidly changing threats and technological advancements
  - Deliver advanced capabilities more quickly and affordably with improved sustainability to the warfighter
  - Foster a culture of innovation

Digital Engineering transforms the way the DoD innovates and operates

History

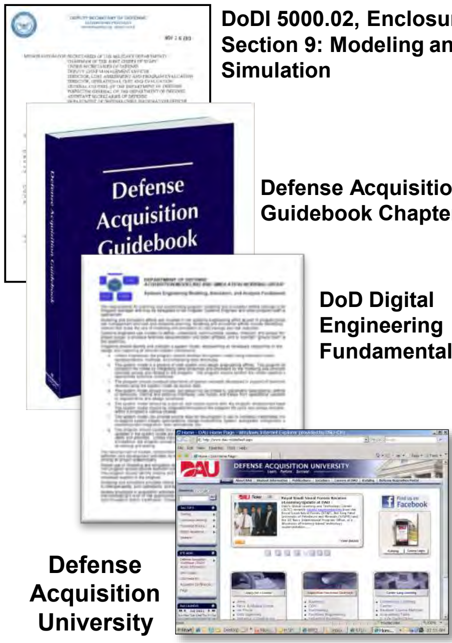


1st
Industrial Revolution
MECHANICAL
Use of mechanical production powered by water and steam
2nd
Industrial Revolution
ELECTRICAL
Use of mass production powered by electrical energy
3rd
Industrial Revolution
INFORMATION TECHNOLOGY
Use of electronics and IT to further automation
4th
Industrial Revolution
DIGITAL
Use of a digitally connected end-to-end enterprise
DE_020b
1800
1900
2000
TODAY
Digital Engineering (DE)
Traditional Models and Simulations (M&S)
Simulation Based Acquisition (SBA)
Model-Based Systems Engineering (MBSE)

Leveraging Multiple Activities

Infusion in Policy & Guidance

http://www.acq.osd.mil/se/pg/guidance.html



DoDI 5000.02, Enclosure 3, Section 9: Modeling and Simulation

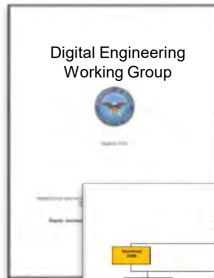
Defense Acquisition Guidebook Chapter 3

DoD Digital Engineering Fundamentals

Defense Acquisition University

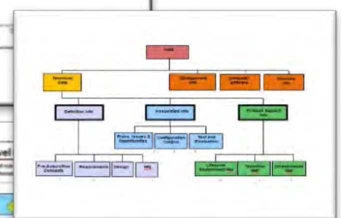
NASA – National Aeronautics and Space Administration
NNSA – National Nuclear Security Administration
NDIA – National Defense Industrial Association
INCOSE – International Council on Systems Engineering
AIA – Aerospace Industries Association
AIAA – American Institute of Aeronautics and Astronautics
OEMs – Original Equipment Manufacturers

ODASD(SE) Initiatives

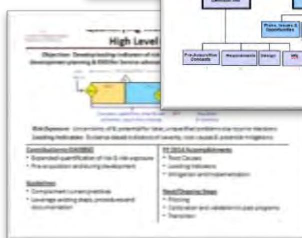


DoD Digital Engineering Working Group (DEWG)

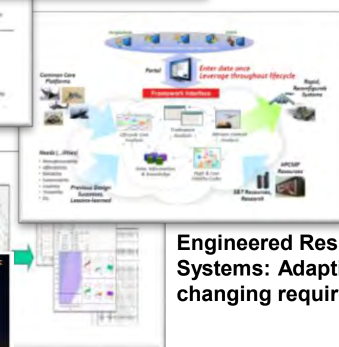
Digital Engineering Strategy



Digital System Model (DSM) Taxonomy: Defining categories of data across acquisition



System Engineering Research Center (SERC): Model Centric Research



Engineered Resilient Systems: Adapting to changing requirements

NASA: Sounding Rocket Program

High Performance Computing Modernization Program (HPCMP) Computational Research and Engineering Acquisition Tools and Environments (CREATE) : Physics Based Modeling

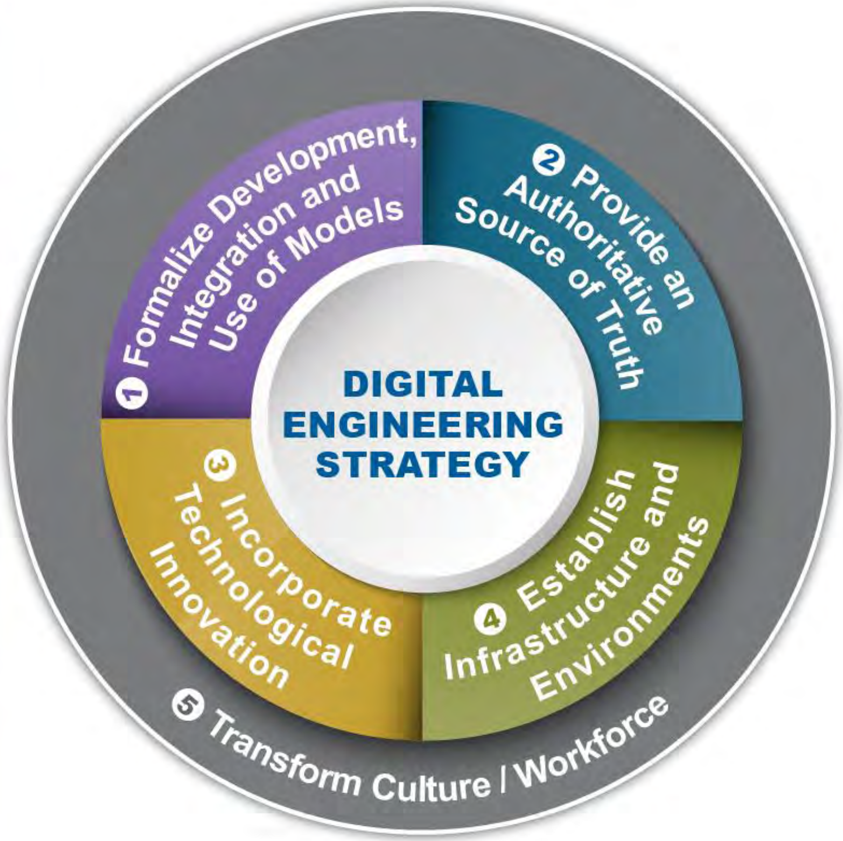
Partnerships

- **Armed Services**
- **DoD Components**
- **Interagency**
- **Industry/OEMs/ Industrial Orgs**
- **Academic**

Advancing the state of practice for Digital Engineering

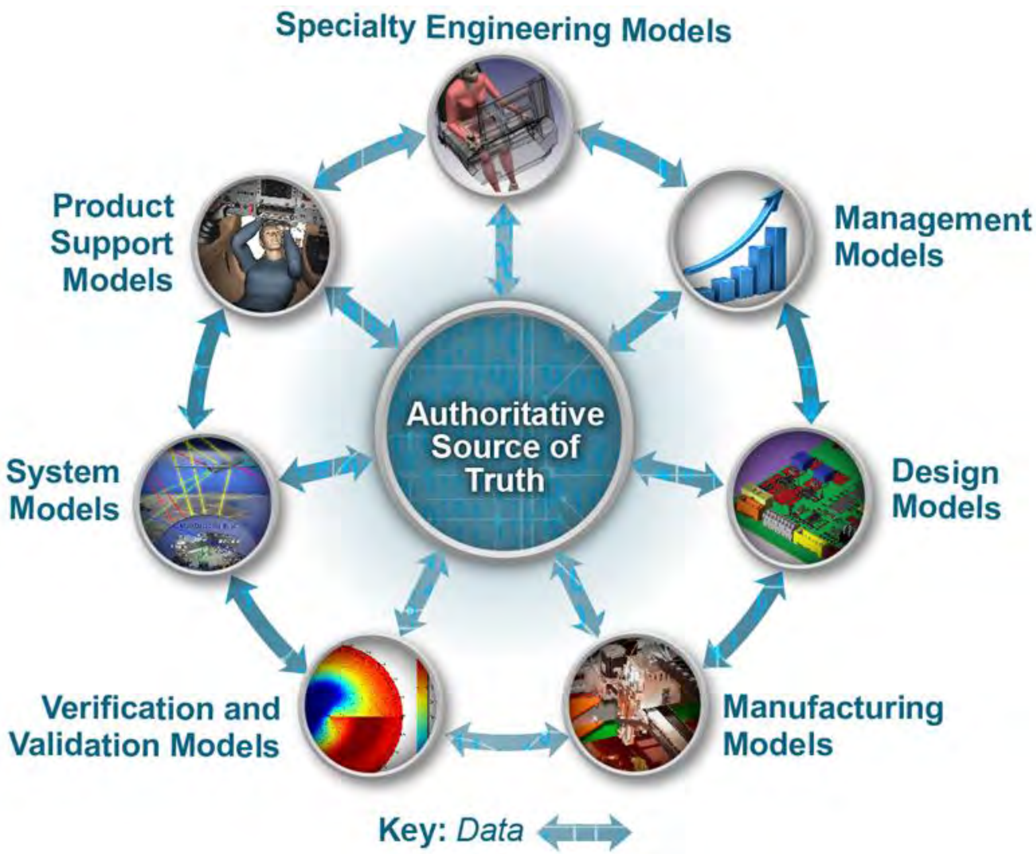
Digital Engineering Strategy: Five Goals

1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** to perform activities, collaborate, and communicate across stakeholders
5. Transform a **culture and workforce** that adopts and supports Digital Engineering across the lifecycle



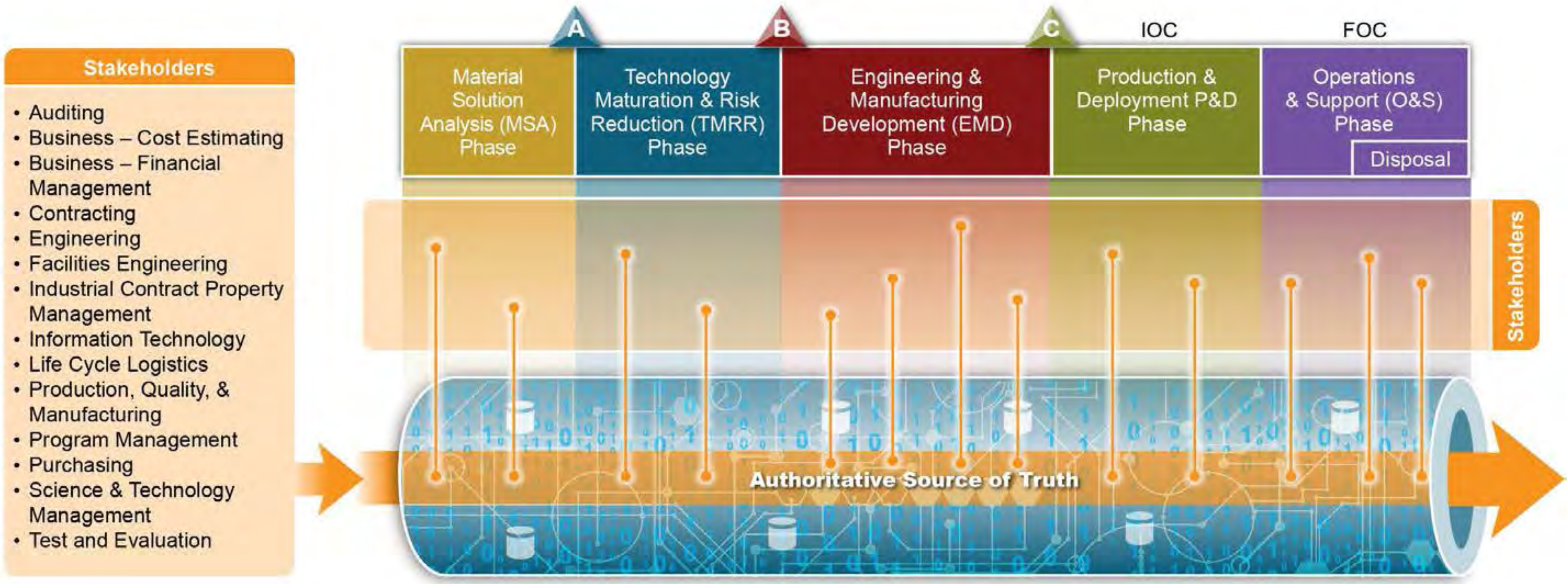
Drives the engineering practice towards improved agility, quality, and efficiency, which results in improvements in acquisition

Goal #1: Formalize Development, Integration & Use of Models



Models as the cohesive element across a system's lifecycle

Goal #2: Provide an Authoritative Source of Truth



Right information, right people, right uses, right time

Goal #3: Incorporate Technological Innovation

- ❖ Big Data and Analytics
- ❖ Cognitive Technologies
- ❖ Computing Technologies
- ❖ Digital-to-Physical Fusion Technologies

Harness technology, new approaches, and human-machine collaboration to enable an end-to-end digital enterprise

Goal #4: Establish Infrastructure & Environments

Foundational support for Digital Engineering environments

Goals #5: Transform Culture and Workforce

Institutionalize Digital Engineering across the acquisition enterprise

Expectations & Big Rocks

Digital Engineering Expectations
Informed decision making/greater insight through increased transparency
Enhanced communication
Increased understanding for greater flexibility/adaptability in design
Increased confidence that the capability will perform as expected
Increased efficiency in engineering and acquisition practices

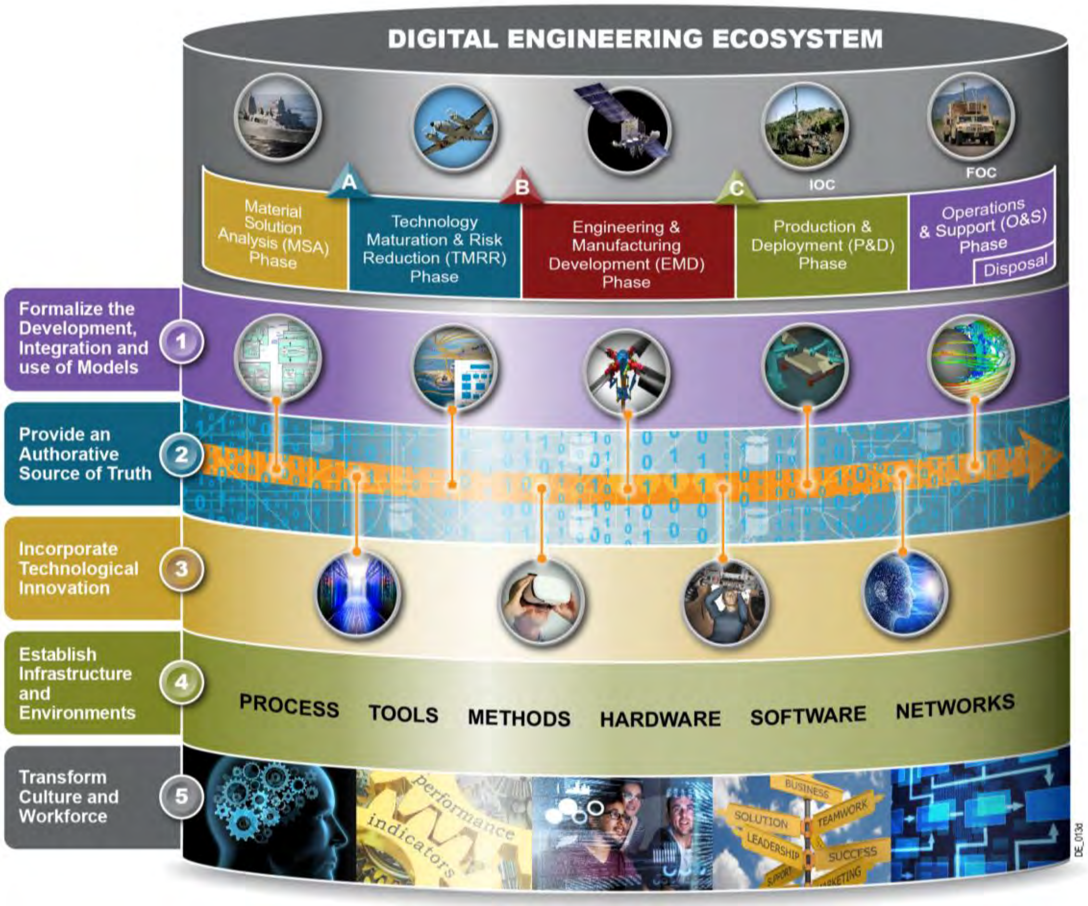
From Inter-Agency Working Group: Model-Based System Engineering (MBSE) Infusion Task Team, "Digital Model-based Engineering: Expectations, Prerequisites, and Challenges of Infusion," 2017

Digital Engineering Big Rocks
Investments
Culture and workforce
Policy, guidance, contracting
Governance
Security
Intellectual property protection
Tool/model portability
Infrastructure and environments
Model quality and assurance

Synthesized from Digital Engineering Working Group; National Defense Industrial Association Model-Based Engineering Report, Aerospace Industries Association Model-based Engineering reports

Coordinating with the Services/Agencies to develop and implement Digital Engineering strategy

A Holistic View of Digital Engineering Ecosystem

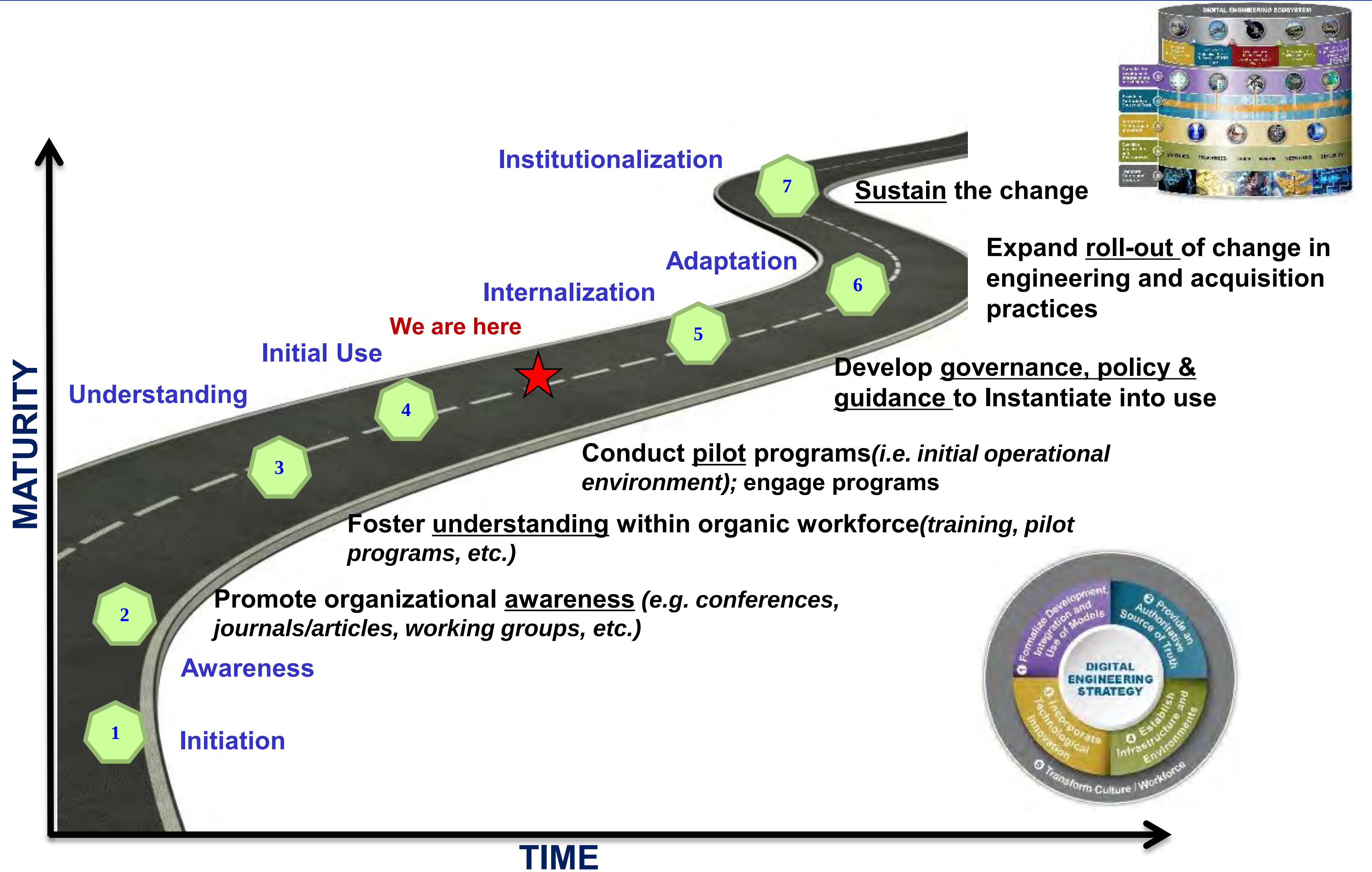


DoD is shifting towards a Digital Engineering ecosystem that will transform the culture, people, technology, and environments

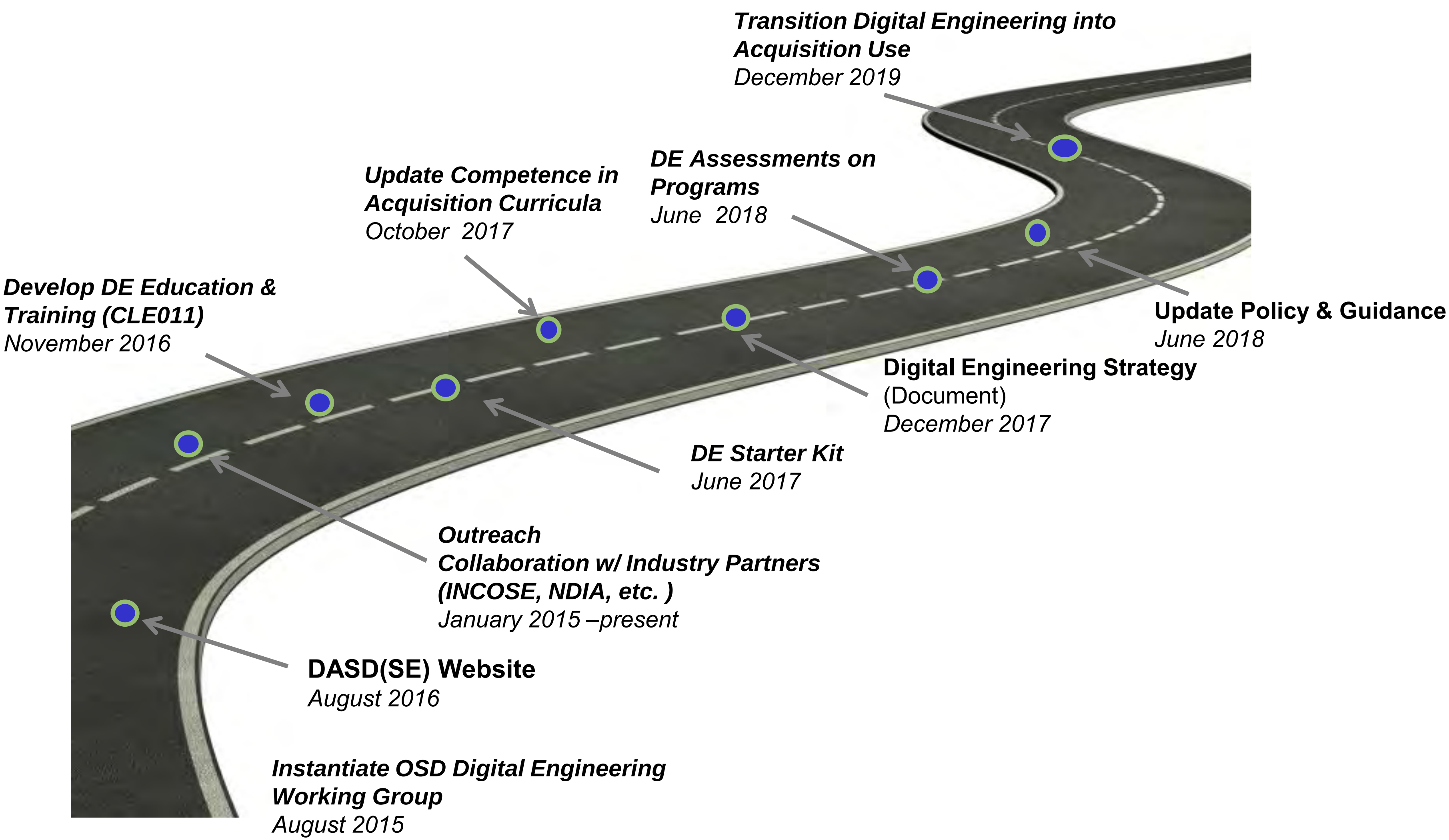
There Is Much More to Do…

- **Publish the Digital Engineering Strategy**
  - Support development of implementation guidance/direction in Services/Agencies
- **Engage with Acquisition Programs**
  - Establish criteria for use of Digital Engineering artifacts for decision points
- **Update Competencies across Acquisition Curricula**
  - Identify education and training outside of acquisition curricula
- **Update Policy and Guidance (Engineering, et al)**
  - Develop/update governance processes, policy, guidance and contracting language
- **Transform Acquisition Practice**
  - Engage acquisition users and incorporate rigor into Digital Engineering practices across the lifecycle

Digital Engineering Road Map



Digital Engineering Transition Across DoD



Summary

- Business processes and behaviors (culture) need to be changed to realize the benefits of Digital Engineering implementation.
- Multiple activities in government, industry, academia and professional organizations are being leveraged to advance digital engineering concepts within DoD enterprise.
- Expected benefits of implementing digital engineering practice outweigh the monetary, time and training needed up front.
- Basic elements of Digital Engineering are in place; we need to weave them together and instantiate with policy, guidance and training.

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695 | philomena.m.zimmerman.civ@mail.mil

Other Contributors:

Tracee Walker Gilbert, Ph.D.

571-372-6145 | tracee.w.gilbert.ctr@mail.mil

Frank Salvatore

973-265-9837 | frank.j.salvatore.ctr@mail.mil

Tyesia Pompey Alexander, Ph.D.

571-372-6697 | tyesia.p.alexander.ctr@mail.mil

Darryl Howell

571-372-6699 | Darryl.I.Howell.ctr@mail.mil

Modeling the Digital System Model (DSM) Data Taxonomy

Philomena Zimmerman

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

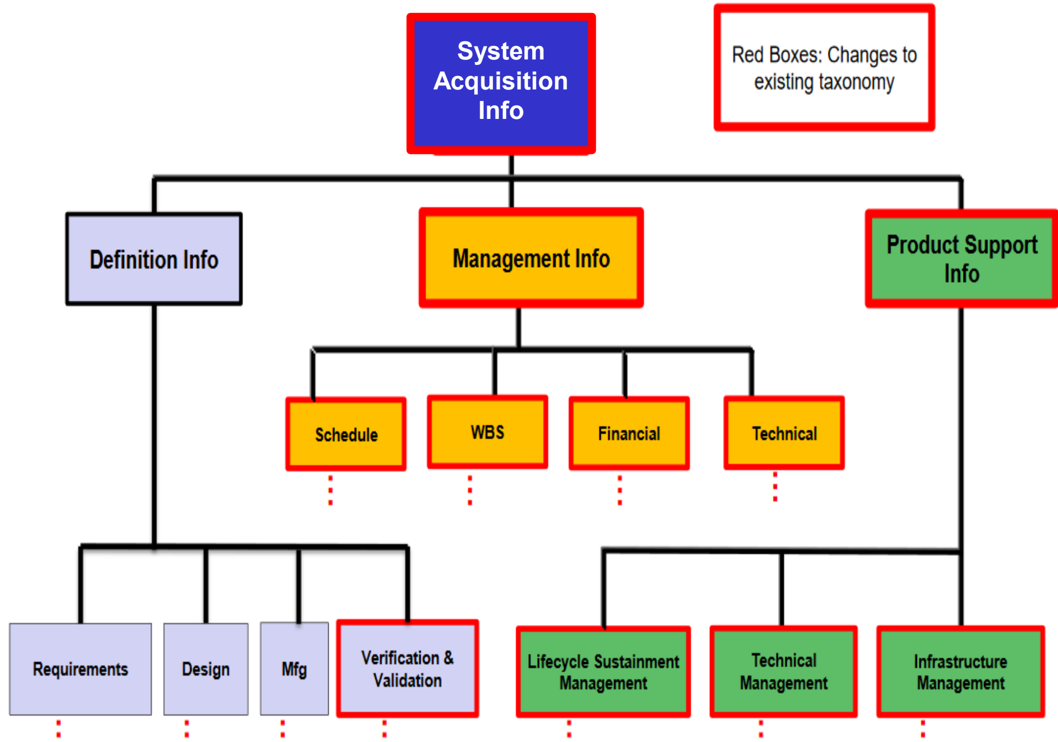
Springfield, VA | October 25, 2017

Agenda

- DSM Data Taxonomy Overview
- Evolution of the DSM Data Taxonomy (Tabular, Mind Map, SysML)
- Modeling the DSM Data Taxonomy
- Benefits
- Path Forward

DSM Data Taxonomy Overview

- **Purpose**
  - Provides a model to aid programs in defining an authoritative source of truth
  - Builds an integrated taxonomy providing stakeholders an organized structure for the types of technical data to be considered across the life cycle
  - Establishes a Common Vocabulary that can be used by all programs



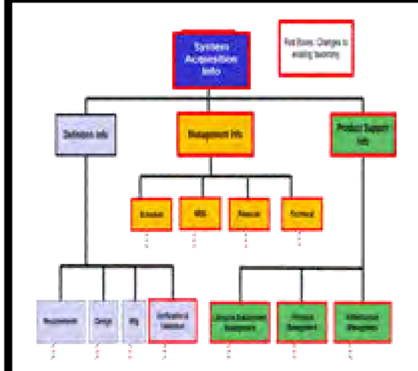
A change from document centric taxonomy in DAG CH 3–4.1.7 Technical Data Management Process.

Use as a basis to drive the community towards Digital Engineering across disciplines, systems and enterprises to support life cycle activities from concept to disposal.

DSM Intended Use

Defines the broad categories of data

DSM Data Taxonomy



Component of the DE Infrastructure

Provides the program's DE ecosystem

DE Ecosystem

Requirements
Contracts
Architecture
Cost
Design
Management
Test
Sustainment
Manufacturing
Configuration Management

Identifies the data and data rights

Document Views

Provides multiple views to support ***decisions***

Data Views

Acquisition Views

Other Views

DSM Data Taxonomy provides the broad categories of data that should be considered across the lifecycle

Data Taxonomy Uses

- The taxonomy serves as a common vocabulary for enterprise and program consideration.
- Use it to define the data the program will need to create and manage.
- Use it to determine what tools will use or produce the data.
- Use it to determine who owns and controls the data at any point in time in a programs life.
- Use it to identify what data will be delivered on contract, what format the data should be received in.
- Use it to identify what data has associated data restrictions.
- Use it to identify what data needs to be protected and handled.
- Use it to define the data that belongs in views, digital and or other artifacts.

Evolution to Modeling the DSM Data Taxonomy

Tabular Tool

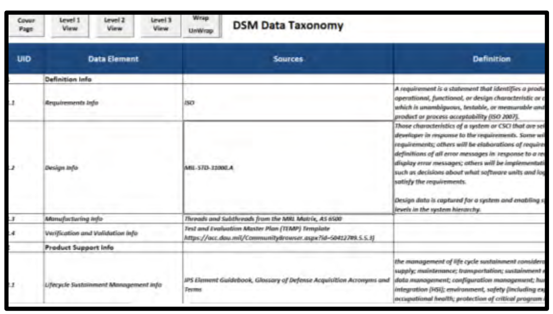
- Initial attempt to organize and construct a hierarchical structure for technical data in a system from documents and guidelines (e.g., DAG, ICD, CDD, SEP, TEMP, MIL-STD, SME, etc.)

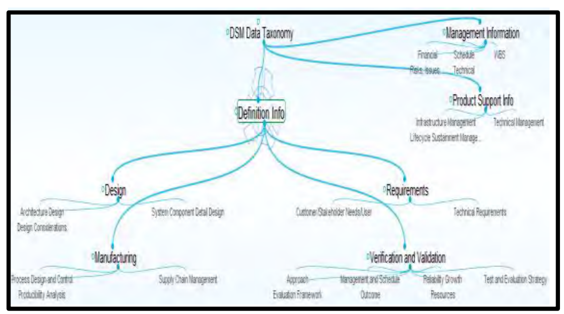
Mind Mapping Tool

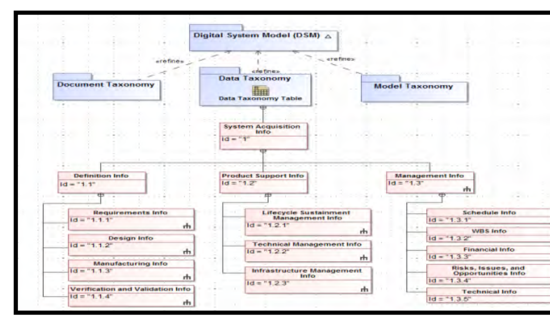
- Prototype testing using a mind mapping tool to visualize hierarchical relationships between system components and their respective digital artifacts

SysML Modeling Tool

- Utilized a System Modeling Language (SysML) modeling tool to construct a hierarchical structure and enable the capture of digital technical data for use and reuse in a model







DSM Data Taxonomy in Excel

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

DSM Data Taxonomy

UID	Data Element	Sources
1	Definition Info	
2	Product Support Info	
3	Management Info	

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

DSM Data Taxonomy

UID	Data Element	Sources	Definition	Comments
1	Definition Info			
1.1	*Requirements Info*	*ISO*	*A requirement is a statement that identifies a product or processes operational, functional, or d*	
1.2	*Design Info*	*MIL-STD-31000A*	*Those characteristics of a system or CSCI that are selected by the developer in response to the req*	

Cover Page | Level 1 View | Level 2 View | Level 3 View | Level All View | Wrap | UnWrap

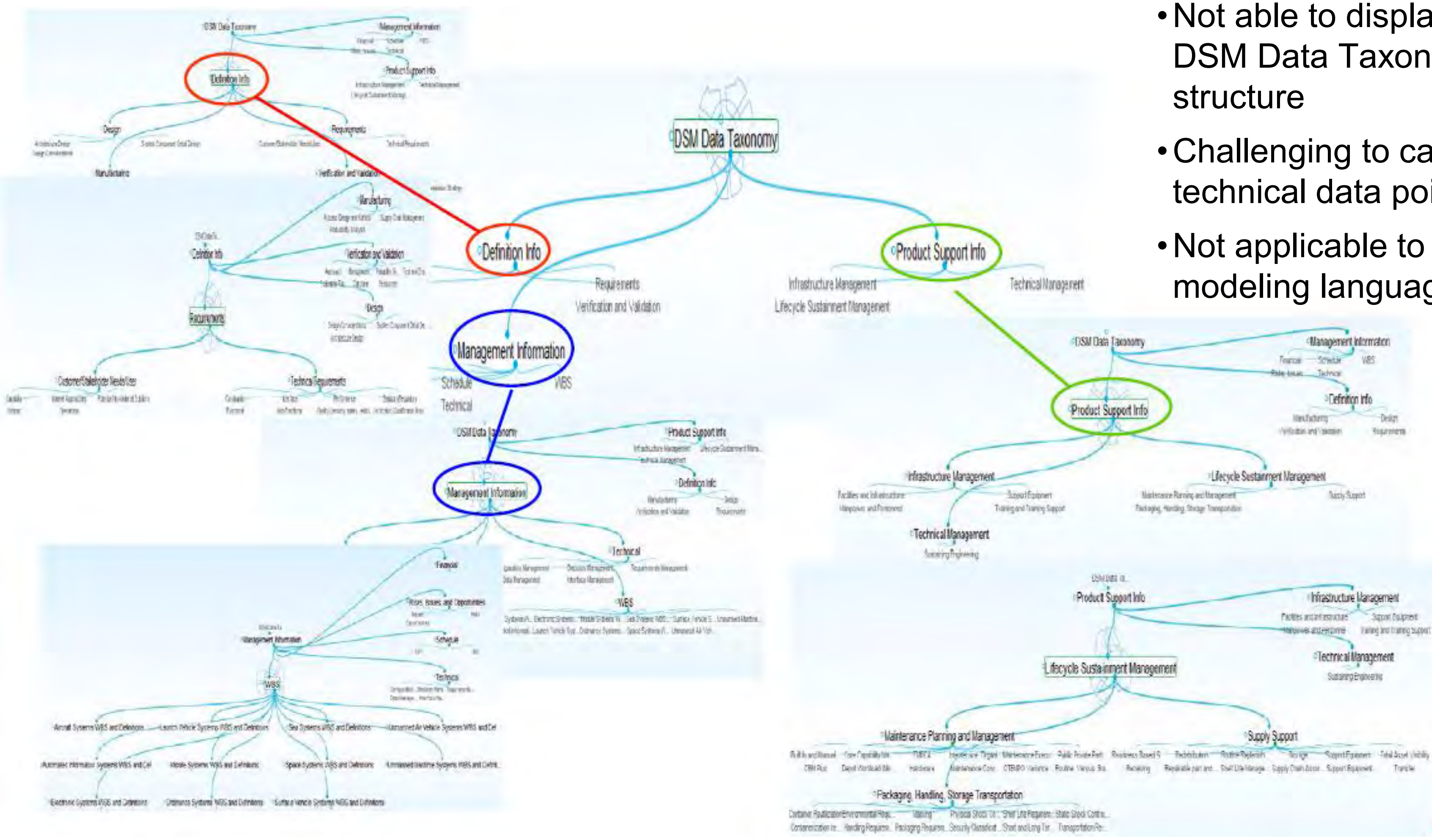
DSM Data Taxonomy

UID	Data Element	Sources	Definition	Comments
1	Definition Info			
1.1	***Requirements Info***	***ISO***	***A requirement is a statement that identifies a product or processes operational, functional, or design***	
1.1.1	Customer/Stakeholder Needs/User Info	DI-IPSC-81431A/SEBOK	Set of stakeholder requirements are clarified and translated from statements of need into engineerin	
1.1.1.1	Capability	ICD	A capability is the ability to achieve a desired effect under specified standards and conditions throu	
1.1.1.1.1	Capability Gap	ICD	The inability to execute a specified course of action. The gap may be the result of no existing capabi	
1.1.1.1.2	Required Capabilities	ICD	A capability required to meet an organization's roles, functions, and missions in current or future op	
1.1.1.1.3	Enabling Capabilities	DoDD 3700.01	services, systems, processes, and related infrastructure that enable the exercise of authority and di	
1.1.1.1.4	Applicable Joint Capability Areas (JCAs)	ICD	JCAs are collections of similar capabilities logically grouped to support strategic investment decisio	
1.1.1.2	Contract	DI-IPSC-81431A/SEBOK		
1.1.1.3	Operational	DI-IPSC-81431A/SEBOK		
1.1.1.3.1	Mission Information	JCIDS products (FAA, FNA, FSA); ICD, CDD, OMS/MP)		
1.1.1.3.1.1	Mission Essential Tasks	Requirements documents (Operational and Functional Concepts; JCIDS pr	A collective task a unit must be able to perform successfully in order to accomplish its doctrinal or	
1.1.1.3.1.2	Mission Objectives/Operational Outcomes/Effects/Military Objective Achieved Info	Requirements documents (Operational and Functional Concepts; JCIDS pr	Effectiveness The overall degree of mission accomplishment by a system under realistic conditions (	
1.1.1.3.1.2.1	Concept of Operations Summary	ICD	A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in	
1.1.1.3.1.2.2	Operational Outcome	ICD	(d) Identify what measurable operational outcomes are required; what effects must be produced to a	
1.1.1.3.1.3	Measures of Effectiveness (MoE)	CDD	Measures designed to correspond to accomplishment of mission objectives and achievement	
1.1.1.3.1.4	Measures of Suitability (MoS)	CDD	Measure of an item's ability to be supported in its intended operational environment. MOS's typical	
1.1.1.3.2	Threat and Operational Environment Info	System Threat Assessment Report (STAR)		
1.1.1.3.2.1	Operational Environment	System Threat Assessment Report (STAR)	This is a composite of conditions, circumstances, and influences that affect employment of military	
1.1.1.3.2.2	Threat Summary	System Threat Assessment Report (STAR)	The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can li	
1.1.1.3.3	Tasks	Functional Area Analysis (FAA); Functional Needs Assessment (FNA); Oper	A clearly defined and measurable activity accomplished by individuals and organizations. (FM 7-0)	
1.1.1.3.3.1	Conditions	Formation OMS/MP (Collective Tasks, Conditions, Standards); System OM	Those variables of an operational environment or situation in which a unit, system, or individual is	
1.1.1.3.3.2	Standards	Formation OMS (Collective Tasks, Conditions, Standards); System OMS (S	A quantitative or qualitative measure and criterion for specifying the levels of performance of a task	
1.1.1.3.3.3	Measures of Performance (MoP)	Formation OMS (Collective Tasks, Conditions, Standards); System OMS (S	A criterion used to assess friendly actions that are tied to measuring task accomplishment. (JP 3-0)	
1.1.1.3.4	Timeframe and Justification	Required Capabilities (RC) (published by ARCIC and/or COEs); Army Warf	The timeframe considered in the CBA is important both to help establish the conditions and threats u	
1.1.1.3.5	Defense Planning Scenarios	DI-IPSC-81431A/SEBOK	This is a graphic and narrative description of area, environment, means (political, economic, social,	
1.1.1.3.6	Using Organization(s) (supported SoS)	Basis of Issue (BOI) Guidance		
1.1.1.3.6.1	Quantities issued per using organization	Basis of Issue (BOI) Guidance		
1.1.1.3.7	Critical Operational Issues and Criteria (COICs)	Test and Evaluation Master Plan (TEMP)		
1.1.1.4	Potential Non-Materiel Solutions	ICD	These are changes in doctrine, organization, training, materiel, leadership and education, personne	
1.1.1.5	Materiel Approaches	ICD	Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that	

Challenges

- Extensive and complex view (The Excel file expands to over 400 line items)
- Difficulty discerning hierarchical relationship between data elements
- Very manual process to render diagrams and show relationships between elements.
- Cumbersome to track changes

DSM Data Taxonomy in The Brain Mind Mapping Tool

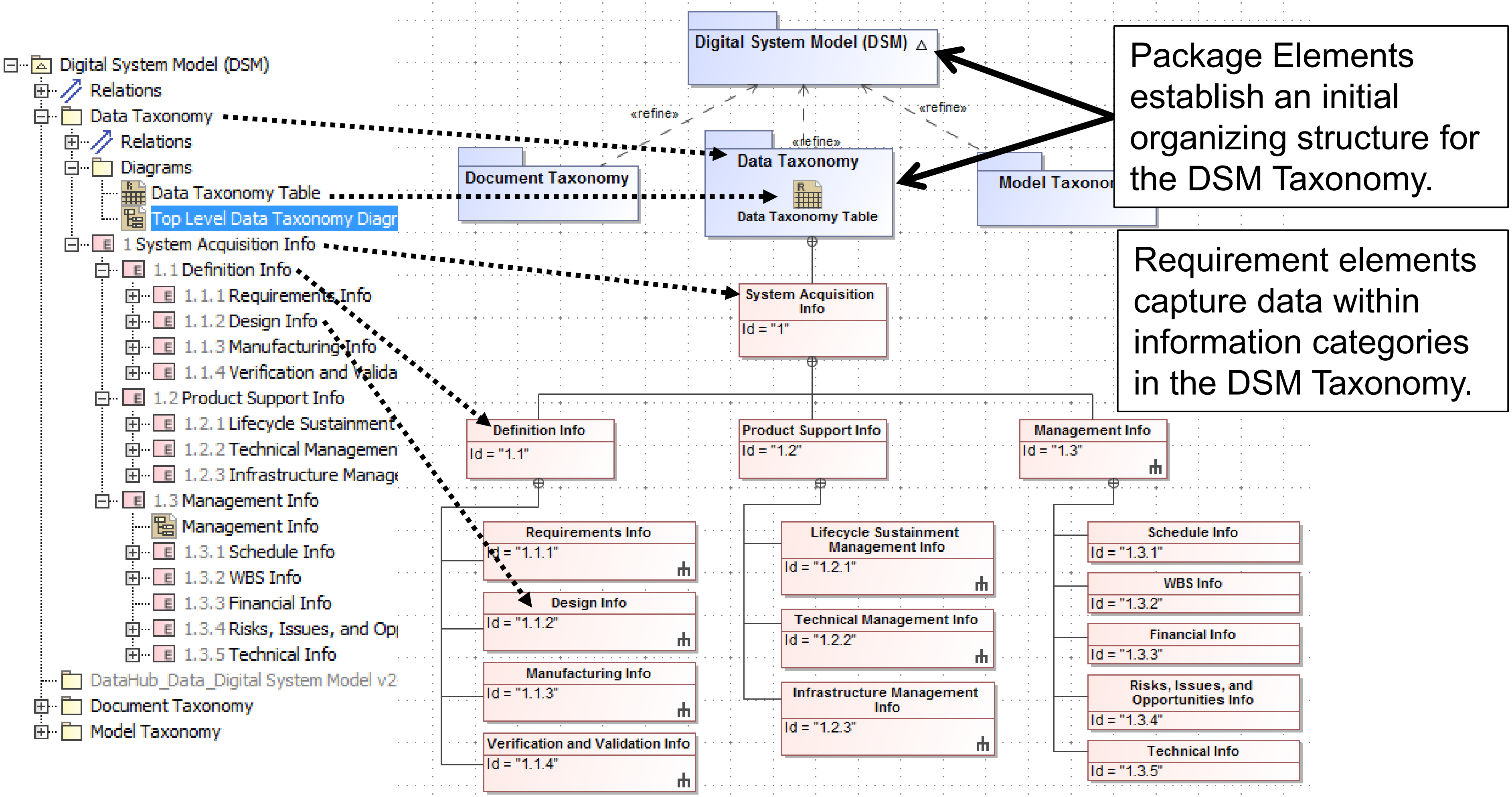


Challenges

- Not able to display the entire DSM Data Taxonomy structure
- Challenging to capture technical data points
- Not applicable to SysML modeling language

Modeling the DSM Data Taxonomy

- **The model is used to create a hierarchy diagram view.**



Modeling the DSM Data Taxonomy (cont.)

- **The model is used to create a table View.**

#	Id	Name	Source	Text
1	1	System Acquisition Info		This taxonomy represents current knowledge about data classes and data types captured in todays defense acquisition systems programs. This taxonomy was built as an organizing construct that could be used by programs as an aid to managing their data and defining viewpoints that would need to be auto generated from the Digital System Model.
2	1.1	Definition Info	ISO	A requirement is a statement that identifies a product or processes operational, functional, or design characteristic or constraint, which is unambiguous, testable, or measurable and necessary for product or process acceptability (ISO 2007).
3	1.1.1	Requirements Info	ISO	A requirement is a statement that identifies a product or processes operational, functional, or design characteristic or constraint, which is unambiguous, testable, or measurable and necessary for product or process acceptability (ISO 2007).
4	1.1.1.4	Customer/Stakeholder Ne	DI-IPSC-81431A/S	Set of stakeholder requirements are clarified and translated from statements of need into engineering-oriented language in order to enable proper architecture definition, design, and verification activities that are needed as the basis for system requirements analysis. Stakeholder needs and requirements represent the views of those at the business or enterprise operations level—that is, of users, acquirers, customers, and other stakeholders as they relate to the problem (or opportunity), as a set of requirements for a solution that can provide the services needed by the stakeholders in a defined environment. Using enterprise-level life cycle concepts (see Business or Mission Analysis for details) as guidance, stakeholders are led through a structured process to elicit stakeholder needs (in the form of a refined set of system-level life-cycle concepts). Stakeholder needs are transformed into a defined set of Stakeholder Requirements, which may be documented in the form of a model, a document containing textual requirement statements or both.
5	1.1.1.4.4	Capability	ICD	A capability is the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. (TRADOC Regulation 71-20)
6	1.1.1.4.4.4	Capability Gap	ICD	The inability to execute a specified course of action. The gap may be the result of no existing capability, lack of proficiency or sufficiency in an existing capability solution, or the need to replace an existing capability solution to prevent a future gap. See CJCSI 3170.01

Modeling the DSM Data Taxonomy (Data Field Descriptions)

- “#” is the number of the data element.
- “ID” indicates the hierarchical location of the data element in the Data Taxonomy.
- “Name” provides a unique name for each data element in the Data Taxonomy.
- “Source” provides one or more references that were used to derive the data element.
- “Text” provides a definition for each data element. Use this column to understand what data to captured for each of the associated data elements.

Benefits to Modeling the DSM Data Taxonomy

- **Manage Complexity**
  - Provides a method to use and navigate the DSM Data Taxonomy
  - Manages hierarchical data structure
- **Preserve and Enable Reuse of Heritage Knowledge**
  - Provides a method to capture, store, and use/reuse data
  - Offers accessible, shareable, and transparent data for current and future workforce
- **Outline Data Structure**
  - Provide an organized structure for the types of program data that should be considered across the life cycle

Path Forward

- **Content Validation of DSM Data Taxonomy**
  - Work with Services to review and provide comment on the DSM Data Taxonomy
  - Incorporate into INCOSE Digital Artifact Challenge
- **Finalize and deploy DSM Data Taxonomy for Usage after Reviews and Revisions**
- **Model Document and Model Taxonomies**
- **Manage Changes**

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695 | philomena.m.zimmerman.civ@mail.mil

Other Contributors:

Frank Salvatore

973-265-9837 | frank.j.salvatore.ctr@mail.mil

Tracee Walker Gilbert, Ph.D.

571-372-6145 | tracee.w.gilbert.ctr@mail.mil

Tyesia Pompey Alexander, Ph.D.

571-372-6697 | tyesia.p.alexander.ctr@mail.mil

Allen Wong

571-372-6788 | allen.wong4.ctr@mail.mil

Nick’s Bio

- Nick has been a Systems Engineer at Raytheon for 3 years, working in the Patriot BMC4I Requirements Team. Nick joined Raytheon after graduating from the University of Massachusetts Amherst with a Bachelor of Science in Electrical Engineering. He is currently pursuing a Master of Science in Industrial Engineering, with a certificate from the Gordon Institute of Engineering Leadership. As a part his capstone project, Nick has developed a series of MBSE work instructions and a proof of concept model of a notional Urban Traffic Control System.

Raytheon

Key MBSE Enablers with Examples

Nick Driscoll (Presenter)
Phil Levesque

Abstract: 19920

11/28/2017

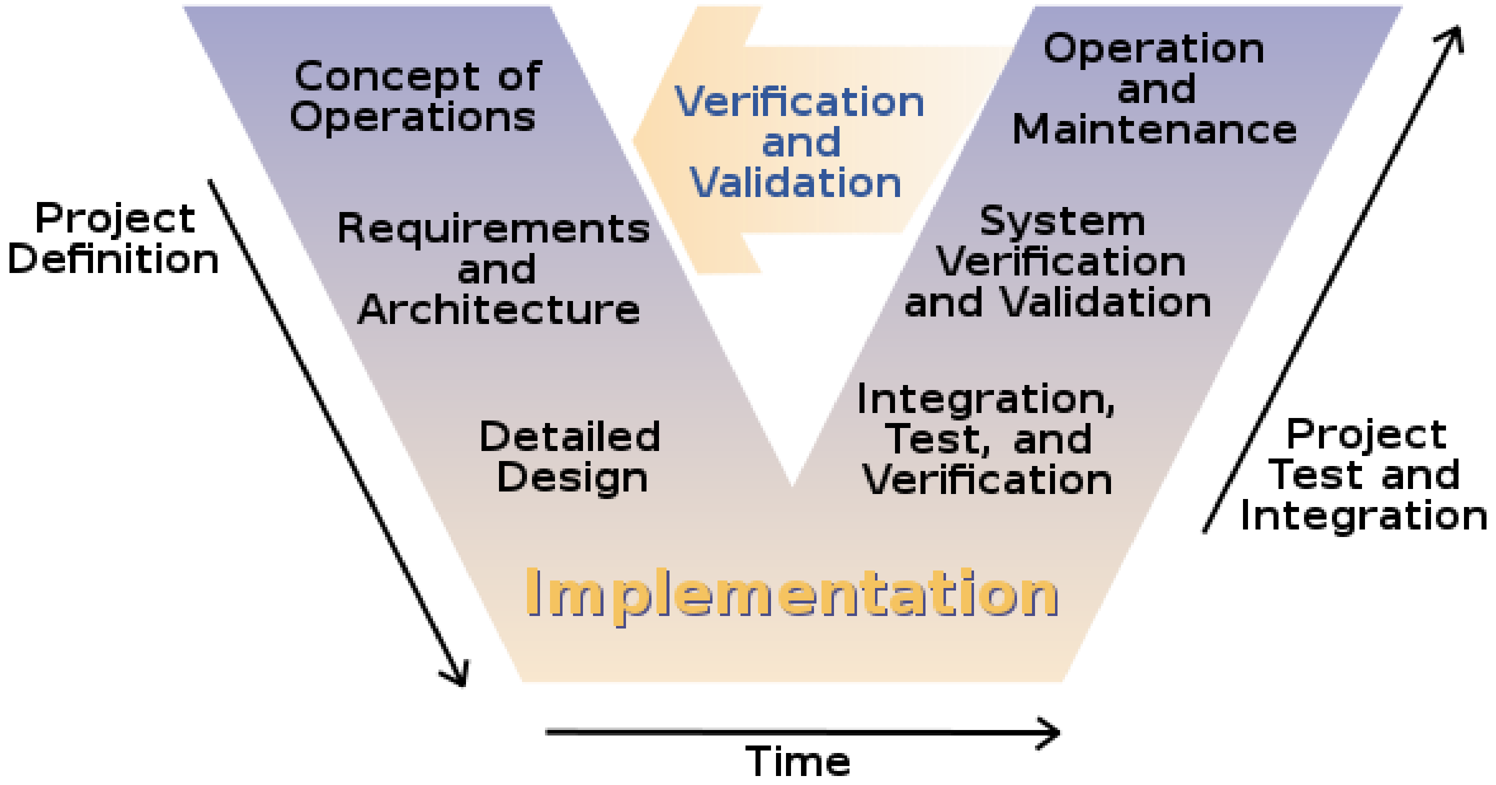
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Agenda

- Model Based Systems Engineering (MBSE) Description
- MBSE Environment and Enablers
- Example Model Using Enablers

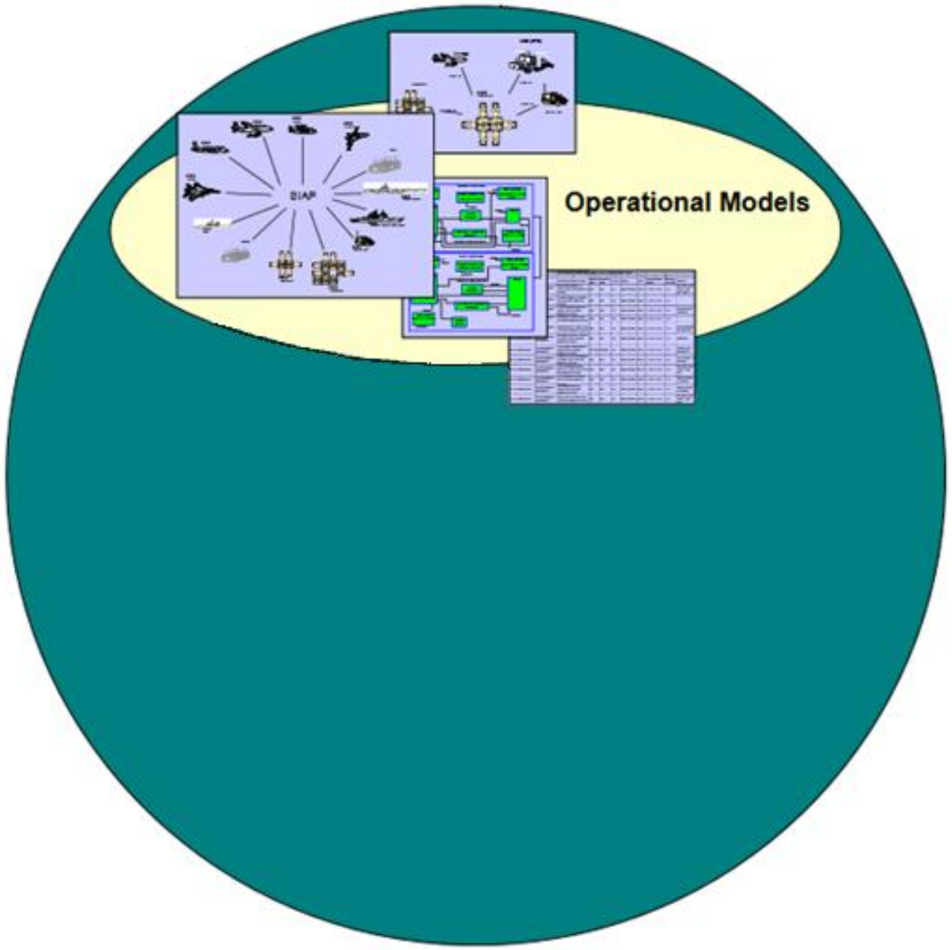
Systems Engineering

- Traditional requirements-based designs have Undesirable Effects over the product lifecycle:
  - Incorrect
  - Incomplete
  - Uninformed
  - Ambiguous
  - Infeasible
  - Unverifiable



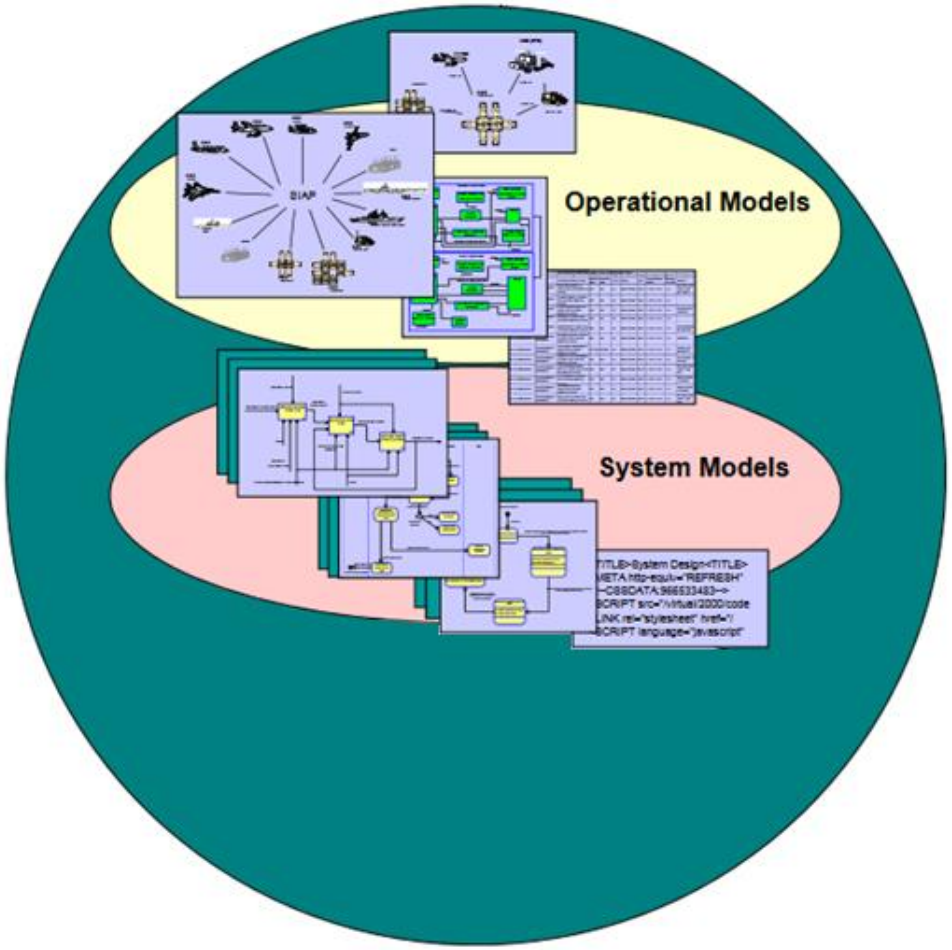
Model Based Systems Engineering

- Visual representations
  - System Composition
  - Interfaces
  - Behaviors
- Multiple levels of Decomposition
  - Operational – Concept of Operations, Operation and Maintenance
  - System – Requirements and Architecture, System Verification and Validation
  - Component – Detailed Design, Integration and Test
- MBSE can provide:
  - Integrated Environment
  - Design Validation
  - Document Generation
  - Generation of code



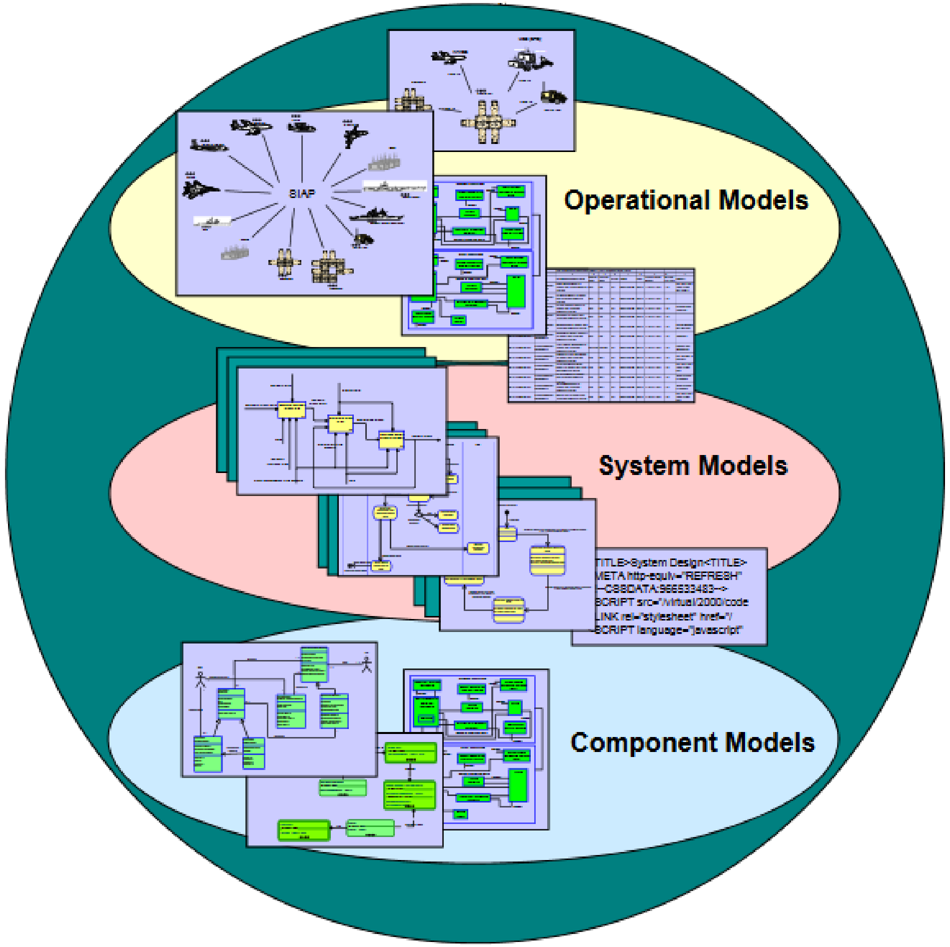
Model Based Systems Engineering

- Visual representations
  - System Composition
  - Interfaces
  - Behaviors
- Multiple levels of Decomposition
  - Operational – Concept of Operations, Operation and Maintenance
  - System – Requirements and Architecture, System Verification and Validation
  - Component – Detailed Design, Integration and Test
- MBSE can provide:
  - Integrated Environment
  - Design Validation
  - Document Generation
  - Generation of code



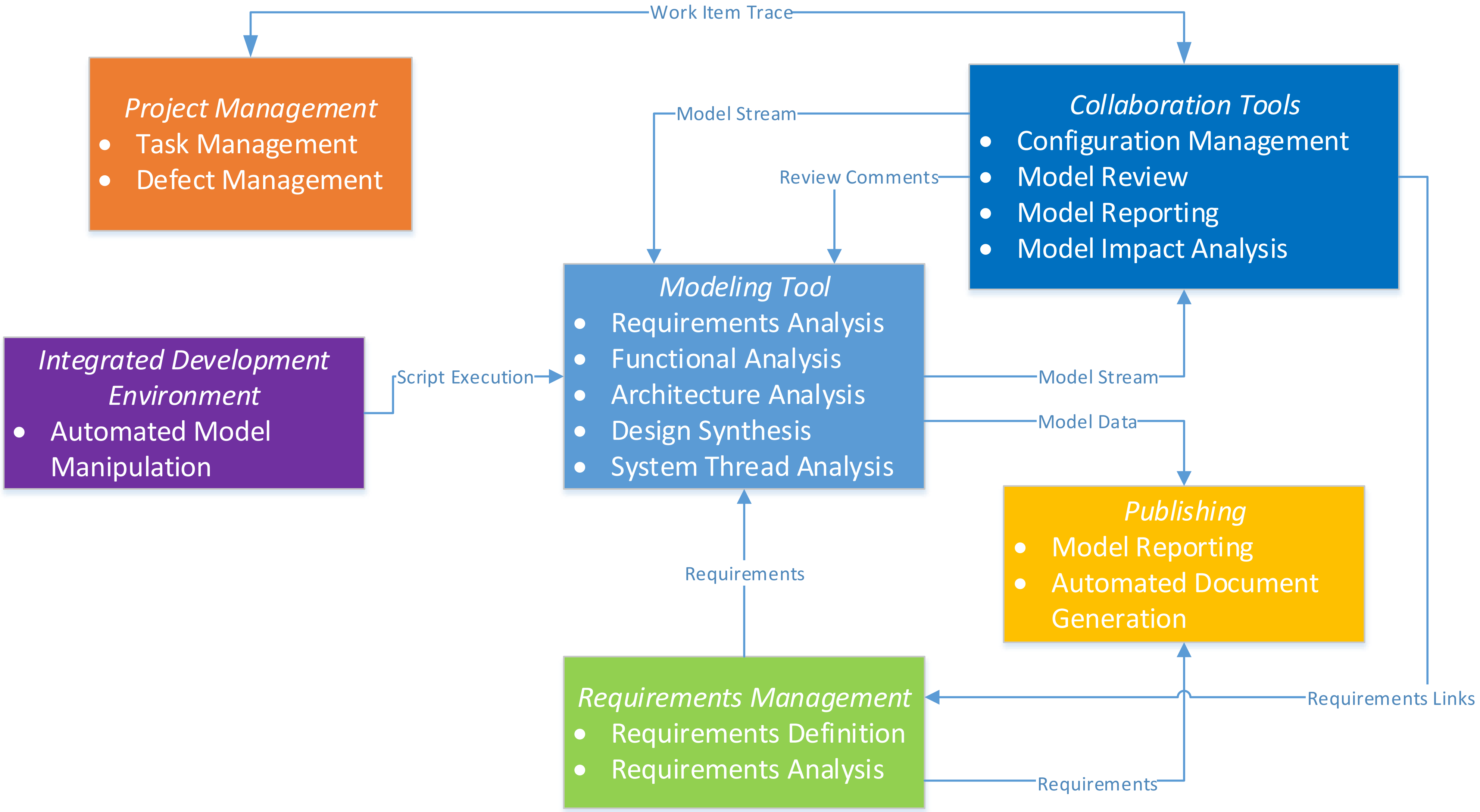
Model Based Systems Engineering

- Visual representations
  - System Composition
  - Interfaces
  - Behaviors
- Multiple levels of Decomposition
  - Operational – Concept of Operations, Operation and Maintenance
  - System – Requirements and Architecture, System Verification and Validation
  - Component – Detailed Design, Integration and Test
- MBSE can provide:
  - Integrated Environment
  - Design Validation
  - Document Generation
  - Generation of code



MBSE Environment

Raytheon



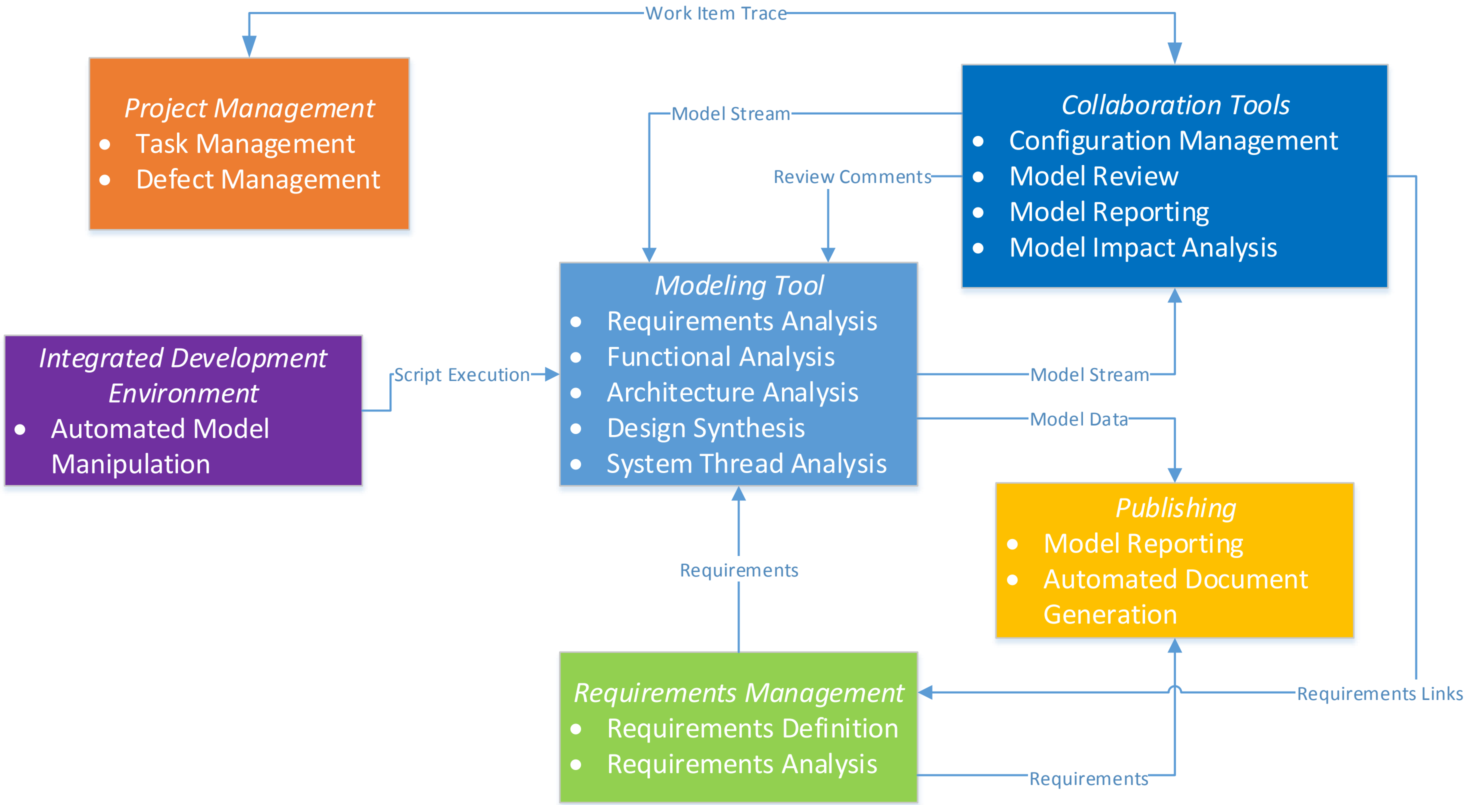
MBSE Impact on Design Methodology

Raytheon

- Design Efficiency
  - Consistent approach to MBSE
  - Stricter Analysis
- Enhanced Communication and Knowledge Transfer
  - Ease complexity management and understanding
  - Graphics and flowcharts are less convoluted than requirements specifications
- Improved Design Quality
  - In-phase defect detection
  - Defect reduction
  - Configuration Management

Enablers Supported by MBSE Environment

- **Modeling Enabler/Methodology**
- Integrated Design Reviews
  - Improved Quality
  - In-phase Correction
  - Knowledge Dissemination
  - Save Costs
  - Reduce Schedule
- Configuration Management
  - Consistency
  - Collaboration
- Team/Metric Tracking
  - Defect Tracking
  - Project Progress Reports



Enablers Supported by MBSE Environment

Raytheon

- Modeling Enabler/Methodology
- **Integrated Design Reviews**
  - Improved Quality
  - In-phase Correction
  - Knowledge Dissemination
  - Save Costs
  - Reduce Schedule
- Configuration Management
  - Consistency
  - Collaboration
- Team/Metric Tracking
  - Defect Tracking
  - Project Progress Reports

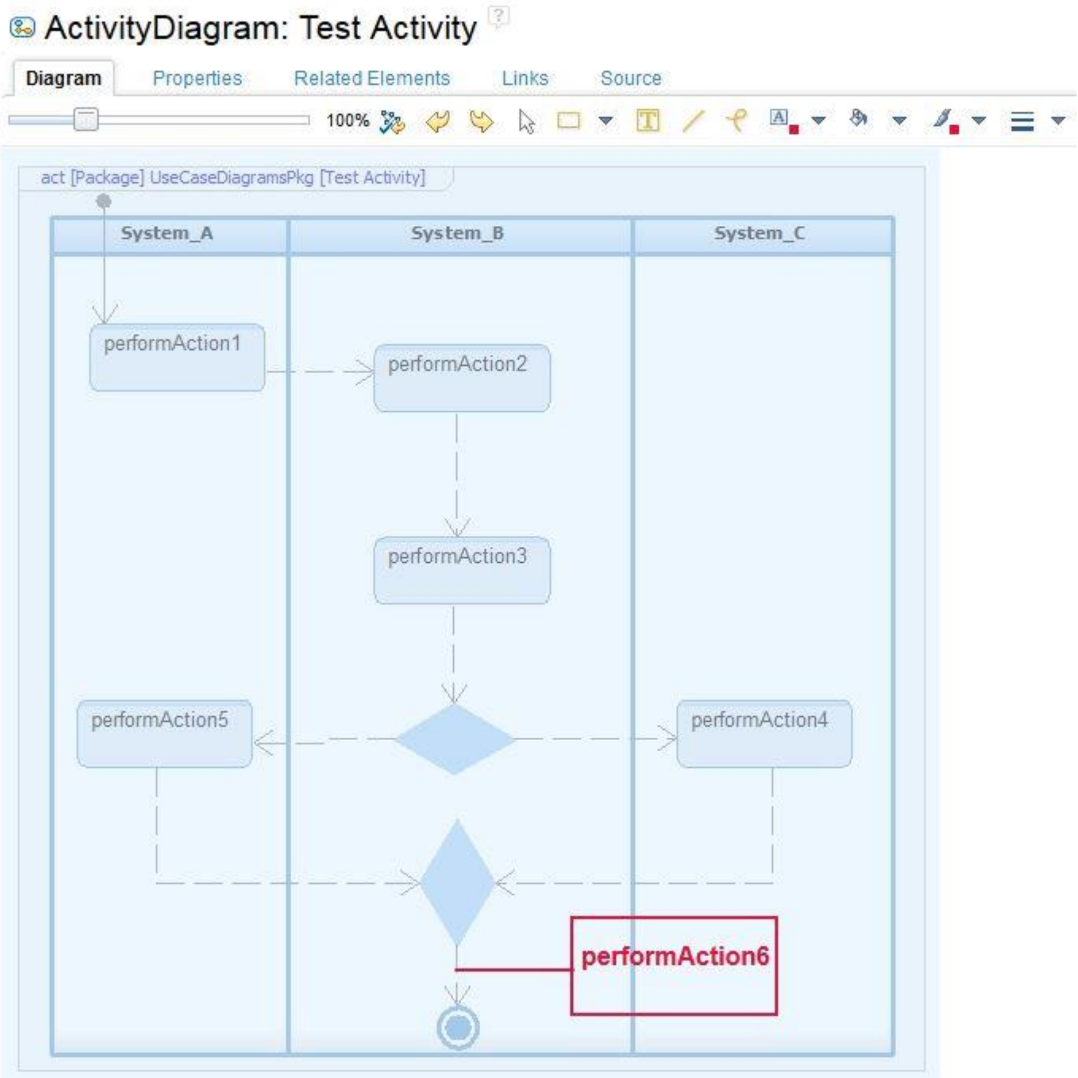


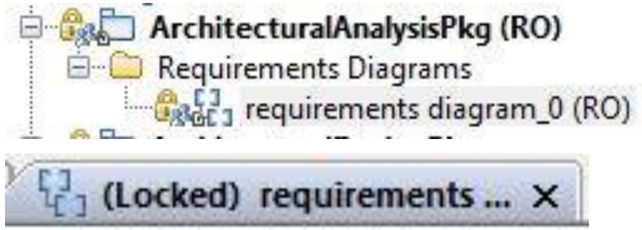
Image Extracted from Rational Design Manager

Enablers Supported by MBSE Environment

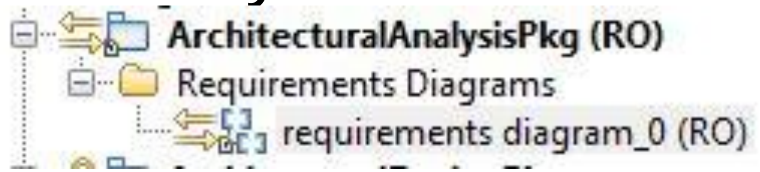
- Modeling Enabler/Methodology
- Integrated Design Reviews
  - Improved Quality
  - In-phase Correction
  - Knowledge Dissemination
  - Save Costs
  - Reduce Schedule
- **Configuration Management**
  - Consistency
  - Collaboration
- Team/Metric Tracking
  - Defect Tracking
  - Project Progress Reports

- Element-wise lockout:

- Collaborative Lockout Notifications:



- Out-of-Sync Notifications:



Images Extracted from Rhapsody using Rational Design Manger

Enablers Supported by MBSE Environment

- Modeling Enabler/Methodology
- Integrated Design Reviews
  - Improved Quality
  - In-phase Correction
  - Knowledge Dissemination
  - Save Costs
  - Reduce Schedule
- Configuration Management
  - Consistency
  - Collaboration
- **Team/Metric Tracking**
  - Defect Tracking
  - Project Progress Reports

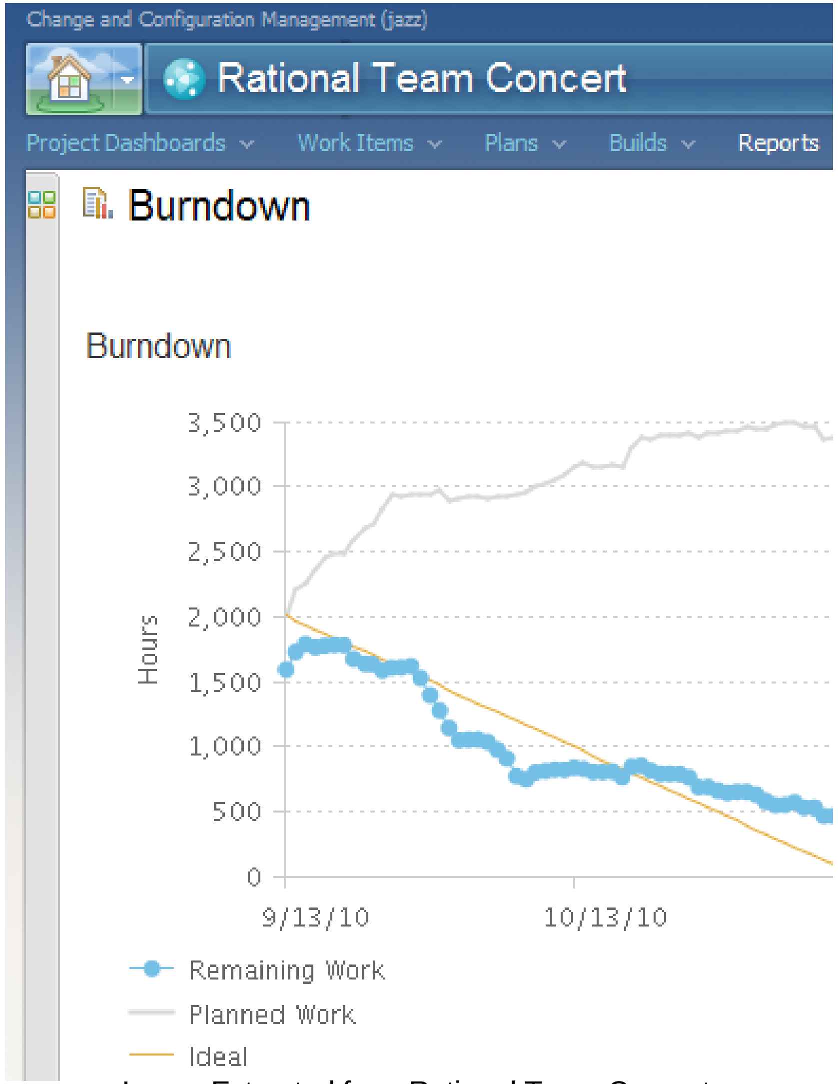


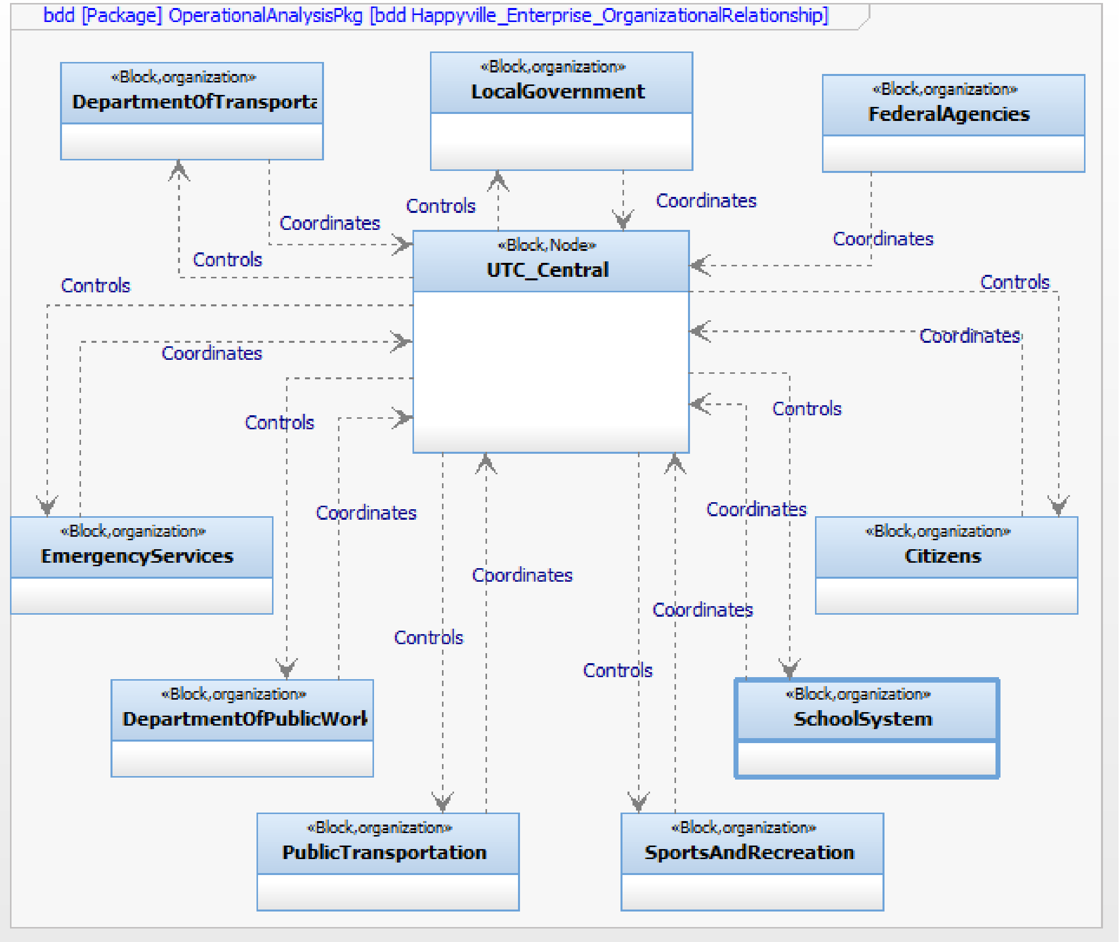
Image Extracted from Rational Team Concert

Example Model Using Enablers

- Rationale for Urban Traffic Control (UTC) System as an Example:
  - Notional example of a highly-variable complex system
  - Multiple levels of decomposition
  - Sharable across-company and externally without divulging customer or company information
- UTC System Customer Needs:
  - Maintain Traffic Flow
  - Public Transportation Priority
  - Timely Response to Incidents
  - Maintain Pedestrian Well-Being
  - Control Center Design Constraints
  - System Maintenance and Fault Detection
  - Interface Requirements

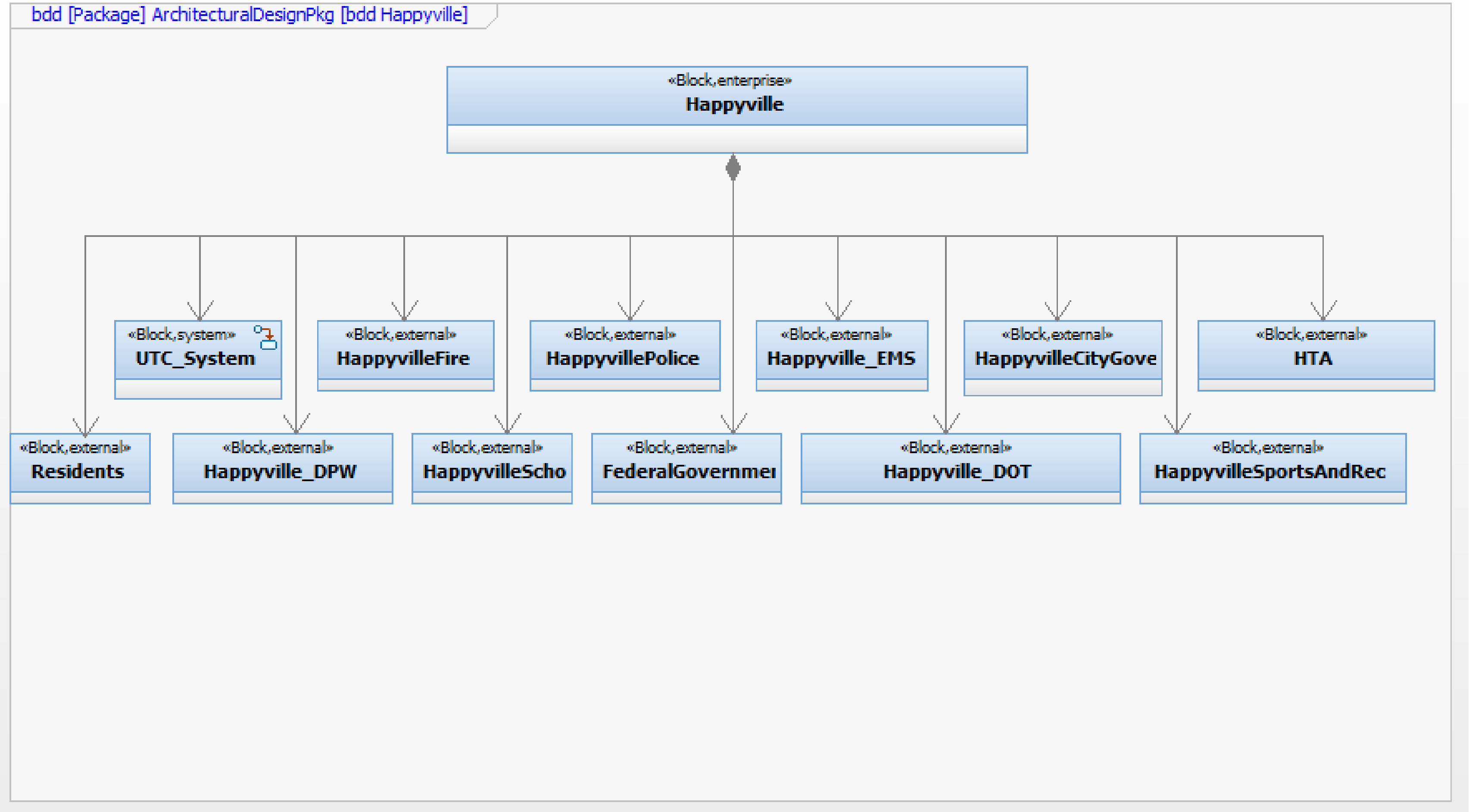
UTC System Operational Block Diagram

- Operational Block Definition Diagram: high level graphical overview of the operational concept
- Identifies the other organizations and systems in the system under design's operational environment
- Describes the relationships between the system under design and the identified organizations and systems



UTC System Block Definition Diagram

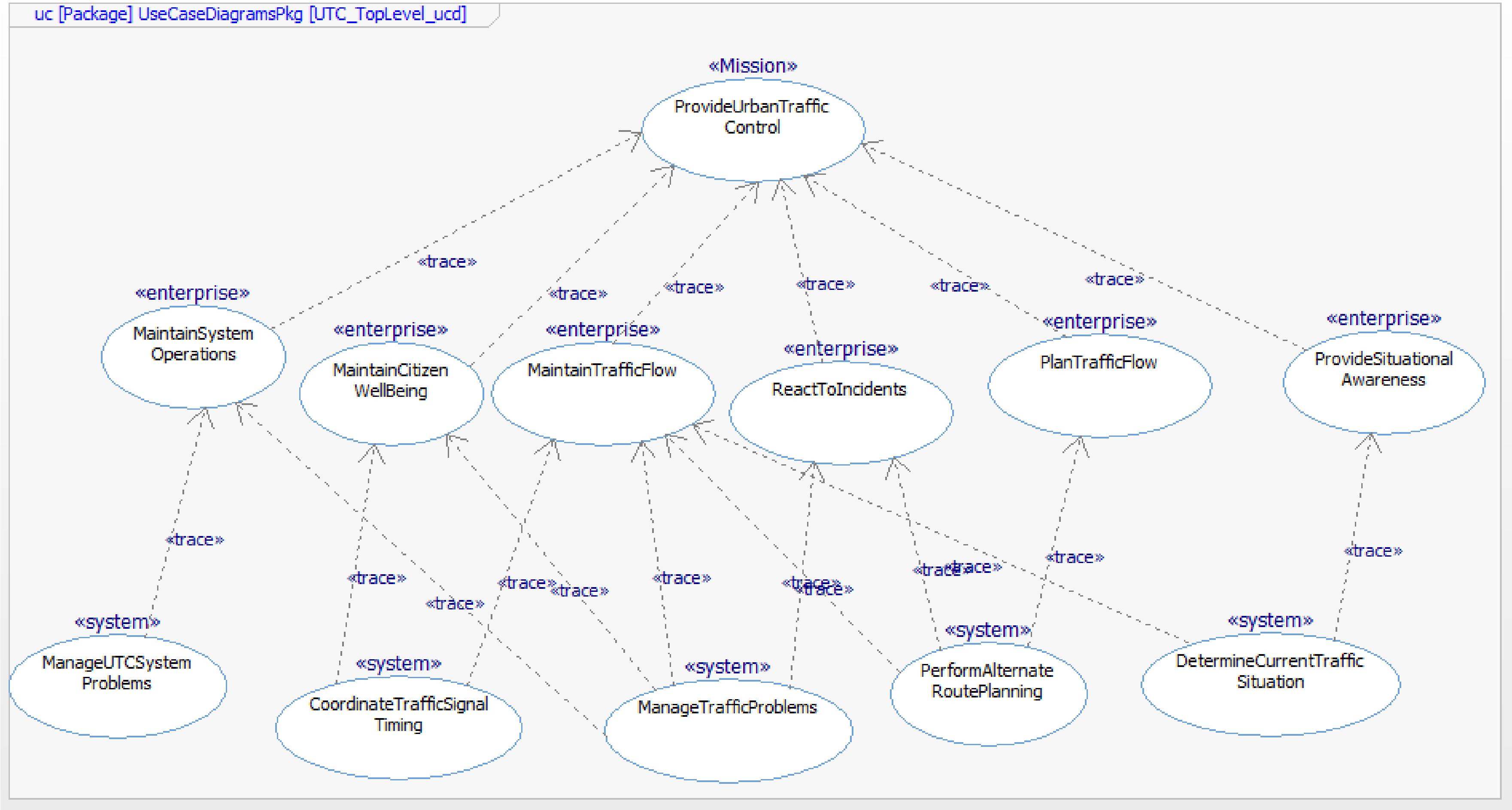
- Block Definition Diagram: A representation of the structure elements and their relationships.



UTC System Use Case Diagram

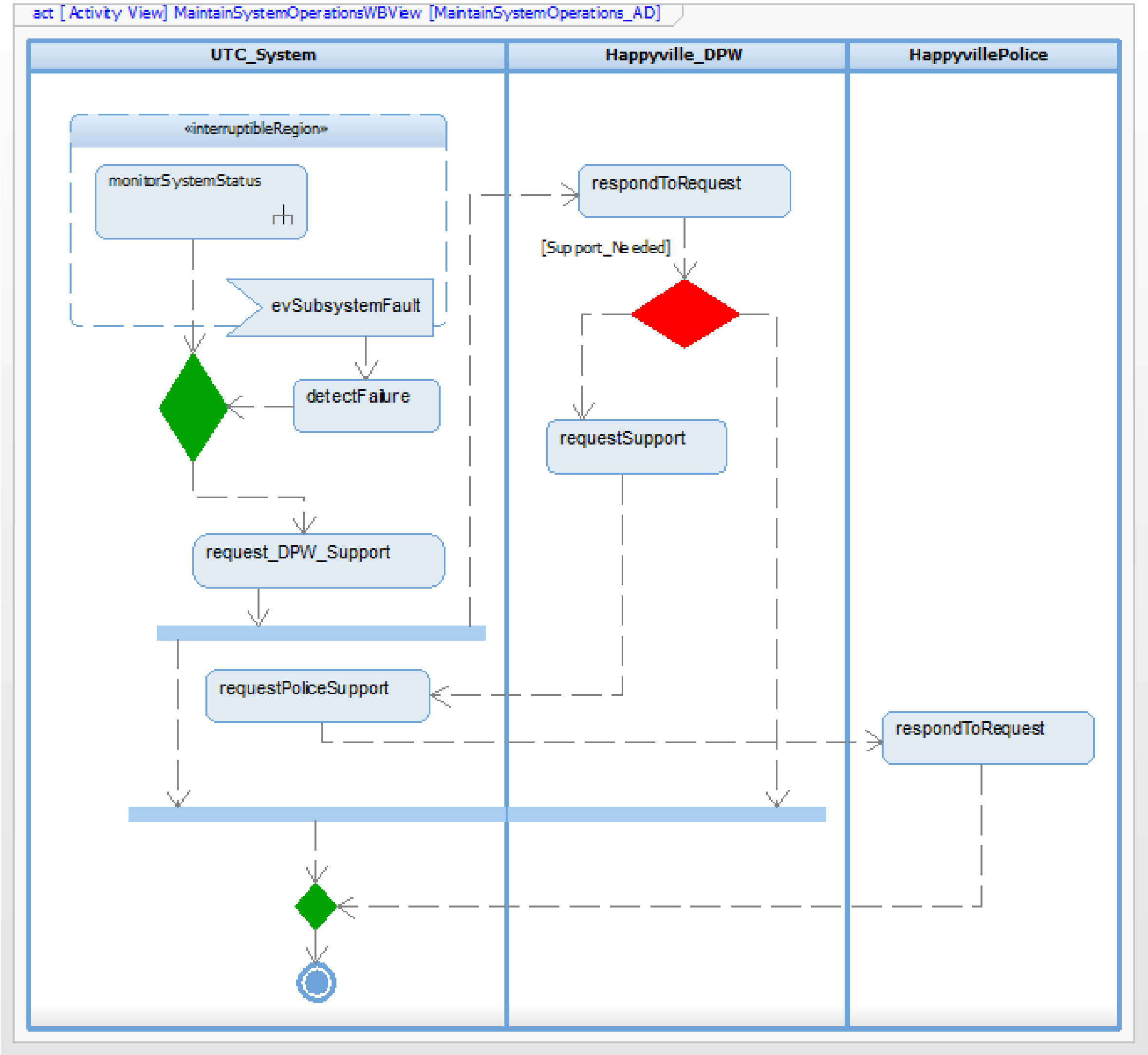
Raytheon

- Use Case Diagram: Define the main functions that the system must perform. Used to develop the operational threads.



UTC System Activity Diagram

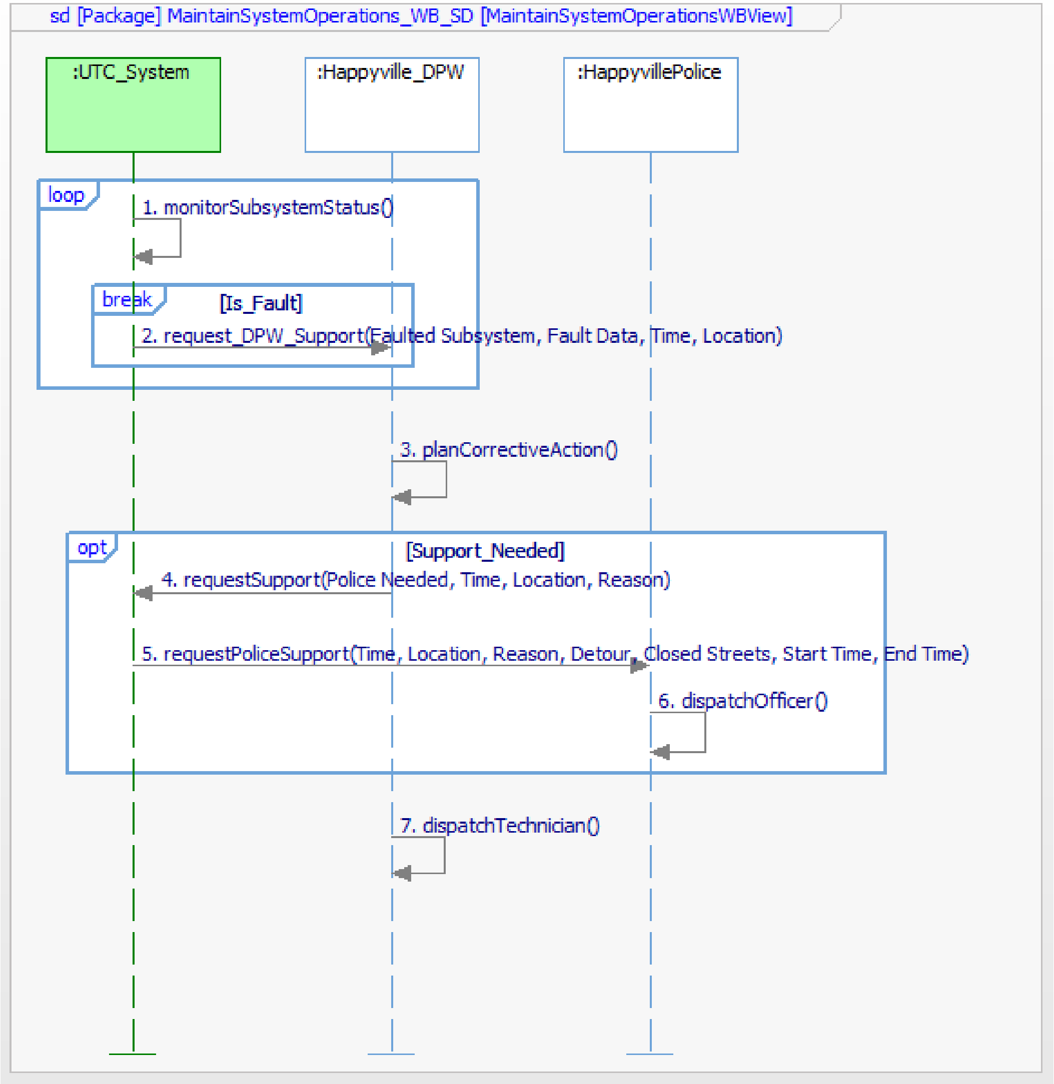
- Activity Diagram: Represents a specific system behavior or set of system behaviors. Similar to a flow chart, can depict the interactions between various external actors, or elements within the system
- Describes flow-based behavior



UTC System Sequence Diagram

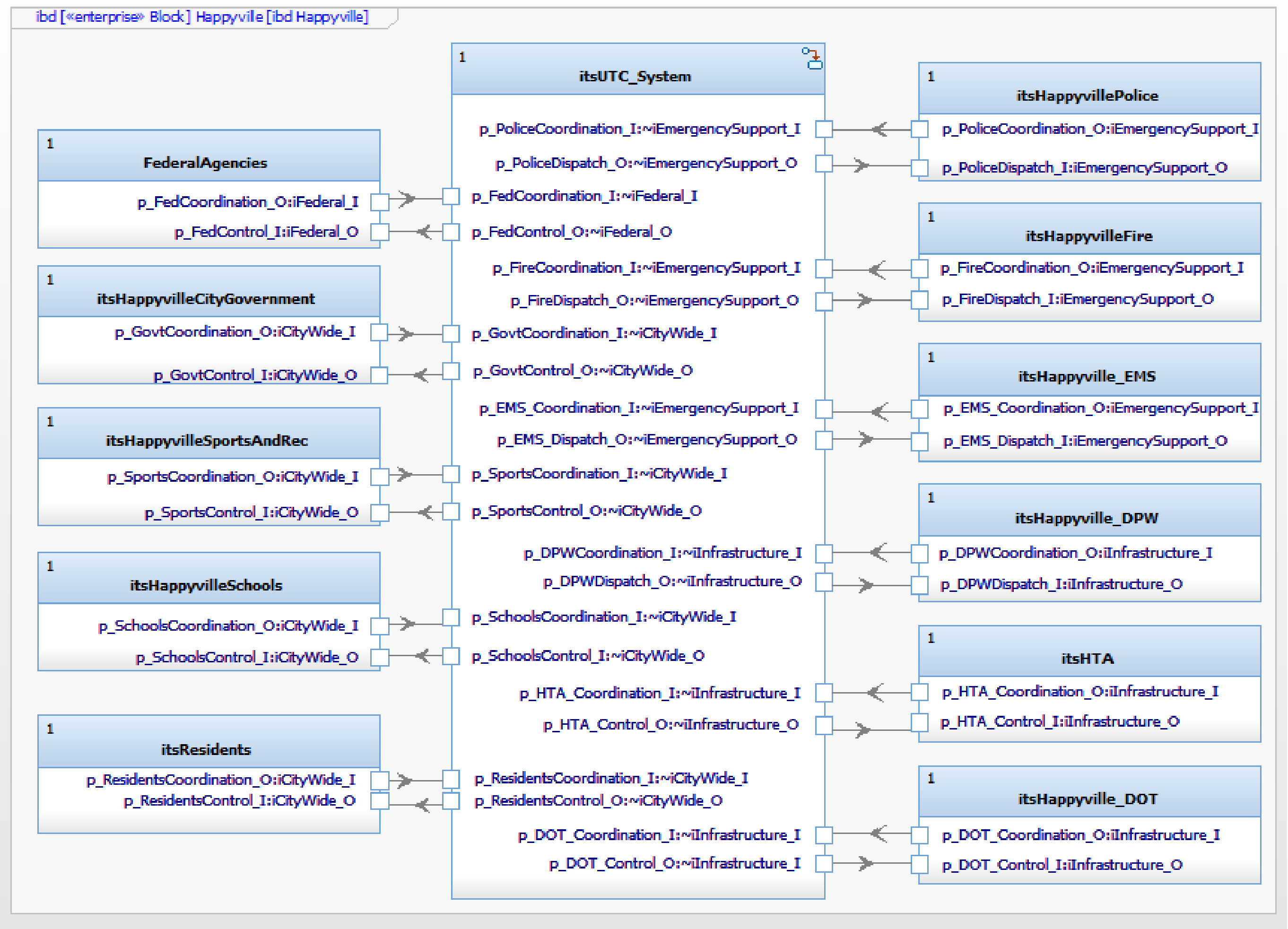
Raytheon

- Sequence Diagram: Represents message exchanges between systems, subsystems, or components.
- Describes message-based behavior



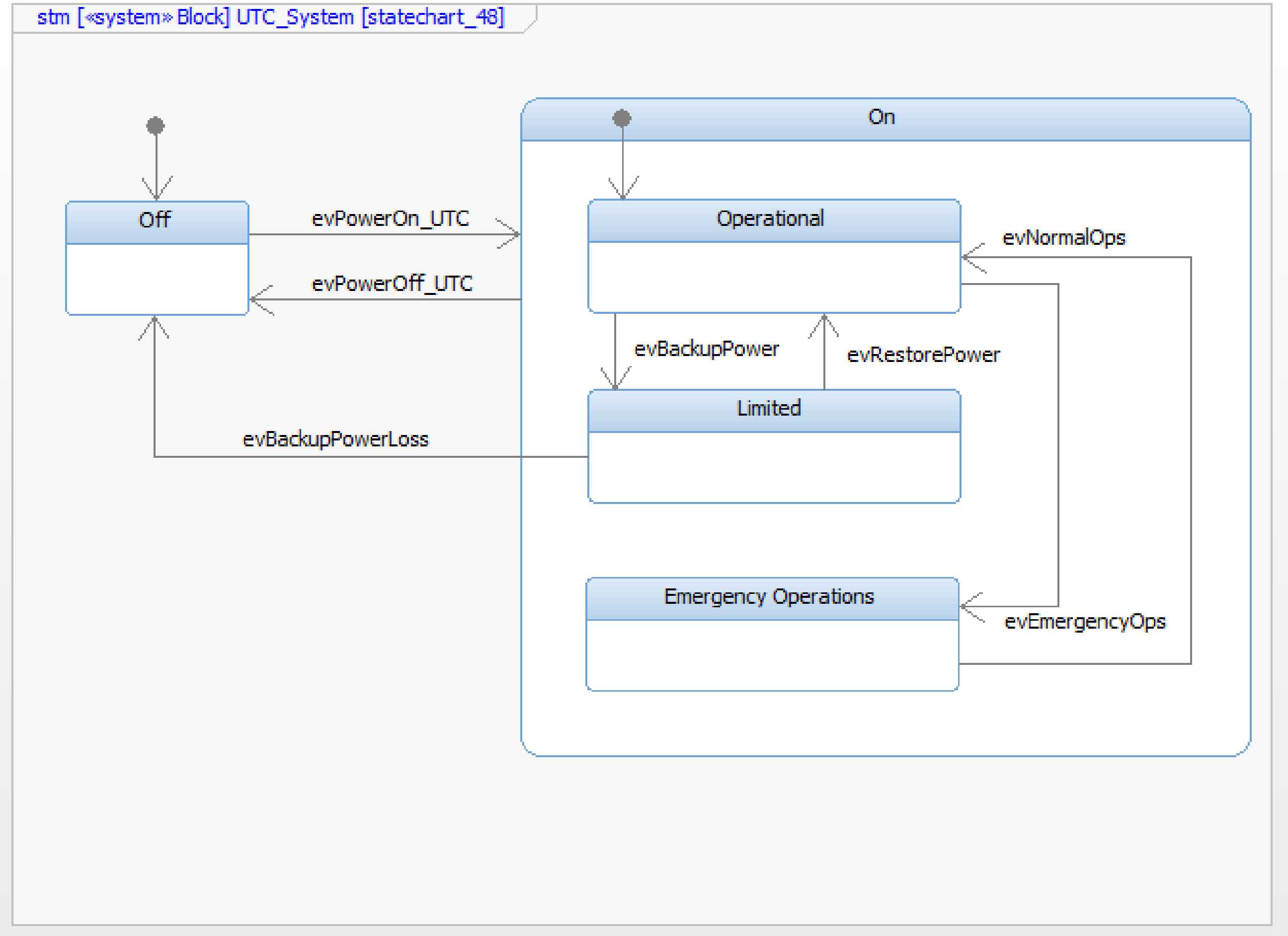
UTC System Internal Block Diagram

- Internal Block Diagram: Represents the interconnection and interfaces between the internal parts of a block (enterprise, system, or subsystem)



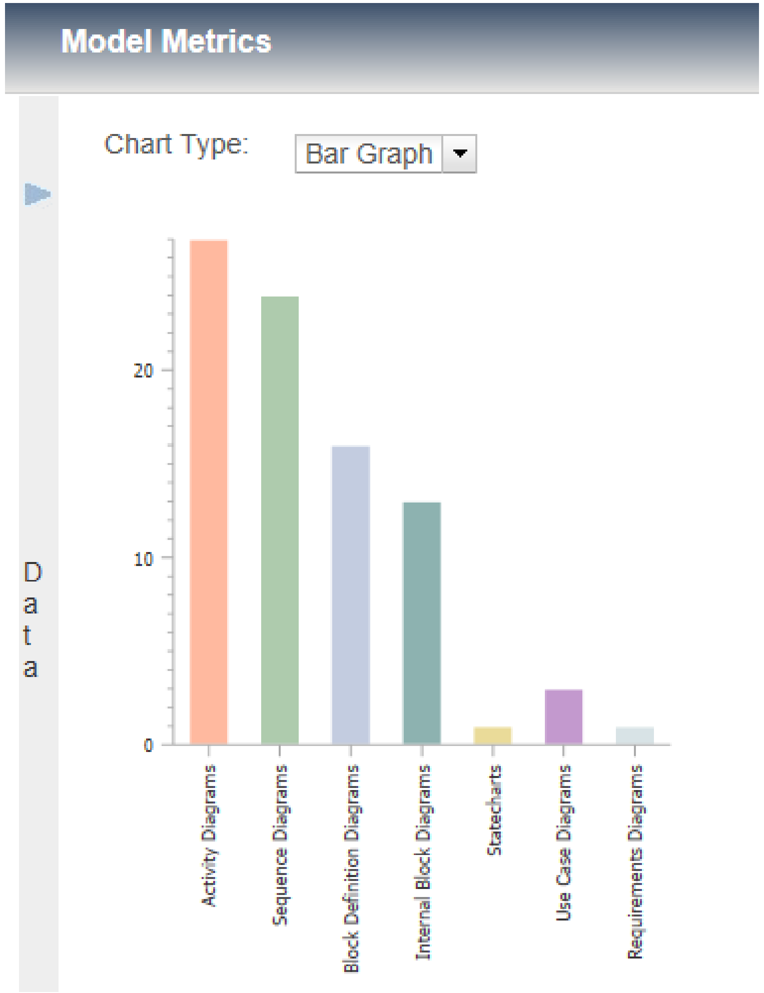
UTC System State Machine Diagram

- State Machine Diagram: Defines the states and modes of the system, and depicts the transitions from one state to another.
- Describes event-based behavior



UTC System Metrics

Metric Type	Count	Description
Diagrams/Views (Total)	85	Total number of diagrams in model
Activity Diagrams	27	Total number of activity diagrams
Sequence Diagrams	24	Total number of sequence diagrams
Block Definition Diagrams	16	Total number of block definition diagrams
Internal Block Diagrams	13	Total number of internal block diagrams
State Charts	1	Total number of state charts
Use Case Diagrams	3	Total number of use case diagrams
Requirements Diagrams	1	Total number of requirements diagrams
Structural Elements	51	Includes blocks for Enterprise, Systems, Subsystems, Nodes, Organizations
Interface Items	142	Includes send event actions, exchanged messages, interfaces, interface blocks
Functional Elements	46	Includes use cases (threads), activities and call behaviors
People Elements	20	Enterprise Actors
Time-Related Events	485	Includes transitions, events, flows, interaction occurrences, sequences, and states
Satisfied Requirements	29	Number of requirements traced to an element
Unsatisfied Requirements	27	Number of requirements not traced to an element
Percent of Requirements Linked	52%	Percentage of total requirements traced to a model element
Percent Under Configuration Control	100%	Model is configure controlled in RDM with the candidate as the only approver



UTC System Requirements Compliance

- Model Elements are linked to requirements within Rhapsody, and satisfaction tables can be output to help determine model completeness:

Requirement ID	Specification	Satisfying Element
UTC_46	The UTC System shall have an Operational State.	Operational
UTC_51	The UTC System shall avoid large fluctuations in traffic control behavior due to temporary traffic pattern changes.	changeSignal, detectCongestion, evDetectCongestion, commandSignalChange, detectCongestion, executeSignalChange
UTC_53	The UTC System shall provide a limited sub-set of capabilities when faced with a disaster scenario.	Limited, Emergency Operations
UTC_54	The UTC System shall be able to transition to Emergency Operations within 1 hour of a State of Emergency Declaration.	evEmergencyOps, Emergency Operations
UTC_56	The UTC system shall provide priority to public transportation without increasing traffic congestion.	commandSignalChange, executeSignalChange, changeSignal, detectBus, evDetectBus
UTC_58	The UTC system shall detect all traffic incidents within 1 minute of occurrence to include: • Multiple Vehicle Collisions • Single Vehicle Collisions with stationary objects (light posts, buildings, etc.) • Single Vehicle Collisions with pedestrians, bicyclists and/or animals • Debris in the roadway.	assessSensorData, senseEnvironment, detectIncident, determineIncidentType, evDetectIncident

Summary

- Facilitating transition to Model Based Systems Engineering
- Enhanced communication and knowledge transfer
- Reduced lifecycle cost through improved design quality
- MBSE and SysML to model complex systems
- Potential re-use

Questions?

Contact Information

Nicholas Driscoll

IDS HQ, Tewksbury, MA

Nicholas.J.Driscoll@Raytheon.com

Nick has been a Systems Engineer at Raytheon for 3 years, working in the Patriot BMC4I Requirements Team. Nick joined Raytheon after graduating from the University of Massachusetts Amherst with a Bachelor of Science in Electrical Engineering. He is currently pursuing a Master of Science in Industrial Engineering, with a certificate from the Gordon Institute of Engineering Leadership. As a part his capstone project, Nick has developed a series of MBSE work instructions and a proof of concept model of a notional Urban Traffic Control System.

Philip Levesque

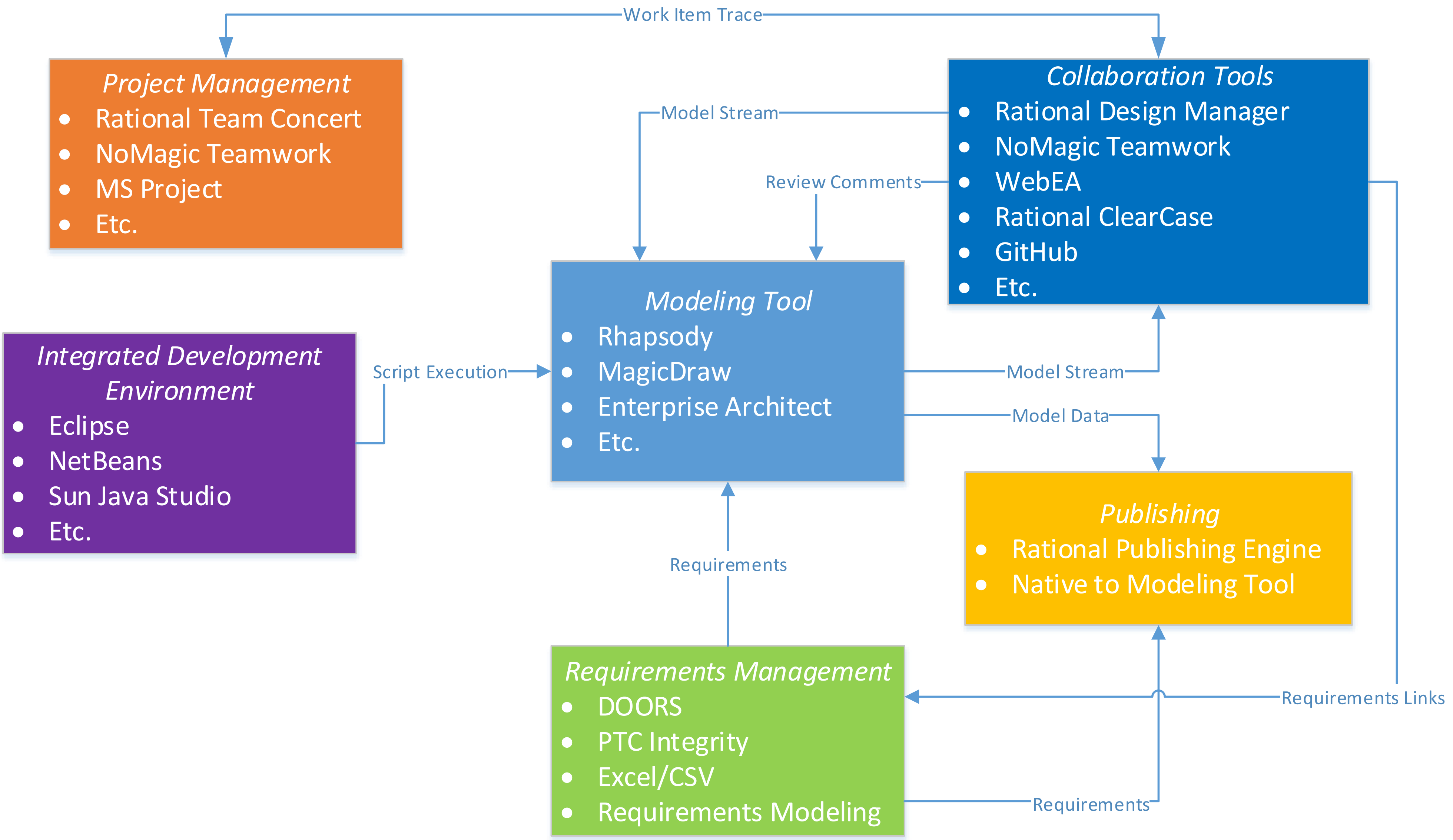
IDS HQ, Tewksbury, MA

Philip_R_Levesque@Raytheon.com

Phil Levesque is a Senior Principal Systems Engineer with Raytheon. Phil is a Raytheon Certified Architect and has worked in Systems Engineering for the past 14 years. Phil holds a MS in Computer Engineering degree from the University of Massachusetts at Lowell and BS in Electrical Engineering degree with a double major in Electrical Engineering & Computer Science from the University of Massachusetts at Lowell.

Backup

MBSE Environment Tooling



INTERFACE MANAGEMENT WITH MBSE – FROM THEORY TO MODELING

Matthew Hause
Engineering Fellow, MBSE Specialist
October, 2017

ptc

AGENDA

1. Introduction
2. Interfaces
3. System of System Interfaces
4. System Interfaces
5. Through the development lifecycle
6. Conclusion

INTRODUCTION

- Interoperability is a key facet of a successful system, and essential to a system of systems.
- Interoperability is a property of a system, whose interfaces are completely understood, to work with other products or systems without any restricted access or implementation.
- Software interoperability is the capability of different programs to exchange data via a common set of exchange formats, (read/write) file formats using same protocols.
- DOD: The condition achieved among communications-electronics systems when information or services can be exchanged directly and satisfactorily.
- So, interoperability begins with interfaces: mechanical, electronic, hardware, software, people-ware, etc.

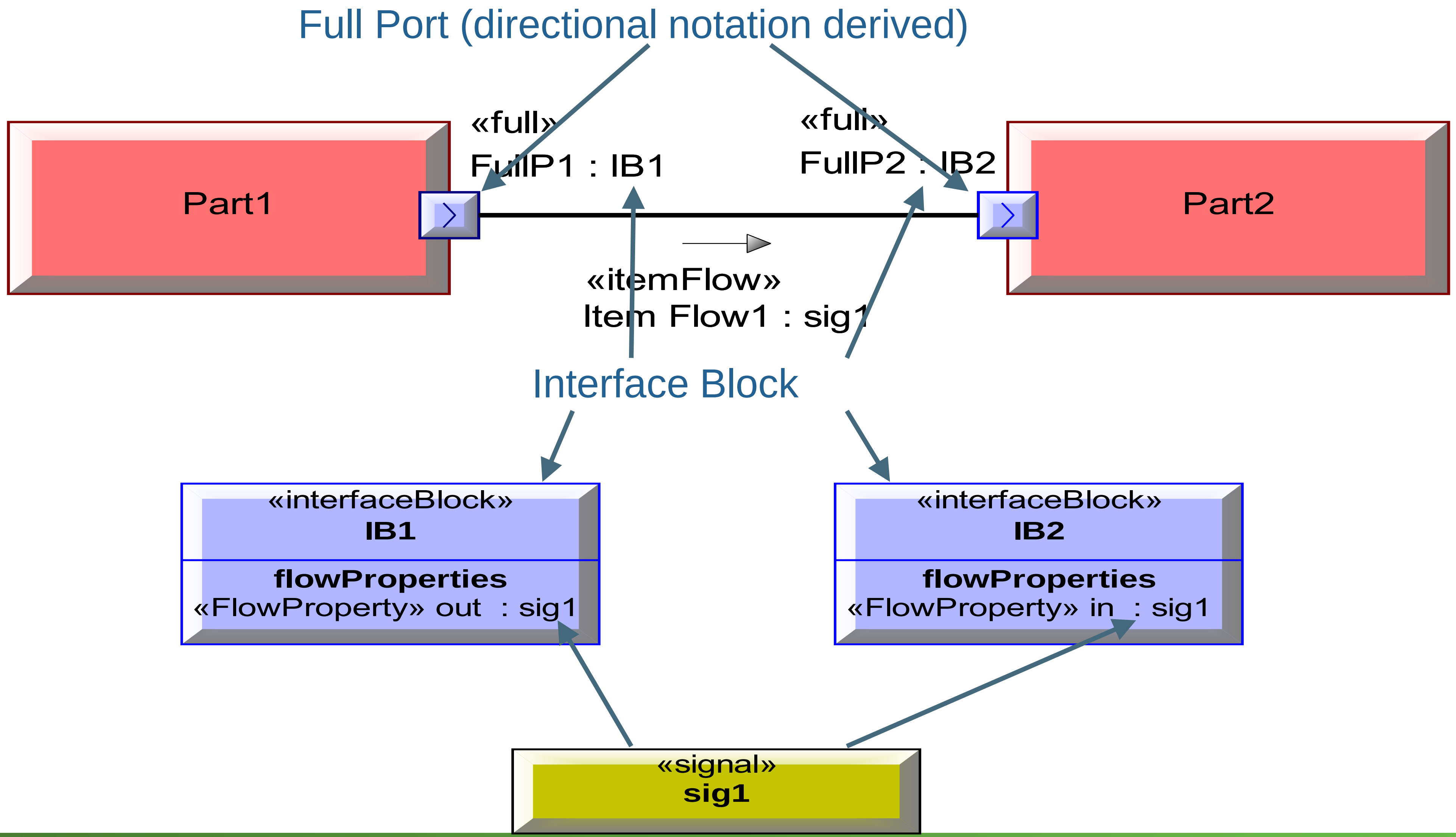
DESIGNING INTERFACES

- Starts with requirements and stakeholder needs

- System-to-System interfaces
  - Define the required behavior/functionality
  - Identify the Dependencies - interaction with other systems and within the subsystems
  - Identify the necessary interactions
    - Data, physical, logical, electrical, etc.
  - Define logical interface requirements
  - Define interaction performance characteristics
  - Allocate to physical interfaces

- Human Interfaces
  - Identify the characteristics of the (Human) users that will interact with the system.
  - Define the required tasks to be performed
  - Identify the Primary User Interface Elements
  - Define the Navigation Map

FULL PORT NOTATION

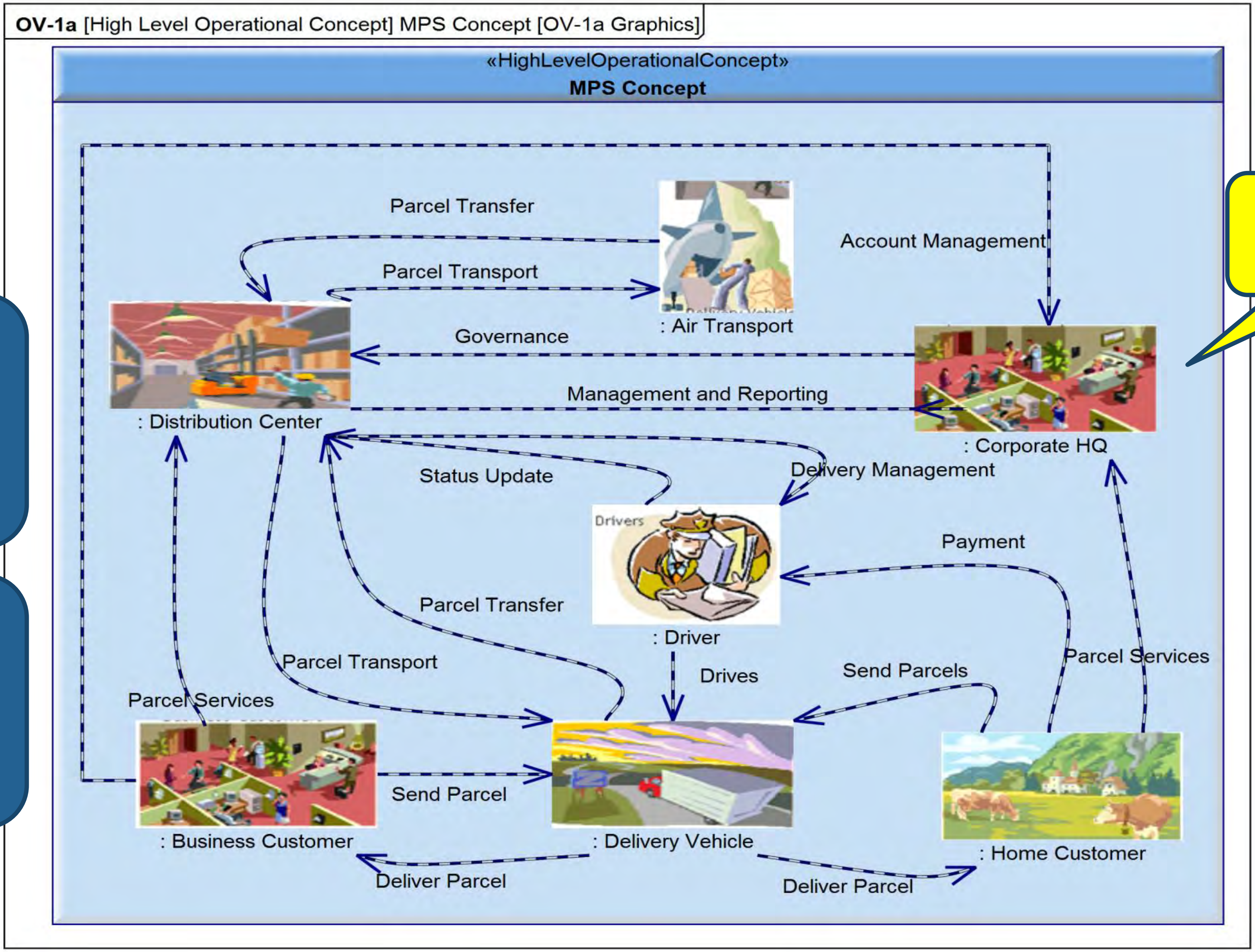


SYSTEMS OF SYSTEMS INTERFACES

OPERATIONAL CONCEPT GRAPHIC

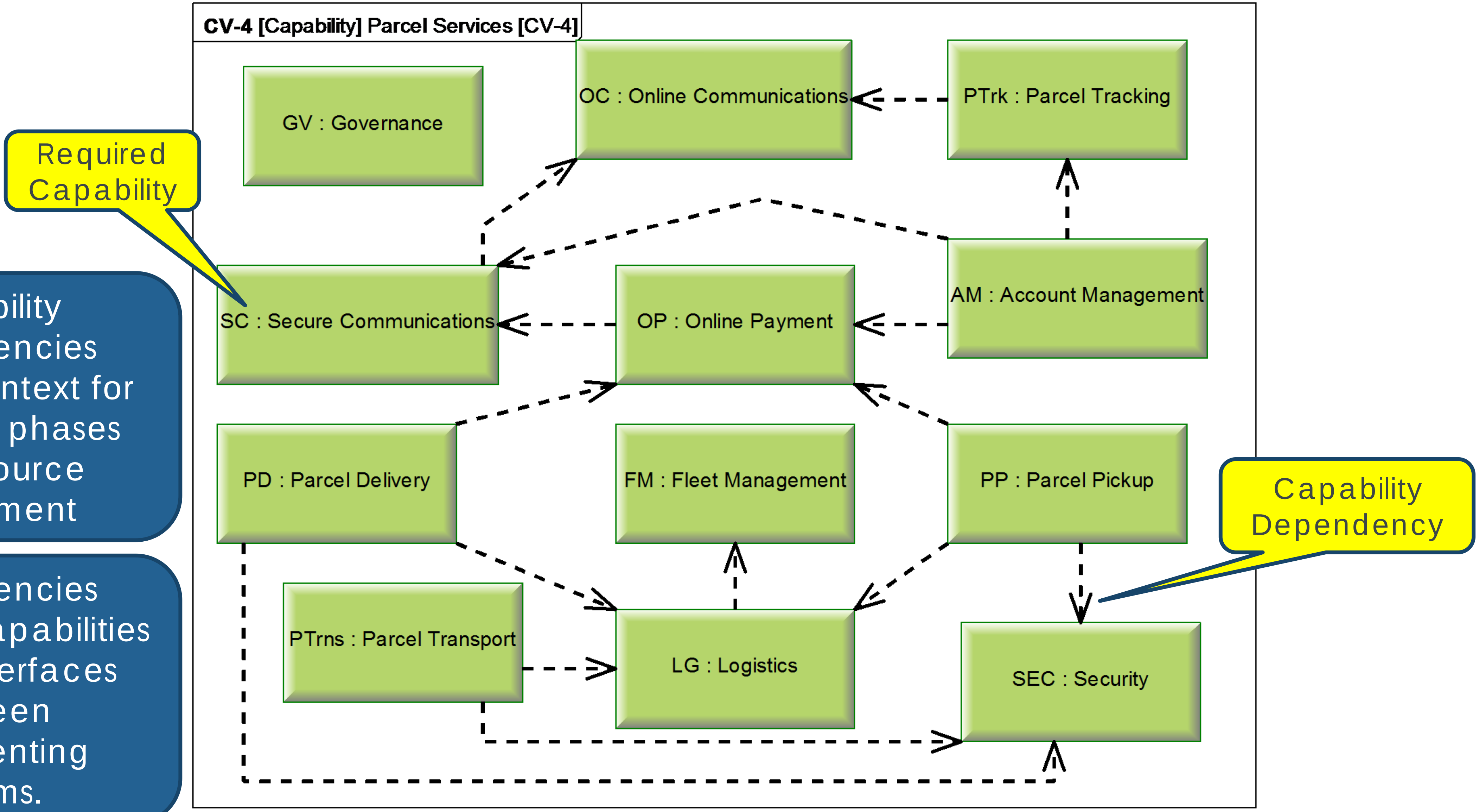
Provides a means to communicate with non-technical stakeholders while maintaining model consistency

Defines nominal interfaces between conceptual entities in the context.



Replaced boxes with graphics

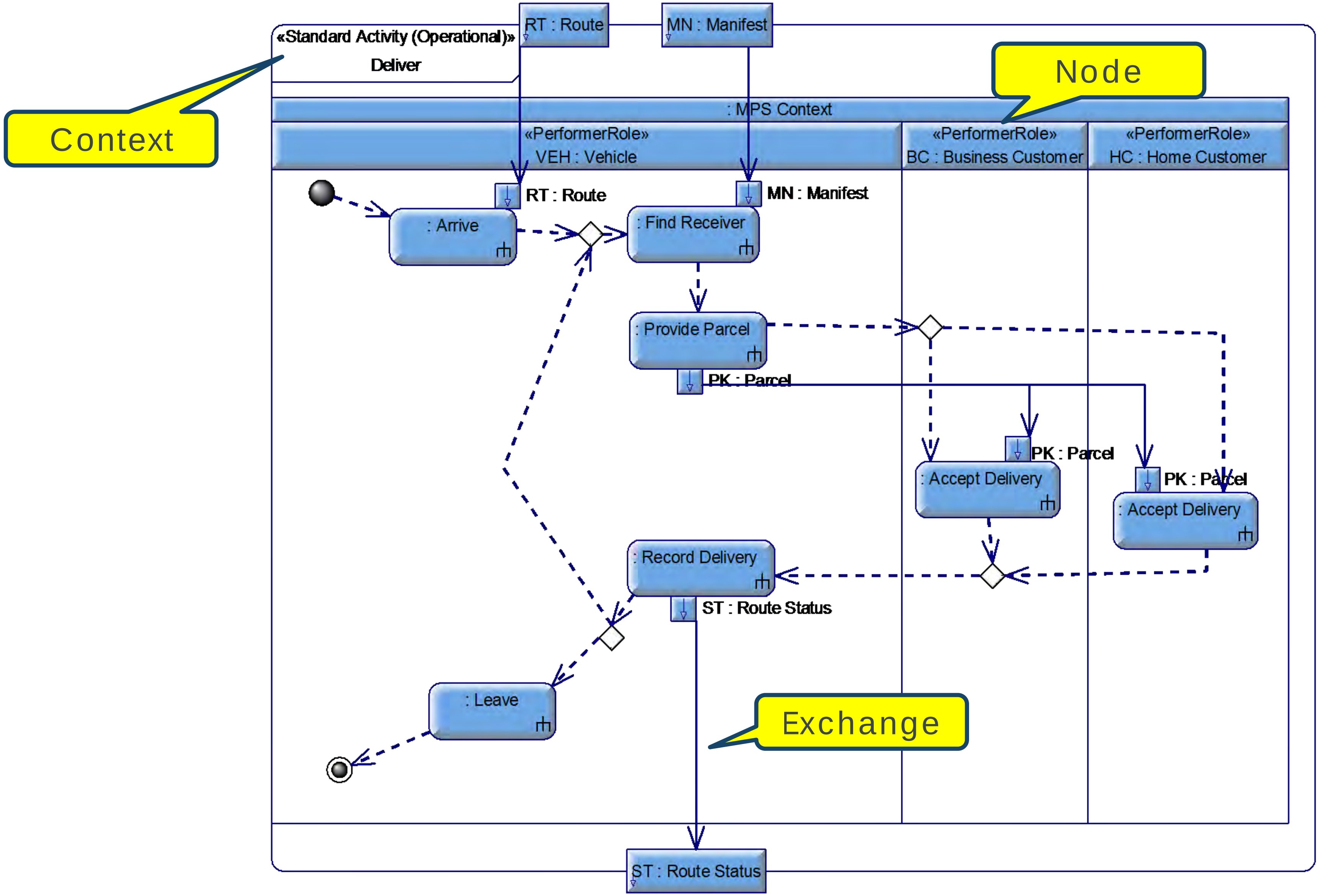
CAPABILITY DEPENDENCIES



Capability dependencies provide context for capability phases and resource deployment

Dependencies between capabilities implies interfaces between implementing systems.

LOGICAL ARCHITECTURE INTERACTIONS



Interactions crossing swimlanes defines system interface characteristics

LOGICAL ARCHITECTURE ICD (FRAGMENT)

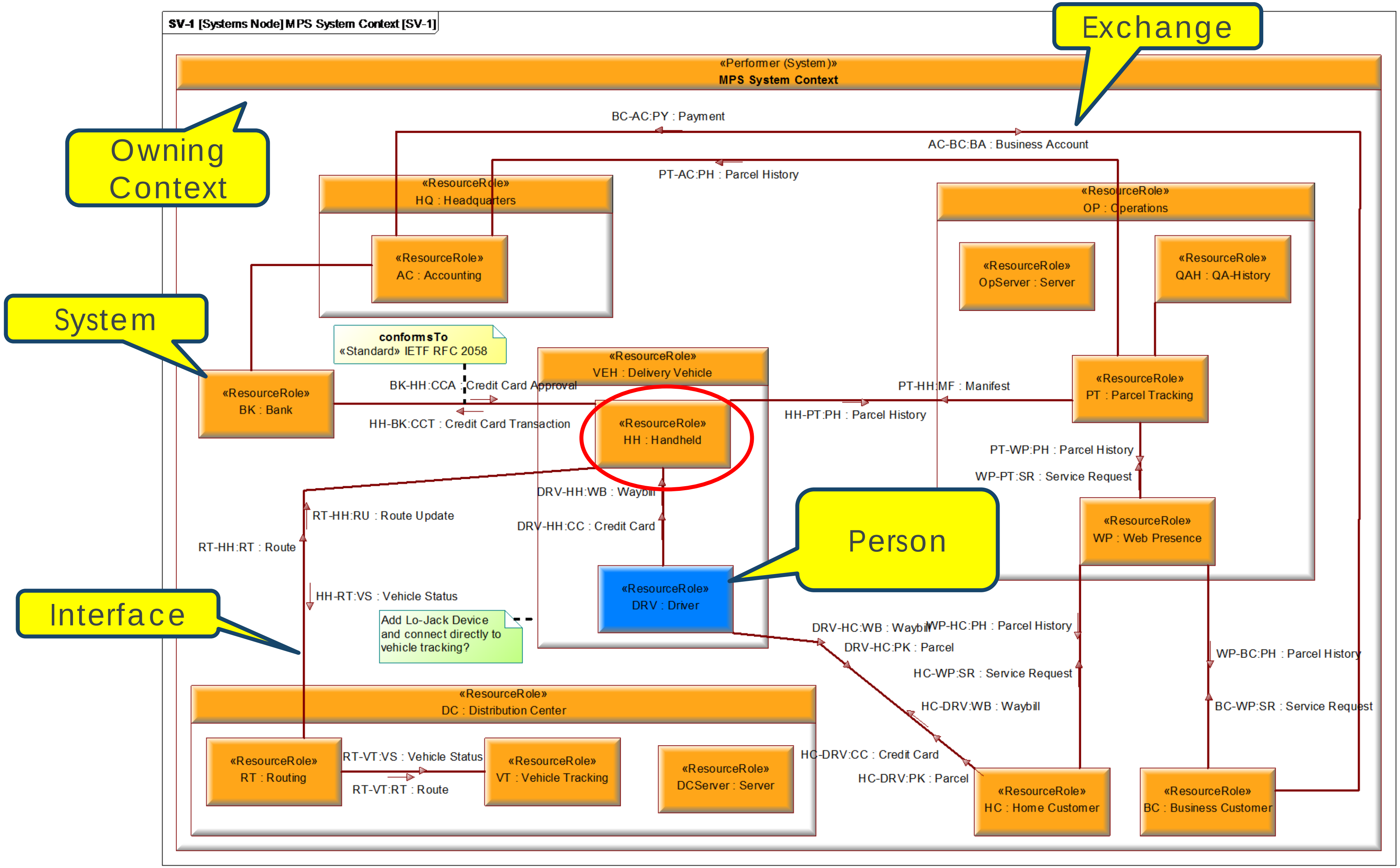
ptc

[Architectural Description] Structure [OV-3 Info Exchange]

Operational		Producer		Needline	Consumer	
Name	Conveyed	Performer (Operational)	Activity (Operational)	Name	Performer (Operational)	Activity (Operational)
CHQ-BC:BL	«Exchange Element» Bill	«Performer (Operational)» Corporate HQ		BC - CHQ	«Performer (Operational)» Business Customer	
BC-VEH:PK	«System» Parcel	«Performer (Operational)» Business Customer	«Activity (Operational)» Provide Waybill	BC - VEH	«Performer (Operational)» Vehicle	«Activity (Operational)» Verify Waybill and Payment
BC-VEH:PW	«Exchange Element» Parcel Waybill	«Performer (Operational)» Business Customer	«Activity (Operational)» Provide Waybill	BC - VEH	«Performer (Operational)» Vehicle	«Activity (Operational)» Verify Waybill and Payment
VEH-BC:PK	«System» Parcel	«Performer (Operational)» Vehicle	«Activity (Operational)» Provide Parcel	BC - VEH	«Performer (Operational)» Business Customer	«Activity (Operational)» Accept Delivery
SF-DC:PK	«System» Parcel	«Performer (Operational)» Storefront		SF - DC	«Performer (Operational)» Distribution Center	
DC-VEH:MN	«Exchange Element» Manifest	«Performer (Operational)» Distribution Center	«Activity (Operational)» Find and Record Outgoing Parcels	VEH - DC	«Performer (Operational)» Vehicle	«Activity (Operational)» Load Vehicle «Activity (Operational)» Find Receiver «Activity (Operational)» Find Sender
DC-VEH:PK	«System» Parcel	«Performer (Operational)» Distribution Center	«Activity (Operational)» Find and Record Outgoing Parcels	VEH - DC	«Performer (Operational)» Vehicle	«Activity (Operational)» Load Vehicle
DC-VEH:PW	«Exchange Element» Parcel Waybill	«Performer (Operational)» Distribution Center	«Activity (Operational)» Find and Record Outgoing Parcels	VEH - DC	«Performer (Operational)» Vehicle	«Activity (Operational)» Load Vehicle
DC-VEH:RT	«Exchange Element» Route	«Performer (Operational)» Distribution Center		VEH - DC	«Performer (Operational)» Vehicle	«Activity (Operational)» Arrive
VEH-DC:MN	«Exchange Element» Manifest	«Performer (Operational)» Vehicle	«Activity (Operational)» Unload Vehicle	VEH - DC	«Performer (Operational)» Distribution Center	«Activity (Operational)» Record and Store Incoming Parcels
VEH-DC:PK	«System» Parcel	«Performer (Operational)» Vehicle	«Activity (Operational)» Unload Vehicle	VEH - DC	«Performer (Operational)» Distribution Center	«Activity (Operational)» Record and Store Incoming Parcels
VEH-DC:PW	«Exchange Element» Parcel Waybill	«Performer (Operational)» Vehicle	«Activity (Operational)» Unload Vehicle	VEH - DC	«Performer (Operational)» Distribution Center	«Activity (Operational)» Record and Store Incoming Parcels
VEH-DC:ST	«Exchange Element» Route Status	«Performer (Operational)» Vehicle	«Activity (Operational)» Record Delivery «Activity (Operational)» Record Pickup	VEH - DC	«Performer (Operational)» Distribution Center	
HC-VEH:PK	«System» Parcel	«Performer (Operational)» Home Customer	«Activity (Operational)» Provide Waybill	VEH - HC	«Performer (Operational)» Vehicle	«Activity (Operational)» Verify Waybill and Payment
HC-VEH:PW	«Exchange Element» Parcel Waybill	«Performer (Operational)» Home Customer	«Activity (Operational)» Provide Waybill	VEH - HC	«Performer (Operational)» Vehicle	«Activity (Operational)» Verify Waybill and Payment
HC-VEH:PY	«Exchange Element» Payment	«Performer (Operational)» Home Customer	«Standard Activity (Operational)» Provide Payment	VEH - HC	«Performer (Operational)» Vehicle	«Activity (Operational)» Verify Waybill and Payment
VEH-HC:PK	«System» Parcel	«Performer (Operational)» Vehicle	«Activity (Operational)» Provide Parcel	VEH - HC	«Performer (Operational)» Home Customer	«Activity (Operational)» Accept Delivery

Generated automatically from the architecture

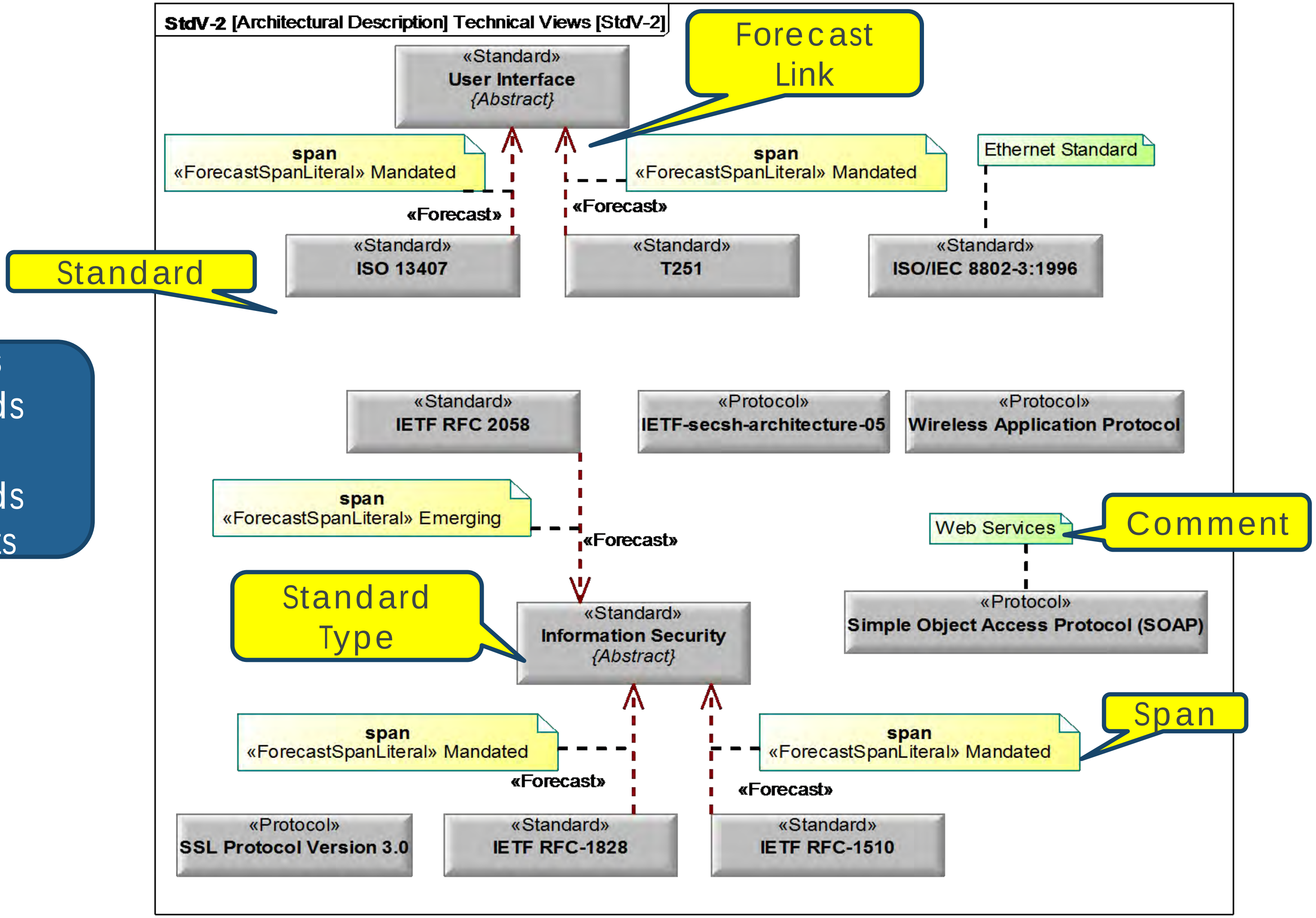
SYSTEM INTERCHANGE SPECIFICATION



Systems can also be specified as services

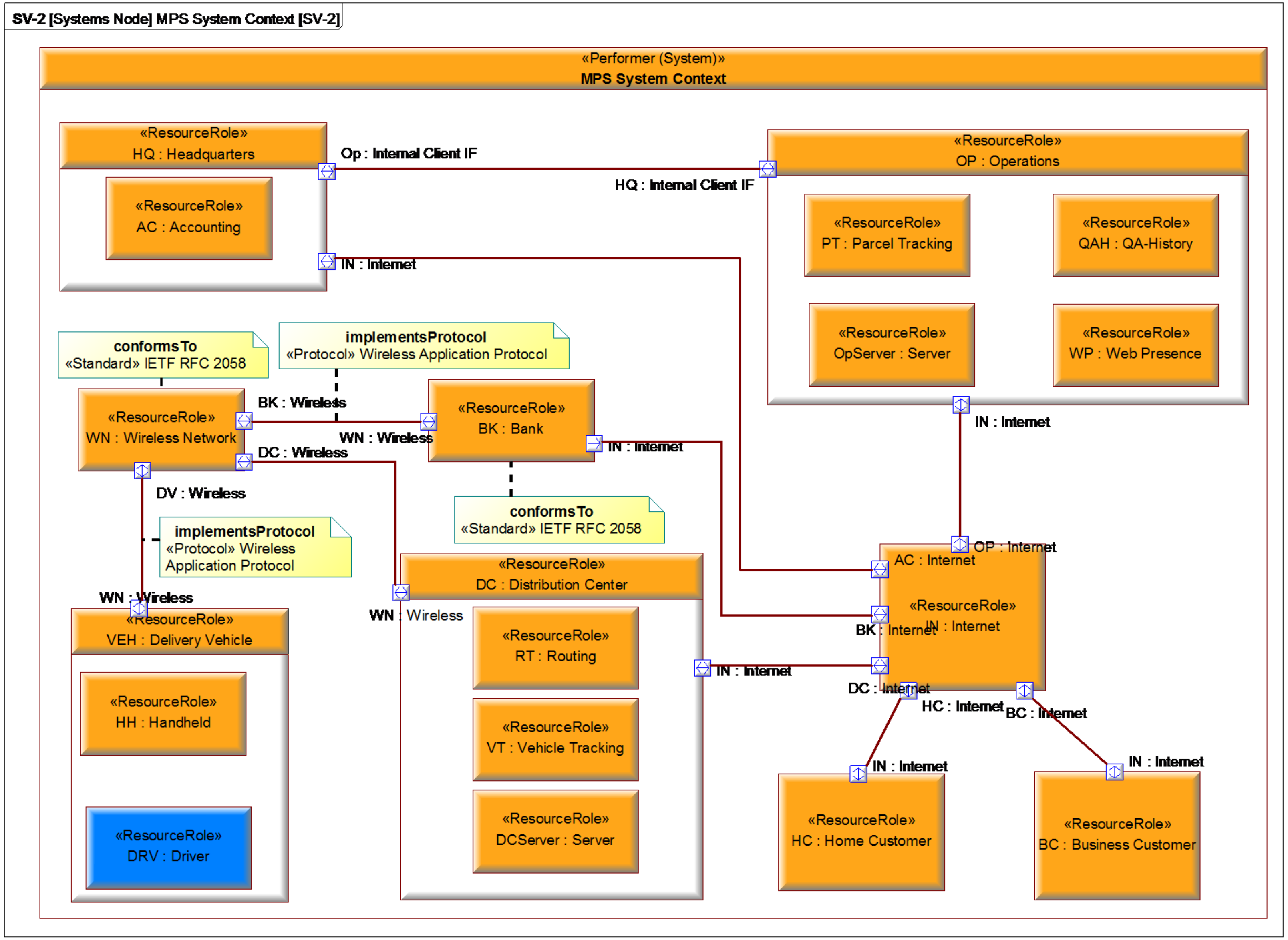
Defines system and human interface requirements and interactions

THE EVOLUTION OF STANDARDS OVER TIME



Defines standards and standards forecasts

SYSTEM INTERFACE SPECIFICATION



Defines how systems will interact to provide capabilities

STANDARDS COMPLIANCE MATRIX

ptc

[Architectural Description] Technical Views [StdV-1 Matrix]

Standards

Model Elements

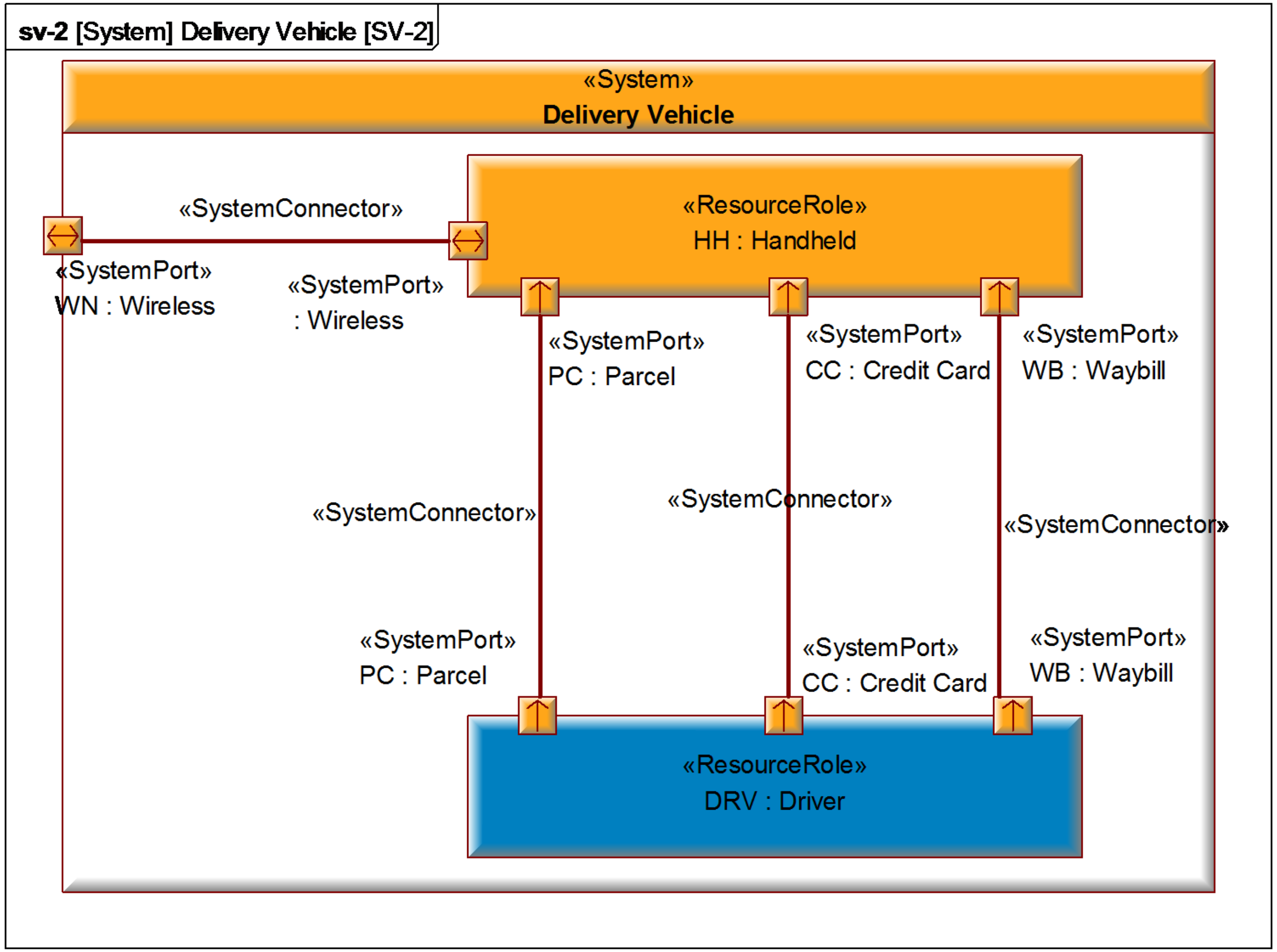
Standard

Conforming Elements	«Protocol» IETF-secsh-architecture-05	«Protocol» Simple Object Access Protocol (SOAP)	«Protocol» SSL Protocol Version 3.0	«Protocol» Wireless Application Protocol	«Standard» IETF RFC 2058	«Standard» IETF RFC-1510	«Standard» IETF RFC-1828	«Standard» Information Security	«Standard» ISO 13407	«Standard» ISO/IEC 8802-3:1996	«Standard» T251	«Standard» User Interface
«ResourceRole» BK					X							
«ResourceRole» HH					X							
«SystemInterface» HH - BK					X							
«Performer (System)» Wireless Network					X							
«ResourceRole» WN					X							
«ResourceRole» WP									X		X	

Generated automatically. Summarizes standards conformance

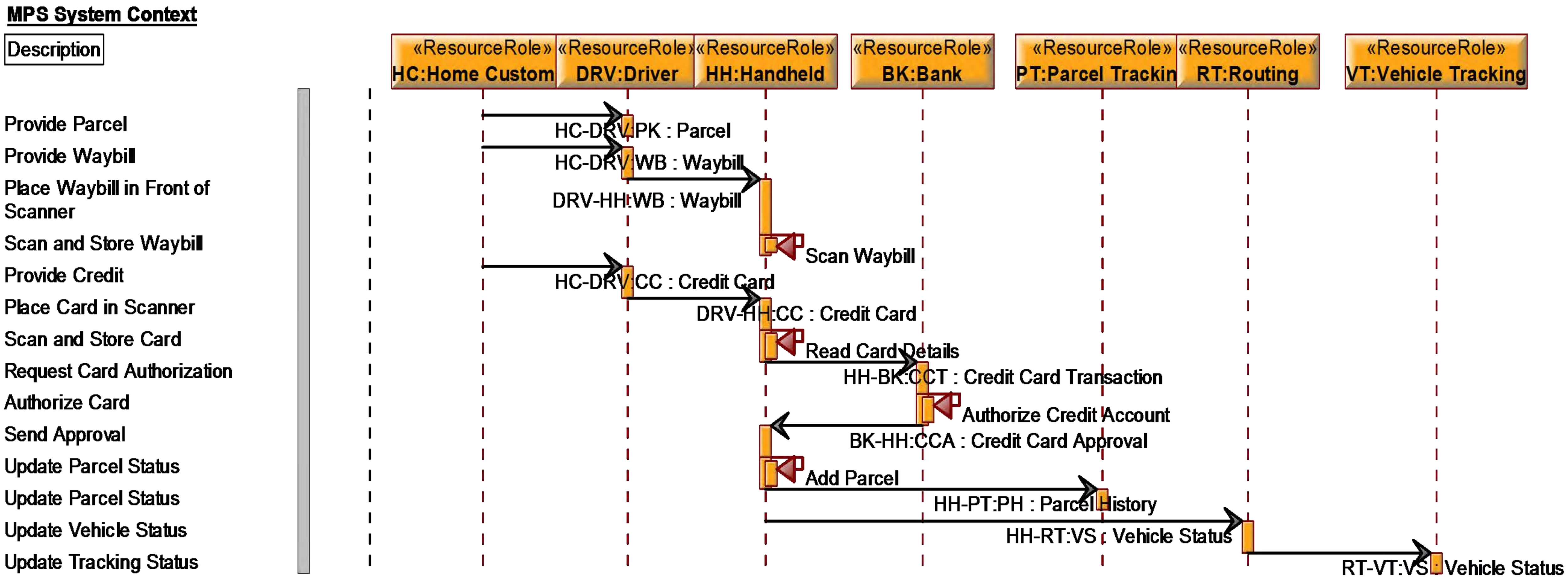
Conformance

DRIVER-HANDHELD MODULAR INTERFACES

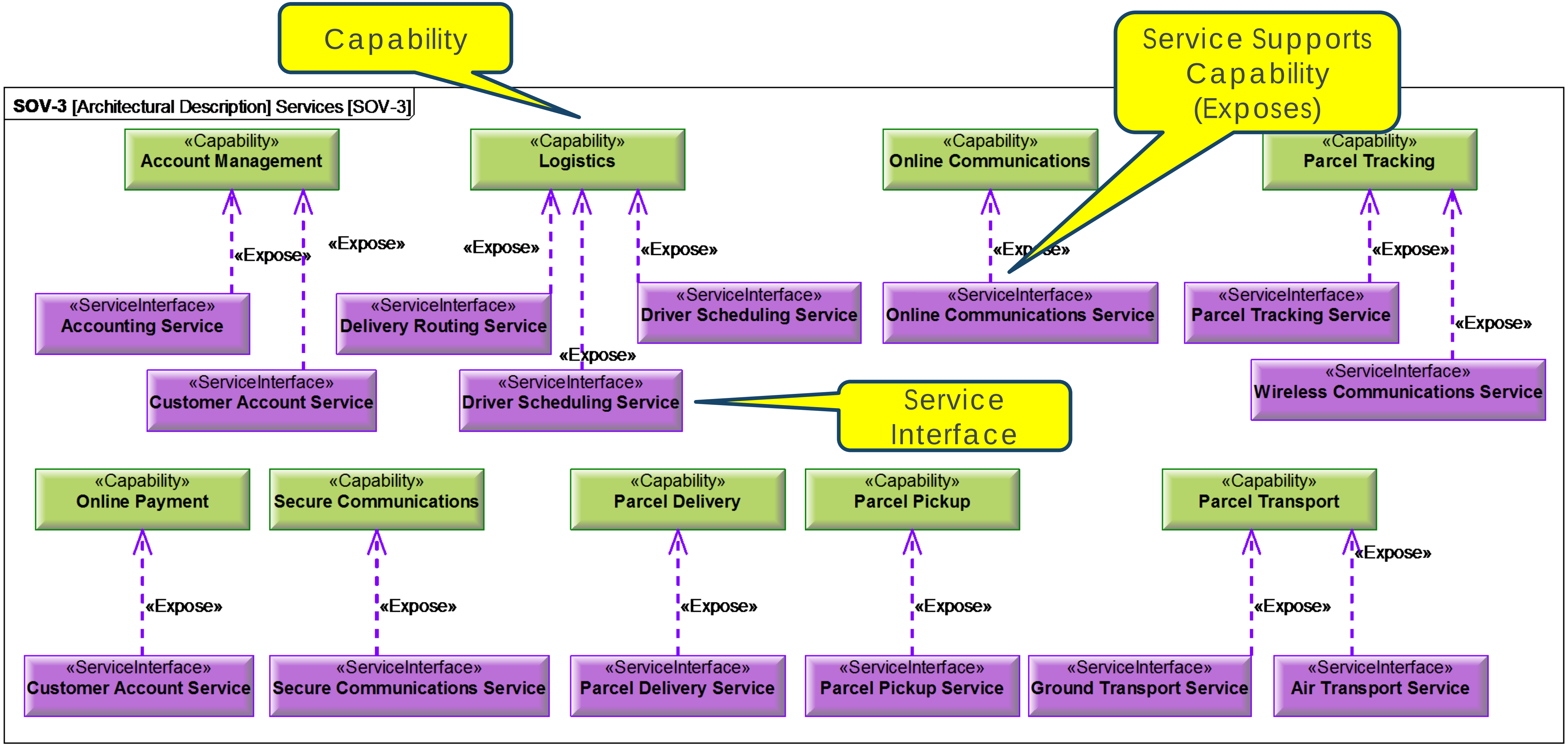


SYSTEM EVENT TRACE DESCRIPTION

- The order and timing of the interactions is just as critical as the interface definition itself: not just what happens, but when and why it happens.

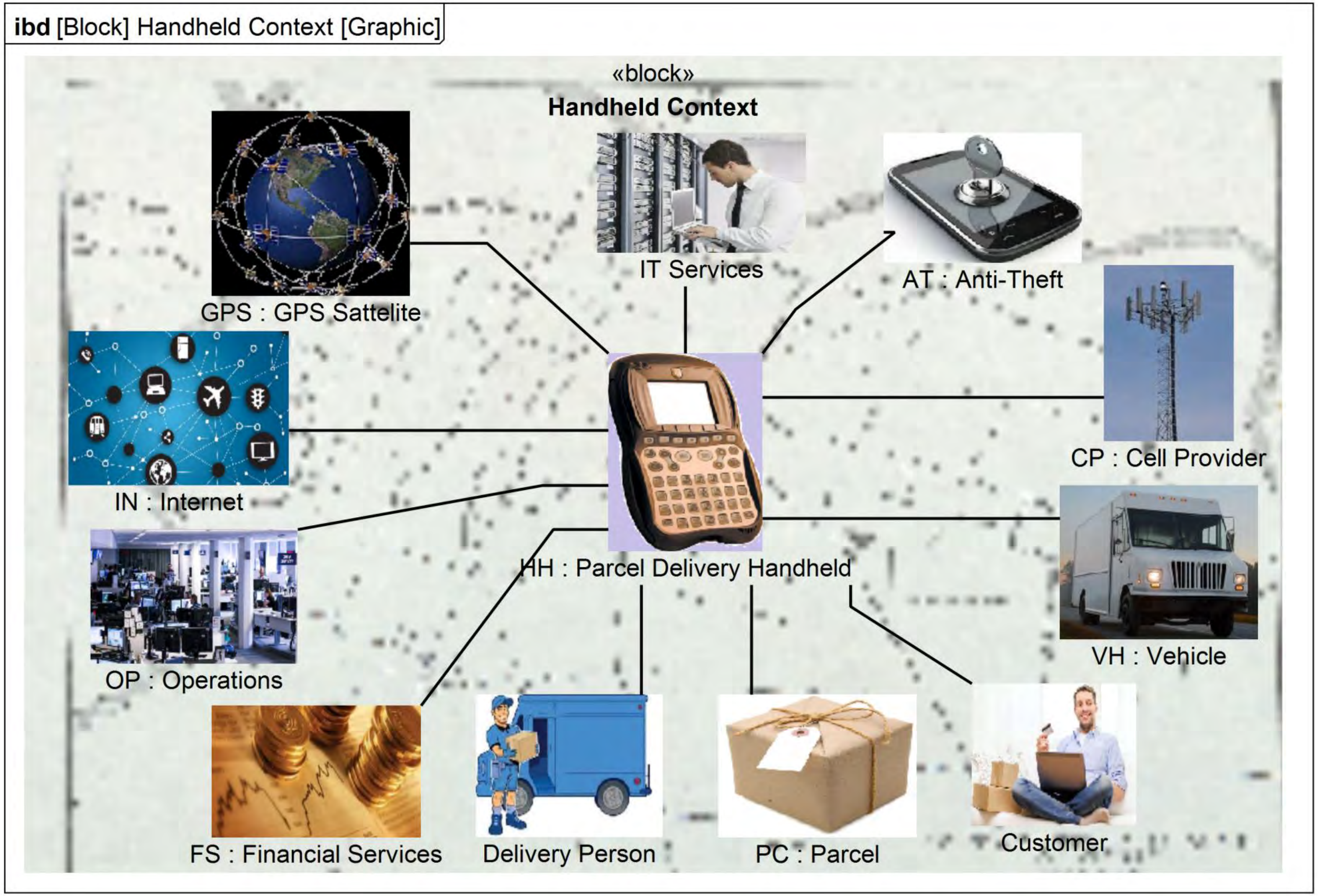


DERIVING SERVICES FROM CAPABILITIES

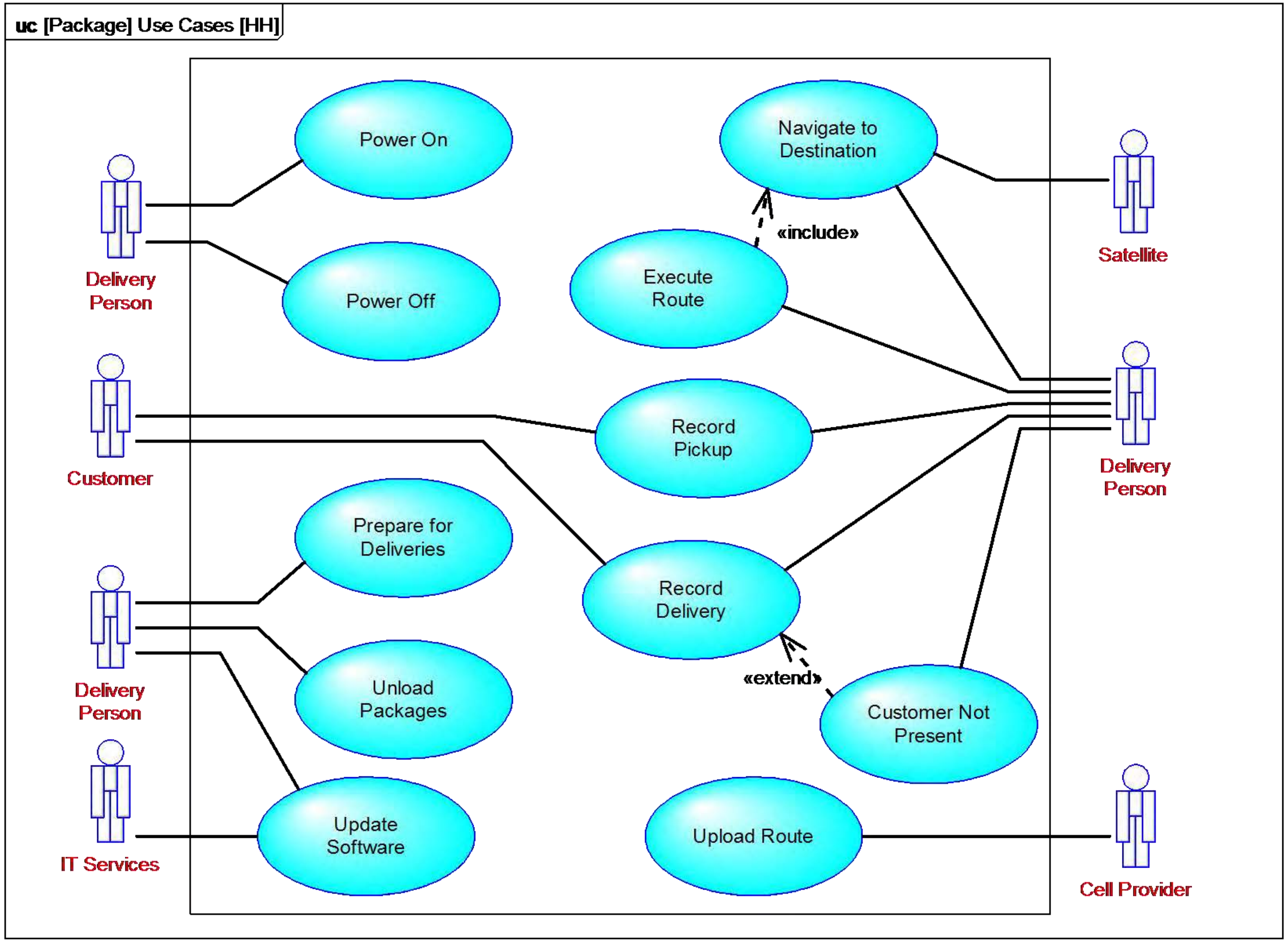


SYSTEMS INTERFACES

CONTEXT OF HANDHELD DEVICE



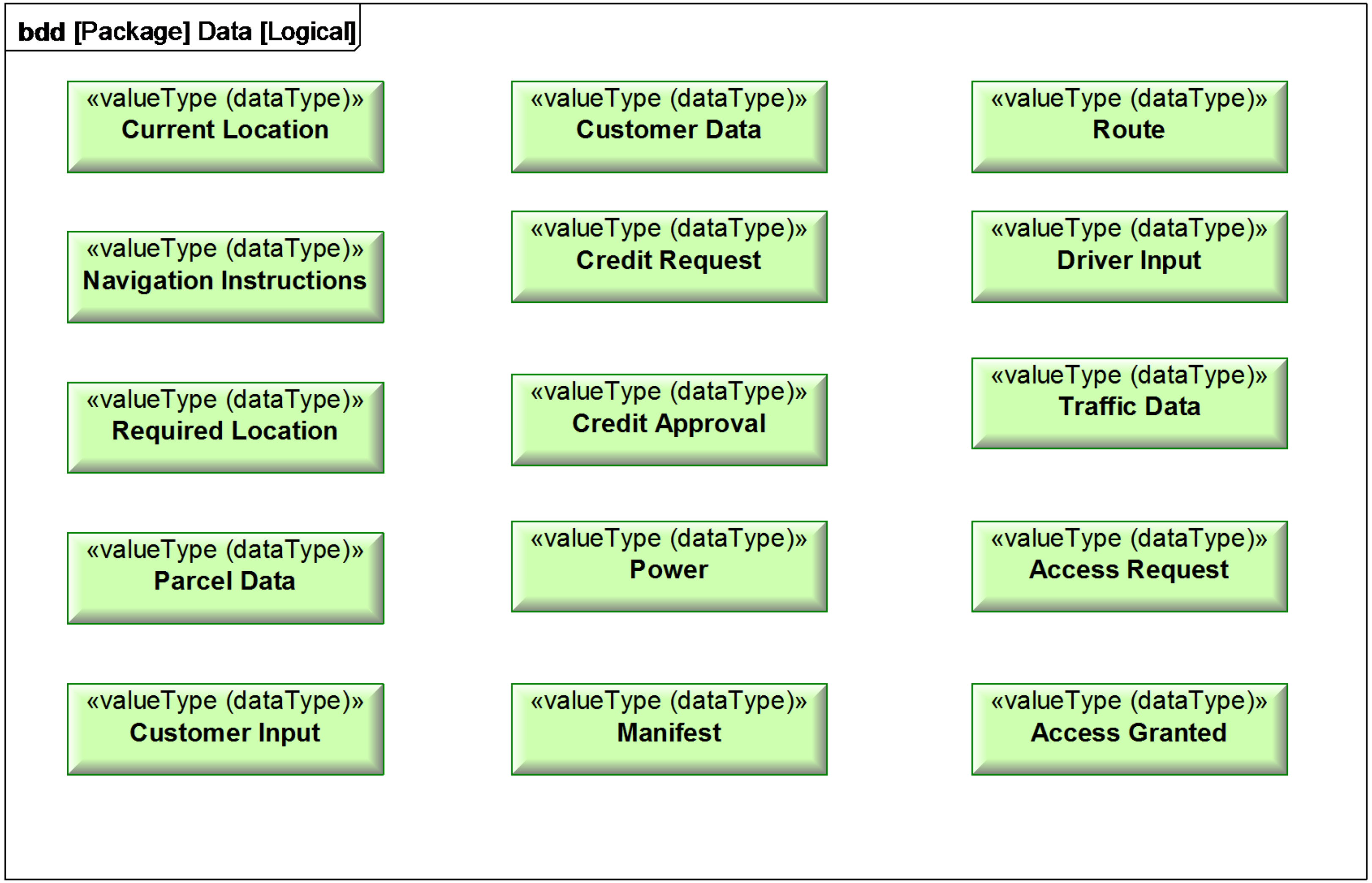
USE CASES DEFINE INTERACTIONS WITH ACTORS



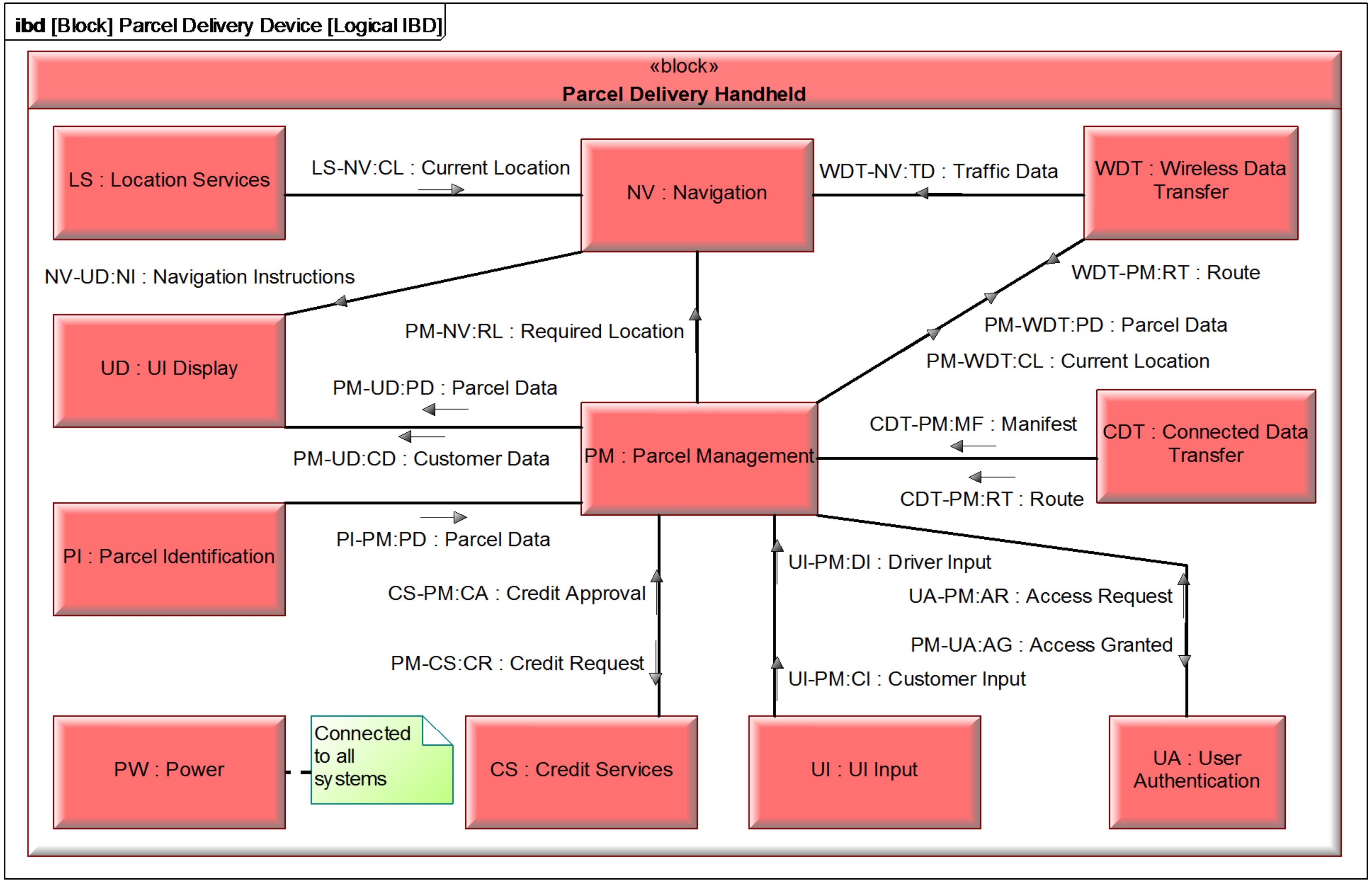
LOGICAL V. PHYSICAL MODELING WITH IBDS

- IBDs can be used to capture both a logical model of parts, connections and flows, and a physical model
- Logical model focuses on logical parts and flows and may not show ports or types (unless logical types defined)
  - Based on specification rather than implementation ('what' not 'how')
  - Abstract types (if any)
- Physical model focuses on physical parts and flows and normally shows ports and physical (implementation) types
  - Normally follows logical modeling
  - May be many physical models for one logical model
  - Real-world types
- May affect package structure
  - Logical package contains logical types
  - Physical package contains physical types
- Can link logical model items to physical model items via Allocation

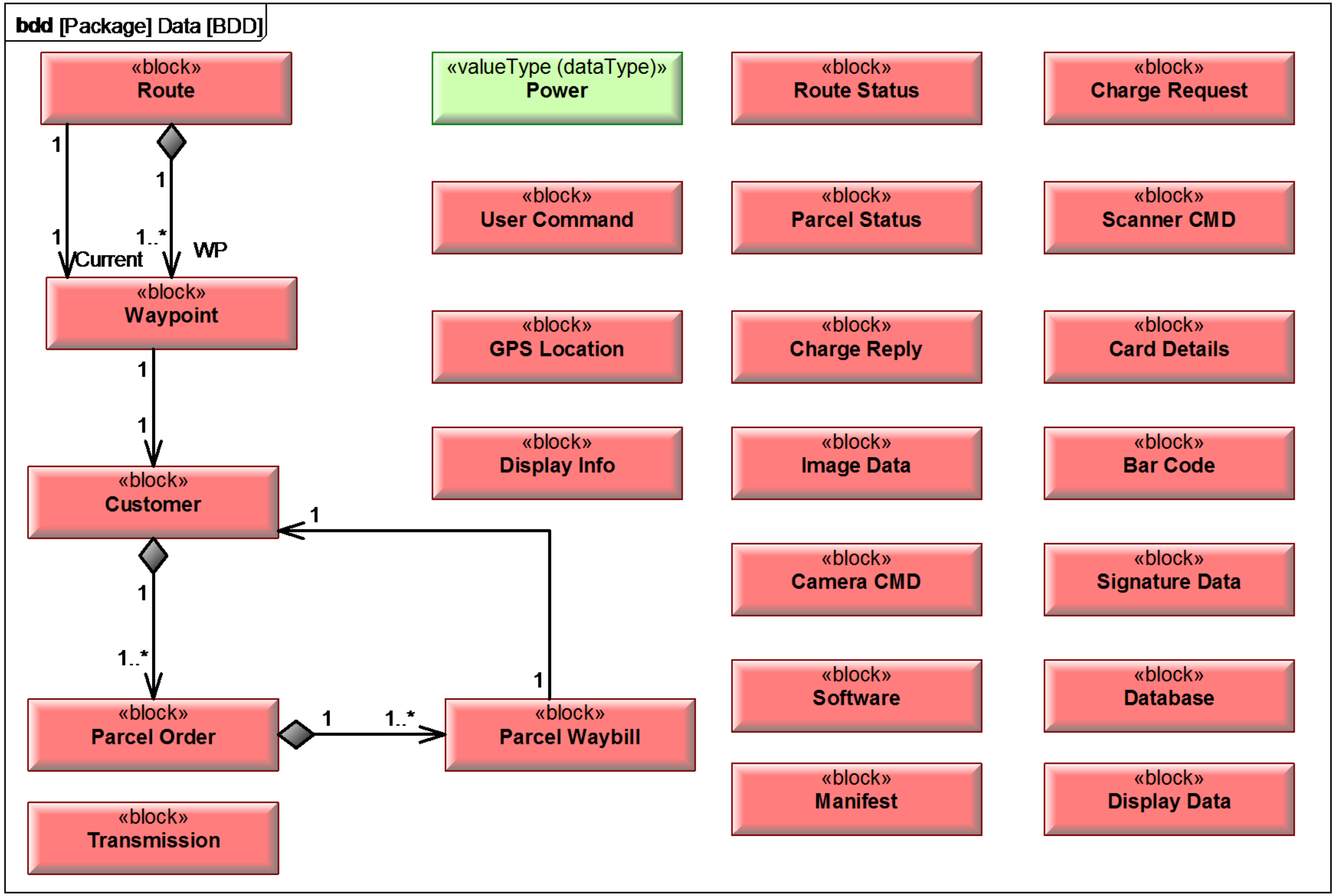
LOGICAL DATA



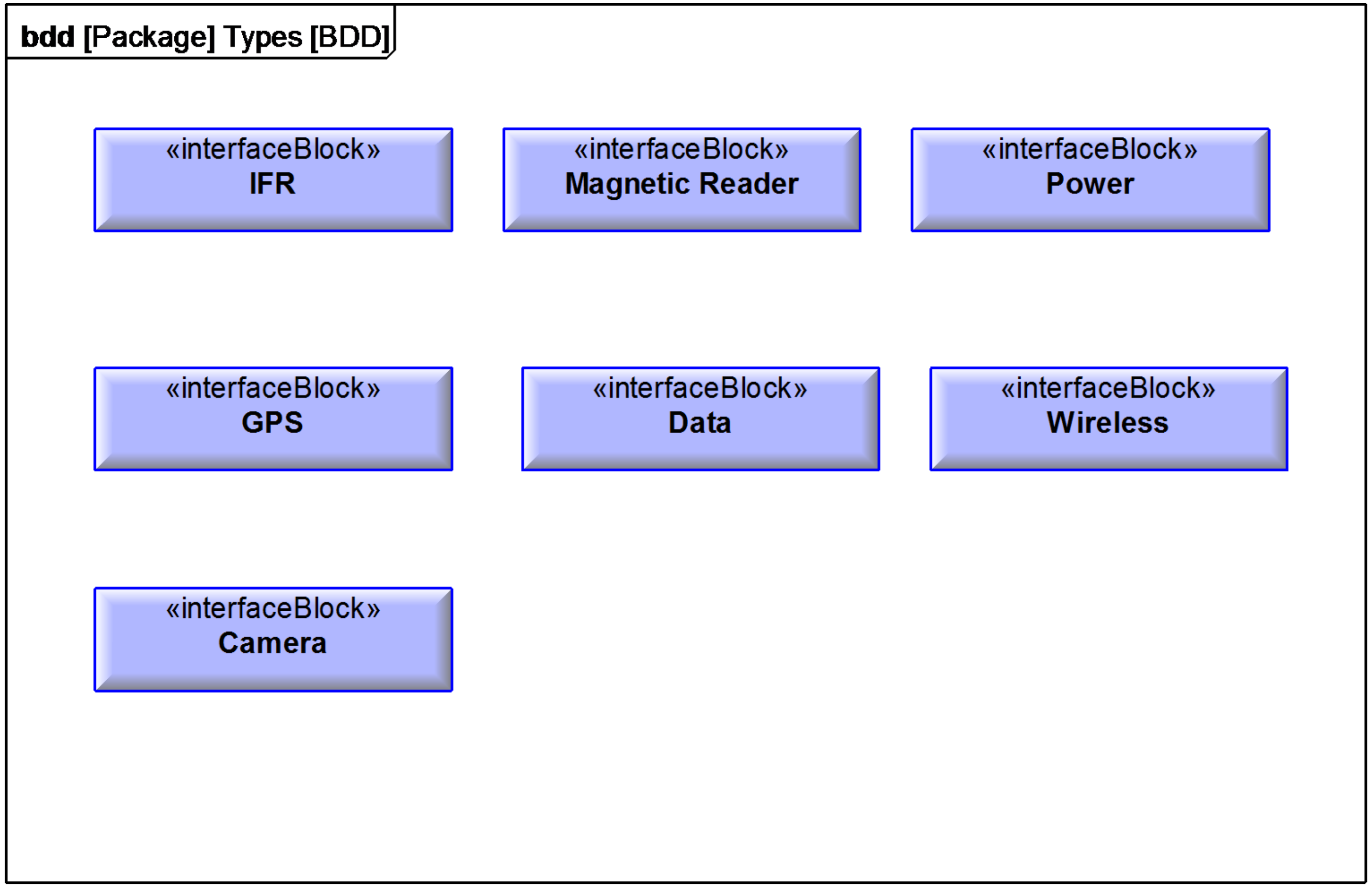
EXAMPLE IBD - LOGICAL MODEL



PHYSICAL DATA

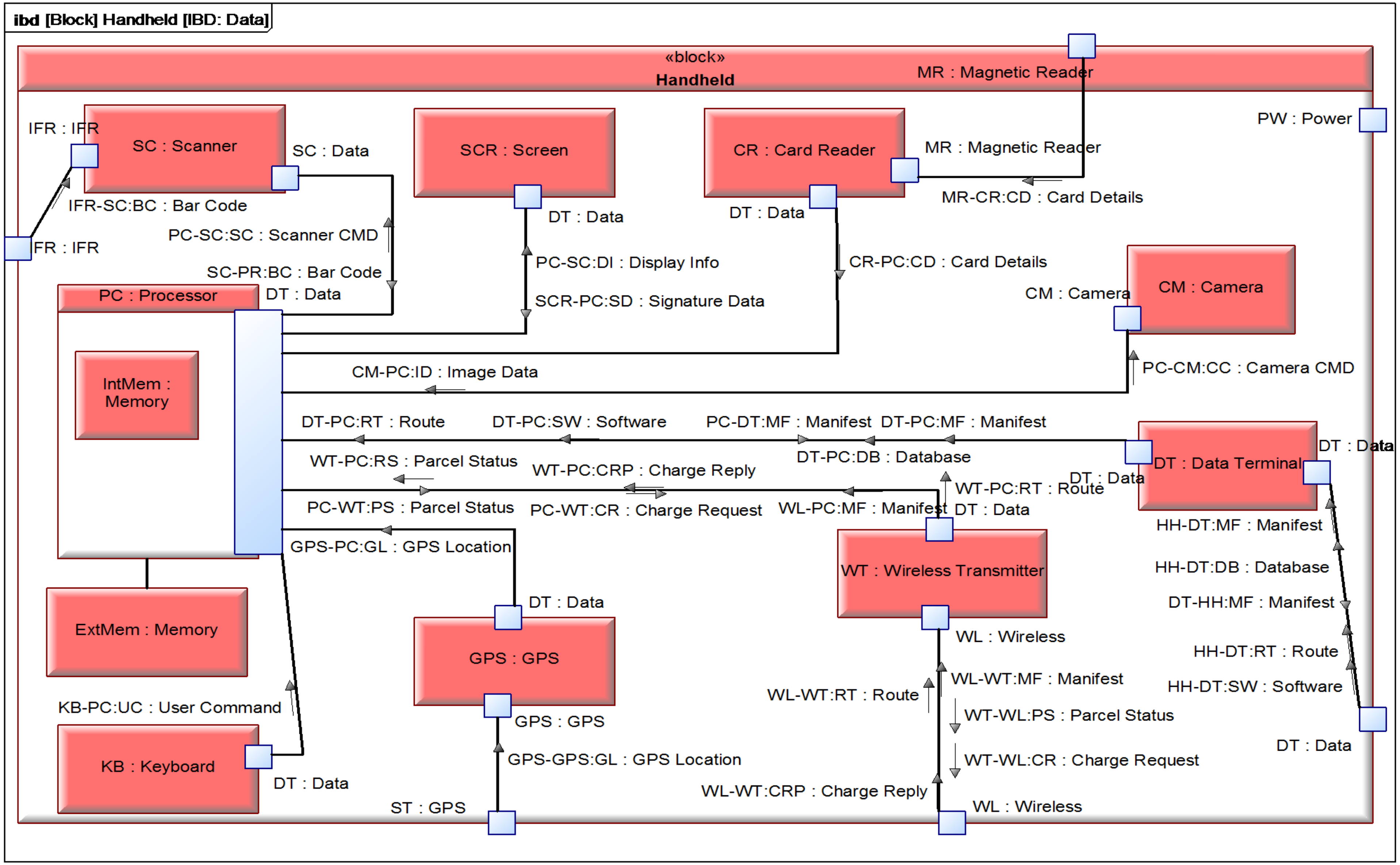


INTERFACES

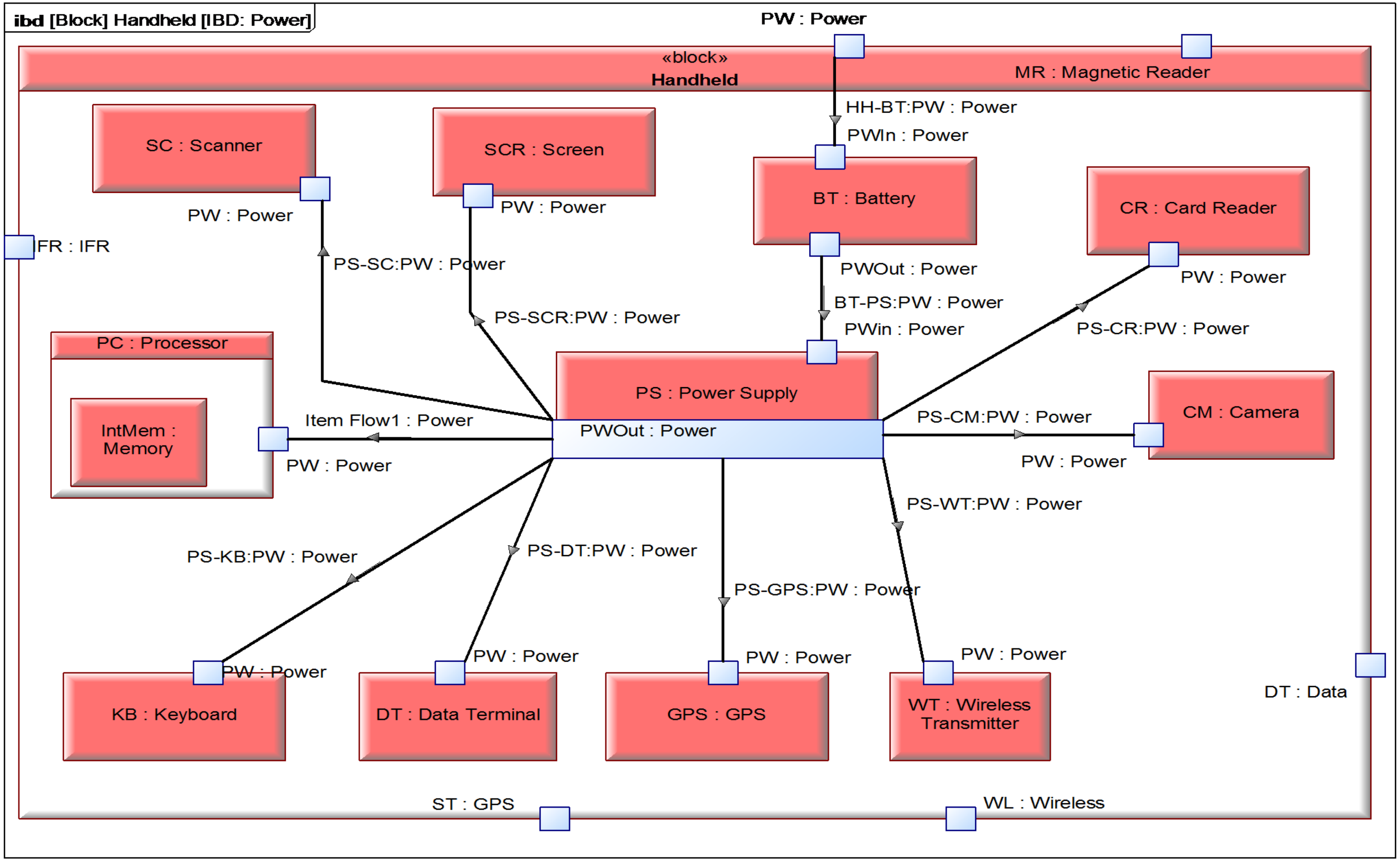


bdd [Package] Types [BDD]
«interfaceBlock»
IFR
«interfaceBlock»
Magnetic Reader
«interfaceBlock»
Power
«interfaceBlock»
GPS
«interfaceBlock»
Data
«interfaceBlock»
Wireless
«interfaceBlock»
Camera

EXAMPLE IBD – PHYSICAL MODEL

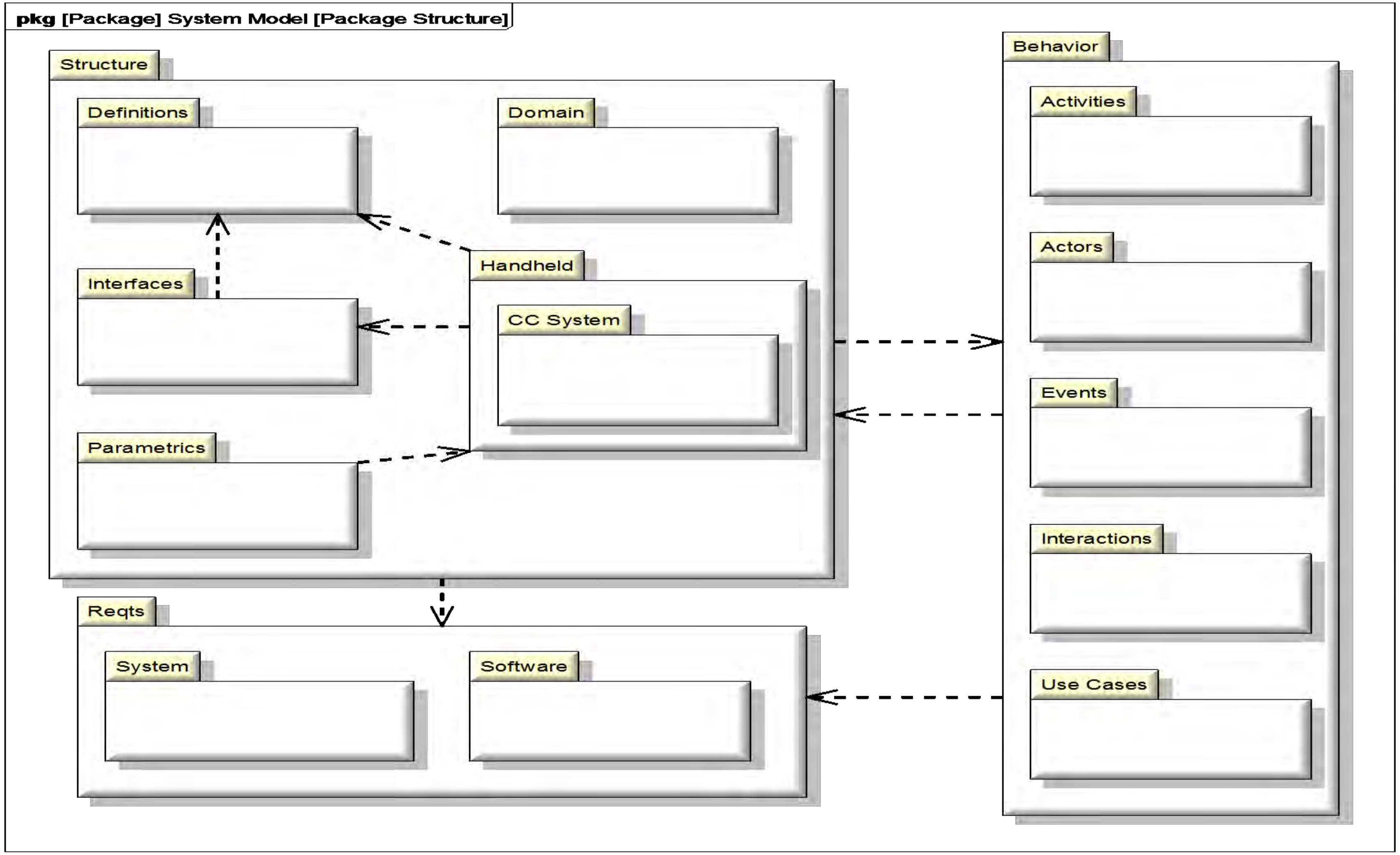


EXAMPLE IBD – PHYSICAL MODEL

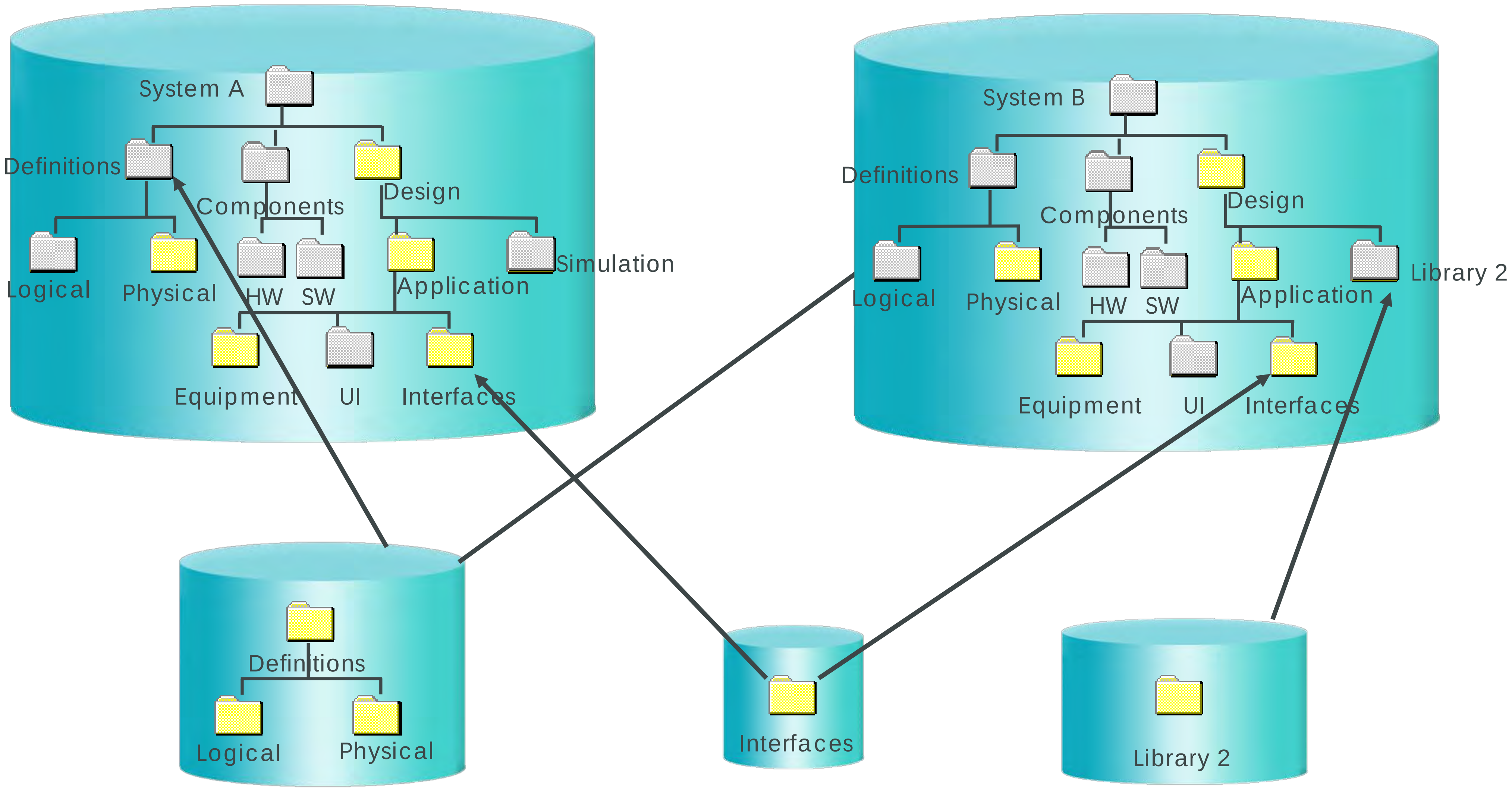


MODEL PACKAGE STRUCTURE

- Shows Dependencies within model to interfaces



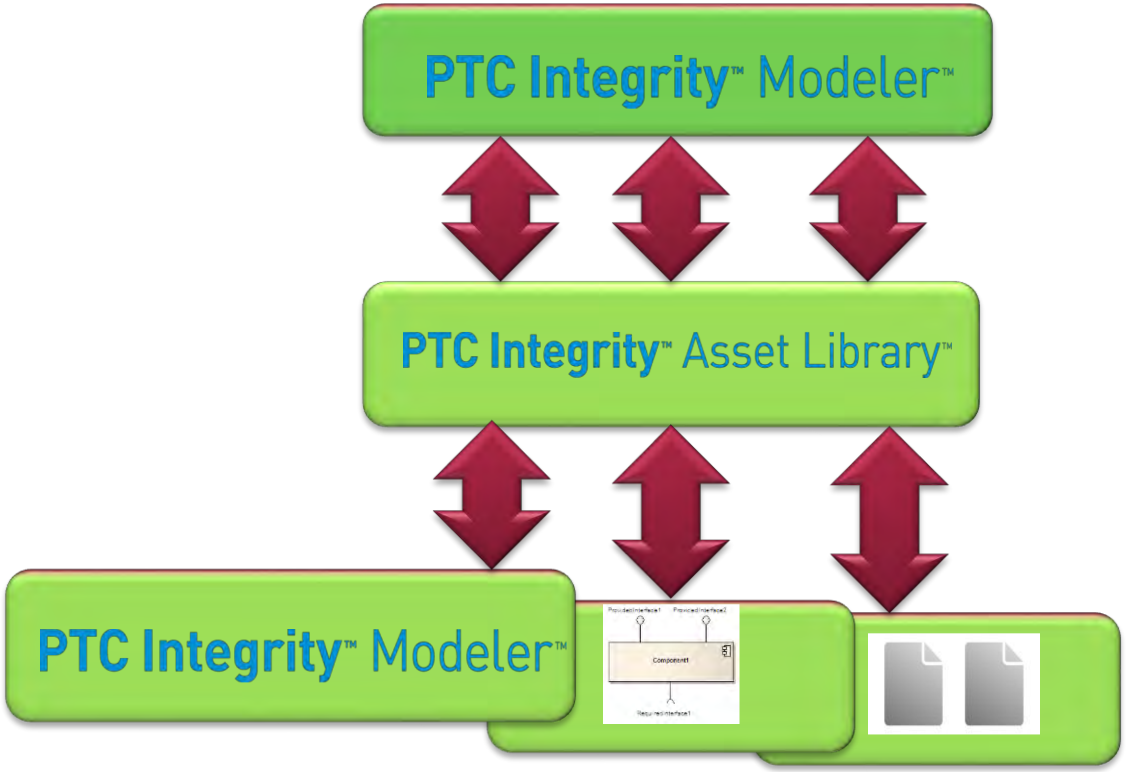
REUSING AND SHARING MODEL LIBRARIES



ASSET-BASED DESIGN ENABLES COLLABORATION AND VIRTUAL TEAMS

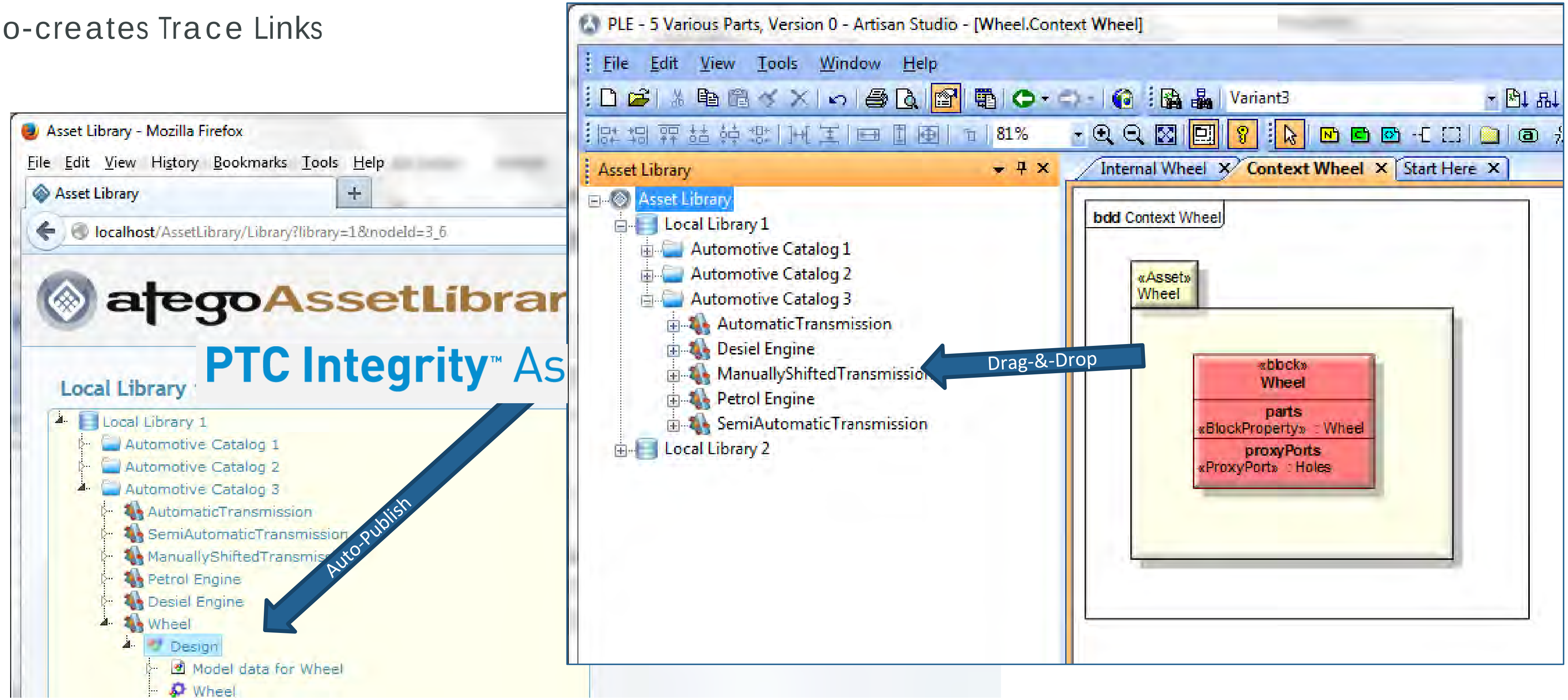
ASSET-BASED MODULAR DESIGN

- Design the same way you Build
  - Construct Systems of Sub-Systems (SoS)
  - Use Services to build your Application (SOA)
  - Plug Components together (CBD)
- Modular Design
  - Top-Down, Architected
    - Specification (& Requirements) Driven
    - Parallel Working
    - Separation of Concerns
  - Bottom-Up, Asset Mining
    - Un-modeled Assets
    - Other Modeling Tools
    - Legacy Integration
    - Published Interfaces (e.g. IDL, SysML)
  - Uses the Reusable Asset Specification (RAS) and OSLC



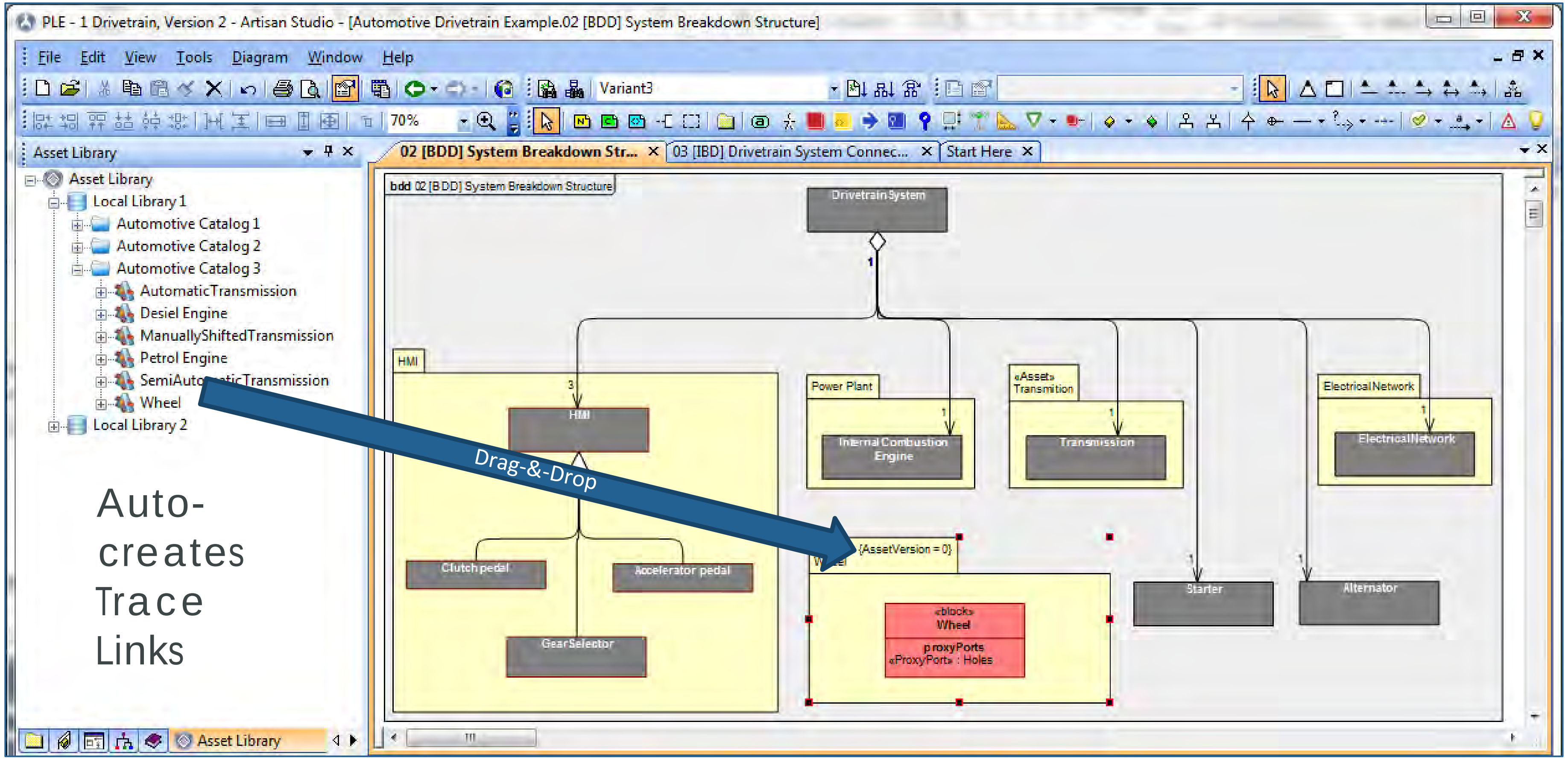
ASSET-BASED MODULAR DESIGN

- Publish from Sub-system model into PTC Integrity Asset Library
  - Publishes the asset as a black box
  - Enables reuse as opposed to clone and own
  - Auto-creates Trace Links



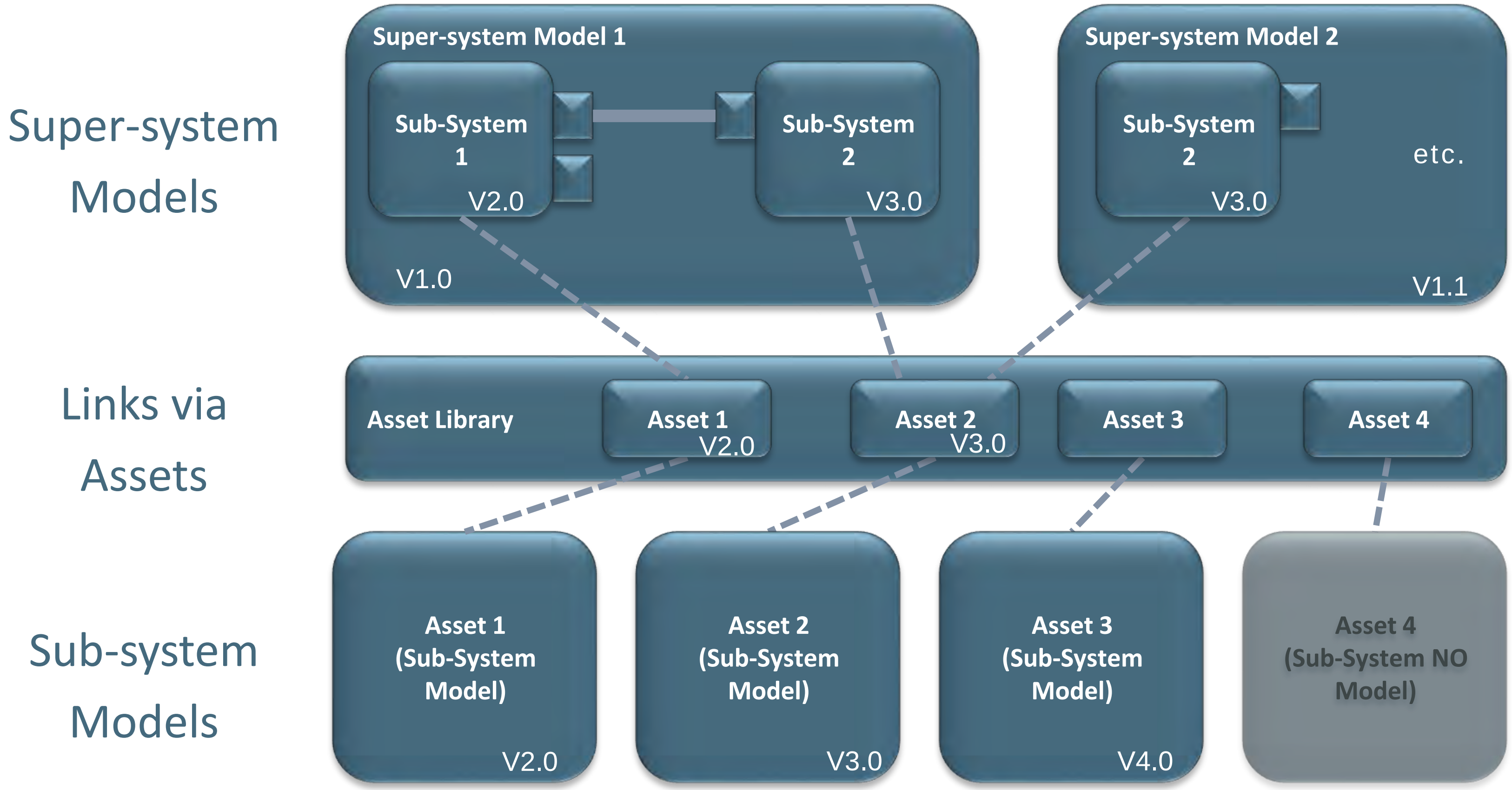
ASSET-BASED MODULAR DESIGN

- Use Sub-system from PTC Integrity Asset Library in Super-system Model
  - Reuse interfaces, requirements, operations, parameters, constraints, etc.



ASSET-BASED MODULAR DESIGN

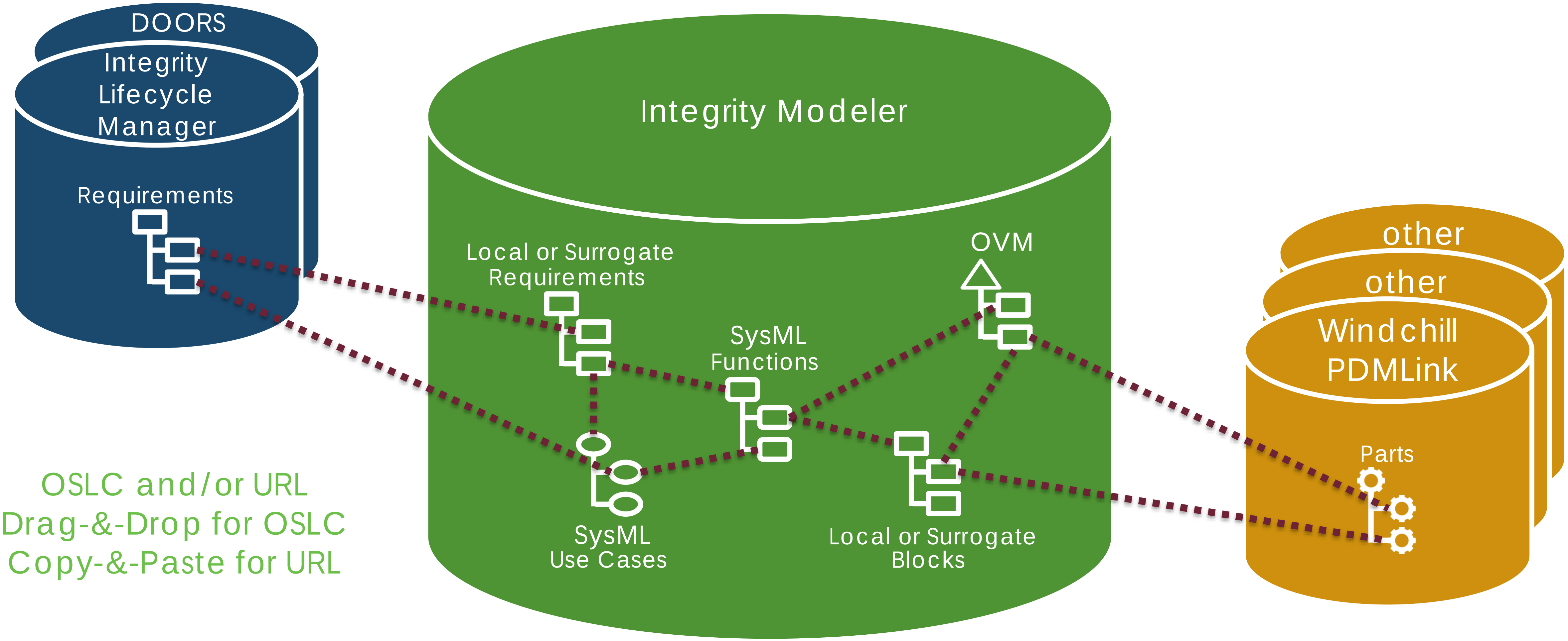
- Super-system Model = Configuration of Versioned Sub-systems



THROUGH THE DEVELOPMENT LIFECYCLE

LINKING FROM REQUIREMENTS TO MODELS TO PLM

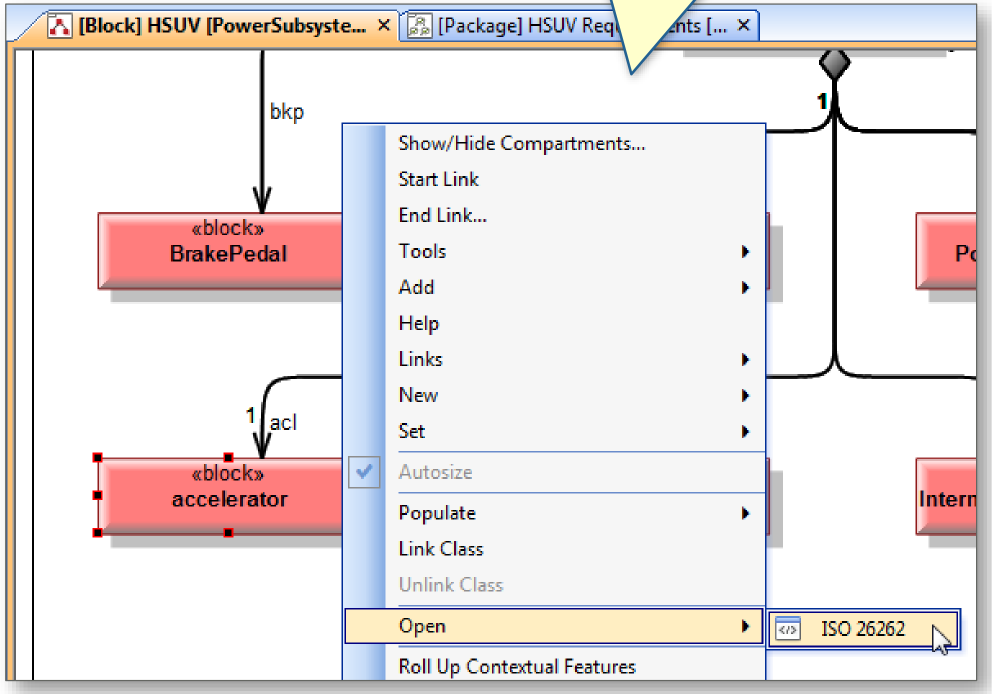
External Traces & Model Surrogates with Visual Model Trace Links



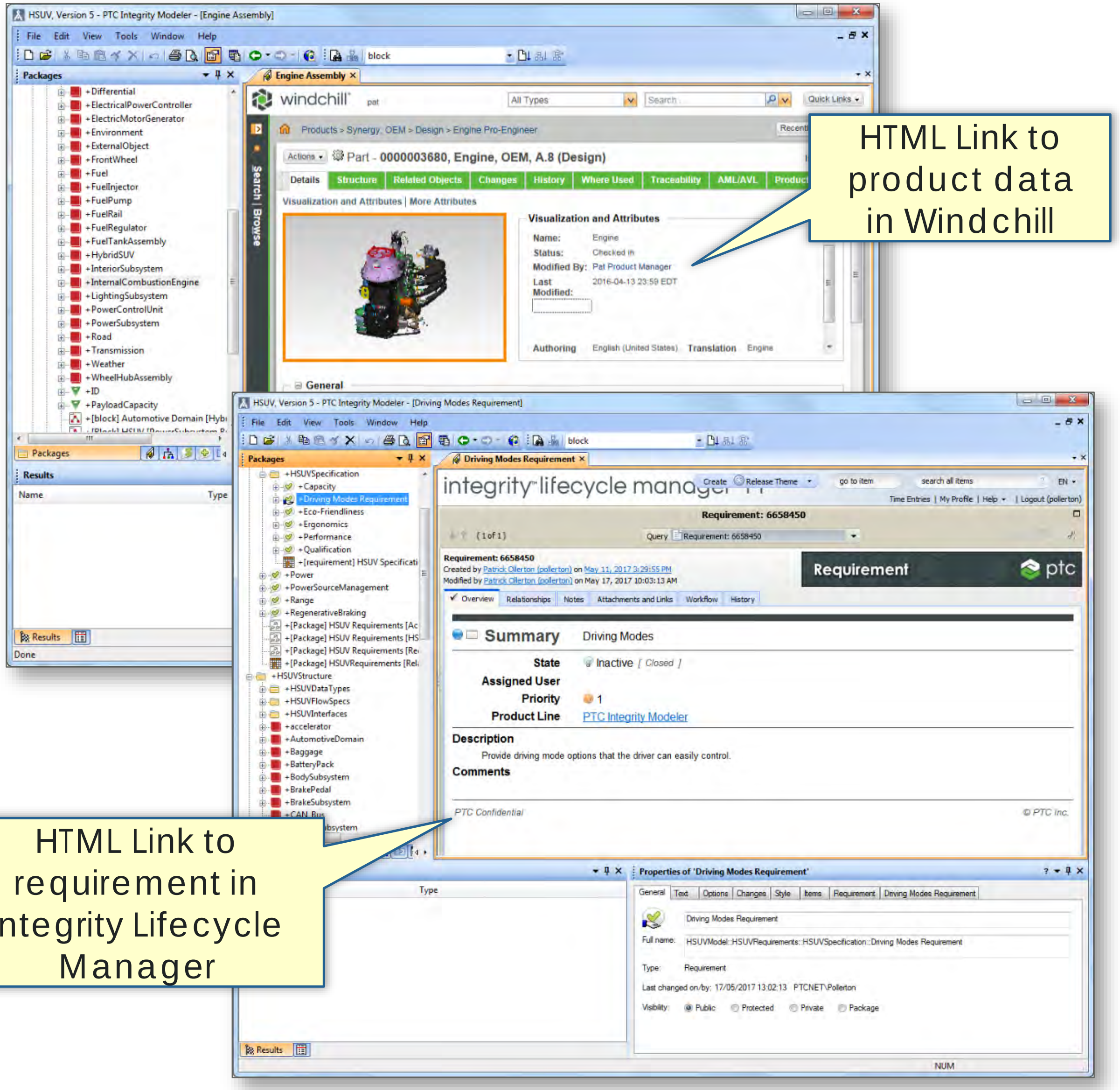
OSLC and/or URL
Drag-&-Drop for OSLC
Copy-&-Paste for URL

TRACING FROM REQUIREMENTS TO SYSML TO CAD

Right-click on items in browsers or on diagrams to open HTML Links and Surrogates



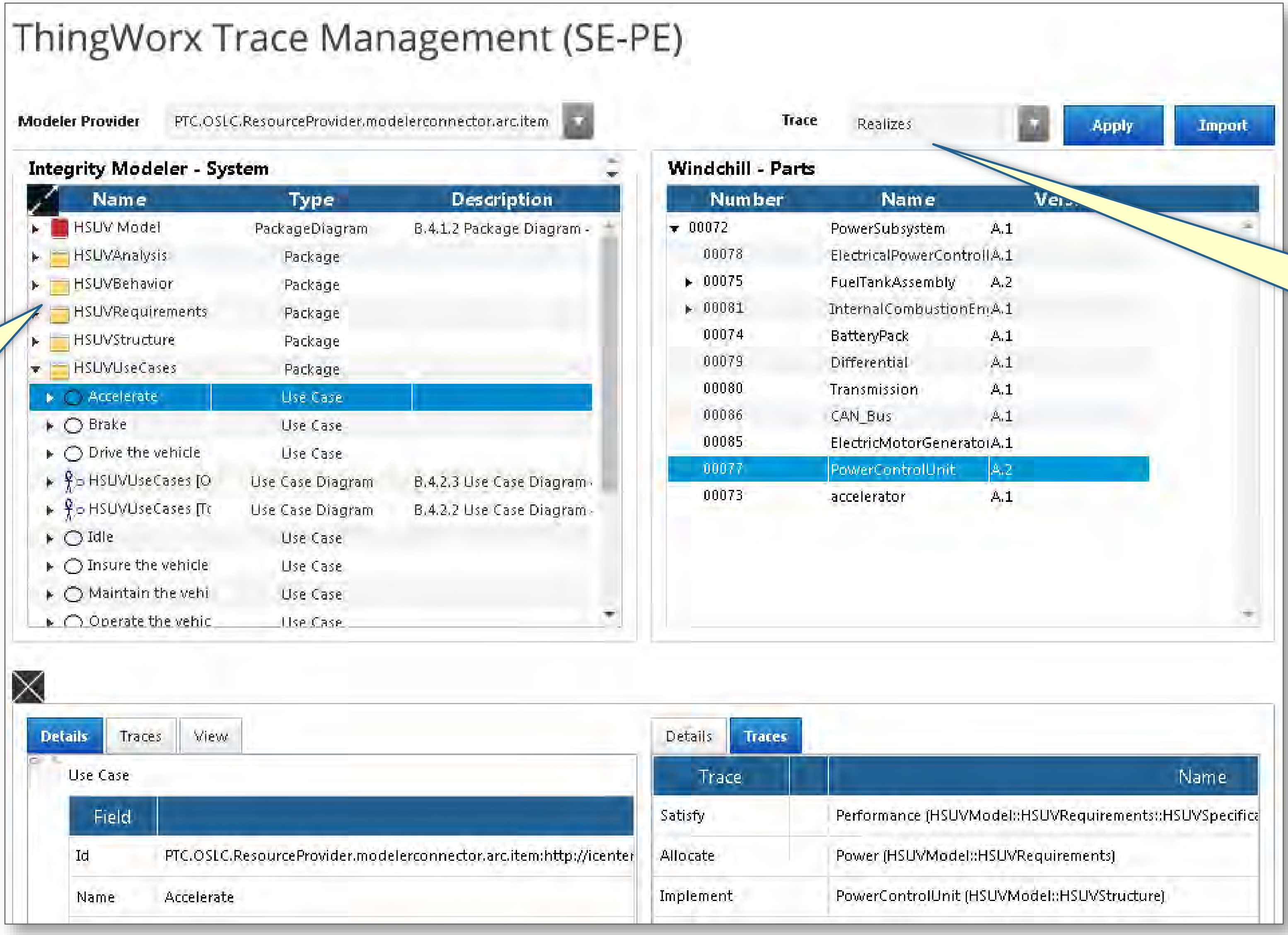
HTML Link to product data in Windchill



HTML Link to requirement in Integrity Lifecycle Manager

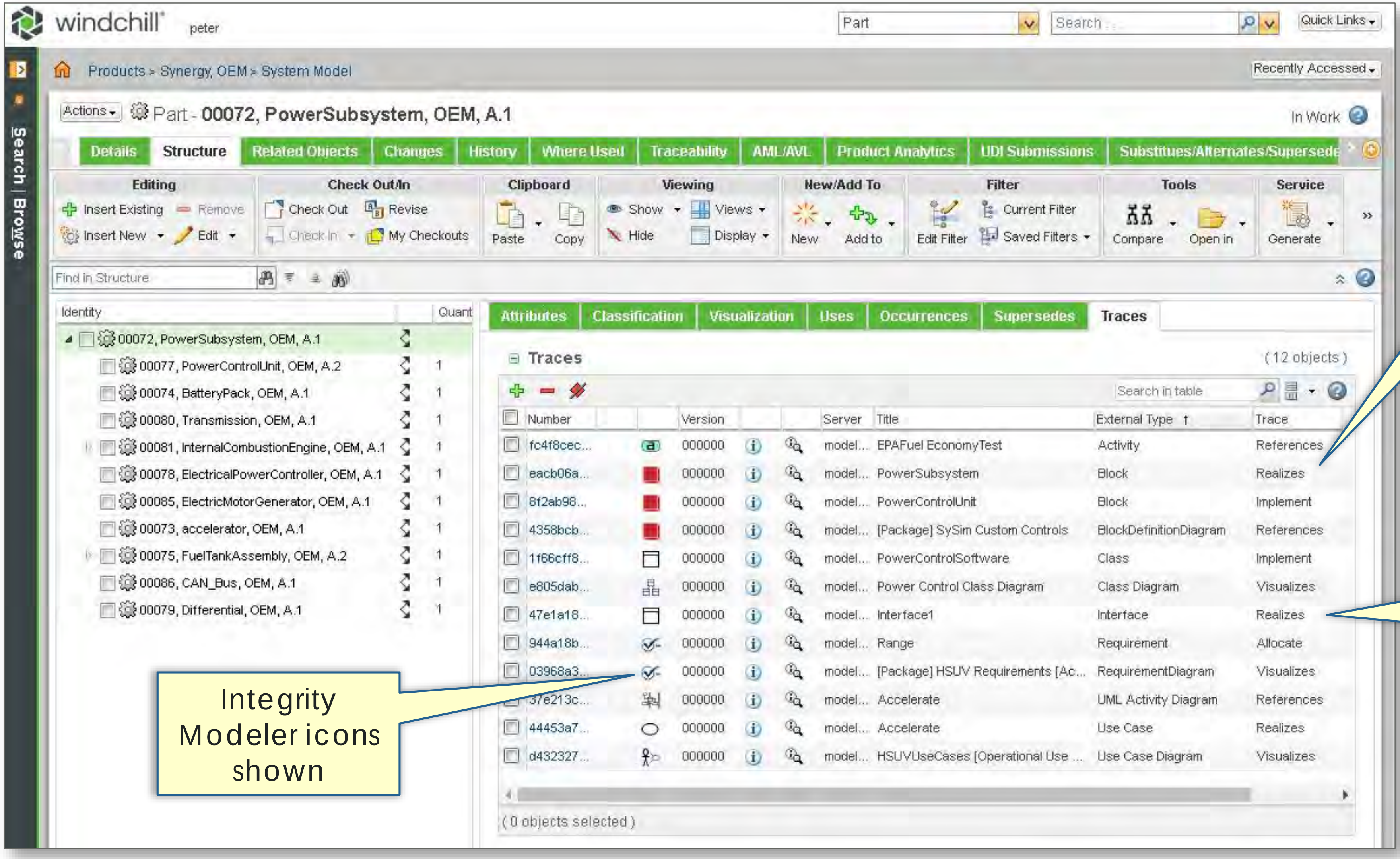
THINGWORX TRACE MANAGEMENT (SE-PE) DISPLAY

You define the Integrity Modeler types that are available in the ThingWorx Trace Management app



You define the valid link types for your organization

WINDCHILL LINKS TO INTEGRITY MODELER



Trace links to all Integrity Modeler items are displayed in Windchill

Integrity Modeler type and trace link type displayed

Integrity Modeler icons shown

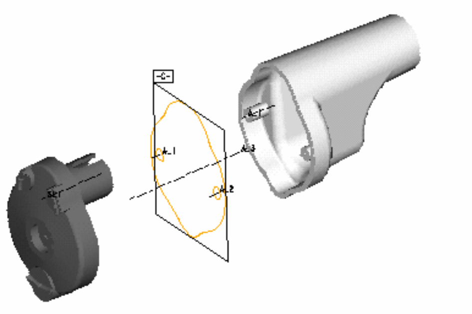
PHYSICAL INTERFACES

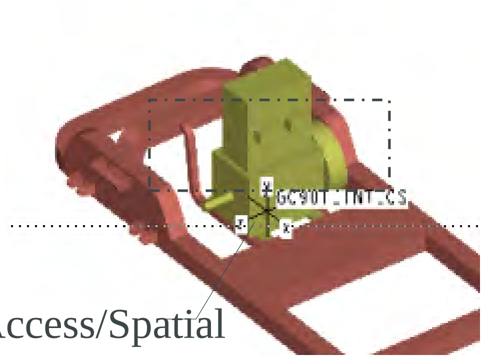
Interfaces are controlled boundaries between modules, components or parts

Types include:

- Attachment, Spatial (envelope)
- Transfer (e.g. power)
- Communication
- User Interface

Direct/Attachment





Access/Spatial

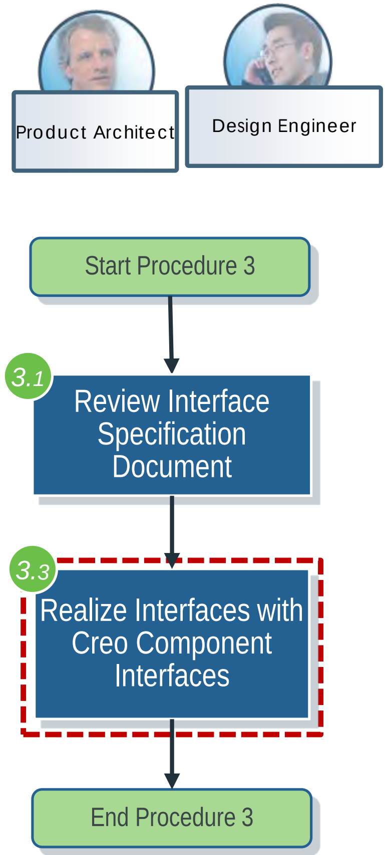
Communication

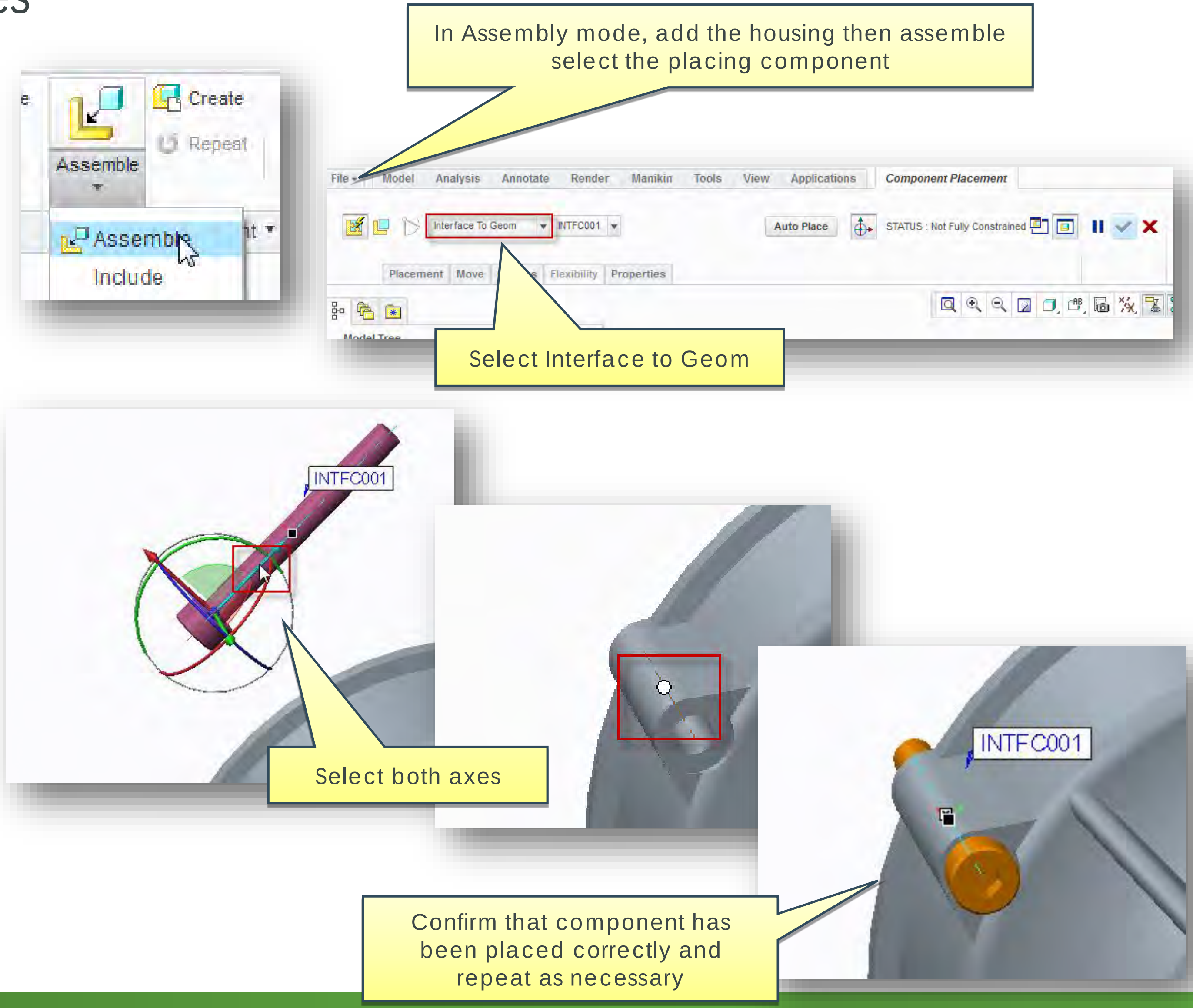
Transfer of Power

User Interface

REALIZING INTERFACES

▶ Develop and Propagate Interfaces

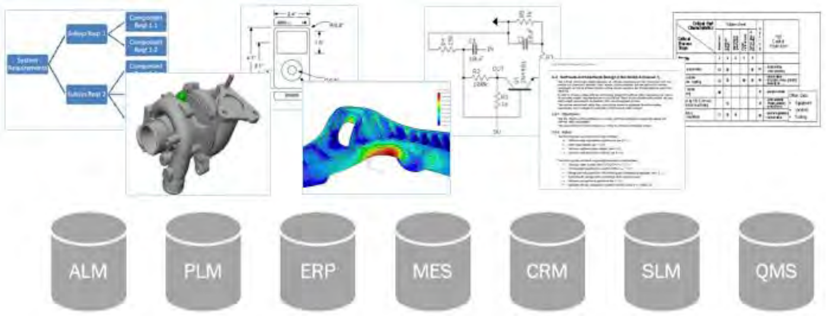




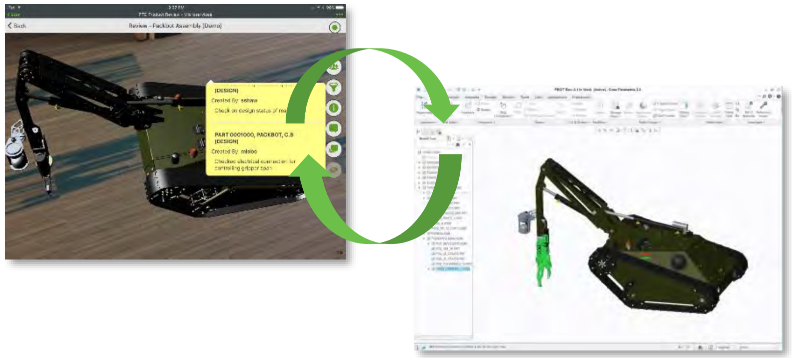
COLLABORATIVE AR/VR DESIGN

A Few Simple Steps from CAD to AR/VR

Collaborate Globally



Effortlessly Collect all Relevant Information



Closed-Loop Change Management

DIGITAL TWIN

ptc

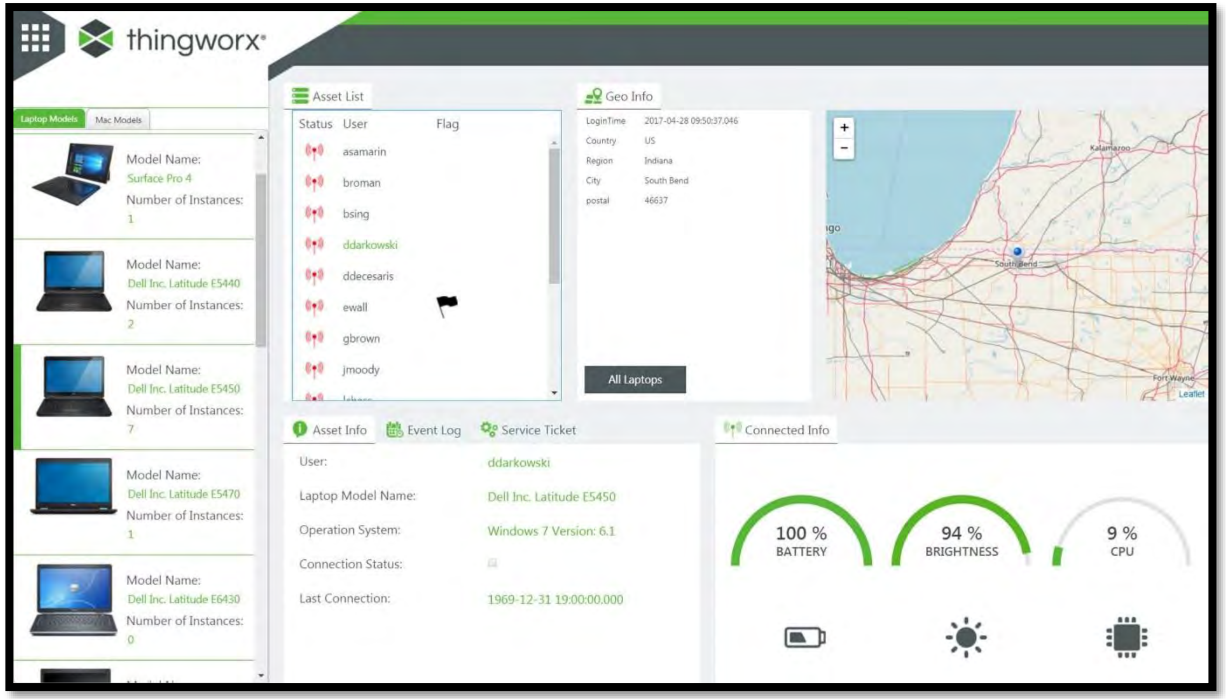
QA Engineer

Understand Your Product in the Field

Registry of Information

Identify Solutions

A digital record of each product's designed, manufactured, serviced and real-world state

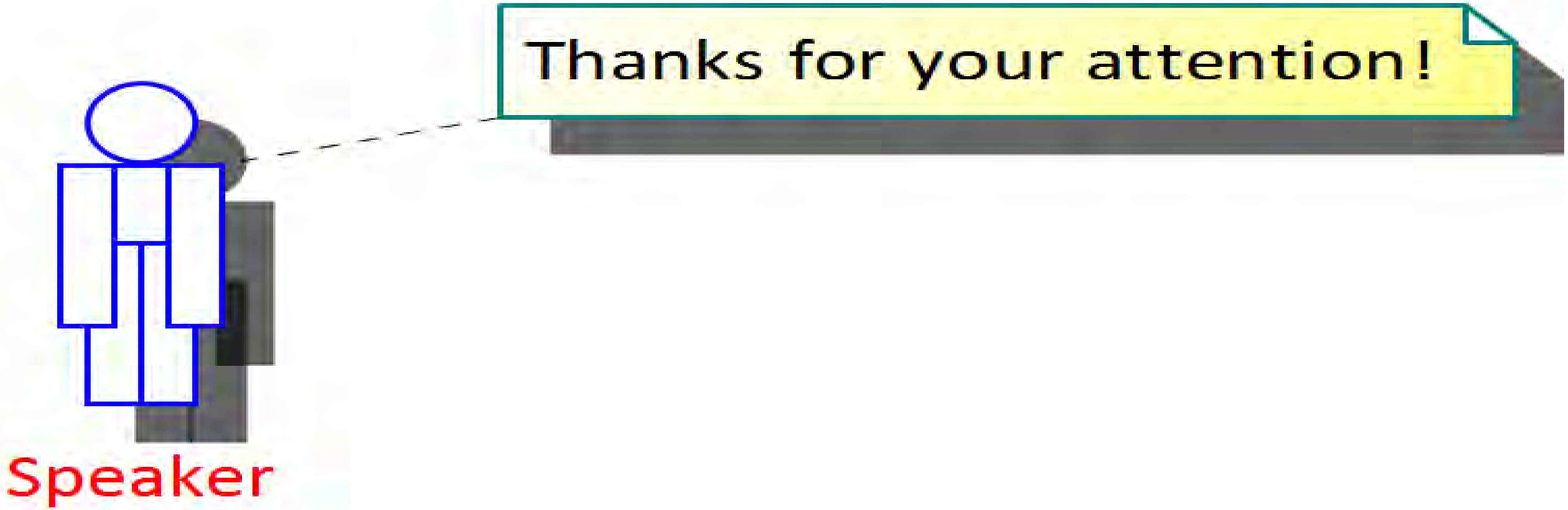


- Improve profitability by analyzing the configurations of fleets of assets for future sales, recalls or update opportunities
- Improve decision making by analyzing individual assets again their real-world usage
- Ensure security, legal and regulatory compliance with hardware and software configuration traceability

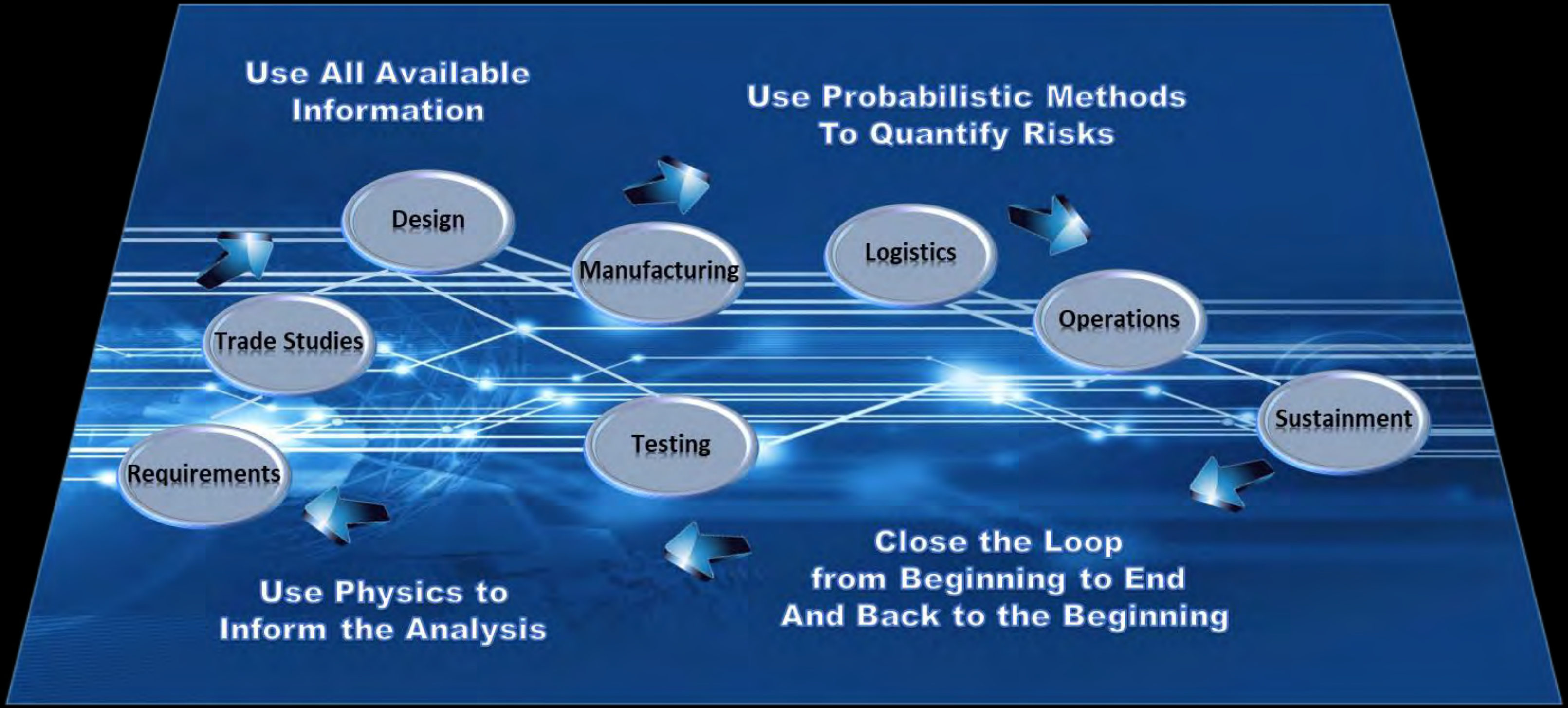
CONCLUSION

- Interface requirements start at the very beginning of development
- They are many ways to define an interface. The best one depends on particular circumstances and will change over time
- Interfaces can be traced from requirements through to architecture through to design and physical implementation
- Define common interfaces first in a collaborative environment.
  – This means they will be available when people need them.
  – They will also only be defined once
- Interfaces are where things usually go wrong so it is best to get them right.

QUESTIONS AND ANSWERS



Challenges and Innovations in Digital Systems Engineering



Dr. Ed Kraft
Associate Executive Director for Research
University of Tennessee Space Institute

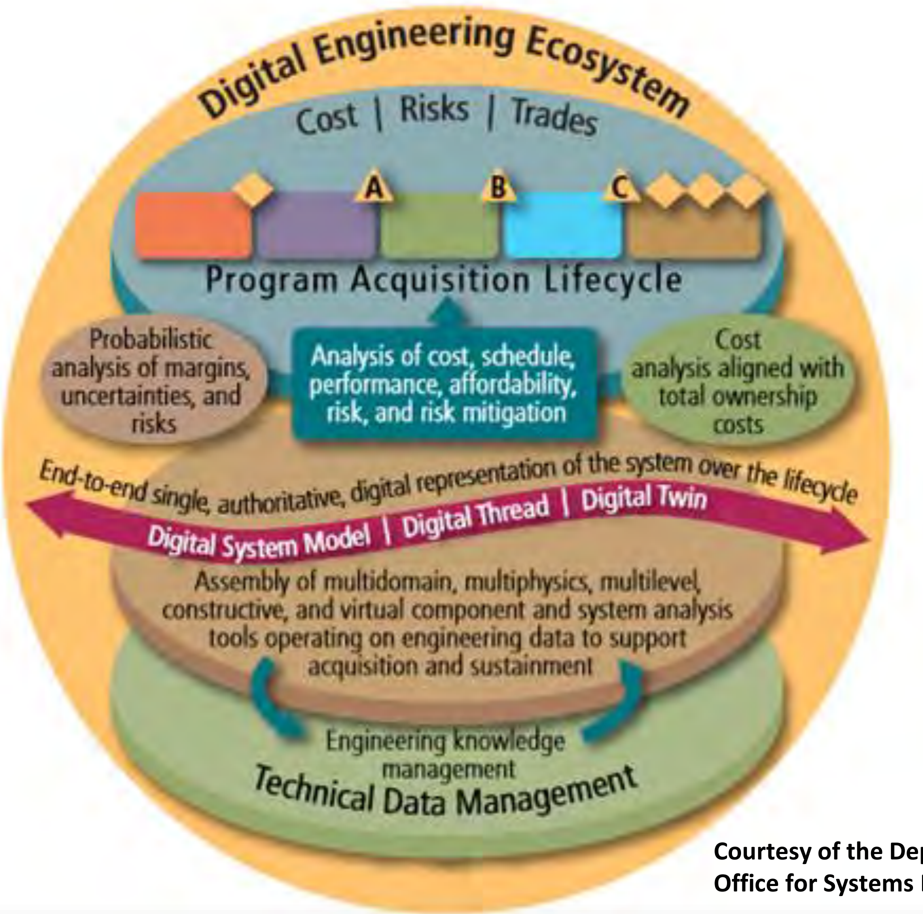
October 25, 2017

Introduction

- **The Aerospace & Defense Industry is investing heavily in Industry 4.0 for their commercial opportunities**
- **The AF in particular, and the DoD in general, are at the threshold of developing Digital Engineering Ecosystems in collaboration with Industry to take advantage of the Digital Revolution for defense programs**
- **Challenges to developing a Government / Industry Digital Environment for Defense Systems include:**
  - **Technologies and Tools for a cyber-physical world**
  - **Policies – data rights, intellectual property**
  - **Processes – moving from document-centric to fully digital model-based processes**
  - **Culture – education and training in Systems Engineering and Program Management consistent with the Digital Revolution**

It is Time to Move From Abstraction to Realization in the Integration of Modeling into Digital Engineering Ecosystems

Digital Engineering Ecosystem

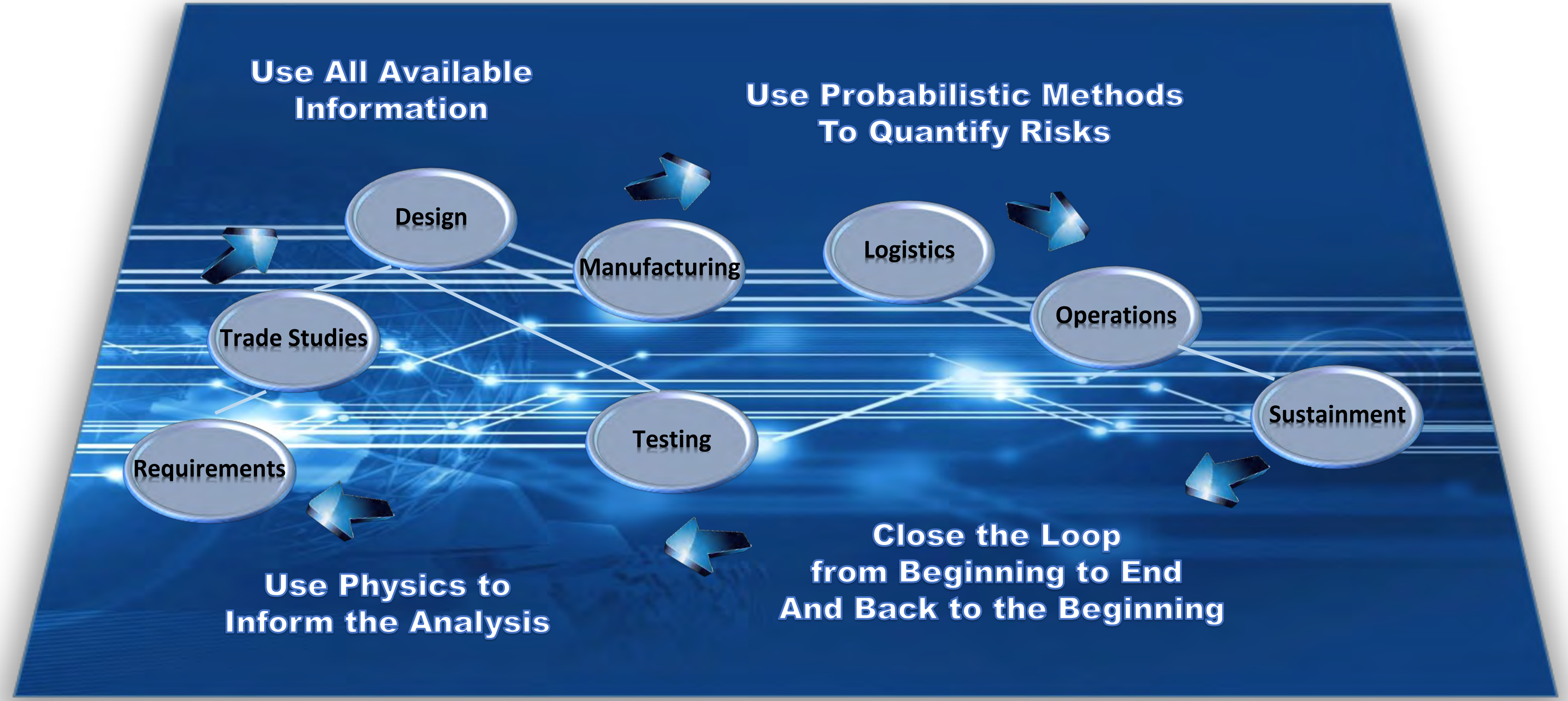


Courtesy of the Deputy Assistant Secretary of Defense Office for Systems Engineering

The interconnected infrastructure, environment, and methodology (process, methods, and tools) used to store, access, analyze, and visualize evolving systems' data and models to address the needs of the stakeholders.

Defense Acquisition Guide

Connected and Integrated Data
Digital Thread / Digital Twin



Make Informed Decisions Throughout the Lifecycle

Tenets of the Digital Thread/Digital Twin

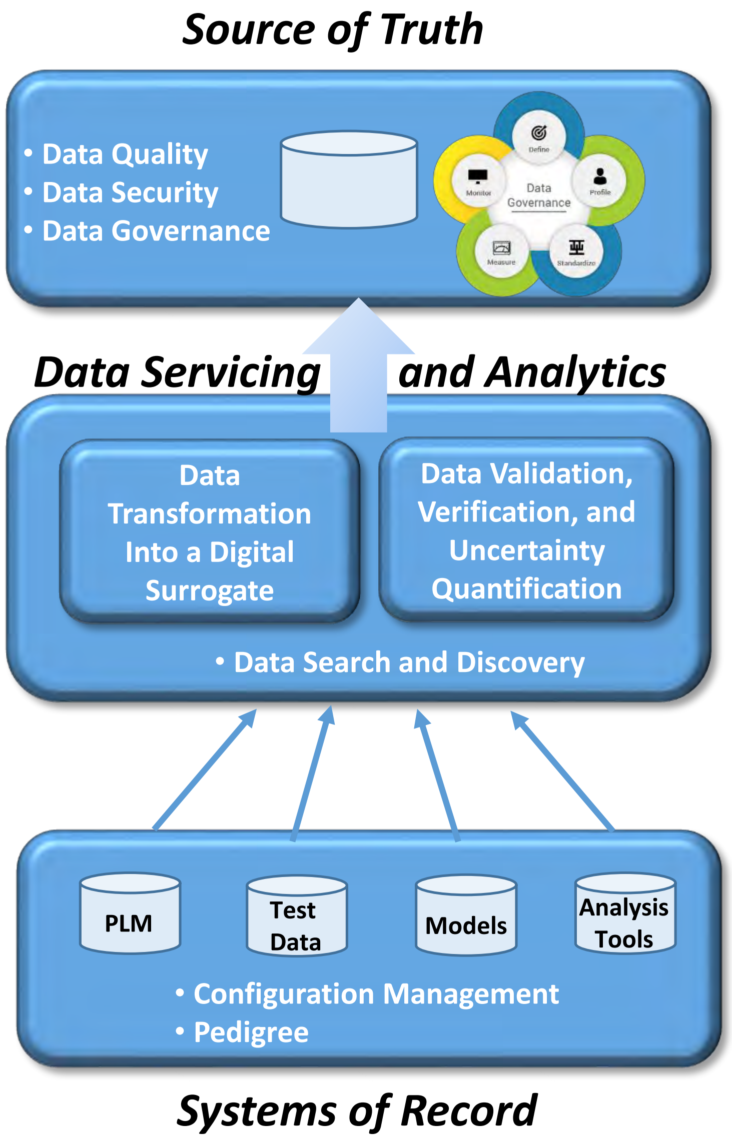
SPACE INSTITUTE

- Access to and ability to exercise data to understand performance and technical risks
- End-to-end system model – ability to transfer knowledge upstream and downstream and from program to program
- Single, authoritative digital representation of the system over the life cycle – the authoritative digital surrogate "truth source"
- Application of reduced order response surfaces and probabilistic analyses to quantify margins and uncertainties in cost and performance
- Preserve meta-data on decision processes and outcomes

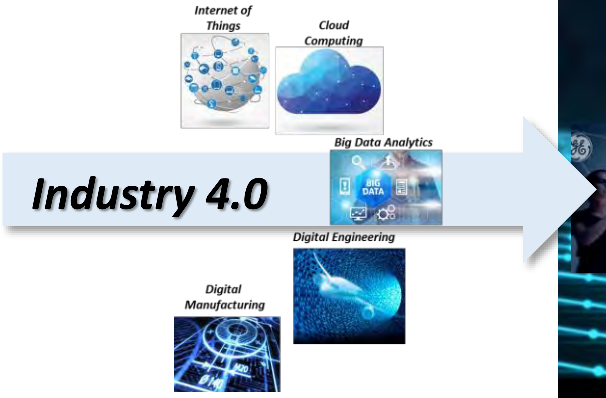
It is Not Sufficient to Just Digitize Current Processes – We Need to Reinvent Processes Leveraging the Digital Connectivity of <u>Trusted</u> Data and Knowledge

A Single, Authoritative Digital Surrogate "Truth Source"

- A technical definition declares quality of a truth source to be "the state of completeness, validity, consistency, timeliness and accuracy that makes the data appropriate for a specific use"
- System of Record (SOR) – the authoritative data source for a given element or piece of information
- Source of Truth (SOT) – <u>trusted</u> data source that gives a complete picture of the data object as a whole
- Trusted data source connotes
  - An entity authorized by a <u>governing authority</u> to develop or manage data for a specific purpose
  - Shared by all stakeholders with all equities preserved

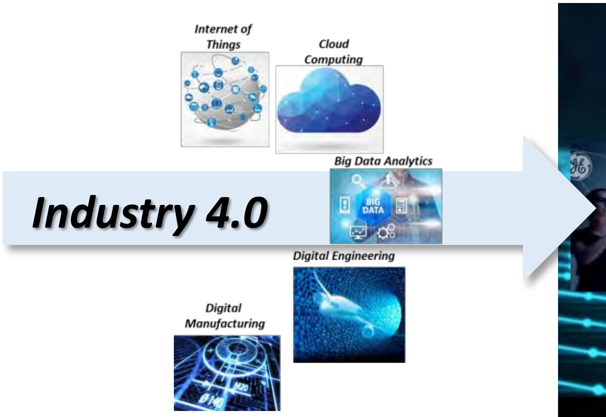


Current Industry Digital Engineering Ecosystems



- Single Owner Enterprises
- Expanding Rapidly, Significant Investments – Next Big Thing in Industry 4.0
- Internally Connected to Enterprise Business Model
- Proprietary, Competition Sensitive ***Digital*** Processes and Tools
- Early Successes in Aerospace Industry

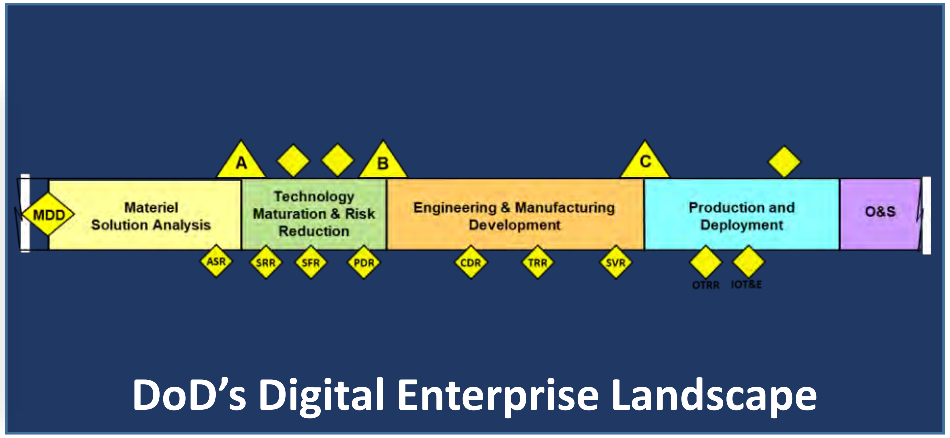
Challenges to Shaping a DoD Digital Engineering Ecosystem



- Single Owner Enterprises
- Expanding Rapidly, Significant Investments – Next Big Thing in Industry 4.0
- Internally Connected to Enterprise Business Model
- Proprietary, Competition Sensitive ***Digital*** Processes and Tools
- Early Successes in Aerospace Industry

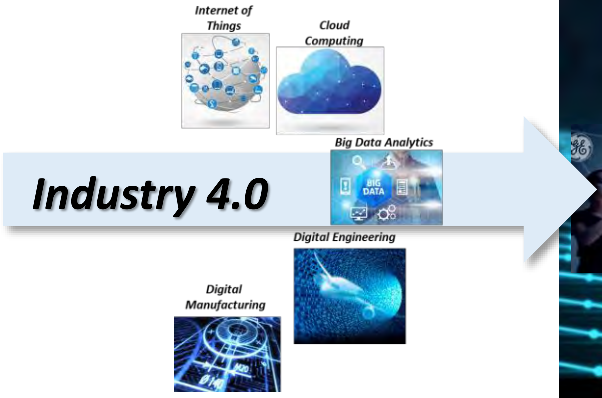
How do we build a Public / Private Partnership to create a DoD Digital Engineering Ecosystem?

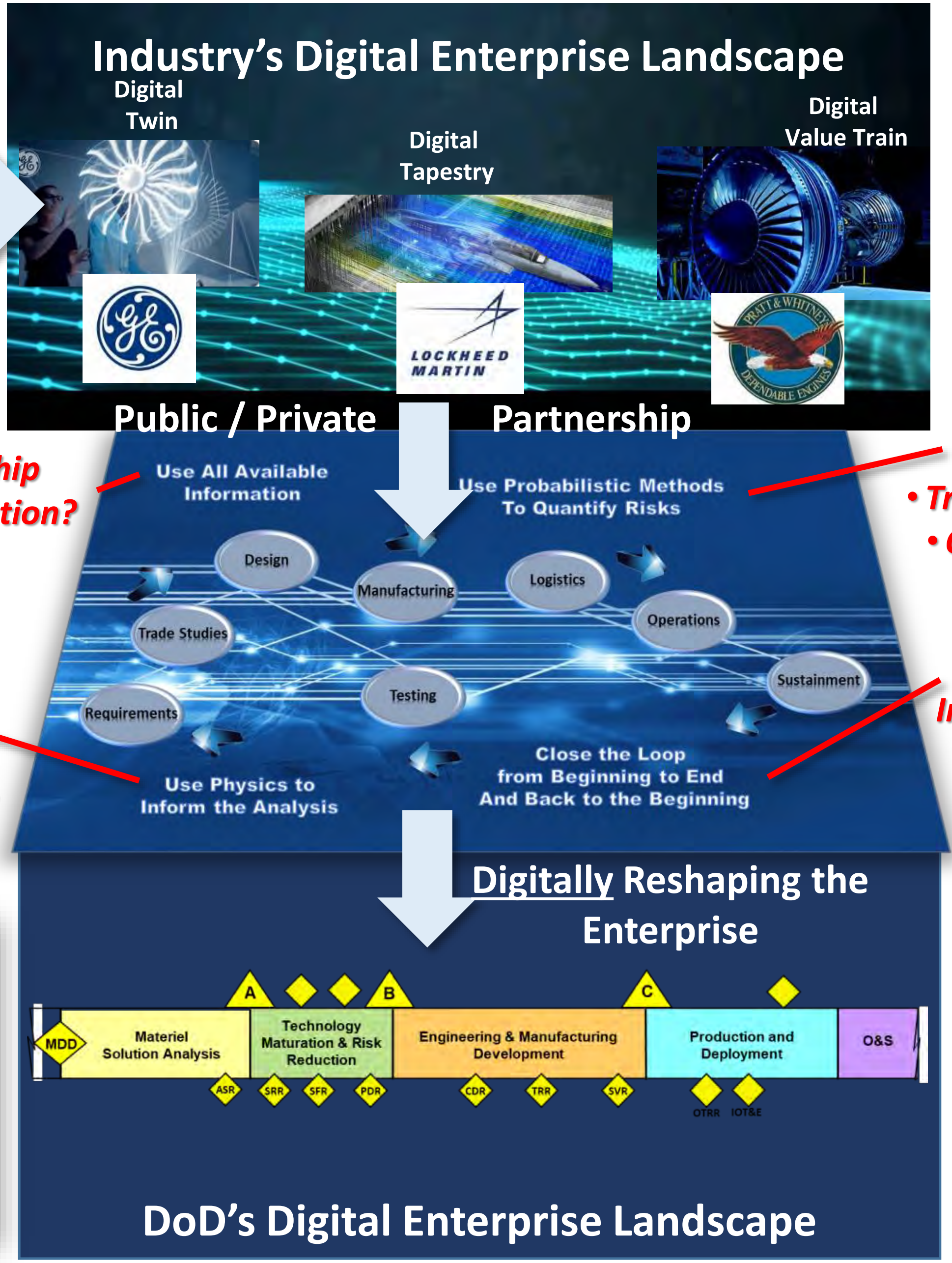
How do we shift from a positional document to a digital approach to meet the intent?



- Complex Enterprise
- Arcane, Positional, Paper-Driven, Policies and Processes Not Easily Changed to Digital Processes
- Entrenched Functional Stovepipes Not Necessarily Digitally Savvy
- No Architecture for a Digital Enterprise
- Still in Conceptual Phase – No Dedicated Funding

Challenges to Shaping the Digital Engineering Ecosystem





- Single Owner Enterprises
- Expanding Rapidly, Significant Investments – Next Big Thing in Industry 4.0
- Internally Connected to Enterprise Business Model
- Proprietary, Competition Sensitive *Digital* Processes and Tools
- Early Successes in Aerospace Industry

Source / Ownership of Needed Information?

Digital Authoritative Truth Source
- ***Trust Between Government and Industry?***
- ***Quantified Margins and Uncertainties?***

Digital Thread / Digital Twin
The Bridge

MBSE/MBE Tools
- ***Commonly Accepted Tools?***
- ***Connectivity of Models and Data?***
- ***V&V?***

Digital Connectivity Between Functional Areas?
Interfaces with IoT, Cloud Computing, Big Data Analytics?

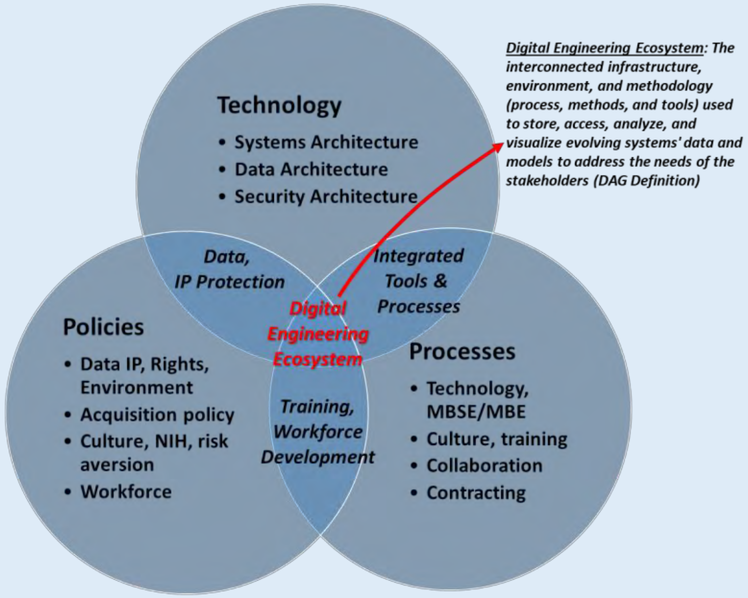
How do we shift from a positional document to a digital approach to meet the intent?

- Complex Enterprise
- Arcane, Positional, Paper-Driven, Policies and Processes Not Easily Changed to Digital Processes
- Entrenched Functional Stovepipes Not Necessarily Digitally Savvy
- No Architecture for a Digital Enterprise
- Still in Conceptual Phase – No Dedicated Funding

Digital Thread Workshops
Working the Government / Industry Interface

Workshop #1

Objective – Provide an assessment of the tools & technologies, policies & practices affected, and the barriers to establishment of a digital engineering ecosystem across AF systems



Workshop # 2

Objective - develop a concept for a Government / Industry collaborative partnership to develop the principles, practices, and concept of operations for a common Digital Engineering Ecosystem

SCOPE

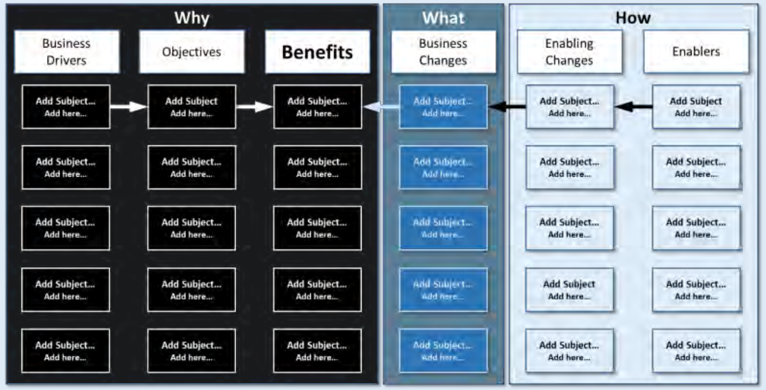
- Effect on Policy and Guidance
- Extension from Service (AF initially) to DoD to Aerospace & Defense
- Initial smaller functional scope, simple demo, expandable to the lifecycle

CONOPS

- Shape the architecture for model/data traceability from concept throughout lifecycle
- Produce modeling guide and V&V as output
- Demonstrate and mature MBSE/MBE from the start – appropriate level of detail
- Identify non-traditional process using the advantages of a digital ecosystem, e.g., a digital TEMP process
- Connections with DMDII CONOPS?

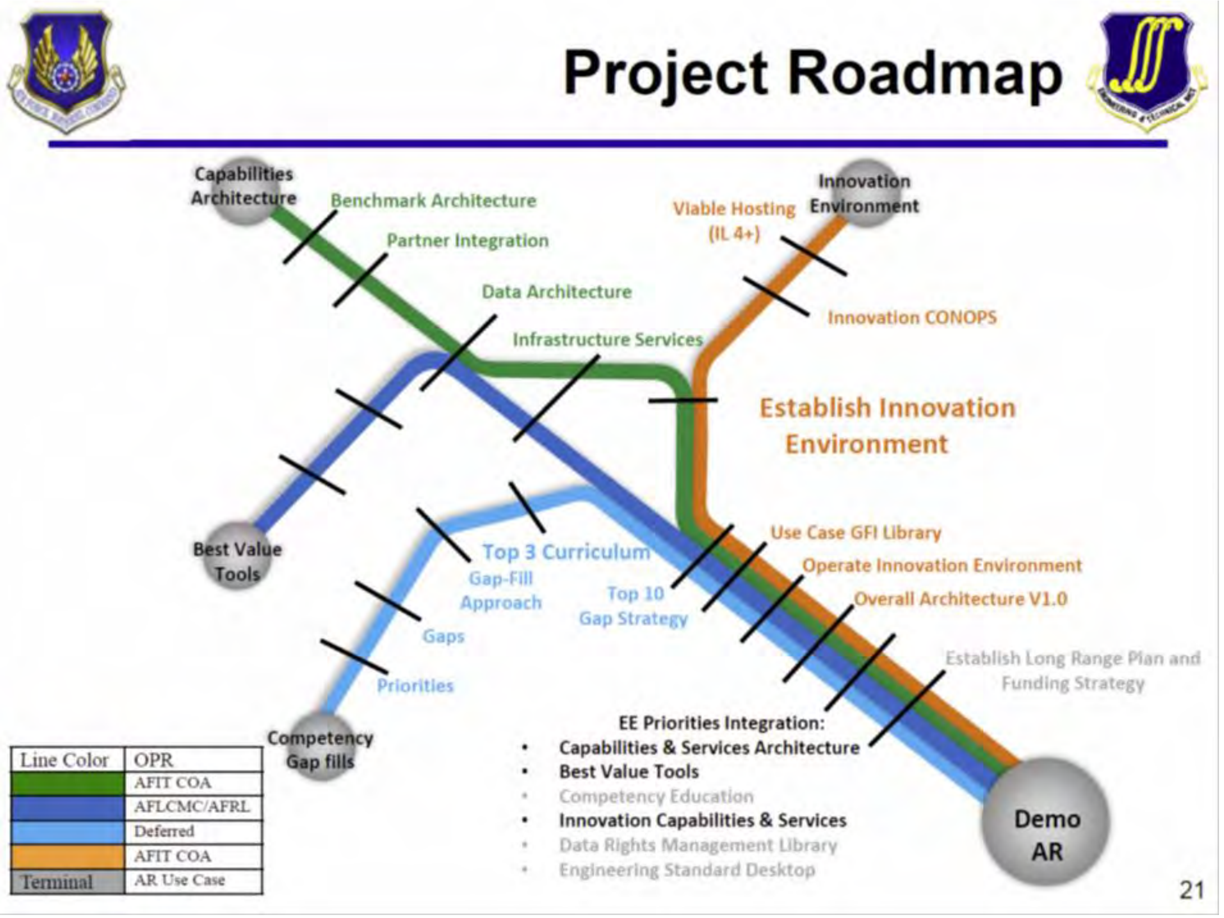
Workshop #3

Objective - develop a value proposition for implementation of a Digital Engineering Ecosystem to support applications of the Digital Thread / Digital Twin concept to improve the acquisition and sustainment of defense systems.



- IT Enablers have *__no inherent value__*
- Benefits arise when IT enables people do things *__differently.__*
- Benefits come from *__Policy and Operational Changes__*

Air Force Materiel Command Digital Ecosystem Pilot Project



Contacts:

Col Paul Harmer AFMC/EN paul.harmer@us.af.mil

Dr. Philip Hanna AFMC/ENS philip.hanna@us.af.mil

Approved for Public Release, AFMC-2017-0025

Pilot Project (year 1-2, $2M)

Sandbox / Proof of Concept Demo

Allow Tool Experimentation, Use Cases Analysis

Demo: Assistance Request (AR) requiring a modified part

- Receive AR
- Engineering to Access all historical data, current data and tools
- Perform analysis Using M&S, demonstrate CREATE value beyond S&T
- Down select to final design
- Produce (Additive Manufacturing if possible) prototype, test
- Deploy Representative Architecture to WPAFB DEATHSTAR
- Document new configuration
- Store for future use

Inform Strategy, Roadmap, Requirements, Data Needs…

Transforming to a Digital World
A Digital Test and Evaluation Master Plan (TEMP)

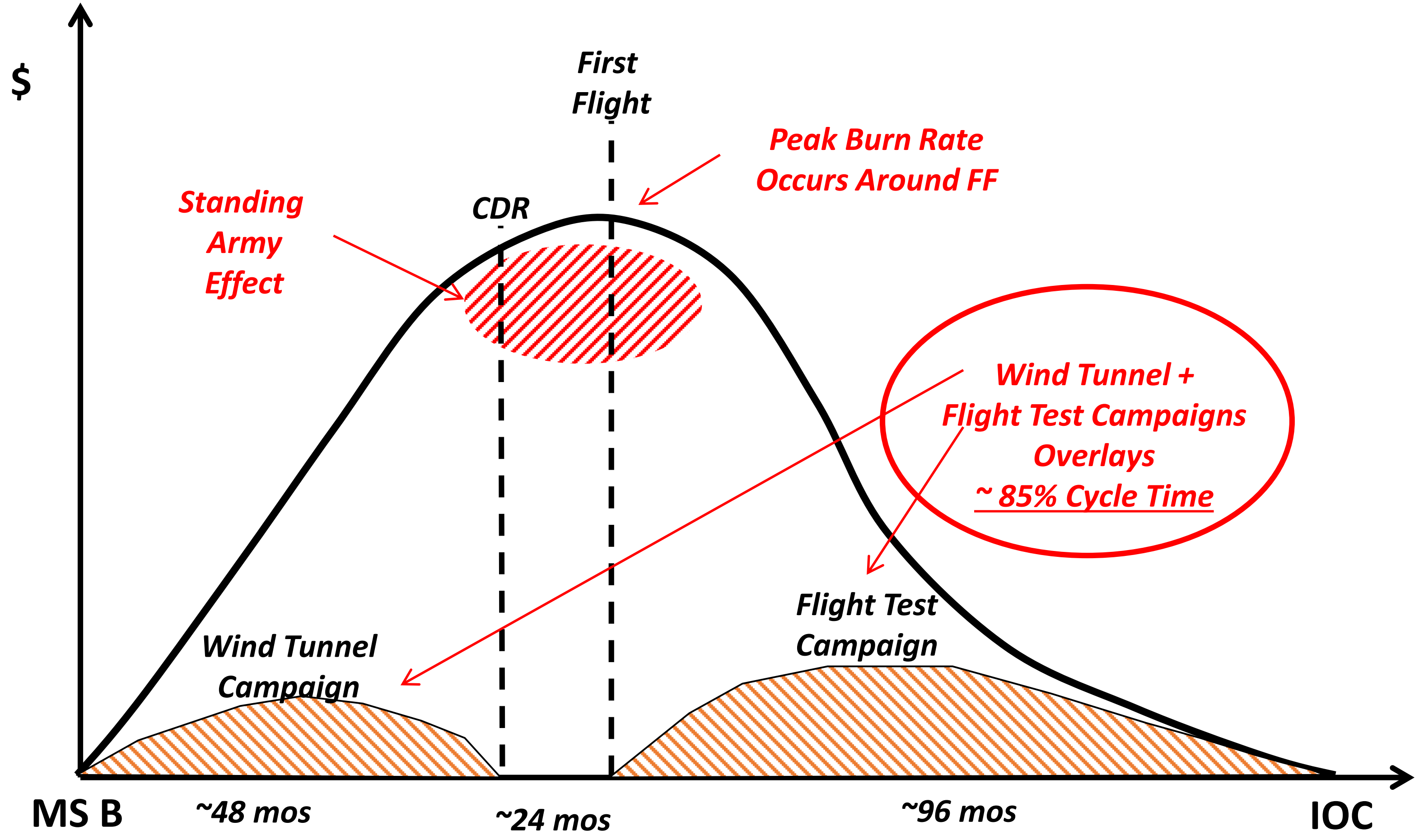
Integrated Test Team -
Stuck in a Document Centric Mode…

…or Moving to a Digitally Connected WIPT

A Digital TEMP would

- Provide a model-centric approach focused on delivering the intent of the test planning processes in 5000.02 dynamically coupled to digital Requirements
- Apply digitally preserved Systems of Record (SOR) such as
  - Capability/performance maps for MRTFB test capabilities,
  - System performance parametric sensitivities from trade studies,
  - Modeling Tools V&V, uncertainty quantification
  - Quantified epistemic and aleatory uncertainties for MRTFB test capabilities and processes
- Use early model-based authoritative digital surrogates and SORs combined with requirements and uncertainties to develop an optimum test campaign to reduce time/costs and close the design
  - Digitally complete the Developmental Evaluation Framework
    - Decisions supported
    - Knowledge Required
    - Summary and top-level objectives for evaluation, test, and modeling
    - Key resources
    - Program schedule

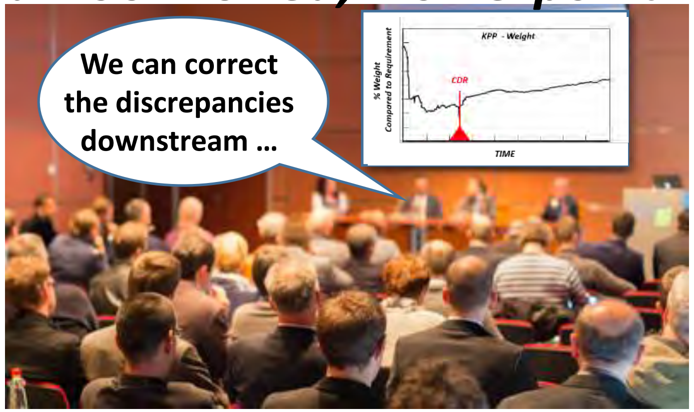
Target of Opportunity for a Digital TEMP



Use the Digital TEMP to Either Reduce the Resources and Cycle Time for DT&E and/or Increase the Probability of Design Closure at CDR

A Digital Critical Design Review (CDR)

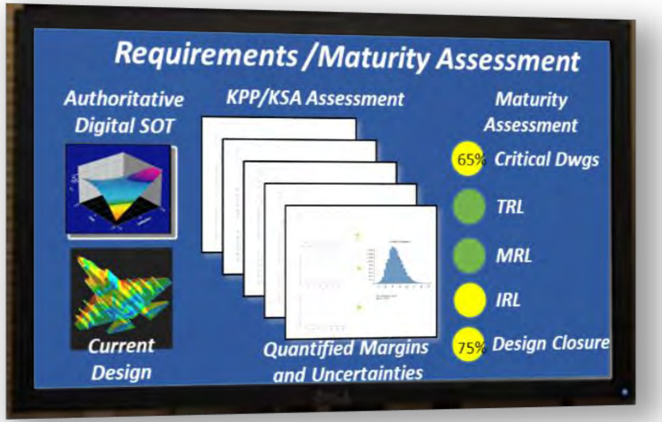
Moving From a Calendar-Driven, Ballroom-Sized, Powerpoint Event . . .



…to a Digitally Current, Quantified Risk Assessment to Support Better Decision Making

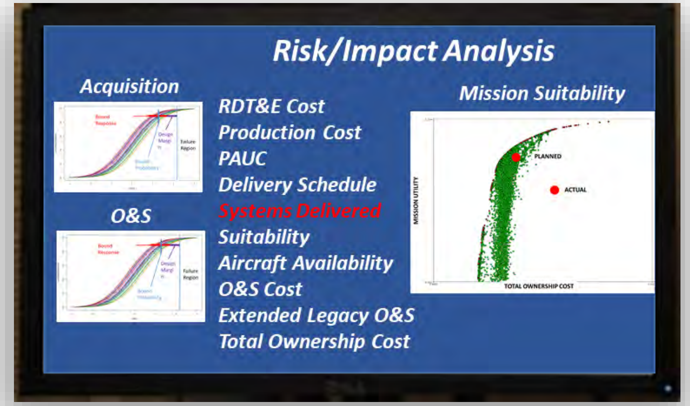
- **See** – bring all authoritative digital surrogate truth sources to understand the performance of the system at CDR vs requirements **– target 90% confidence level in design closure**
- **Think** – use data analytics/probabilistic analyses to assess risk, impact on military utility, and total ownership cost of any requirements gaps
- **Do** – analyze multiple decision scenarios to select the best value course of action including data-driven mitigation strategies

See



Use All Available Information

Think



Use Probabilistic Analysis to Inform

Do

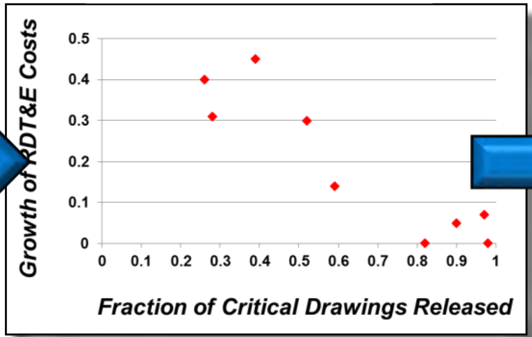
Select Best Value COA

Risk = Uncertainty with Consequences

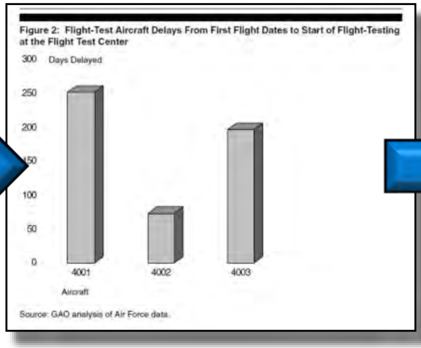
Value of a Digital CDR
Connecting Critical Decisions to Lifecycle Value

Previous Knowledge
- *Requirements Volatility*
- *% Design Closure at PDR*
- *TRL at MS B*

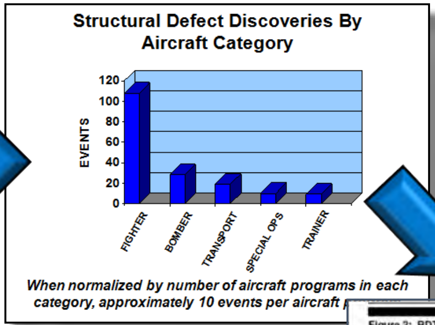
Close the Design at CDR…



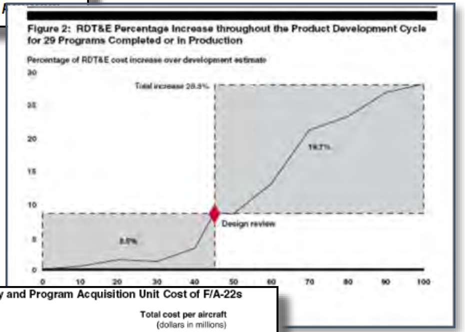
Deliver First Flight Vehicle On Time…



Minimize Late Defects



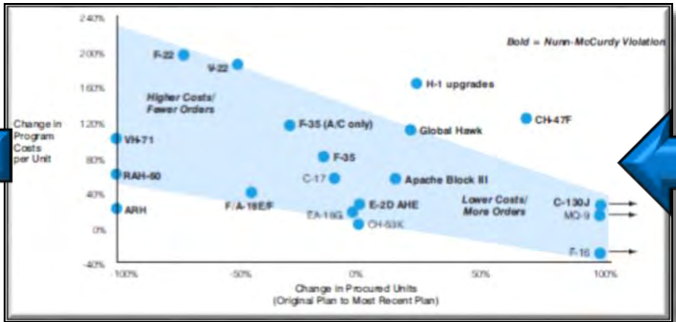
Minimize RDT&E Overruns

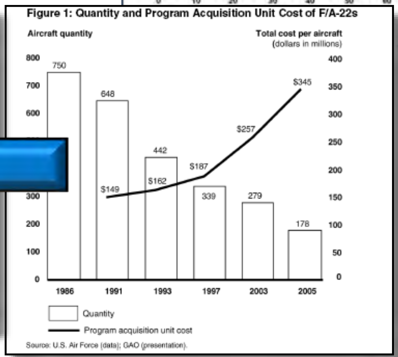


It All Starts with Quantified Performance Margins and Uncertainty Assessments at CDR

Maximize RDT&E Impact on Lifecycle Value

$$VALUE \equiv \frac{AIRCRAFT\ AVAILABLE}{PV(TOTAL\ OWNERSHIP\ COST)}$$





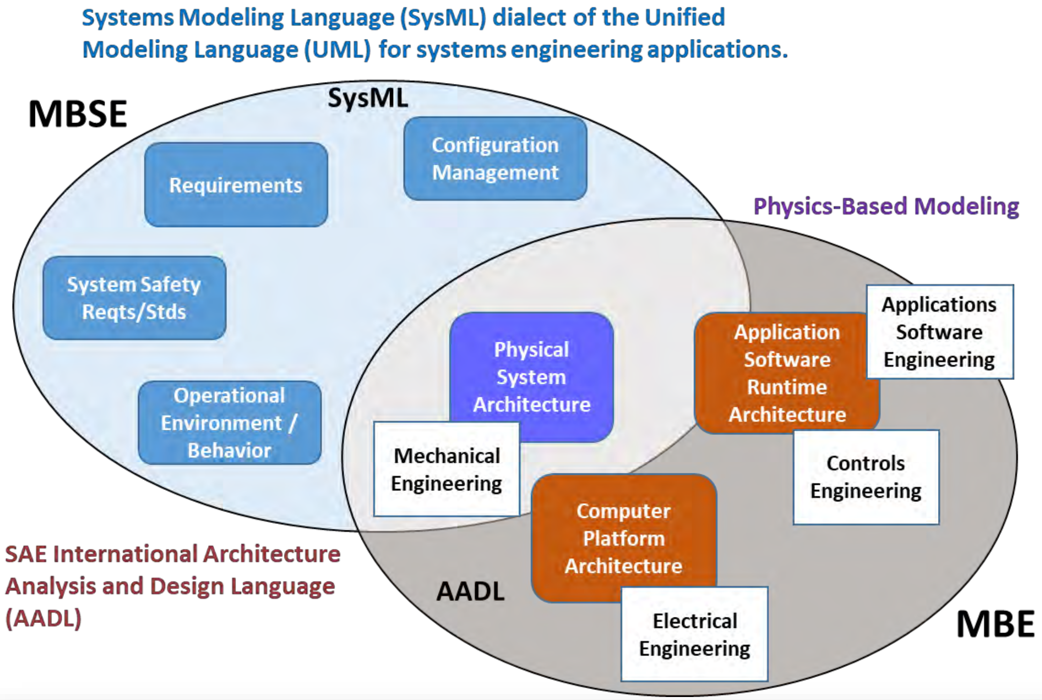
Deliver Contracted Number of Systems on Time/Cost

Consequence of implementing DODI 5000.02 as a <u>positional</u> vice an <u>intentional</u> process has lead to a cascade effect of unconnected decisions not supported by quantified risk assessments

The Next Generation of Digital Systems Engineers Training/Education

- Trained in Digital Modeling
  - Systems Modeling Language (sysML)
  - Architecture Analysis and Design Language (SAE AADL)
  - Physic-Based Modeling
  - Uncertainty Quantification / Risk Analysis
  - Systems Thinking / Systems Dynamics
- Translate traditional Case Study reports to scenario emulators for a digital engineering ecosystem
- Train on Systems Engineering / Program Manager "Flight Simulators" with real world consequences for decisions made
- Use the Digital Engineering Ecosystem to "See-Think-Do"
- Capstone projects focused on streamlining digital processes to increase value

Move from a Build-Test SE paradigm to a new Integrate-Analyze-Build SE Paradigm



Early SE analysis of the total system including the architecture for software intensive systems will be essential for cyber and autonomous systems

Summary

- The Digital Revolution is reshaping the development, fielding, and sustainment of aerospace and defense systems
- The DoD is at the front end of a significant journey toward a Digital Engineering transformation mandated by the need to maintain technical dominance over adversaries
- The Keys to Success encompass
  - Connecting tools and technologies to support a Digital Engineering Ecosystem
  - Establishing policies to enable a public/private partnership while respecting data rights and intellectual property
  - Moving from positional document-centric to fully digital, model-based, intentional processes
  - Educating and training Systems Engineers and Program Managers to lead the Digital Revolution

The Value of the Digital Revolution to the Development, Operation, and Sustainment of DoD Systems Seems Self-Evident But Must Be Proven at Each Stage of Implementation

Dr. Edward M. Kraft

Associate Executive Director for Research

University of Tennessee Space Institute

411 B. H. Goethert Parkway

Tullahoma, TN 37388-9700

ekraft@utsi.edu

Office 931-393-7284

Mobile 931-434-2302

Model-Centric Decision Making:
Insights from an Expert Interview Study

Donna H. Rhodes
E. Shane German
Massachusetts Institute Of Technology
rhodes@mit.edu
617.324.0473

Why is Human-Model Interactivity Important to the Future of Model-Centric Engineering?

Addressing complex systems problems requires human intelligence and use of models

Models are useful for generating data and analytics that can be used in human decision making

Human cognitive limits drive necessity of using models and computational resources

Models can “automatically” perform certain human functions but humans provide context: under which conditions is the model appropriate and useful?

While progress has been made on model-based engineering

… there has been relatively little investigation of the complexities of **human-model interaction**

Interview-Based Study

model-centric decision making

- *MIT and DoD IRB Approved*
- *Investigators: German and Rhodes (PI)*

Exploratory study to gain insight into how various types of decision makers interact with and perceive models (2016 - 2017)

Motivated by increasing need for individuals and teams to **make decisions using models** and model-generated information

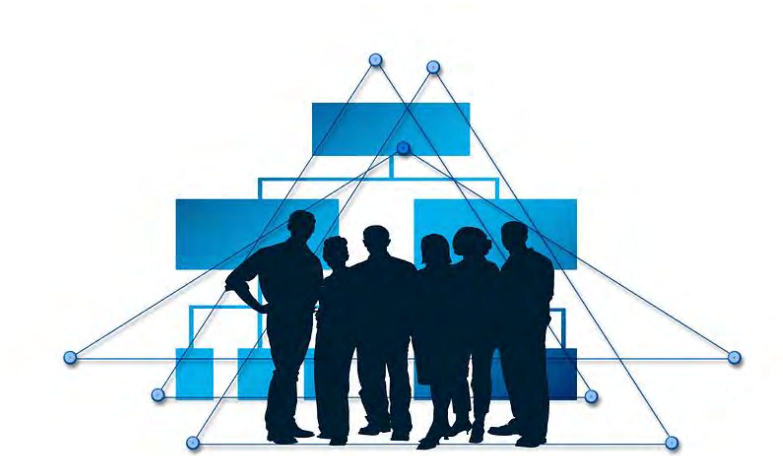
While anecdotal stories of success and failure exist, **empirical studies are needed to truly understand** the many facets of human decision-making in model-centric engineering

Resulted in insights regarding **how decision makers build trust in models and to what degree models are used to make decisions** that may inform current/future practice, and areas for more extensive study

German, E.S. and Rhodes, D.H., "Model-centric decision-making: exploring decision-maker trust and perception of models" 15th Conference on Systems Engineering Research, 2017

Study findings (unordered)

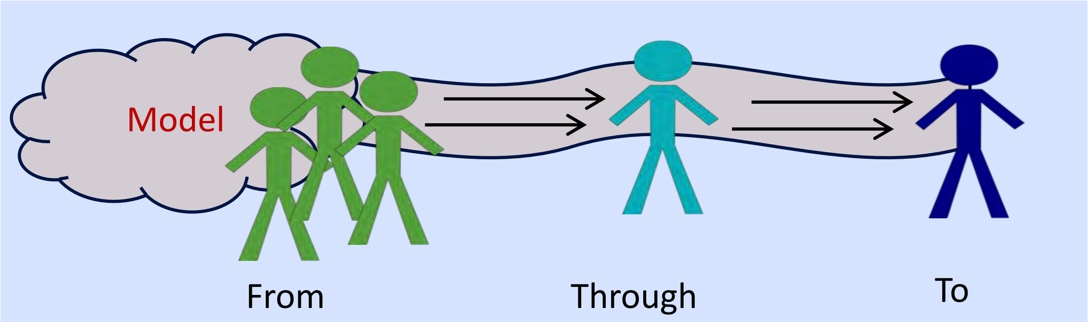
Three actor decision flow
Importance of intercommunication
Understanding of assumptions and uncertainty
Technological and social factors influencing trust
Importance of model-related documentation
Need for model pedigree
Using models as primary versus supplementary
Non-advocate role in reviews
Transparency and trust
Model investment bias and confirmation bias
Factors limiting model-centric decisions
Real-time interaction with models
Viewing humans as endogenous



30 recognized experts

Study Finding

Three actor decision flow

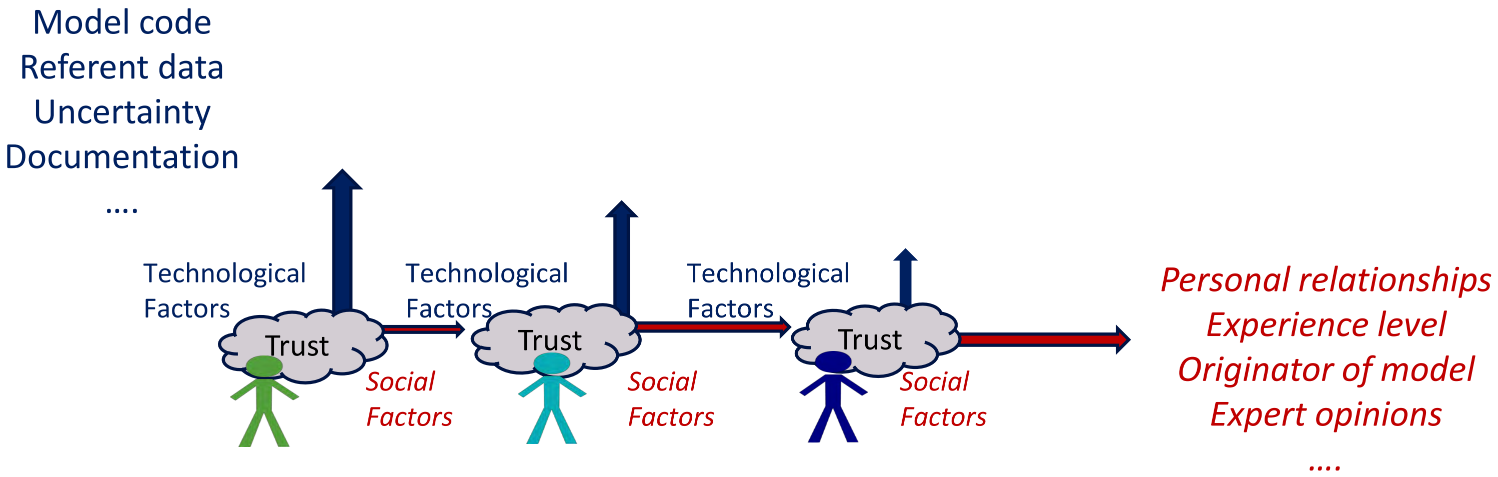


The data suggests that as actors move further along the flow of information and have less time and ability to personally investigate a model and build their own trust in the model, their trust instead shifts more onto their people to investigate the model for them.

… the trust for ultimate decision-maker is “implicitly on the models, but explicitly on the people.”

Study Finding

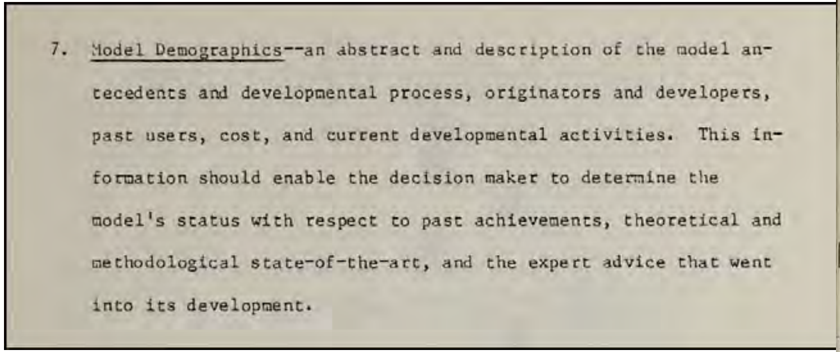
Technological and social factors influencing trust



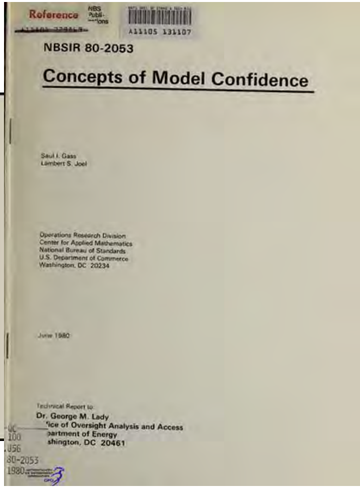
Study Finding

Model pedigree

The models generated by various actors and used in various decision-making situations are vast, and this generation and use of models produces information that may influence decision-maker trust in using these models in other situations



7. Model Demographics--an abstract and description of the model antecedents and developmental process, originators and developers, past users, cost, and current developmental activities. This information should enable the decision maker to determine the model's status with respect to past achievements, theoretical and methodological state-of-the-art, and the expert advice that went into its development.



NBSIR 80-2053

Concepts of Model Confidence

Saul I. Gass
Lambert S. Joel

Operations Research Division
Center for Applied Mathematics
National Bureau of Standards
U.S. Department of Commerce
Washington, DC 20234

June 1980

Technical Report to
Dr. George M. Lady
ffice of Oversight Analysis and Access
partment of Energy
shington, DC 20461

Study Finding

Model transparency

Varied opinions on how much transparency others need/want

Everyone cares about transparency
…but personally may not need to
“see the code”, rely on others to do that

I like to be able to get way down in my code…to see the algorithms doing the calculation.

I never look at the lowest levels…I have associates working on that.

If I have somebody who I trust, as I know their expertise, background … I will trust their model

Study Finding

Factors limiting effective model-centric decisions

MODEL	HUMAN		
Data availability	Talent of people	Time and money	Educated leadership
Data quality	Inertia to change	Team agreement	Lack of desire to understand
Model complexity	Communication barriers	Skill level	Bad past experiences
Inadequate methods	Changing preferences of decision-makers	Ability to socialize models	Generational differences
Lack of transparency and documentation	Unwillingness to share models or information	Lack of trust/fear of the unknown	Organizational differences
Interactivity with models		Lack of understanding	

Study Finding

Viewing humans as endogenous

Understanding the behavior of a model-centric enterprise requires viewing human actors as endogenous constituents

- Models influence decision maker behavior
- Human interaction with models influences how models are conceived and used

Endogenous point of view (J. Forrester)

Formulating a model of a system should start with the question "Where is the boundary, that encompasses the smallest number of components, within which the dynamic behavior under study is generated?" (G.P. Richardson , 2011)

Six categories
Human-model interaction heuristics

1. **designing models for human use**
2. **using models in decision-making**
3. sociotechnical considerations
4. **context and assumptions**
5. transparency and trust
6. **mitigating biases**

Heuristics encapsulate insights and strategies discovered by experts though experience

Experts apply these intuitively

Heuristics can be used to educate and guide practice of novices, as they learn through their own experiences

Validated heuristics inform the development of policy and practices

Selected Heuristic

Designing models for human use

Humans should not be forced to adapt to models, rather, models should be designed for humans

Evolving technology enables more complex and capable models but may not result in increased effectiveness if humans are not appropriately considered

Humans have cognitive and perceptual limitations that limit amount and types of information they can effectively comprehend and use to make decisions

Designing for humans requires understanding their capabilities and limitations so that the model intelligence can extend the overall system intelligence

Selected Heuristic

Using models in decision making

Models do not have agency -- the ultimate responsibility for decisions must be upon humans

Ultimate decision-making authorities are people, and blame cannot be placed upon models for poor decisions

Model developers, users, and decision-makers have the responsibility to ensure that models are properly understood and appropriately used

Individuals should be aware of the potential for improperly diffusing responsibilities for decisions upon models

Policies should clearly establish the responsibilities for which individuals are held accountable in model-centric enterprises

Selected Heuristic

Context and assumptions

Models are created for specific reasons and contexts, and those assumptions fundamentally bound a model's applicability

A model may be insightful and valuable within one problem context, but the assumptions built into the model may not be valid within some other context

Evaluating a model's applicability should not just consider whether it has been validated, but in what contexts it has been validated

Using a model outside of its inherent bounds may lead to model results that are inappropriate for the problem under consideration

Selected Heuristic

Mitigating biases

Increasing speed of decision-making implies a decrease in time spent analyzing a problem that in turn increases chance of biased judgment

Model-centric environments enable interaction to build intuition and speed decision-making, but may increase bias

Complex problems may require focused time and attention to fully understand and develop an accurate mental model of the situation

While faster decisions are desired if effective, speed itself may set people up for failure by encouraging them to rely upon fast and intuitive, yet bias-susceptible, judgment… rather than more cognitively demanding rational and analytical thought processes

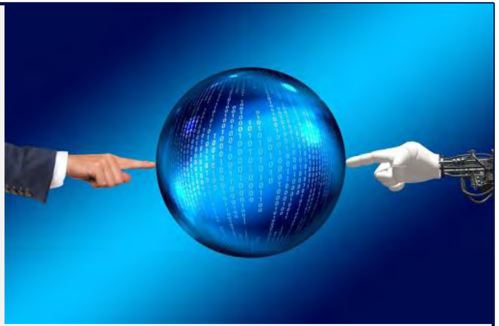
Implications for practice and research

Empirical data (vs anecdotal evidence) on human-model interaction “state of practice” (based on 30 expert interviews)

Heuristics encapsulate human-model interaction strategies for use in education, training and practice guidelines

Confirms need for further investigation ….

- Capture patterns of why, when and how various stakeholders interact with models
- Understand most effective means for interaction
- Determine where human interaction is preferred over augmented intelligence
- Inform model-centric enterprise transformation and new leadership roles



Questions?

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Department of Defense.

Contact:
Dr. Donna H. Rhodes

Massachusetts Institute of Technology

rhodes@mit.edu

617.324.0473

seari.mit.edu

SYSTEMS ENGINEERING Research Center

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

Stevens Institute of Technology & Systems Engineering Research Center (SERC)

Model Centric Engineering Enabling a New Operational Paradigm for Acquisition

Presented by:

Dr. Mark R. Blackburn (PI)

Dr. Mary Bone

Dr. Dinesh Verma

With Contributing Sponsors (NAVAIR, ARDEC, DASD(SE))

With Contributing Researchers (RT-48, 118, 141, 157, 168, 170, 176)

October 25, 2017

Copyright and Disclaimer

Certain commercial software products are identified in this material. These products were used only for demonstration purposes. This use does not imply approval or endorsement by Stevens, SERC, NAVAIR, or ARDEC nor does it imply these products are necessarily the best available for the purpose. Other product names, company names, images, or names of platforms referenced herein may be trademarks or registered trademarks of their respective companies, and they are used for identification purposes only.

Outline

- Historical perspective and resources
- Systems Engineering Transformation (SET) Framework for a new operational paradigm between government and industry
- Surrogate pilot experiment(s) for ***Executing*** the SET Framework
  - —Research emphasis
  - —Methodology for modularizing models
  - —Integrated Modeling Environment and approach to demonstrate Authoritative Source of Truth
  - —“Specification generation” from models

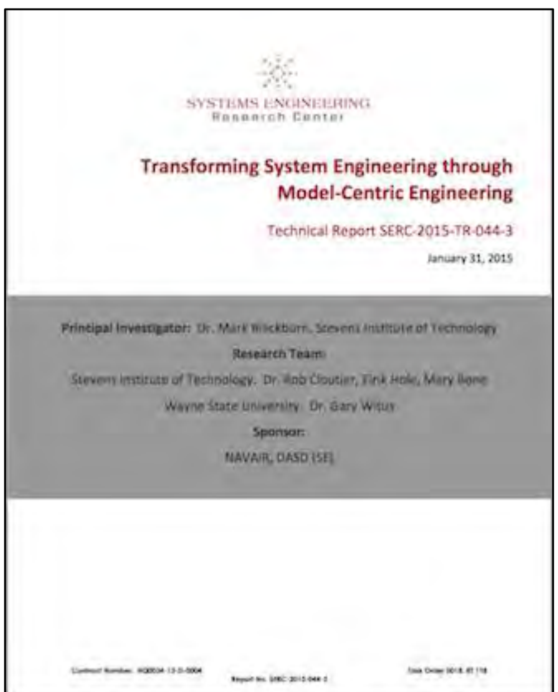
NAVAIR is Interested in Sharing Concept and Getting Feedback

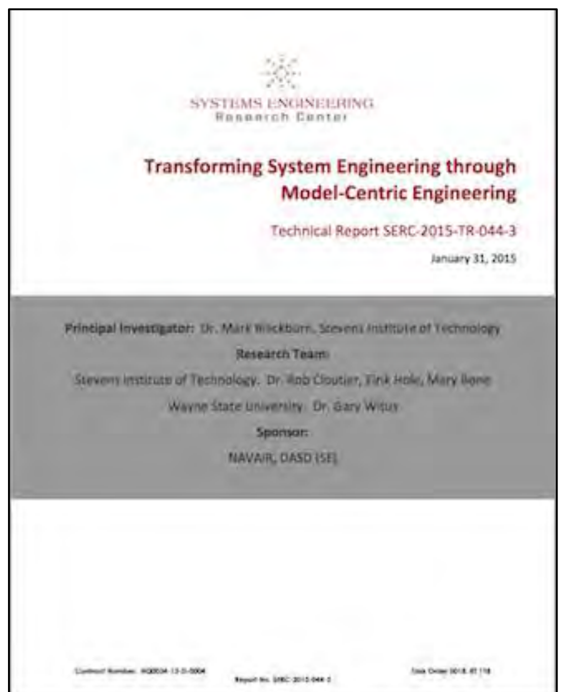
SYSTEMS ENGINEERING
Research Center

Historical Perspectives and Resources

- Resources
  - Technical reports link: http://www.sercuarc.org/researcher-profile/mark-blackburn/
  - Comprehensive briefing: http://www.sercuarc.org/publications-papers/presentation-systems-engineering-transformation-through-model-centric-engineering-past-why-present-what-and-future-how/

NAVAIR: RT-141 Phase I Summary	NAVAIR: RT-157 Phase II – SET Initiated	ARDEC: RT-168 Synergistic





SYSTEMS ENGINEERING
Research Center

Research Tasks and Collaborator Network

RT-48
- Mark Blackburn (PI), Stevens
- Rob Cloutier (Co-PI) - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-118
- Mark Blackburn (PI), Stevens
- Rob Cloutier - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-141
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Gary Witus – Wayne State

RT-157
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Roger Blake - Stevens
- Mark Austin – Univ. Maryland
- Leonard Petnga – Univ. of Maryland

RT-170
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Deva Henry - Stevens
- Paul Grogan - Stevens
- Steven Hoffenson - Stevens
- Mark Austin – Univ. of Maryland
- Leonard Petnga – Univ. of Maryland
- Maria Coelho (Grad) – Univ. of Maryland
- Russell Peak – Georgia Tech.
- Stephen Edwards – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.

RT-168 – Phase I & II
- Mark Blackburn (PI), Stevens
- Dinesh Verma (Co-PI) – Stevens
- Ralph Giffin
- Roger Blake - Stevens
- Mary Bone – Stevens
- Andrew Dawson – Stevens (Phase I)
- John Dzielski, Stevens
- Paul Grogan - Stevens
- Deva Henry – Stevens (Phase I)
- Bob Hathaway - Stevens
- Steven Hoffenson - Stevens
- Eirik Hole - Stevens
- Roger Jones – Stevens
- Benjamine Kruse - Stevens
- Jeff McDonald – Stevens (Phase I)
- Kishore Pochiraju – Stevens
- Chris Snyder - Stevens
- Gregg Vesonder – Stevens (Phase I)
- Lu Xiao – Stevens (Phase I)
- Brian Chell (Grad) – Stevens
- Luigi Ballarinni (Grad) – Stevens
- Harsh Kevadia (Grad) – Stevens
- Kunal Batra (Grad) – Stevens
- Khushali Dave (Grad) – Stevens
- Rob Cloutier – Visiting Professor
- Robin Dillon-Merrill – Georgetown Univ.
- Ian Grosse – Univ. of Massachucetts
- Tom Hagedorn – Univ. of Massachusetts
- Todd Richmond – Univ. of Southern California (Phase I)
- Edgar Evangelista – Univ. of Southern California (Phase I)

RT-176
- Kristin Giammaro (PI) – NPS
- Ron Carlson (Co-PI), NPS
- Mark Blackburn (Co-PI), Stevens
- Mikhail Auguston, NPS
- Rama Gehris, NPS
- Marianna Jones, NPS
- Chris Wolfgeher, NPS
- Gary Parker, NPS

Research Phase I: Model Based System Engineering (MBSE) versus Model-Centric Engineering (MCE)

- Over 30 organizational discussions "**tell us about most advanced and holistic approach**…":
  - —Model-Based Engineering (MBE), Integrated Model-Centric Engineering, Interactive Model-Centric Systems Engineering (IMCSE), Model-Driven Development, Model-Driven Engineering (MDE), and even Model-Based Enterprise, which brings in more focus on manufacturability
- **MCE** characterizes the goal of integrating different model types with simulations, surrogates, systems and components at different levels of abstraction and fidelity across discipline throughout the lifecycle with manufacturability constraints
- SERC Research Supports **Digital Engineering** (DE) Thrust by DoD:
  - —***An integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support lifecycle activities from concept through disposal***

Phase II: Systems Engineering Transformation Initiated at NAVAIR

- Organizations (with a few exceptions) were unwilling to share quantitative data, however
- Qualitative data in the aggregate suggests that **MCE technologies and methods are advancing and adoption is accelerating**

NAVAIR Executive Leadership Response:

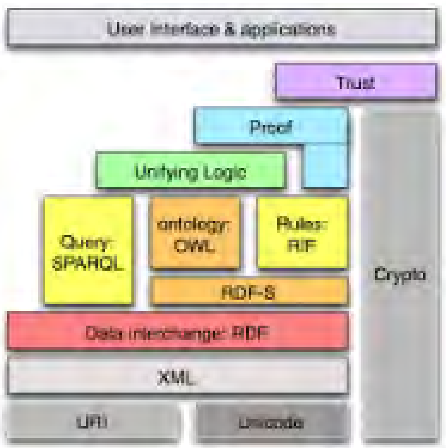
- NAVAIR must move quickly to keep pace with other organizations that have adopted MCE
- NAVAIR must transform in order to perform effective oversight of primes that are using modern modeling methods for system development

March 2016: Change of Command has Accelerated the Systems Engineering Transformation and Broadened the Scope

Current Research Trusts Investigated in Evolving Pilots

SYSTEMS ENGINEERING
Research Center

Semantic Web Technologies



Enforces **Modeling Methods**

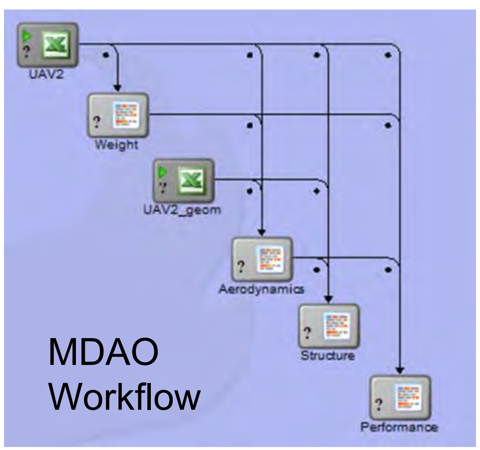
Underlying technologies for reasoning about completeness and consistency **Across Domains** in modeling tool agnostic way

Modeling Methodologies

Guides proper usage to ensure **Model Integrity** (trust in model results) for decision making

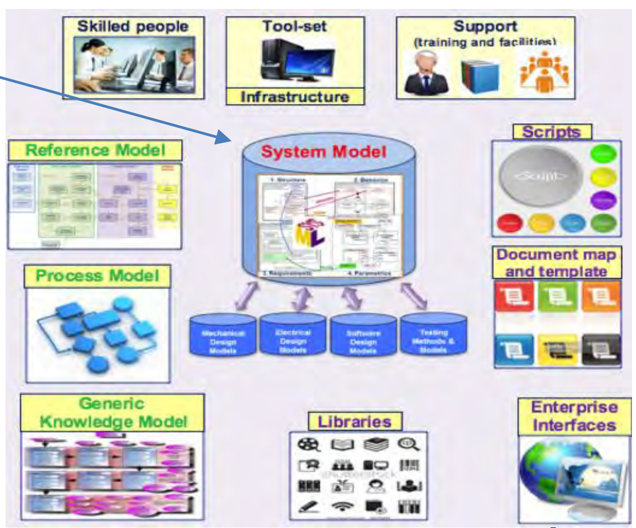
Digital System Model:
Single Source of Truth
(*authoritative source of truth*)

Multidisciplinary Design, Analysis and Optimization MDAO



Provides optimization analysis **Across Domains** to support KPP and alternatives trades at mission, system, & subsystem levels

Integrated Modeling Environment

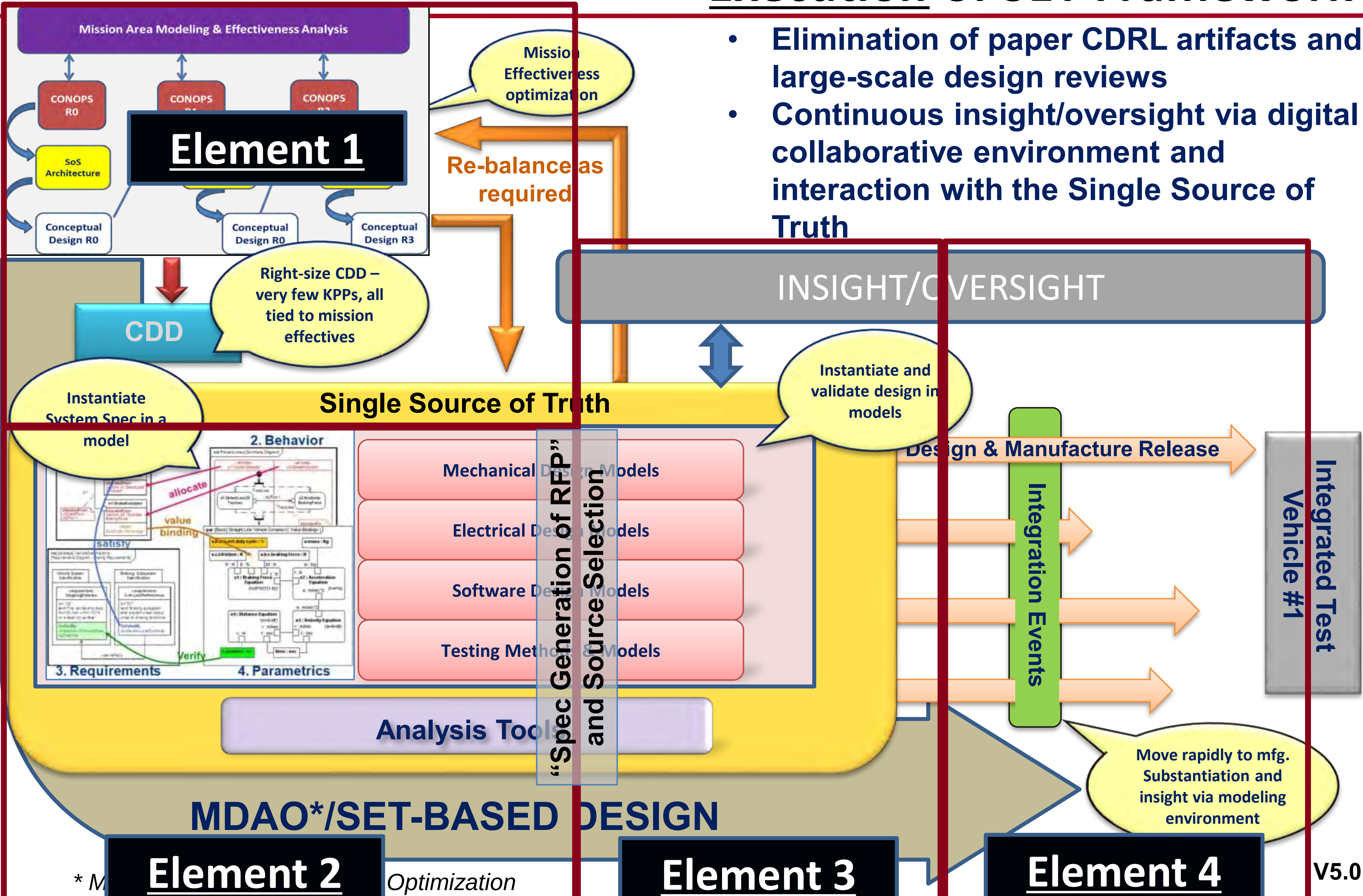


SERC 168/170.

SYSTEMS ENGINEERING
Research Center

Surrogate Pilot focus is on *Execution* of SET Framework

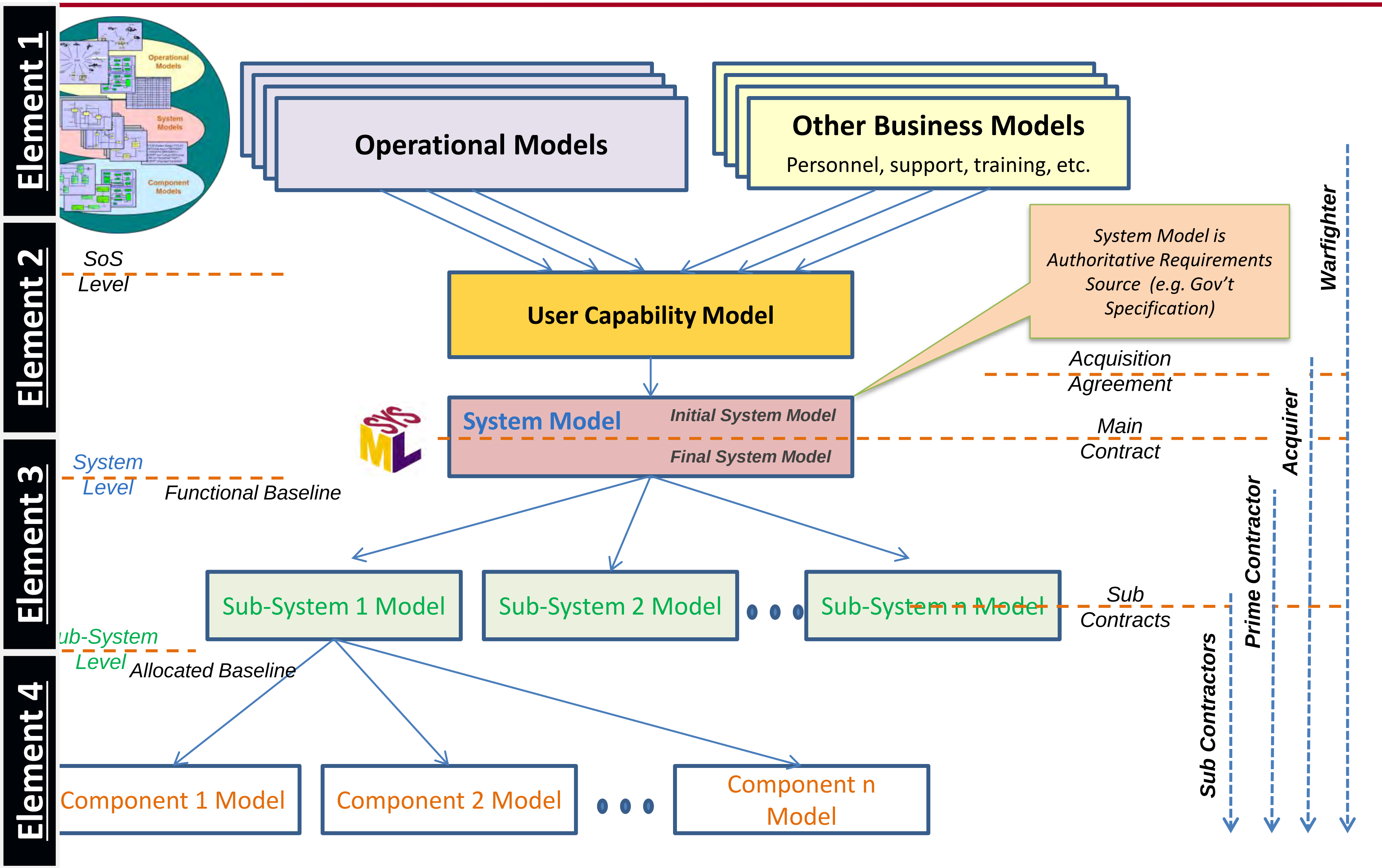
- **Elimination of paper CDRL artifacts and large-scale design reviews**
- **Continuous insight/oversight via digital collaborative environment and interaction with the Single Source of Truth**



Surrogate Pilot Overview

- Mission: Collaboration between Government and Industry in Model-based Acquisition under SET Framework
- Goal: Execute SET Framework to Assess, Refine, and Understand a New Paradigm for Collaboration in Authoritative Source of Truth (AST)
- Objectives (non exhaustive):
  - Formalize experiment to answer questions about executing SET framework using Surrogate Contractor (SC)
  - ”Government team” creates mission, system (& other) models, “generates specification/RFP,” & provides acquisition models to SC as Government Furnished Information (GFI)
  - SC refines GFI reflects corrections/innovations with physical allocation views with multi-physics-based Initial Balanced Design
  - Simulate continuous virtual reviews and derive new objective measures for assessing maturing design in AST
  - Demonstrate visualizations for real-time collaboration in AST
  - Demonstrate and document methods applied
  - Investigate challenging areas and research topics in series of pilots

Formalizing the Use of Models…
Creating a Digital Thread…

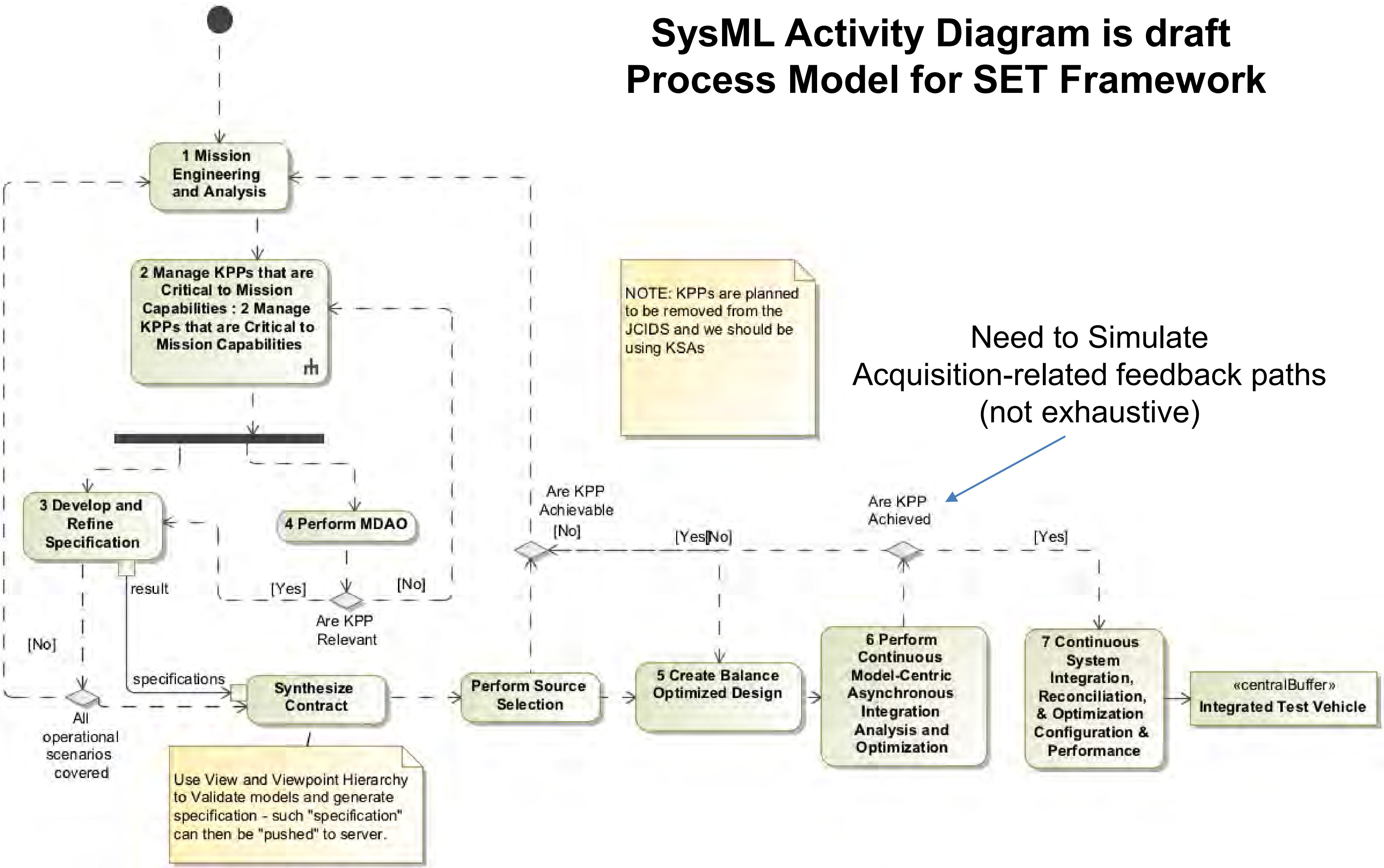


Example of Surrogate Questions (not exhaustive)

- Learning about new operational paradigm between government and industry in the **Execution** the SET Framework (NOT an air vehicle design)
- We are concerned with interactions (non-exhaustive):
  - Simulating prior to contract award (now)
  - Formalization of a “specification” for “Request for Proposal (RFP)” and methods for providing models to contractor
  - Simulating “Execution” of Oversight / Insight in AST per SET Framework for real-time collaboration in heterogeneous environments
  - **Simulating feedback back to mission engineering caused by specified objectives for unachievable Key Performance Parameters (KPP)**
  - Objective measures for evaluating evolving design maturity, with the reduction of risk
  - Simulating approach for “faults in specification/model” detected after contract award
  - Simulating source selection – desirably as a dynamic simulations and V&V
  - Working with contracts/legal to get agreement on what a “specification” would be
  - Methods for modularizing model used to “generate specification”
  - How will we use the Systems Engineering Technical Review (SETR) guide and checklist that NAVAIR uses? And, how will we make recommendations for its evolution
  - Use of Multidisciplinary Design, Analysis and Optimization (MDAO) at mission, systems, and subsystems (by surrogate contractor)

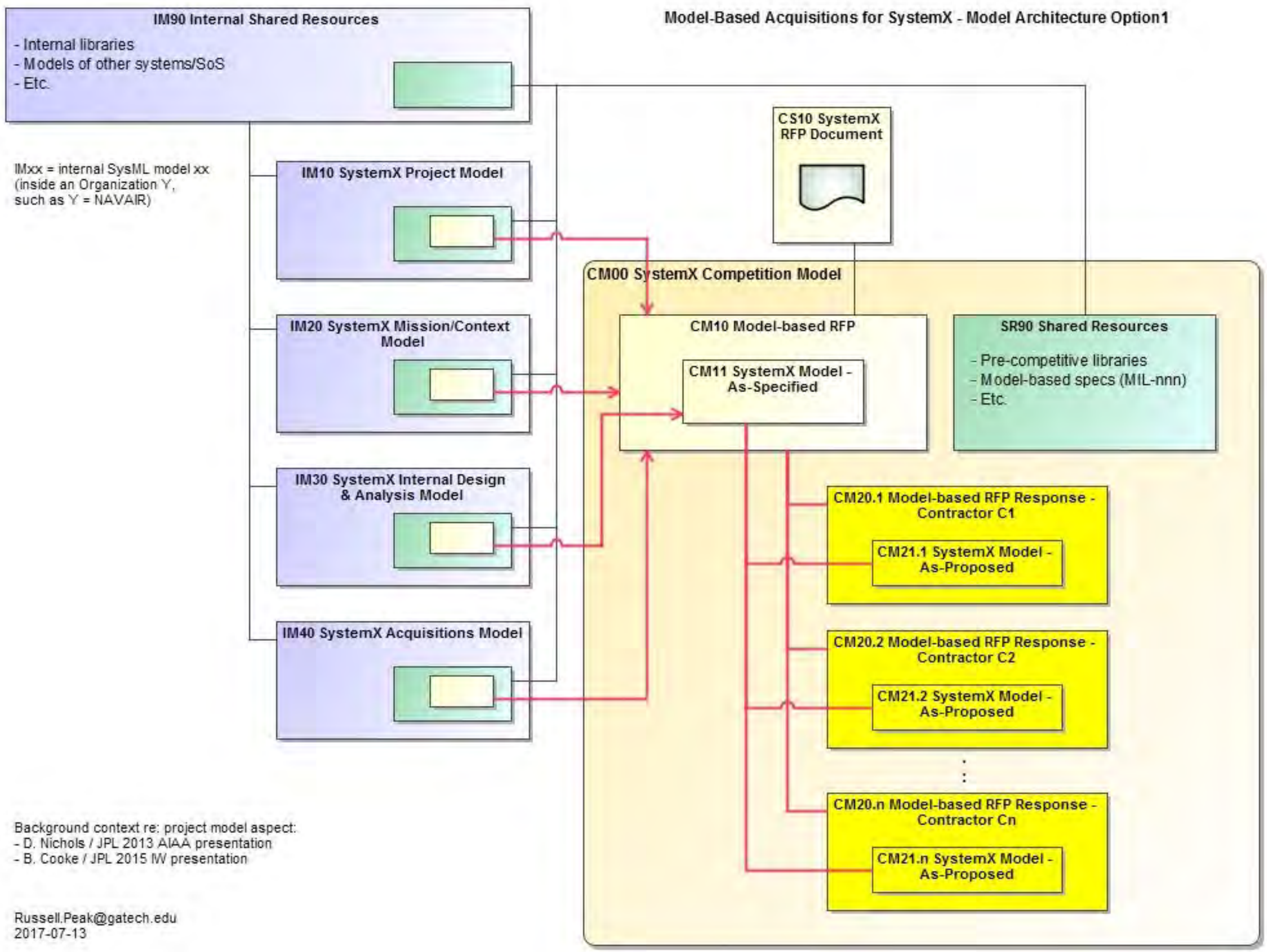
Formalize and Refine SET Framework

SysML Activity Diagram is draft Process Model for SET Framework

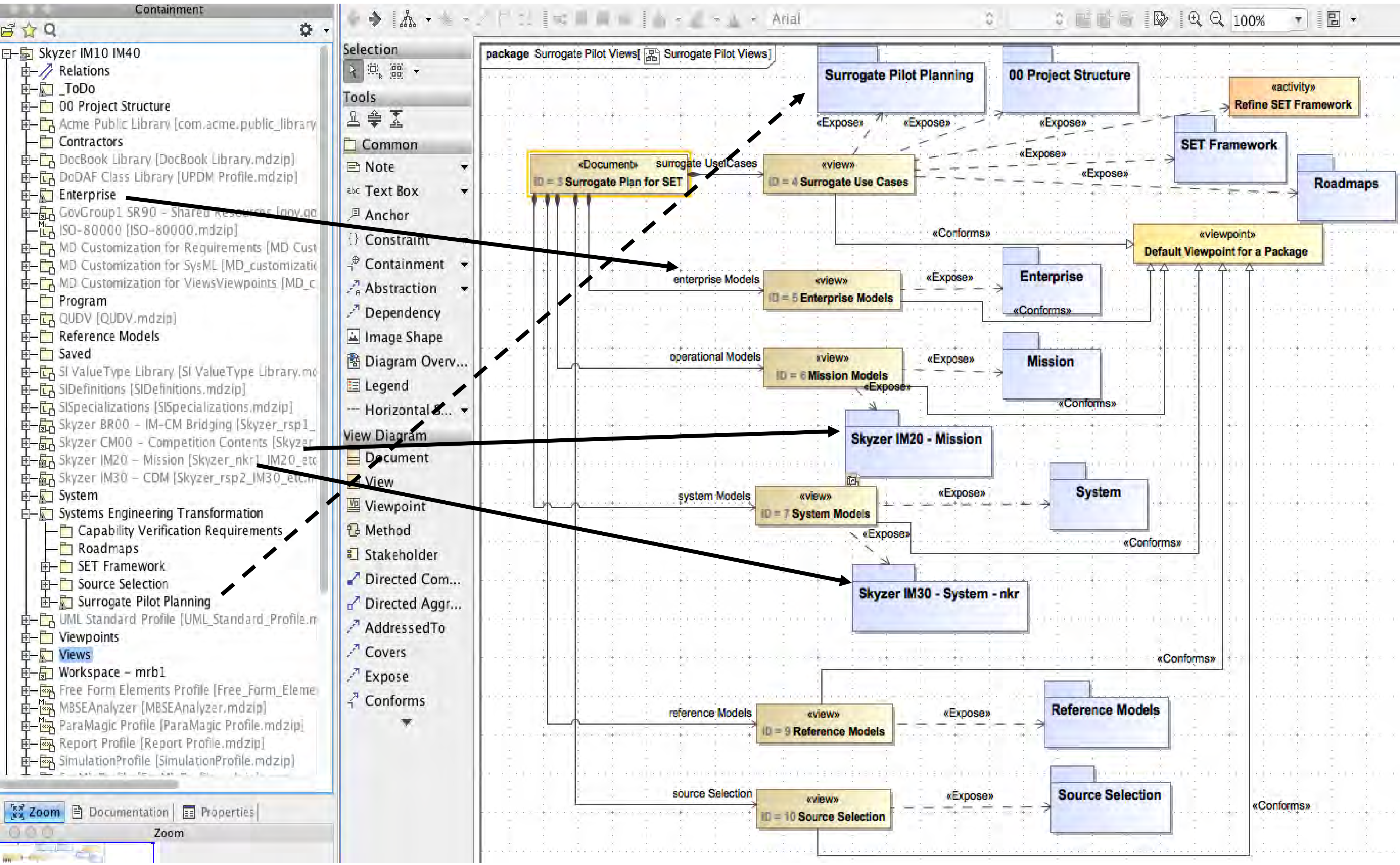


Need to Simulate Acquisition-related feedback paths (not exhaustive)

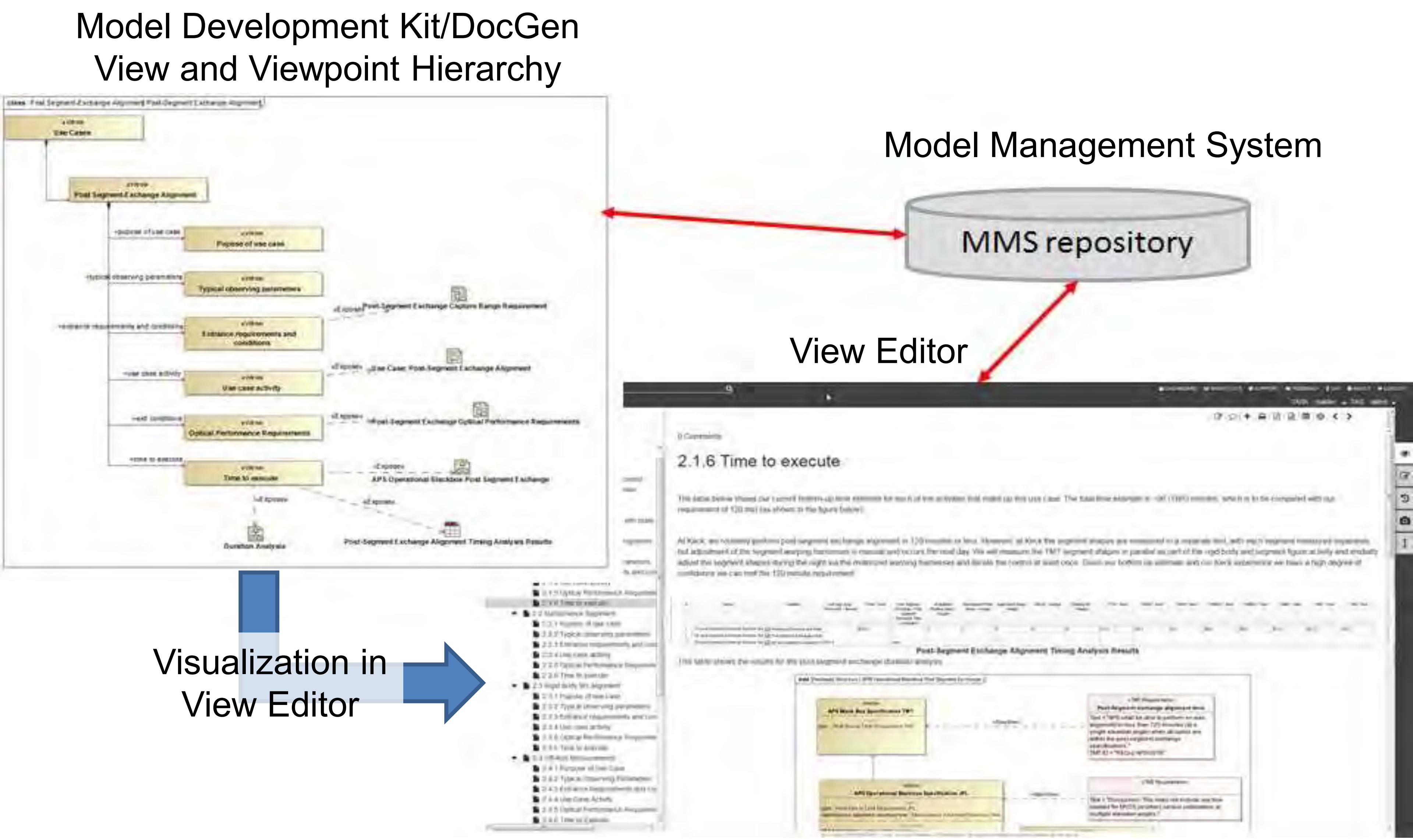
Methods for Partitioning of Work and Modularization of Models



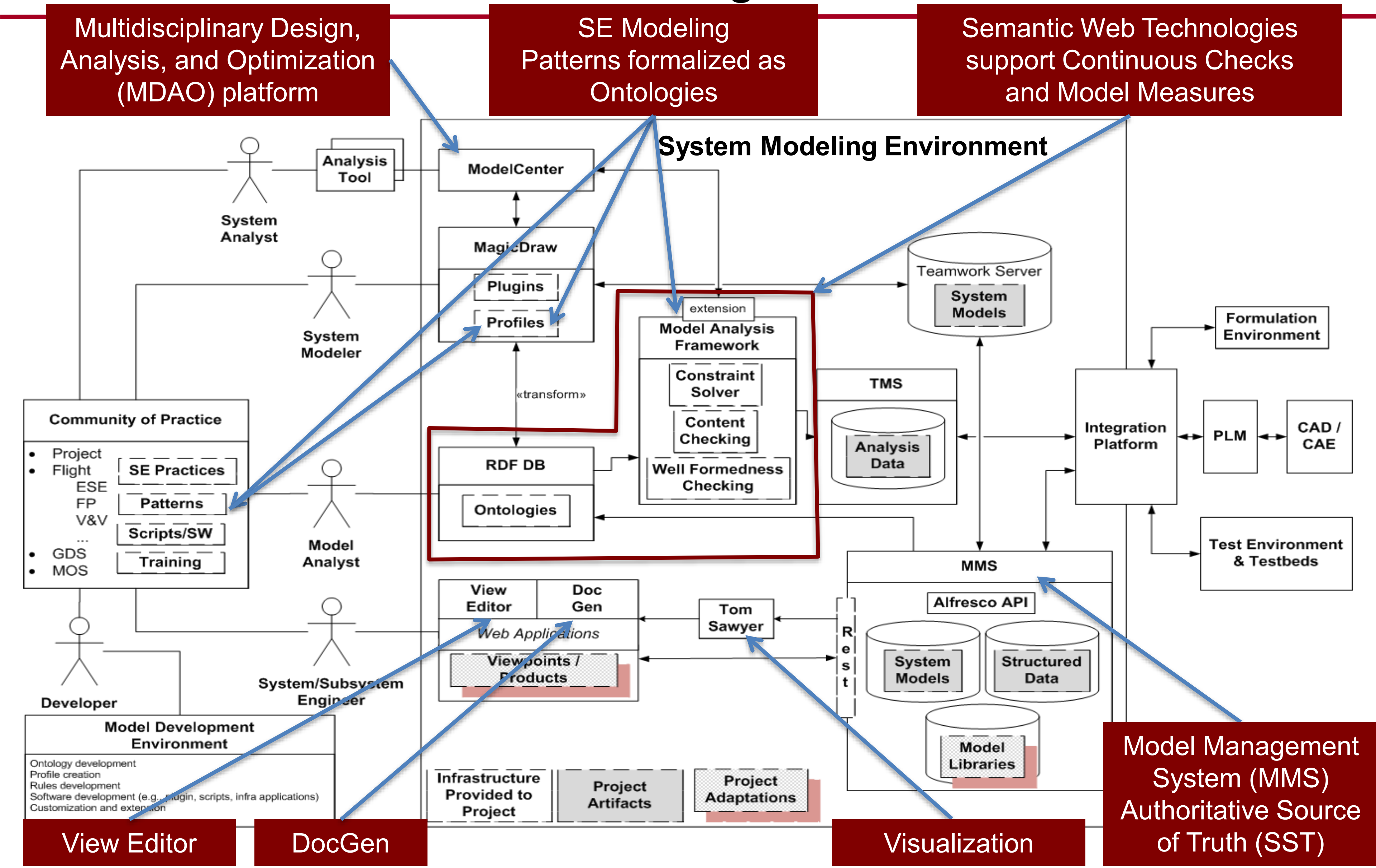
Using OpenMBEE Model Development Kit/DocGen for Generating Specification from Modularized Model



Open Model Based Engineering Environment (OpenMBEE)

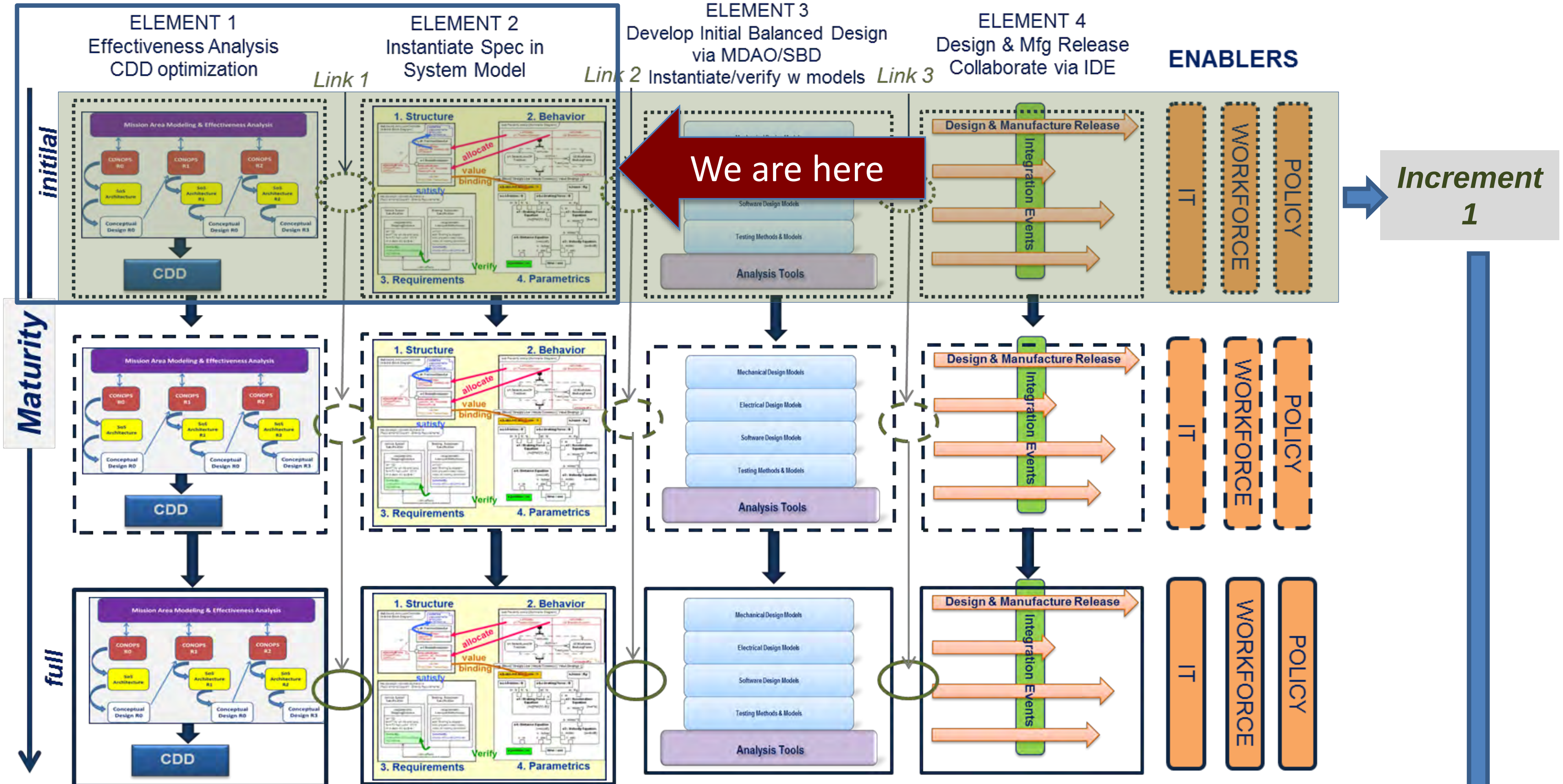


Surrogate Pilot Using OpenMBEE as Basis for Demonstrating Authoritative Source of Truth

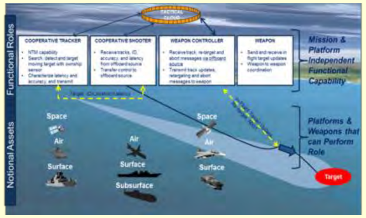


*An Integrated Model Centric Engineering (IMCE) Reference Architecture for a Model Based Engineering Environment (MBEE), NASA/JPL, Sept, 2014.

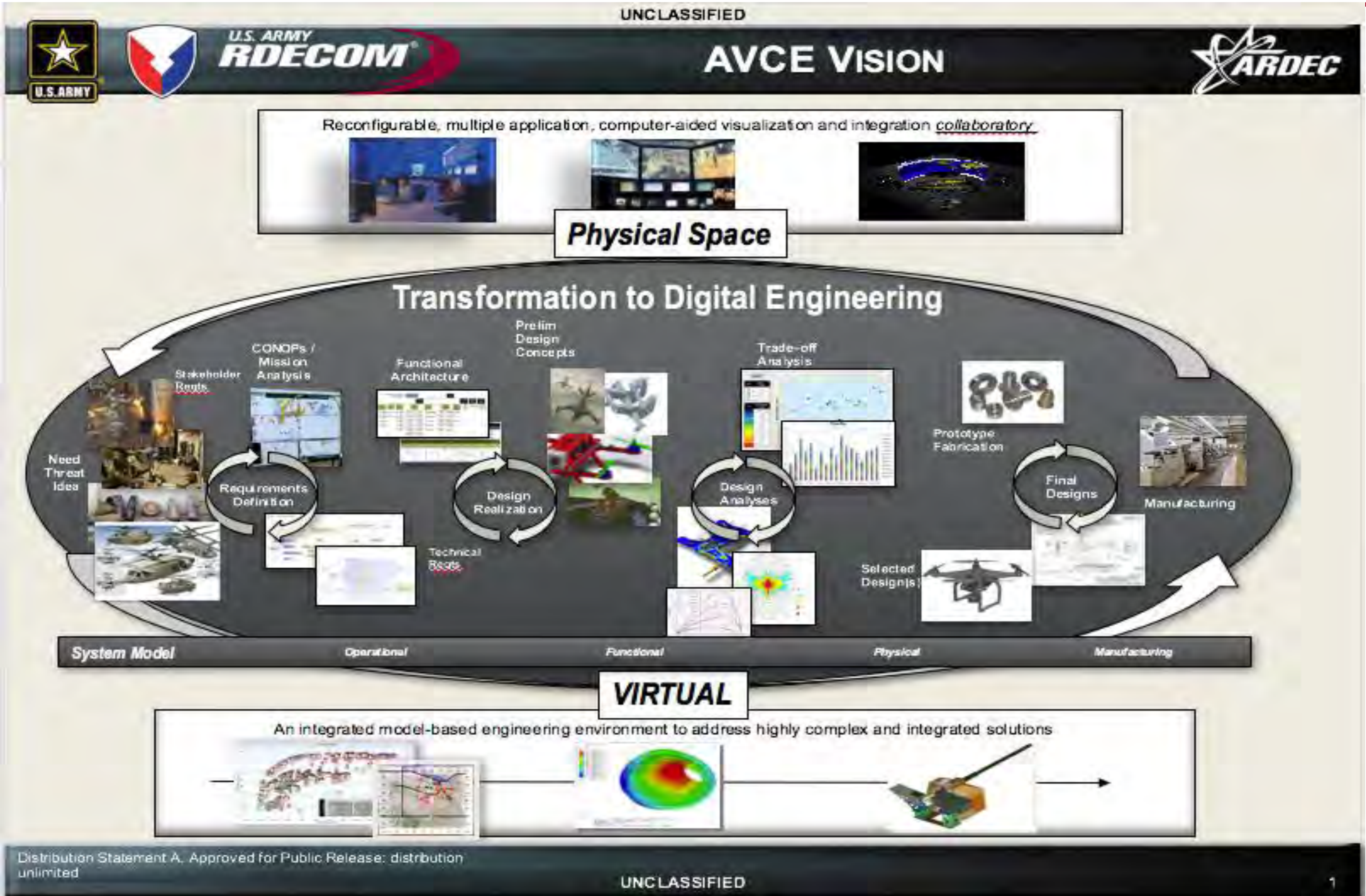
Where Are We:
Increment 1 and Elements 1 & 2



PILOTS



Our Research Efforts are Synergistic With Our ARDEC Sponsor and Other Collaborators



Collaborations

- SERC Collaborator: Georgia Tech, Georgetown, Naval Postgraduate School, Univ. of Maryland, Univ. of Massachusetts, Univ. of Southern Cal., Wayne State
- Digital Engineering Working Group
- Airspace Industry Association: CONOPS for Industry/Government Collaborative Framework
- Semantic Technologies for Systems Engineering Foundation
- NDIA Working Group – Using Digital Engineering for Competitive Down Select
- NASA/JPL
- OpenMBEE Collaborator Group
  - https://groups.google.com/d/forum/openmbee/

Thank You

- For more information contact:
  - Mark R. Blackburn, Ph.D.
  - Mark.Blackburn@stevens.edu
  - Stevens Institute of Technology
  - Links to technical reports: http://www.sercuarc.org/researcher-profile/mark-blackburn/
  - Overview briefing of both projects from SERC Sponsor Review 2016: http://www.sercuarc.org/wp-content/uploads/2014/05/05B_SSRR-2016_RT157_Blackburn_v2.pdf
  - Historical perspective with a long briefing: http://www.sercuarc.org/publications-papers/presentation-systems-engineering-transformation-through-model-centric-engineering-past-why-present-what-and-future-how/

Acronyms

CDD	Capability Description Document
CONOPS	Concept of Operations
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFD	Computational Fluid Dynamics
DARPA	Defense Advanced Research Project Agency
DASD	Deputy Assistant Secretary of Defense
DoD	Department of Defense
DoE	Design of Experiments
FEA	Finite Element Analysis
HPC	High Performance Computing
IMCE	Integrated Model-Centric Engineering
IMCSE	Interactive Model-centric Systems Engineering
IoT	Internet of Things
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
MBSE	Model-based System Engineering
MBE	Model-Based Engineering
MCE	Model-Centric Engineering
MCSE	Model-Centric System Engineering
MDAO	Multidisciplinary Design Analysis and Optimization
MDE	Model-Driven Engineering
NAVAIR	Naval Air Systems Command
OV	Operational View
P&FQ	Performance and Flight Quality
PDR	Preliminary Design Review
PLM	Product Lifecycle Management
RT	Research Task
SLOC	Software Lines Of Code
SE	Systems Engineering
SET	Systems Engineering Transformation
SERC	System Engineering Research Center
SETR	Systems Engineering Technical Review
SFR	System Functional Review
SRR	System Requirements Review
SoS	System of Systems
SOW	Statement of Work
SSTT	Single Source of Technical Truth
SV	System View
UAV	Unmanned Air Vehicle
V&V	Verification and Validation

CREATE

Accelerating Defense Innovation with Computational Prototypes and Supercomputers

NDIA 20th Annual Systems Engineering Conference
October 23-26, 2017, Springfield, VA

DOD HPC MODERNIZATION PROGRAM

Dr. Douglass Post, HCPMP CREATE Associate Director

HPCMP Ecosystem

DOD HPC MODERNIZATION PROGRAM

Users

DOD HPC

A technology-led, innovation-focused program committed to extending HPC to address the DoD's most significant challenges

DoD Supercomputing Resource Centers (DSRCs)

U.S. Air Force Research Laboratory DSRC

U.S. Army Research Laboratory DSRC

U.S. Army Engineer Research and Development Center DSRC

Maui High Performance Computing Center

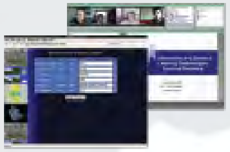
U.S. Navy DSRC

Networking and Security

Defense Research & Engineering Network (DREN)

Computer Network Defense, Security R&D, and Security Integration

Software Applications



Core Software

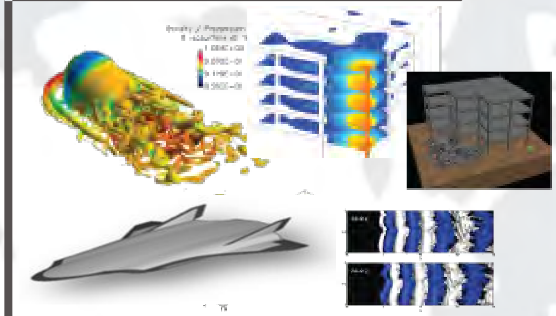
Computational Environments

Education and Training

HPC User Support

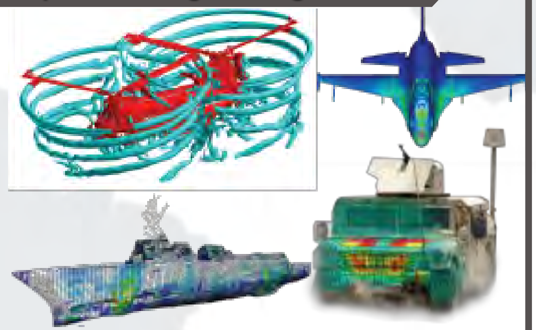
Results

Science and Technology



Test and Evaluation

Acquisition Engineering



Distribution A: Approved for Public release; distribution is unlimited.

Who May Run on HPCMP Resources?

- DoD Employees and Contractors (Researchers and Engineers)
- University Staff with a DoD Research Grant

Interested?

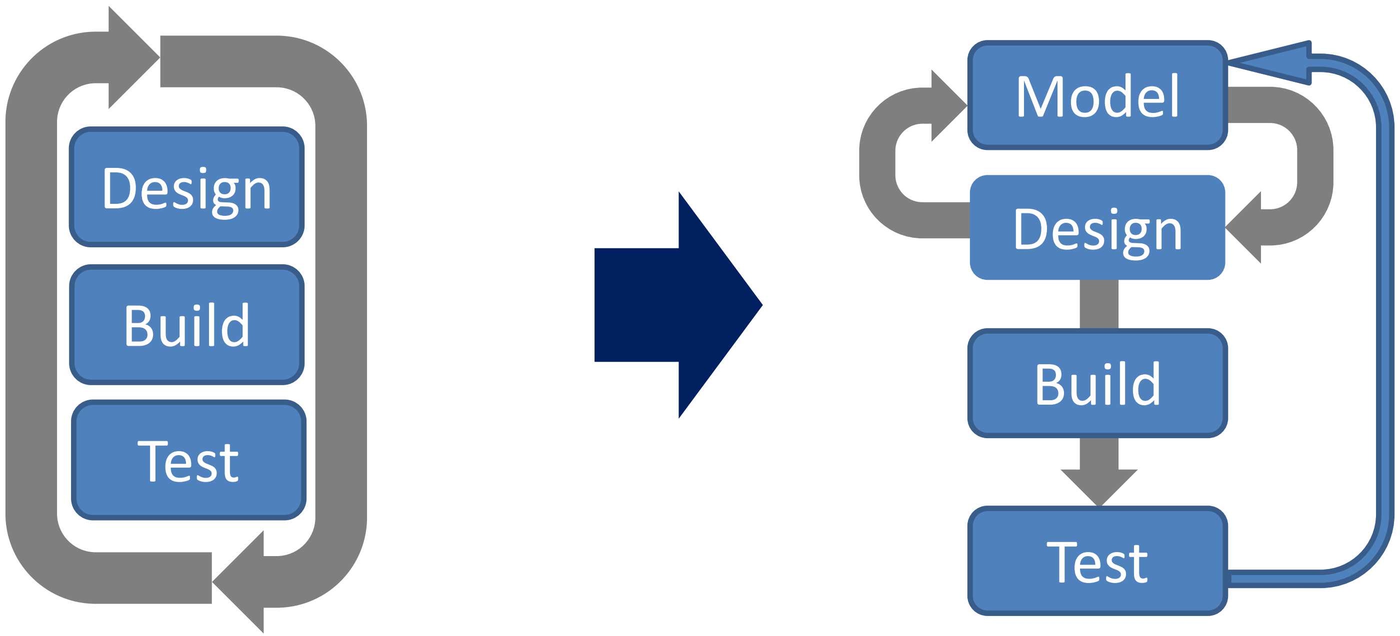
- Contact your Service (Army, Navy, Air Force, OSD, DARPA, MDA, DTRA,…) representative
- Information available at www.hpc.mil under the "For Users" menu with the Topic: "Who May Run on HPCMP Resources"
- Send an email to REQUIRE@hpc.mil to find your Service Representative

See the CREATE Exhibit in the Lobby

A Paradigm Shift Enabled by 60 Years of Progress in Computing

Time ~20-30 yrs

~5-7 yrs



Cost $$$$$

$$$

Empirical Basis

Computational Basis

Innovation with Computational Prototyping and HPC

Try, Fail, and Fix Early and Often, Before You Cut Metal!

CREATE 5 Projects: 11 Multi-Physics Software Tools

- **Air Vehicles—CREATE-AV**
  - Genesis - Rapid conceptual design for academic use
  - Kestrel - High-fidelity, full-vehicle, multi-physics analysis tool for fixed-wing aircraft
  - Helios - High-fidelity, full-vehicle, multi-physics analysis tool for rotary-wing aircraft
- **Ships—CREATE-Ships**
  - Rapid Ship Design Environment (RSDE) - Rapid Design and Synthesis Capability
  - Navy Enhanced Sierra Mechanics (NESM) - Ship Shock & Shock Damage Assessment
  - NAVYFOAM - Ship Hydrodynamics — predicts hydrodynamic performance
  - Integrated Hydro Design Environment (IHDE) - Facilitates access to naval design tools
- **RF Antenna—CREATE-RF**
  - SENTRi- Electromagnetics antenna design integrated with platforms
- **Ground Vehicles—CREATE-GV**
  - Mercury – High-fidelity, multi-physics simulation tool for vehicle systems and components
  - Mobility Analysis Tool (MAT) – Analysis tool to evaluate ground vehicle performance metrics
- **Meshing and Geometry—CREATE-MG**
  - Capstone - Components for generating geometries and meshes needed for analysis
- **HPC Portal—Secure access to computers through a browser**

CREATE-AV
Aircraft (AV) Design Tools

CREATE-SHIPS
Ship Design Tools

CREATE-RF
Radio Frequency (RF) Antenna Design and Integration Tools

CREATE-GV
Ground Vehicle Design Tools

CREATE-MG
Meshing and Geometry (MG) Support

180+ user orgs
- 50% industry
- 40% government
- 10% other

- >1600 licenses
- 70+ programs

CREATE reduces risk, increases decision space, and supports accelerated production schedules

CREATE is 11 separate partnerships with 11 individual DoD Service Engineering Organizations

HPCMP Director

CREATE Program Associate Director

Official HPCMP Advisory Panel

Ships Project
Project Manager
HPCMP Lorton

NavyFOAM
NSWC, Carderock

Integrated Hydro Design Environment
NSWC, Carderock

Navy Enhanced Sierra Mechanics
NSWC, Carderock

Rapid Ship Design Environment
NSWC, Carderock

Air Vehicles Project
Project Manager
HPCMP, Lorton

Kestrel
46th Test Wing, Eglin AFB

Quality Assurance
NAVAIR, Patuxent River

Helios
Army AFDD, Ames

Genesis Design
HPCMP, WPAFB

RF Antennas Project
Sensors Directorate, AFRL, WPAFB

SENTRi
Sensors Directorate, AFRL, WPAFB

Meshing & Geometry Project
Capstone
Project Manager
Navy NRL

Ground Vehicles Project
Project Manager

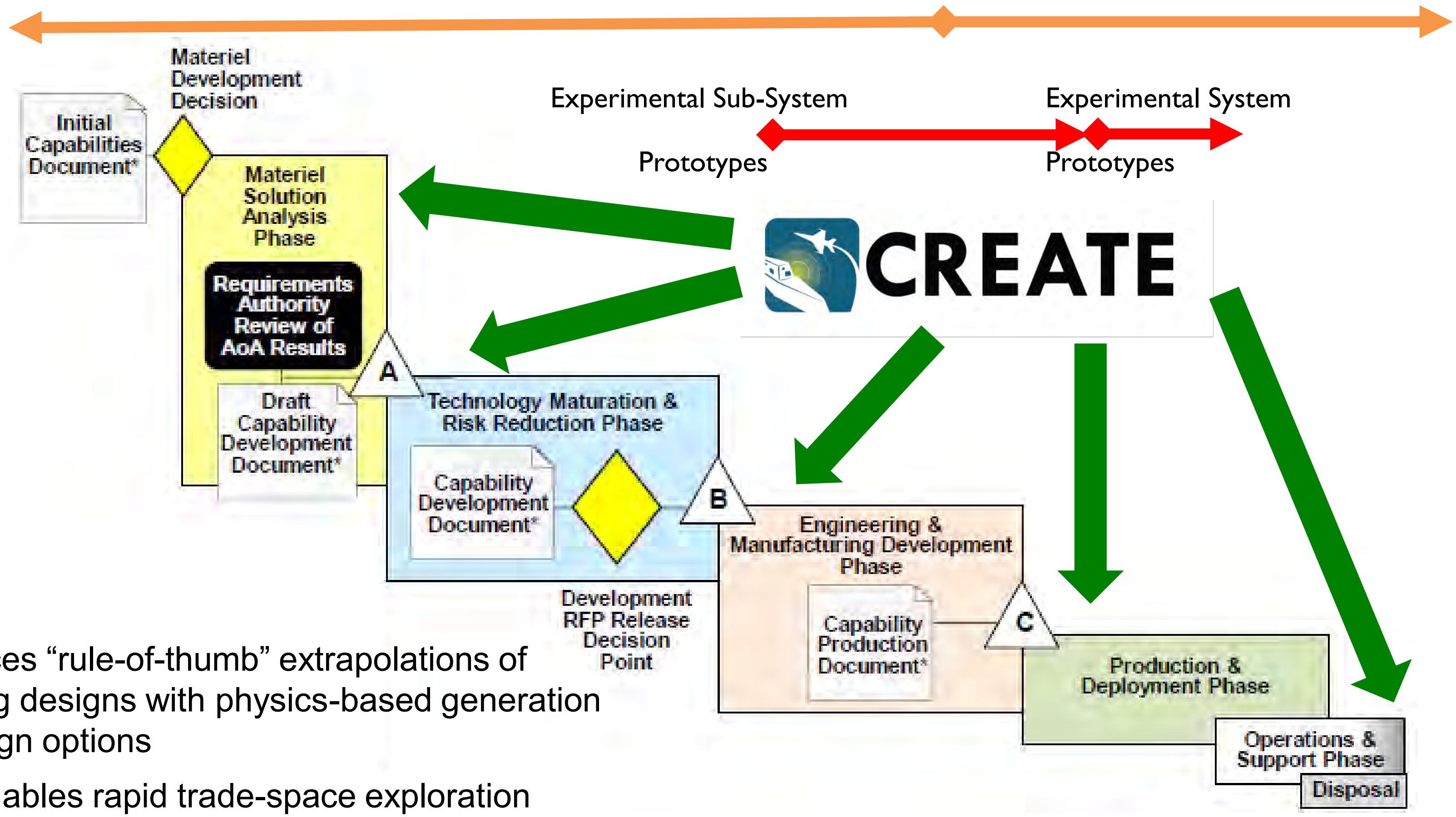
Mercury
ERDC

MAT
TARDEC

A Multi-Institutional, Multi-Organizational, Distributed Program

CREATE: Agility for the Acquisition Cycle

Physics-based Computing Tests of Computational Prototypes—Moves "Testing to the Left (and Right)"



- Replaces "rule-of-thumb" extrapolations of existing designs with physics-based generation of design options
  - Enables rapid trade-space exploration
  - Provides physics-based analysis tools to assess the feasibility of the design options
- CREATE augments "failure data from live tests" with "predictions of computational prototype performance," providing timely decision data that identifies design flaws and performance shortfalls early, allowing them to be fixed before metal is cut

CREATE: Enabler of Digital Engineering

DOD HPC MODERNIZATION PROGRAM

1. **Formalize development, integration and use of models**
   – CREATE Develops and Deploys 11 Physics-based HPC tools being used by over 180 DoD engineering organizations to design, analyze, and predict the performance of over 70 weapon systems instantiated in a digital model of each weapon platform
2. **Provide an enduring authoritative source of truth**
   – The laws of physics applied to digital models of weapon platforms with potential to aggregate all the important information produced during acquisition process
3. **Incorporate technological innovation**
   – CREATE Tools include all the important physics, address full-size systems, utilize accurate algorithms, and are extensively verified and validated with DoD T&E data
4. **Establish supporting infrastructure and environments**
   – High Performance Computing Modernization Program Eco-system (High Performance Computers, Secure high-speed networks, CREATE tools, T&E data for V&V,… for DoD engineers)
5. **Transform a culture and workforce**
   – Enables paradigm transition from iterated “design, build, test,…” to iterated “model, design,…” followed by build and test. Builds organic workforce and enables it to “own” design process, take risks, and identify and fix design defects before metal has been cut.

CREATE Grows and Trains DoD Organic Workforce

Getting the tools into the hands of design engineers

Example: CREATE RF—4 to 5 Training Sessions per year


GTRI: Atlanta


Raytheon, NGC, GA, SPAWAR: San Diego

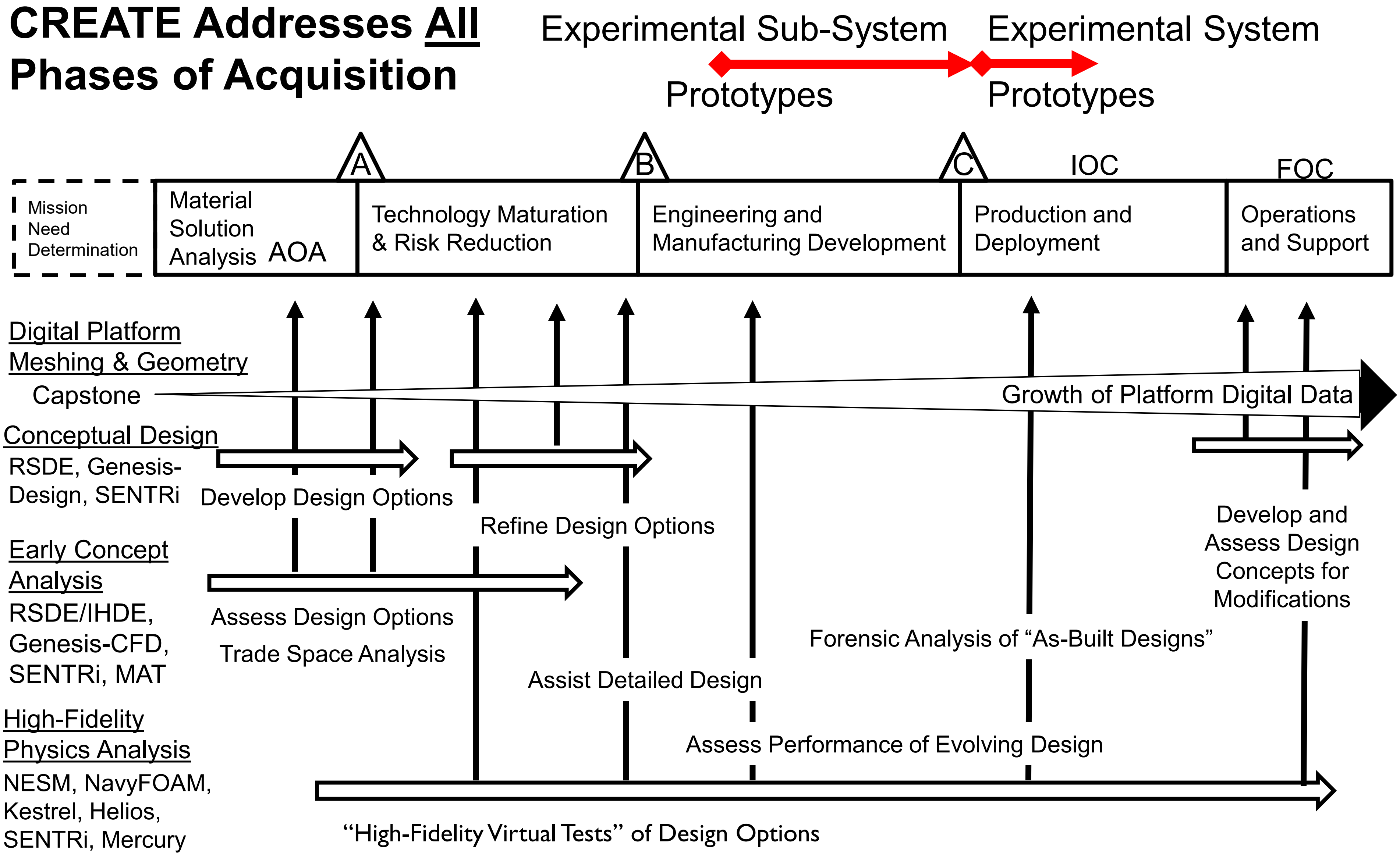

AFRL, SI2, L3, Leidos, ONI, RRI: Dayton


NASIC, MDA, MSIC, AMRDEC: Dayton


MITRE, NGC, AFRL, NASA, Boeing: Dayton

CREATE Designed to Enable Digital Engineering

DOD HPC MODERNIZATION PROGRAM



CREATE Tools Impact Many DoD Programs

NAVSEA

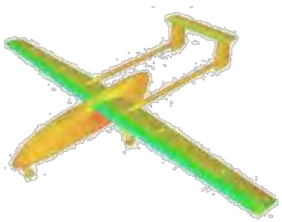
DDG-1000

CVN-78 Class

Columbia SSBN

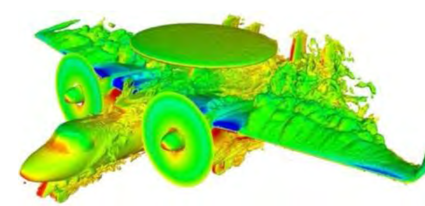
LX(R)

NAVAIR



Aerostar & Raven UAVs

F/A-18 E/F/G

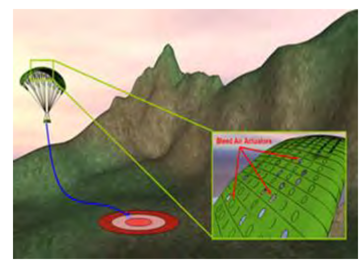


E-2D

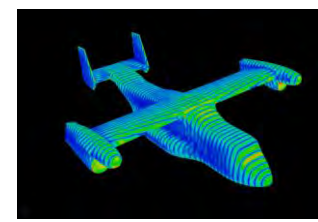
ARMY/USMC

UH-60

CH-47 (ACRB)



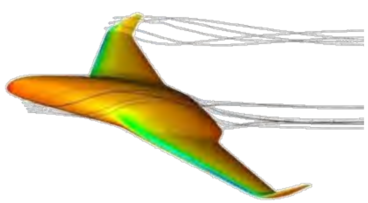
Guided Airdrop (RDECOM)



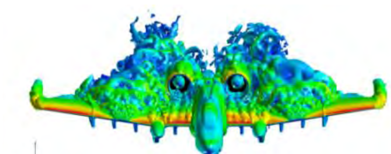
V-22

AFLCMC

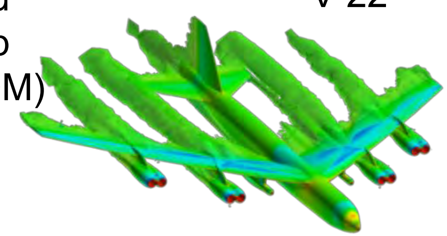
F-15 SA/DB-110



Strategic Airlift CP&A



A-10



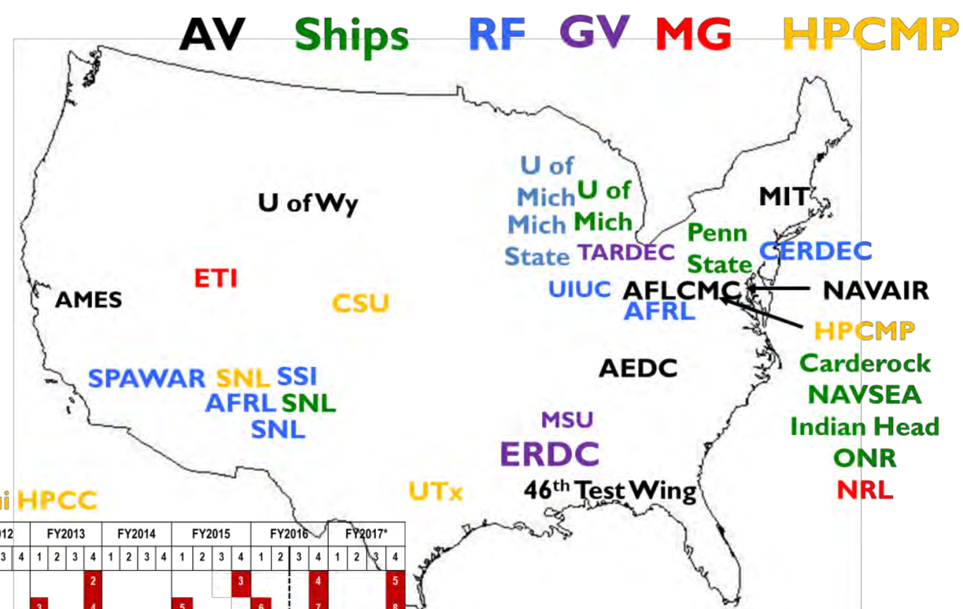
B-52

Build the Right Software, and Build it Right!

- **Software built by government-led teams of 5 to 10 staff**
  - **<u>Technical team</u> and <u>team leader</u> embedded in customer organizations**
  - **Optimal balance of team agility, structured process, and accountability**
- **<u>Highly Disciplined</u> Software Development Processes**
  - **Strong emphasis on software quality and accountability**
  - **Supportive code development environment—virtual clusters, central servers and code repository, high performance computers**

<u>Annual releases</u>

- Increased capability annually
- Extensive beta-tests of each release
- Rigorous V&V process
- Improved scalability for massively parallel computers
- Improved usability
- Responsive to evolving requirements
- Extensive documentation



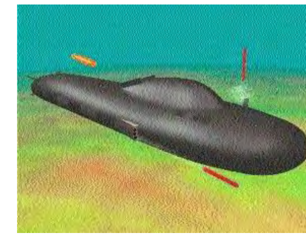
Fiscal Year	FY2011				FY2012				FY2013				FY2014				FY2015				FY2016				FY2017*			
Quarter	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
AV-DaVinci					1							2								3				4				5
AV-Helios					2				3			4					5				6			7				8
AV-Kestrel			2						3			4				5			6				7				8	
MG-Capstone	1				2				3				4				5				6				7			
RF-SENTRi				2					3				4				5				6				7			
Ships-IHDE	2				3				4				5				6				7				8			
Ships-NavyFoam	1				2				3					4			5				6				7			
Ships-NESM	1				[illegible]					2					[illegible]				3				4				5	
Ships-RSDE					[illegible]				[illegible]				[illegible]				[illegible]						2				3	

13 military sites
48 contracts
2 WFOs (SNL)

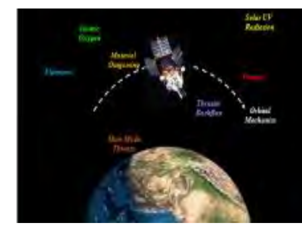
Distribution A: Approved for Public release; distribution is unlimited.

CREATE—Looking to the Future

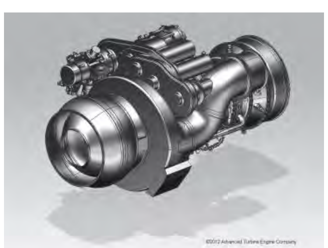
Areas for near-term impact:



- **Hypersonics**: Investments are impacting current and future timeframes (CREATE- AV Kestrel potential)
- **New Submarine Development**: Planning and design work underway (CREATE-Ships RSDE) with ERS help
- **Vertical Heavy Lift (JMR-TD)**: Critical capability for the future for both manned and unmanned systems. Needed for future force structure planning and operational execution. (CREATE-AV Helios has been used for the down-select from 4 to 2 concepts)



- **Space Technology**: critical design space exploration impacting all Services (e.g., satellites, weapons, sensors, etc.)
- **Improved Turbine Engine Program (ITEP)**: CREATE-AV Kestrel & Helios in use for analysis of engine integration
- **EW/Radar/Antenna Modeling**: S-Band, X-Band, Phased Array design analysis electronic warfare opportunities
- **Directed Energy**: Analysis of EM and aerodynamic systems being investigated by Kestrel and SENTRi
- **Service Life Prediction**: Contributes to sustainment of existing DoD systems through advanced mechanics



Take Aways

- CREATE: Physics-based computational engineering tools to meet DoD needs in aviation, maritime, ground, and electromagnetic warfare domains
  - Government-developed, government-owned, and government-supported to meet DoD needs
  - Adoption expanding across DoD government, industry, and academic enterprises
  - Major enabler of the OSD Digital Engineering, the Air Force Digital Thread/Digital Twin, and the Engineered Resilient Systems Programs
  - Excellent growth potential to meet needs for many future DoD warfare domains

CREATE Leadership Team Contacts

DoD High Performance Computing Modernization Program (www.hpc.mil)

CREATE@hpc.mil

Dr. Douglass Post—Associate Director for CREATE: Douglass.post@hpc.mil

(O) 703-812-4423, (C) 703-851-7065

CREATE Project Managers

Dr. Robert Meakin, CREATE-AV: robert.meakin@hpc.mil

Dr. Richard Vogelsong, CREATE-Ships: richard.vogelsong@hpc.mil

Dr. John D'Angelo, CREATE-RF: john.dangelo.4@us.af.mil

Dr. Larry Lynch, CREATE-GV Project Manager: larry.n.lynch@usace.army.mil

Dr. Saikat Dey, CREATE-MG Project Manager: saikat.dey@nrl.navy.mil

CREATE Senior Operations Director

Scott Sundt (CAPT, USN (ret.))—scott.sundt@hpc.mil

(O) 703-812-3747, (C) 703-424-8582

Digital Engineering (DE) and Computational Research and Engineering Acquisition Tools and Environments (CREATE)

Ms. Phil Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

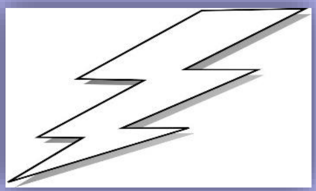
History

1st Industrial Revolution

MECHANICAL

Use of mechanical production powered by water and steam

2nd Industrial Revolution



ELECTRICAL

Use of mass production powered by electrical energy

3rd Industrial Revolution

INFORMATION TECHNOLOGY

Use of electronics and IT to further automation

4th Industrial Revolution

DIGITAL

Use of a digitally connected end-to-end enterprise

1800 | 1900 | 2000 | **TODAY**

Traditional Models and Simulations (M&S)

Simulation Based Acquisition (SBA)

Model-Based Systems Engineering (MBSE)

DIGITAL ENGINEERING (DE)

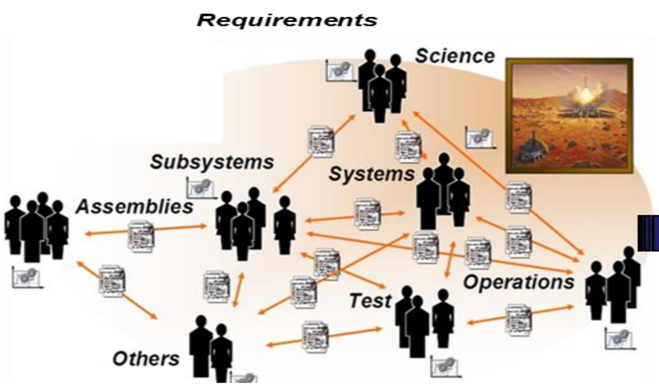
Digital Engineering: MBSE approach for DoD

Current State

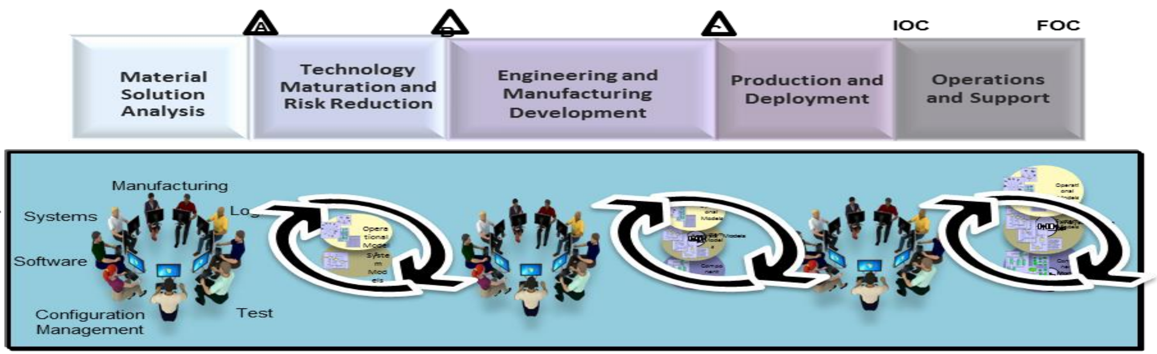
- Our workforce uses stove-piped data sources and models in isolation to support various activities throughout the life-cycle
- Current practice relies on standalone (discipline-specific) models
- Communication is through <u>static</u> <u>disconnected</u> documents and subject to interpretation

Future State

- Digital Engineering moves the engineering discipline towards an integrated model-based approach
  - Through the use of digital environments, processes, methods, tools, and digital artifacts
  - To support planning, requirements, design, analysis, verification, validation, operation, **<u>and/or</u>** sustainment of a system
- Digital Engineering ecosystem links our data sources and models across the lifecycle
  - Provides the authoritative source of truth



Current: Stove-piped models and data sources



Future: Digital Engineering Ecosystem

CREATE Products in Digital Engineering Context

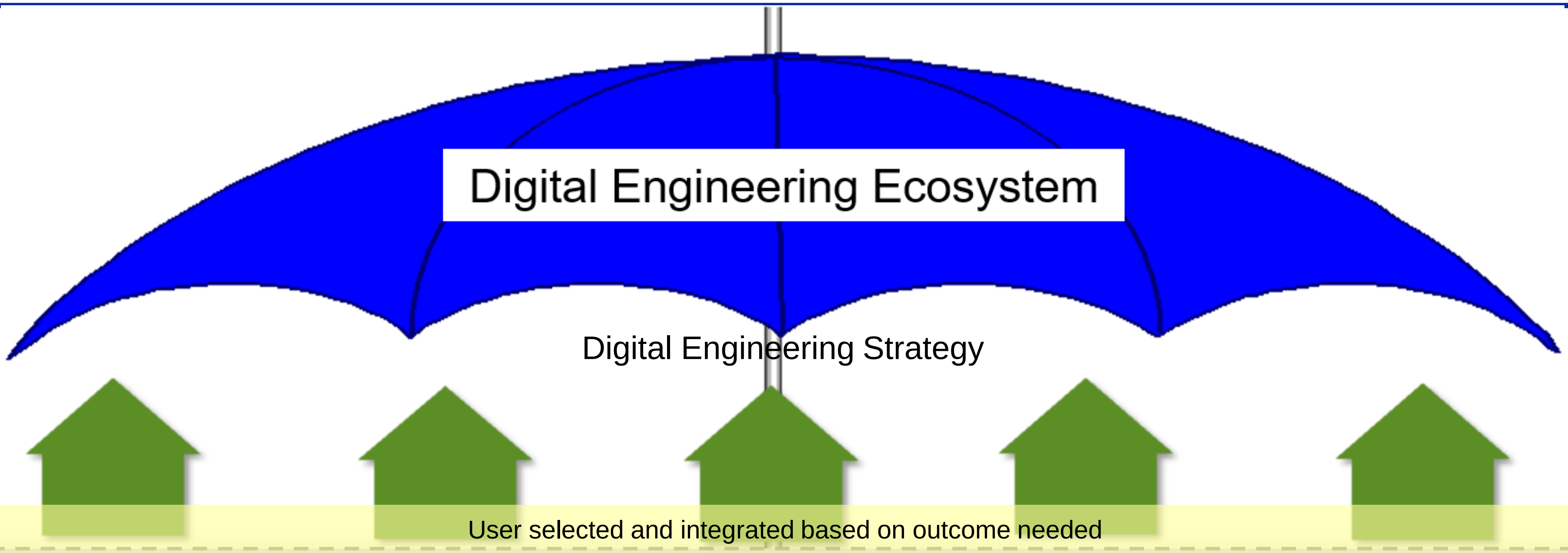
Digital Engineering

- **Digital Engineering vision moves the engineering discipline towards an integrated model-based approach through the use of digital environments, processes, methods, tools, and digital artifacts**
- **Model is a representation of reality**
  - Model is 'composed of' data, algorithms and/or processes
  - Computable or used in a computation

CREATE

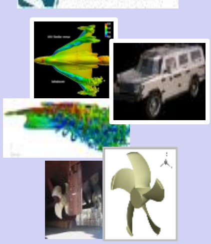
- **CREATE program develops and deploys validated physics-based High Performance Computing (HPC) applications to enable DoD engineers to implement and execute the digital engineering paradigm for major DoD platforms (naval, air, & ground vehicles and RF antennas)**
- **Includes ability to construct and improve digital product models for weapon platforms**
  - Tools address all stages of the acquisition process

Digital Engineering Relationships



Physics-based / Engineering Design Tools

CREATE



Computational Research and Engineering Acquisition Tools and Environments (CREATE)

World-class Computational Resources (High Performance Computing), Software, Networking

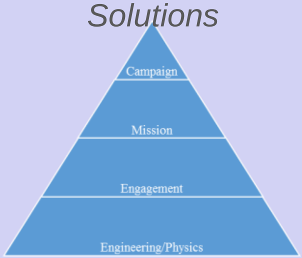
DOD HPC MODERNIZATION PROGRAM

Other Initiatives

Supporting tools: (Large Tradespace Analytics datasets, Analysis of Alternatives, Virtual Prototyping Evaluation, etc.)

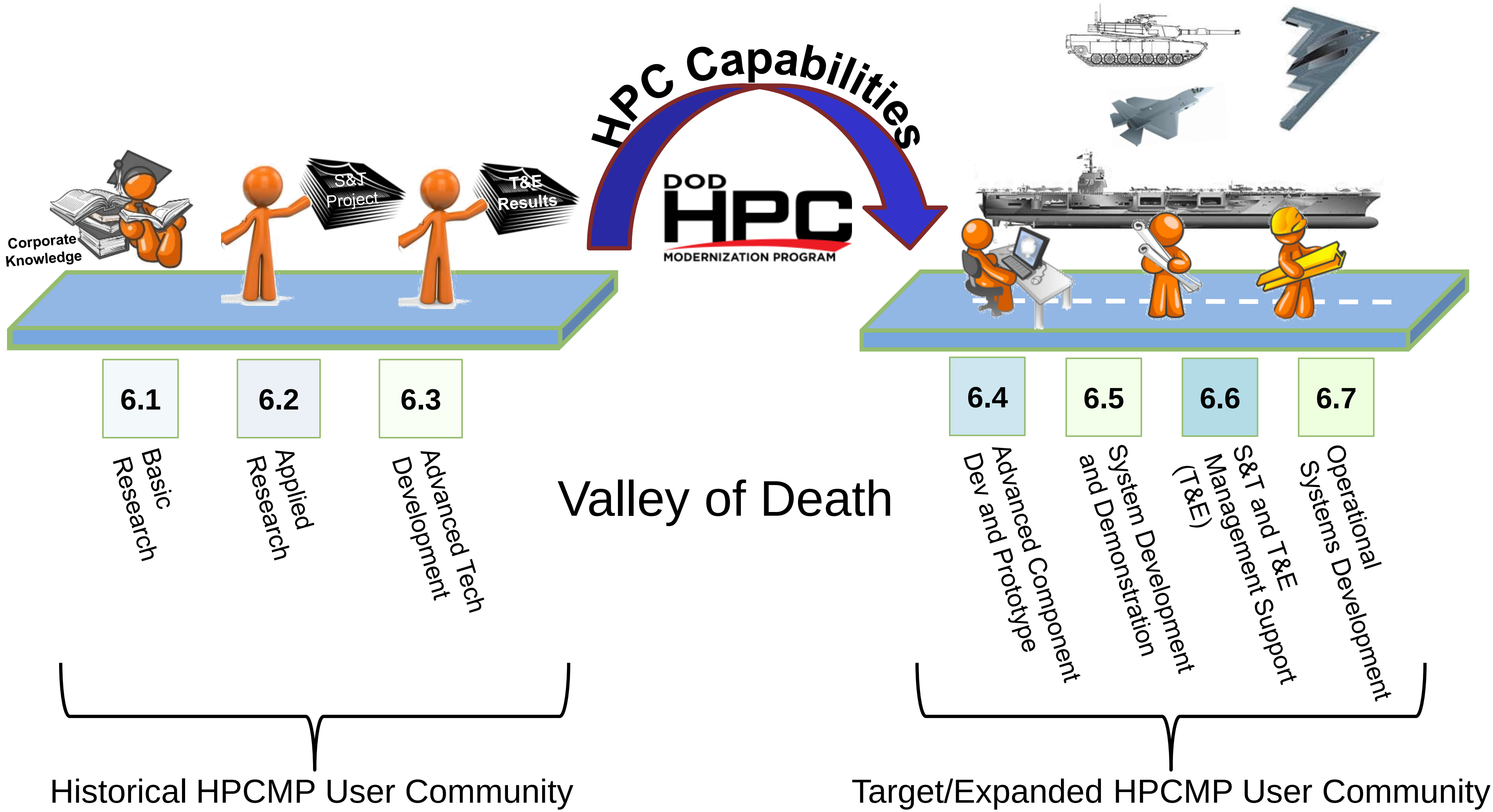
ERS ENGINEERED RESILIENT SYSTEMS DEPARTMENT OF DEFENSE

Traditional Mod/Sim Solutions



(DoD) Modeling and Simulation Coordination Office (DMSCO)

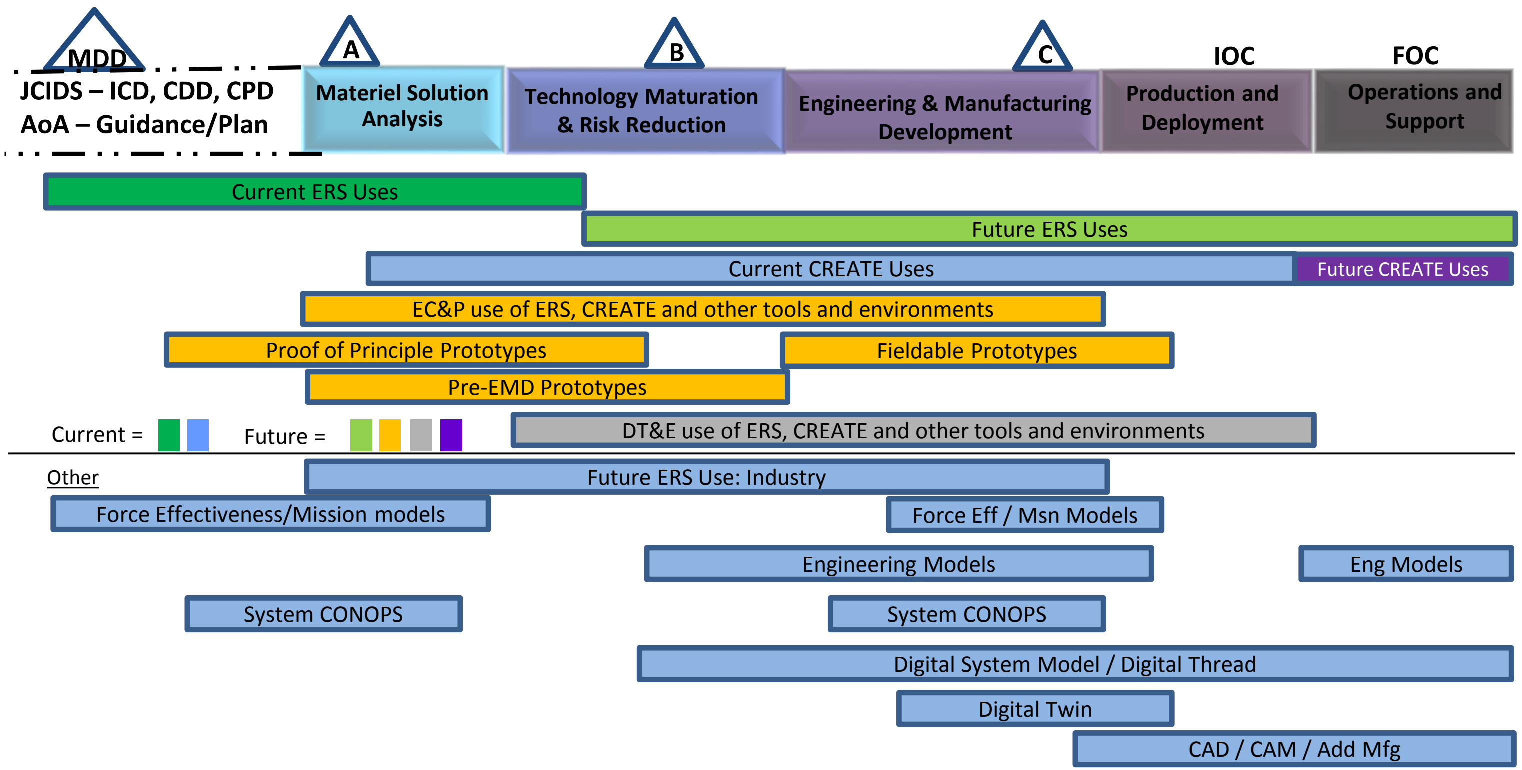
Transitioning S&T, T&E and Corporate Knowledge to Engineering & Acquisition



DRAFT Vision for ERS, CREATE, et al (crossing the Valley of Death)

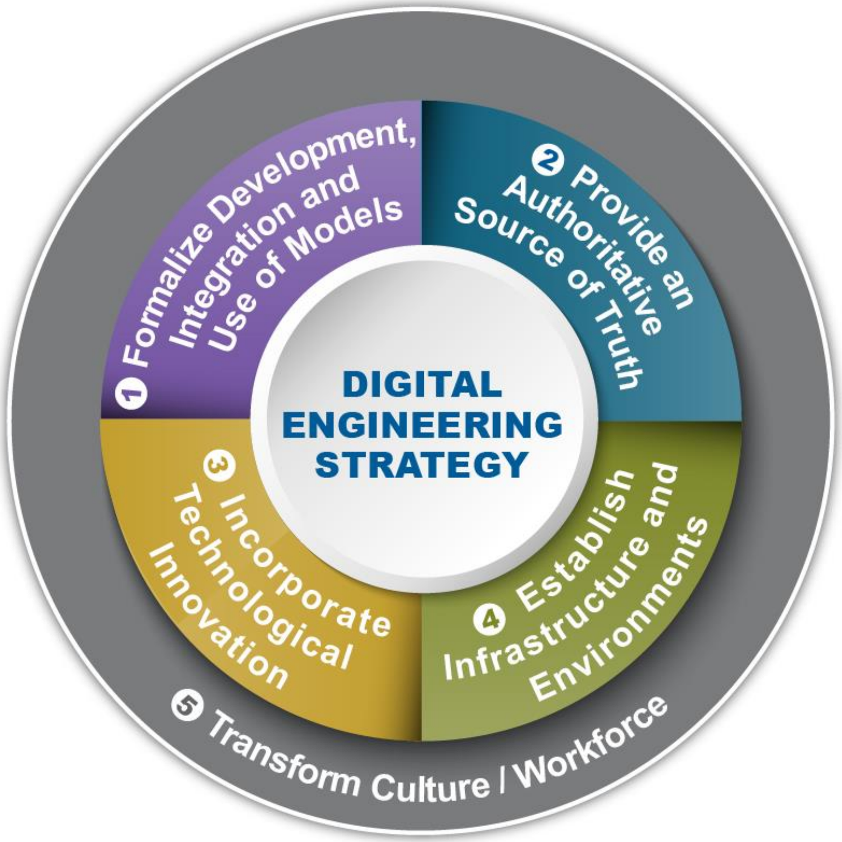
DRAFT DRAFT

Current Domains: Air (Fixed & Rotary), Surface, Subsurface, Ground, RF, Meshing, Geometry
Future Domains: Space, Hypersonics, Improved Turbine Engine, EW, Directed Energy, Others?



Digital Engineering Strategy: Five Goals

1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** to perform activities, collaborate, and communicate across stakeholders
5. Transform a **culture and workforce** that adopts and supports Digital Engineering across the lifecycle



Drives the engineering practice towards improved agility, quality, and efficiency, resulting in improvements in acquisition

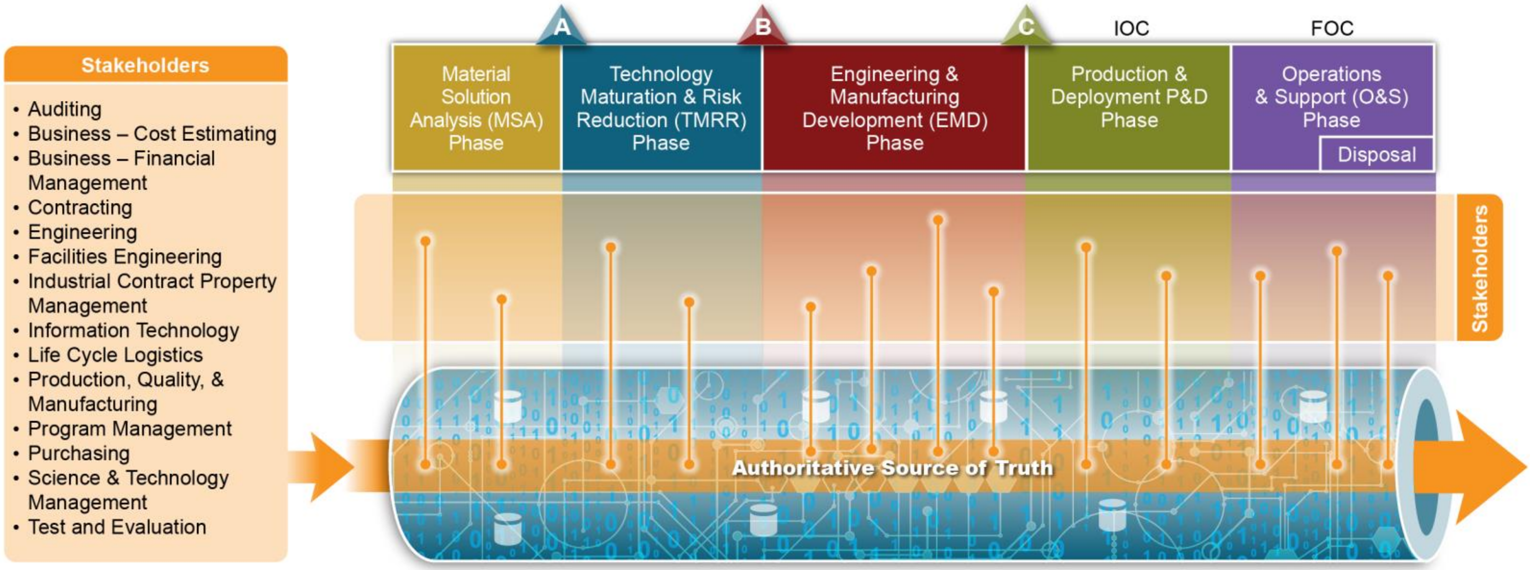
Goal #1: Formalize Development, Integration & Use of Models

CREATE in DE Goal 1:

- Develop, deploy and support physics-based software applications that enable DoD engineers to rapidly:
  - Develop digital product models (virtual prototypes) for weapon systems which can be used to populate design spaces
  - Analyze the performance of the of the systems, using medium- and high-fidelity physics-based HPC tools, identifying and fixing system design defects and performance shortfalls thus reducing rework, and costs, risks, and schedule, and improving performance for all stages of the acquisition process

Models as the cohesive element across a system's lifecycle

Goal #2: Provide an Authoritative Source of Truth



<u>CREATE in DE Goal 2:</u>

- Develop and deploy verified and validated physics-based HPC tools that include: all important effects, accurate solution algorithms, and model the complete system i.e. everything needed to <u>accurately</u> predict the performance in short enough compute times for parameter studies

Right information, right people, right uses, right time

Goal #3: Incorporate Technological Innovation

❖ **Big Data and Analytics**

❖ **Cognitive Technologies**

❖ **Computing Technologies**

❖ **Digital-to-Physical Fusion Technologies**

CREATE in DE Goal 3:

- HPCMP eco-system employs innovative technologies (High Performance Computers, high speed networks and advanced software).
- DoD engineers develop innovative systems by rapidly and efficiently generating many design options; identifying the failures and successes; and improvements
- Use of small teams to take risks, fail early and quickly in order to identify successful product designs

Harness technology, new approaches, and human-machine collaboration to enable an end-to-end digital enterprise

Goal #4: Establish Infrastructure & Environments

CREATE in DE Goal 4:

- High Performance Computing Ecosystem:
    - Subject matter experts from relevant stakeholders
    - Validated and verified data for use in engineering and acquisition activities
    - HPC Distributed Resource Centers
    - High-bandwidth network (DREN)
    - Software applications (CREATE codes now and in the future)

Foundational support for Digital Engineering environments

Goals #5: Transform Culture and Workforce

CREATE in DE Goal 5:

- HPCMP Partnerships with Service Engineering Organizations
- Development and use of CREATE builds computationally skilled DoD workforce
- Training and support is provided for those accessing CREATE – over 180 DoD organizations with ~1400 users.
- CREATE software is being incorporated into Service Academy and other university curricula
- Regular release of upgraded software capability

Institutionalize Digital Engineering across the acquisition enterprise

There Is Much More to Do…

- **Publish the Digital Engineering Strategy**
  - Support development of implementation guidance/direction in Services/Agencies
  - Follow with policy?
- **Finish the Digital Engineering Starter Kit**
  - Continue development; share/obtain feedback on digital artifact use
- **Engage with Acquisition Programs**
  - Establish criteria for use of Digital Engineering artifacts for decision points
- **Update Competencies across Acquisition Curricula**
  - Identify Digital Engineering education and training outside of acquisition curricula
- **Update Policy and Guidance (Engineering, et al)**
  - Develop/update governance processes, policy, guidance and contracting language
- **Transform Acquisition Practice**
  - Engage acquisition users
  - Incorporate rigor from Digital Engineering practices and artifacts into system lifecycle activities

Instantiation of Digital Engineering practice is necessary to meet new threats, maintain overmatch, and leverage technology advancements

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Ms. Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695

philomena.m.zimmerman.civ@mail.mil

Integrating Computational Engineering Tools into Industrial Product Development Workflow

Loren Miller

DataMetric Innovations, LLC

lorenmiller@mac.com

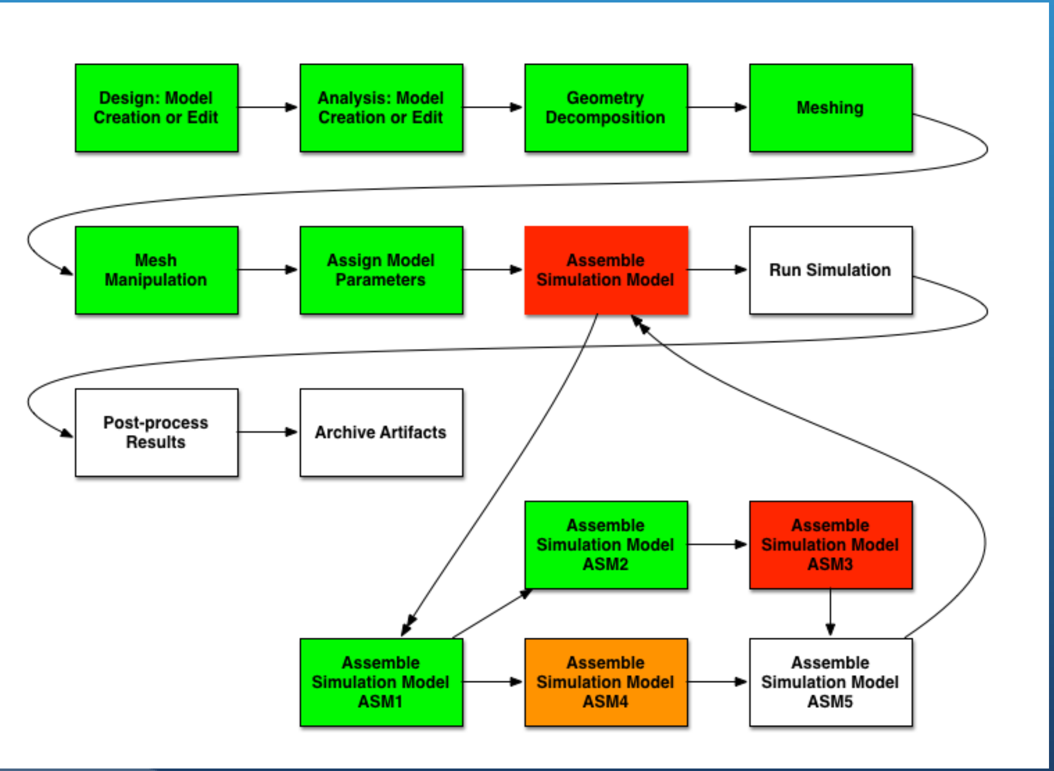
330-310-3341

Abstract # 19776

NDIA Systems Engineering

Springfield, VA

25 October 2017



My Background

- While at Goodyear, my responsibilities included
  - Manufacturing process improvement
  - New product development
  - Project management
  - Physics research
  - Physics-based virtual prototyping
  - RD&E's IT systems including HPC

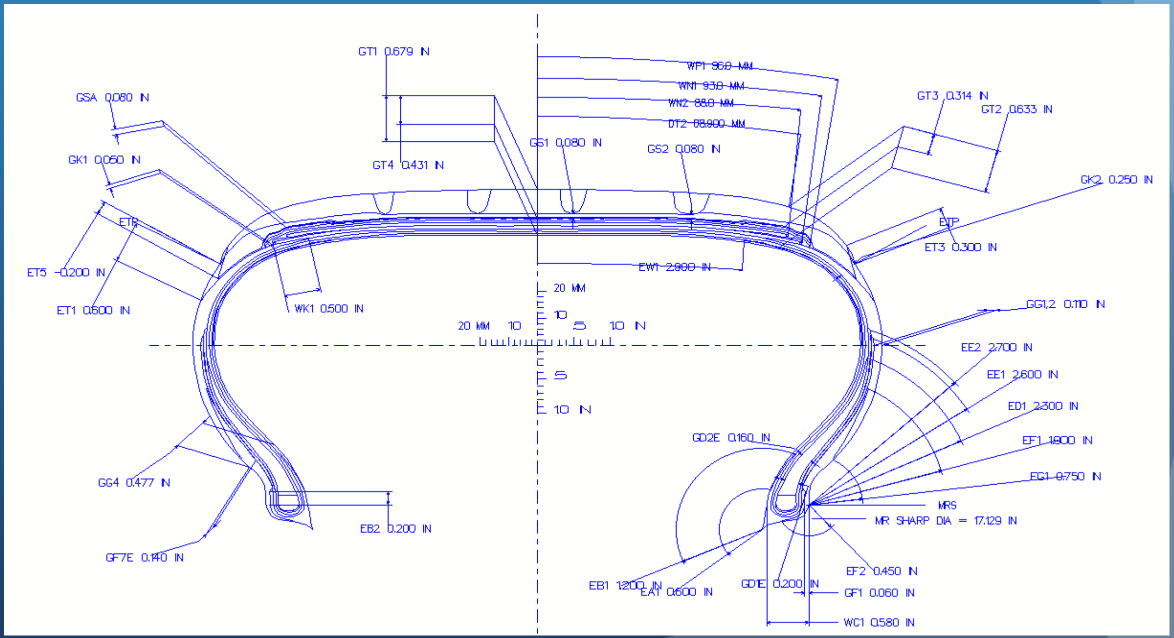
- Now President, DataMetric Innovations, LLC
  - "Intersection of Science, Engineering, and IT"

- The opinions expressed are my own and do not necessarily reflect the views of The Goodyear Tire & Rubber Company.

Systems Engineering Tools

- Platform-based design systems – carcass & tread
  - Carcass system began development in 1986.
    - Existing systems were electronic drafting tools.
    - Commercial packages' "lines & splines" were insufficient.
  - Goodyear's system incorporated
    - Parametric design standards
    - Knowledge-based rules

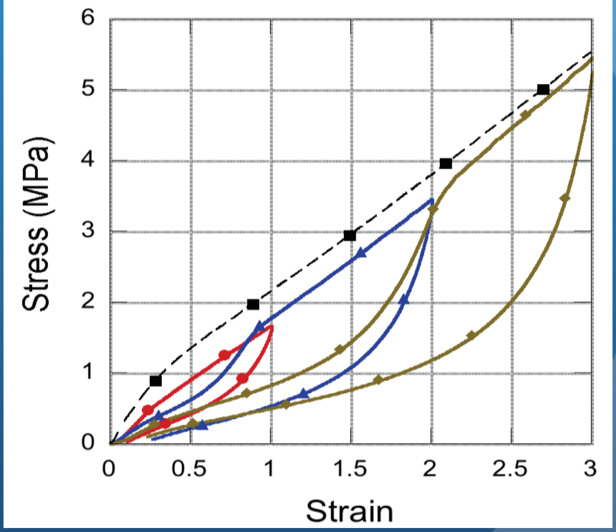
Similar approach for tread patterns



Systems Engineering Tools

- Model-based virtual engineering system
  - Began major development effort in 1992
    - Director of Analysis for a large computational analysis firm recommended their *linear elastic* FEA package. Wrong!
  - Rubber's material properties
    - Highly non-linear
    - Viscoelastic
    - Incompressible
      - Poisson's ratio: .499…
      - Hexahedral meshes required
    - Mullin's effect: stiffness & hysteresis both history dependent
    - Payne effect: modulus depends on temperature, strain, & frequency

Mullins Effect

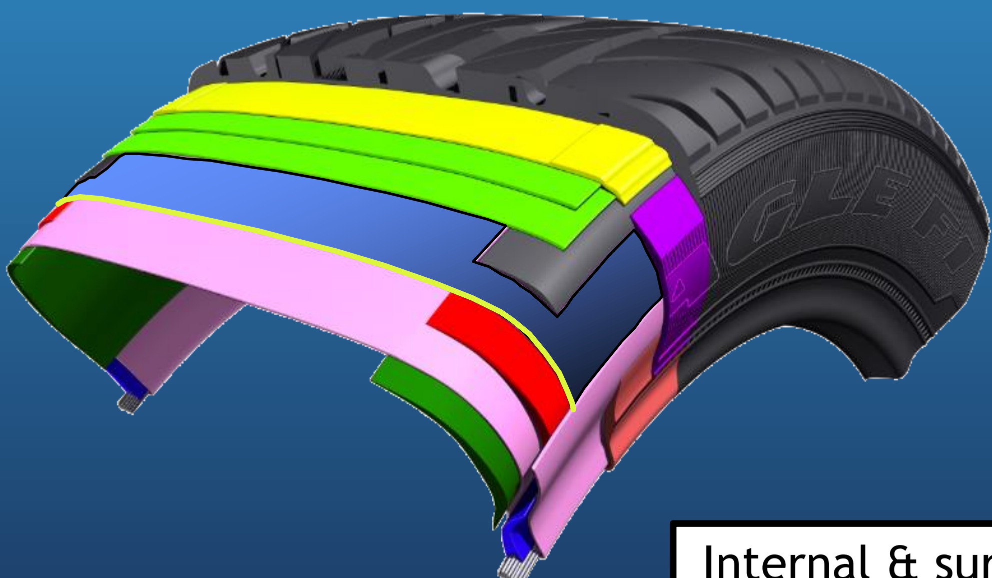


Hanson, Hawley, and Houlton,
Los Alamos National Laboratory,
"A Mechanism for the Mullins Effect," 2006.

Material complexity

Systems Engineering Tools

- Model-based virtual engineering
  - Thin layers with large differences in moduli
  - Inextensible fiber reinforcements
  - Detailed tread patterns
  - Wide eigenvalue spectrum



Internal & surface complexity

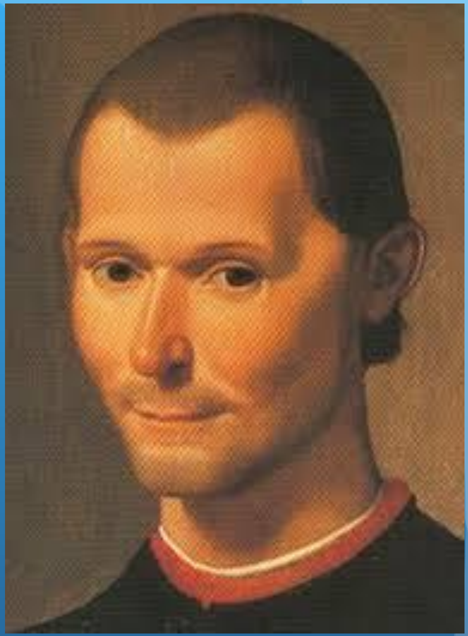
Model-based Tool Creation

- Goodyear’s model-based virtual engineering requirements exceeded 1990’s analysis software capabilities.
- Sandia CRADA began in 1993.
  - Partnership was successful beyond expectations.
    - Lab Director in 1995: “Solved previously intractable nuclear weapons design problems”
    - One of Goodyear’s standard analyses was reduced from *32 years* [*“if possible” estimate using best commercial software*] to *5 days* in 2005.
    - Goodyear provided significant VV&UQ for portions of Sandia’s Sierra Mechanics Tool Suite.
      - Tens of thousands of runs per year on Goodyear’s HPC

Goodyear/Sandia partnership solved key technical problems!

Great Analysis Codes Weren’t Sufficient

- Niccolò Machiavelli, *The Prince*
  - “It must be remembered that there is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than a new system. For the initiator has the enmity of all who would profit by the preservation of the old institution and merely lukewarm defenders in those who gain by the new ones. This coolness arises partly from fear of the opponents,… and partly from the *incredulity of men, who do not readily believe in new things until they have had a long experience of them*.”



Paradigm shifts require both cognitive and emotional adjustments.

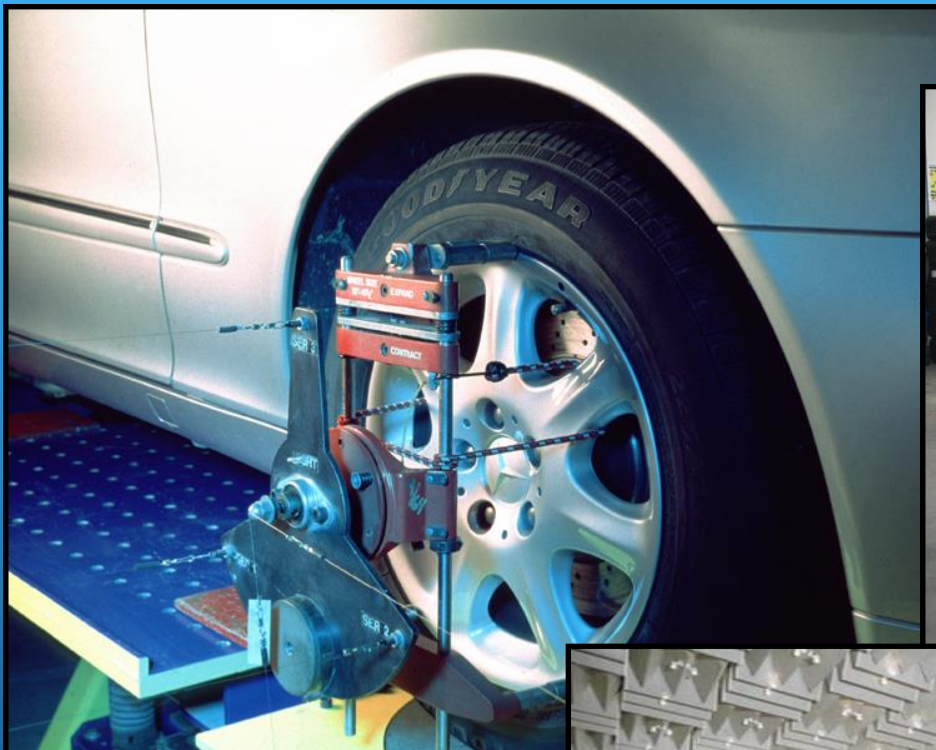
Extensive Test Track Facilities

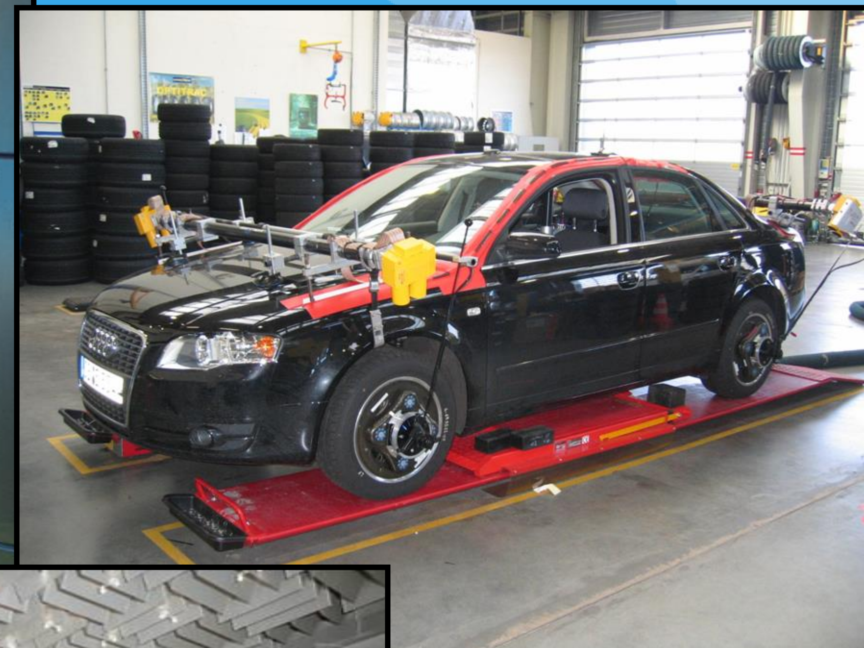
San Angelo, Texas

Americana, Brazil

Seven test tracks worldwide

Extensive Laboratory Test Facilities





Design/build/test

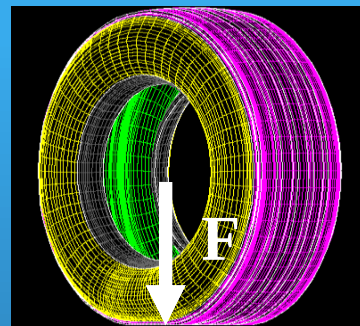
Workflow Was Critical

- Physical prototype-based engineering had been developed, validated, and systematized over a period of 100+ years.
- No one wanted to be the first to take the risk of converting to virtual prototyping, even with validated computations.
- *Designers had confidence in and relied upon a logical sequence of physical tests.*

Physical test workflow was critical!

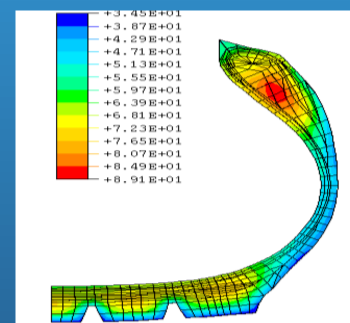
Physical Test Workflow Virtually Replicated

Predict statics



Each virtual test refined the feasible design space in a sequence familiar to the designer.

Predict steady state



Predict transient dynamics

Designers Had to Do Their Own Analyses

- Reliable virtual prototyping and a physical test-based analysis workflow weren't enough.
- P*roduct designers had to do their own analyses*.
  - Designer/analyst interface was problematic.
    - Time delay between a designer's questions and the analyst's answers was too long. Designers forgot their questions.
    - Designers: "Analysts never answered my key questions anyway."
  - Note: virtual prototyping did not eliminate analysts.
    - Analysts transitioned from running "routine analyses" to developing new analytical methods and standardizing them for the designers.
    - Most analysts preferred the new opportunity.

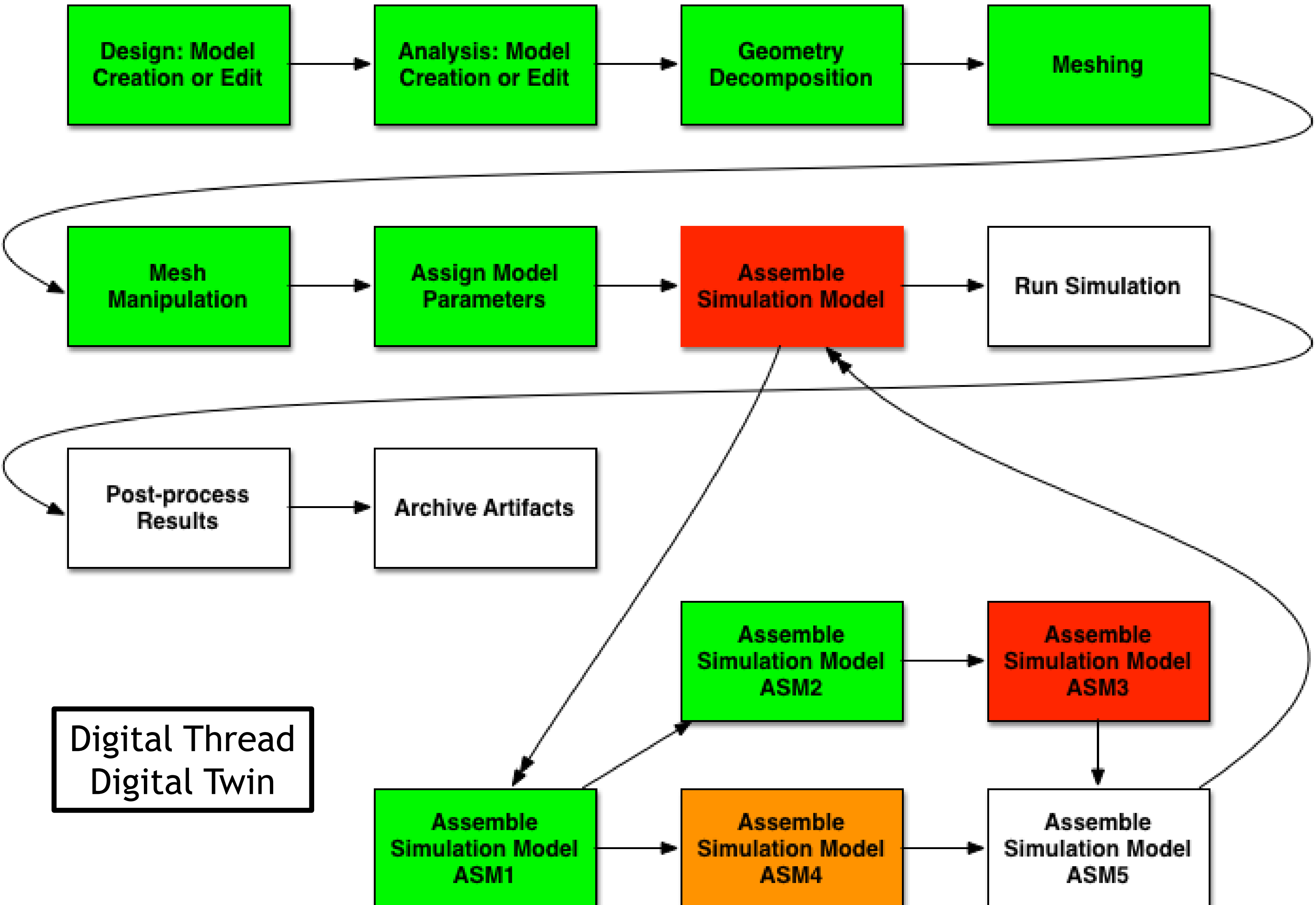
Hands-on analysis expanded designers' knowledge & intuition

Analysis Standardized for Designers' Use

- Entire computational analysis process was standardized and underwent extensive VV&UQ to ensure accurate & repeatable results *regardless of which designer did the analysis*.
  - Data credibility
    - Geometry creation
    - Meshing
    - Boundary conditions
    - Material properties
  - Technical coherence
    - Analysis software
    - Post-processing
    - HPC hardware, compilers, libraries,…

From "art" to "engineering"

Analysis Workflow Automated



Digital Thread
Digital Twin

Bottom Line Results

- ***New product development time was reduced 75%***, from over three years to less than one, including final prototype testing.
- ***Product testing costs were reduced by 60%***, resulting in $100 million annual savings.
- More new products were developed with more innovative designs as a result of improvements in designers' ***knowledge, intuition, and creativity - "Innovation Engine"***.
- The new process and the resulting first product won both ***R&D 100 and CIO 100 awards***.

Time was and is of the essence.

Air Force Wants to Shorten Next Gen Fighter’s Development Timetable

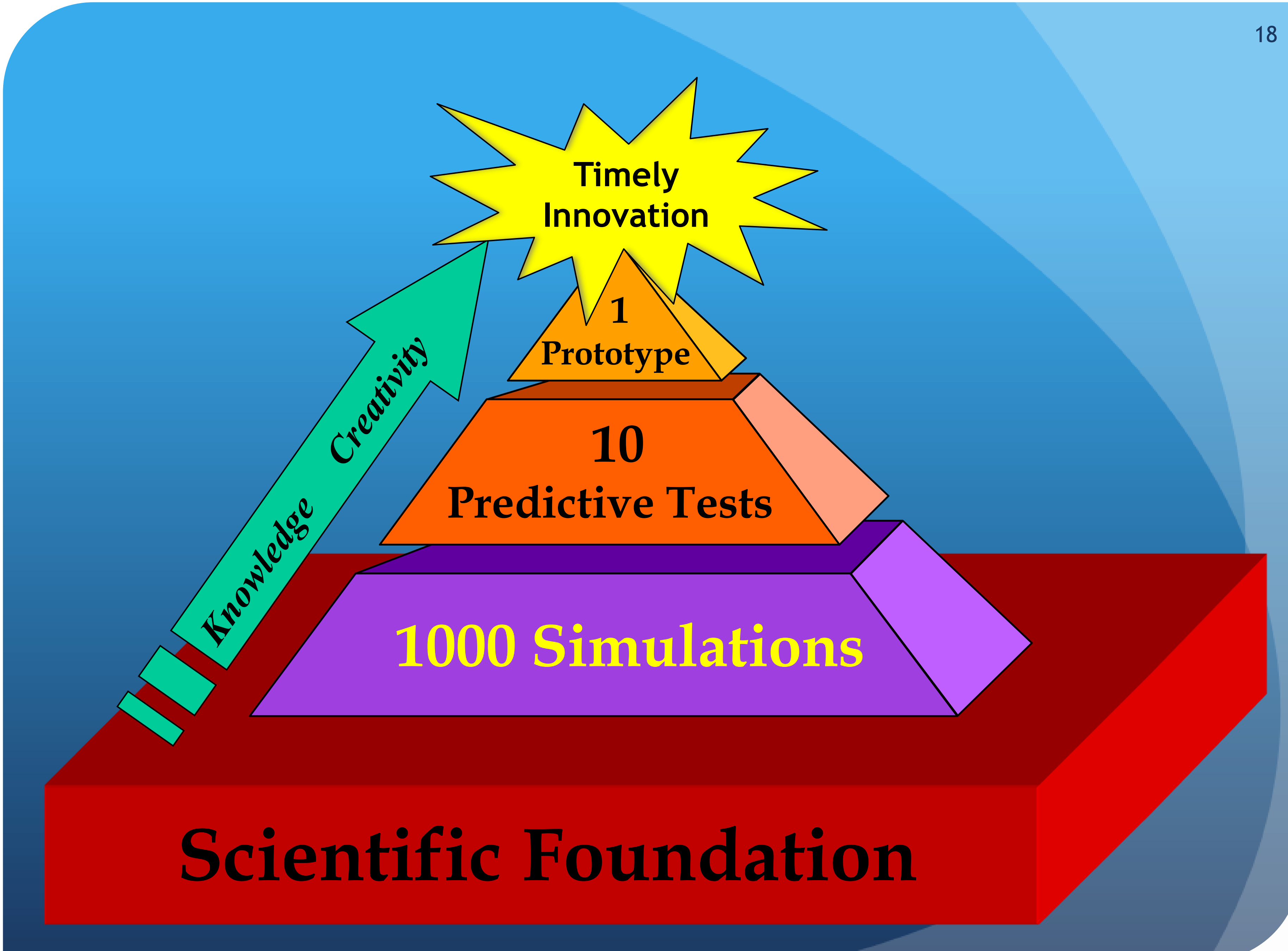
What’s your reaction?

Article by Vivienne Machi, *National Defense*, 9/19/2017
Photo By Rob Shenk, Great Falls, VA

Accelerating Technology Development & Procurement

- Subject: Accelerating Enterprise Cloud Adoption
  - "I am directing aggressive steps to establish a culture of experimentation, adaptation, and risk-taking; to ensure we are employing emerging technologies to meet warfighter needs; and to increase speed and agility in technology development and procurement."

    Patrick M. Shanahan, Deputy Secretary of Defense, 9/13/2017


Timely Innovation
1 Prototype
10 Predictive Tests
1000 Simulations
Knowledge
Creativity
Scientific Foundation

Capstone: A platform for geometry, mesh and attribution modeling for physics-based analysis and design

DOD HPC MODERNIZATION PROGRAM

Dr. Saikat Dey,

Code 7131, US NRL, Washington, DC

Outline

- **Motivation, Strategic needs and Challenges**
- **Capstone – the product**
  - Overview
  - Users and Usage Scenarios
- **Current status**
  - Key capabilities
  - Applications/Impact
- **Closing remarks**

Motivation

Goal

Improve efficiency of DoD acquisition engineering by reducing time, cost and risks in research, development and sustainment of weapon systems

Approach

○ **Develop Next-Generation Computational Solvers & Optimizers**

○ **Insert More (Multi) Physics-Based Analysis Earlier in the Design-Cycle**

Critical Hurdles

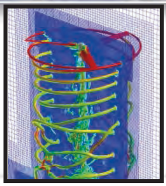
Human Effort & Calendar Time to Produce an Analyzable Representation (Model) of a Design or System

Significantly more time is often spent in 'preparing' the input data needed by solvers than is used by the solvers to solve it.

Computational Research and Engineering Tools and Environments (CREATE) Program Focuses on Four Project Areas

- **Air Vehicles (AV)—Air Force, Army & Navy**
  - Aerodynamics, structural mechanics, propulsion, control, …
- **Ships—Navy**
  - Shock vulnerability, hydrodynamics, concept design
- **Radio Frequency (RF) Antennas—Air Force, Army & Navy**
  - RF Antenna electromagnetics and integration with platforms
- **Mesh and Geometry (MG) Generation**
  - Rapid generation of mesh and geometry representations needed for analysis

CREATE tools will support all stages of acquisition from rapid early stage design to full life-cycle sustainment



Design concept

Seakeeping and resistance

Shock vulnerability

Aircraft and aircraft carrier meshes

Military platforms with antennas

Geometry and Meshing Needs

"Let no one ignorant of geometry enter" - Plato

Geometry needs to be appropriate for analysis and meshing

- Valid
  - Dimensionally correct (1-,2-,3-D or mixed-dimension, non-manifold)
  - "Water-tight" (no gaps), non-self-intersecting
- Accurate
  - Match a shape to a given tolerance
  - Maintain the accuracy and rate of convergence of the solvers/code

Meshing needs to be appropriate for physics and discretization

What takes time and effort ?

- Geometry repair/clean-up
- De-featuring (geometry good for Physics A is not suitable for Physics B)
- Lack of automation and robustness in meshing (all-hex, complex boundary layers)
- Attribution, multi-component model preparation

CREATE-MG: Mission Summary

Develop Capability and Tools for:

Rapid, Scalable and automated generation of analyzable representations (geometry, mesh, attribution data) for accurate and scalable physics-based solvers

Enabling:

- Multi-physics based analyses earlier in the design process
  - ✓ Rapid turnaround time and automation key to effective design optimization
- Generation and adaptation of meshes for complex and hi-fidelity analyses
  - ✓ Reduce time and human effort needed to prepare complex geometries for meshing that is suitable for given (multi)-physics and accuracy needs

Key Technical Challenges:

- Analysis-suitable geometry-preparation
  - Automation of geometry clean-up, repair and de-featuring
- Automated hexahedral mesh generation
  - Hex-dominant, all-hexahedral (unsolved)
- Automated, high-quality boundary-layer meshing for complex geometries
- Parallel (distributed) mesh representation, generation and geometry-based adaptation
  - Needed for ultra-large meshes for high-fidelity analyses
- Multi-scale geometry and mesh modeling
  - Complex antenna patterns (nm-mm) integrated into large structure O(100)m

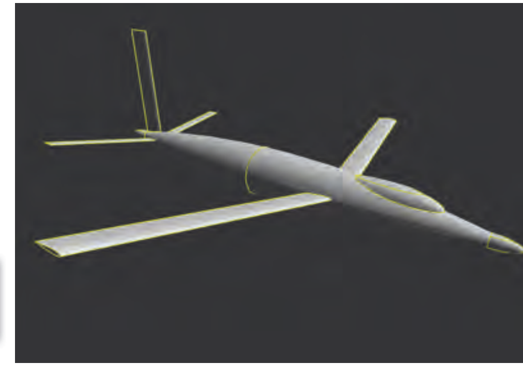
CAPSTONE Critical Requirements

ID	Description
MG-00	Geometry Import (CAD/kernel-native, IGES, STEP)
MG-01	Parameterized Geometry Creation
MG-02	Dependency-based Associative Modeling
MG-03	Geometry Repair
MG-04	Model De-Featuring & Idealization
MG-05	Robust Surface Meshing Algorithms
MG-06	Robust Volume Meshing Algorithms
MG-07	Geometry-based Mesh Generation & Adaptation
MG-08	Multi-Scale Models
MG-09	Legacy Component Integration
MG-10	Analysis Model Attribution
MG-11	Accurate and Scalable Runtime Geometry Access
MG-12	Core framework (MG internal infrastructure requirement to support all of the above)

- Each requirement manifests into one or more ***usecase(s)***
- ***Usecase(s)*** drive development of specific ***capabilities***

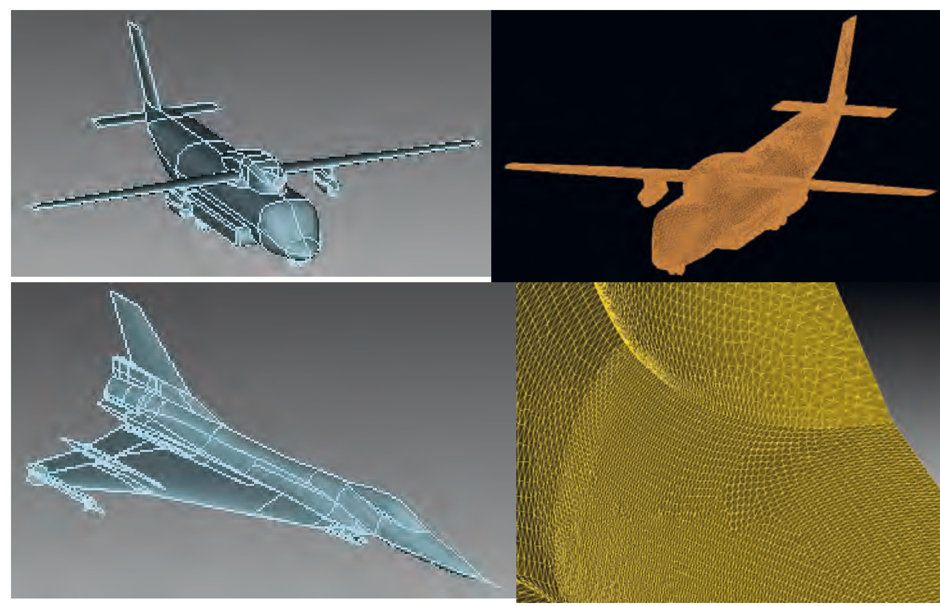
Capstone – Overview

Capstone provides geometry and meshing needs for all phases of acquisition engineering (conceptual-, preliminary-, detailed-design and operational-support)



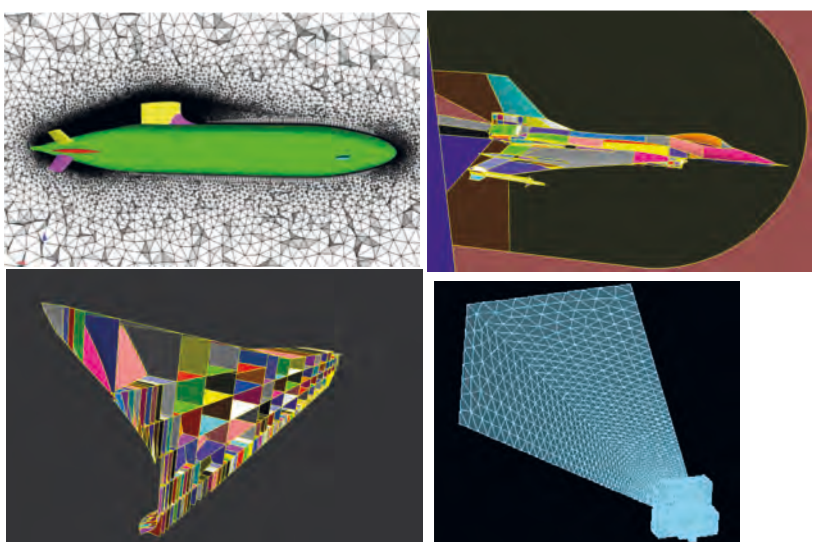
CAPSTONE: SDK

<u>Enable parametric, associative geometry and meshes</u> in AV:DaVinci, Ships:RDI; *geometry-based mesh adaptivity*



CAPSTONE: GUI

<u>Produce analyzable representations</u> for complex and detailed analysis



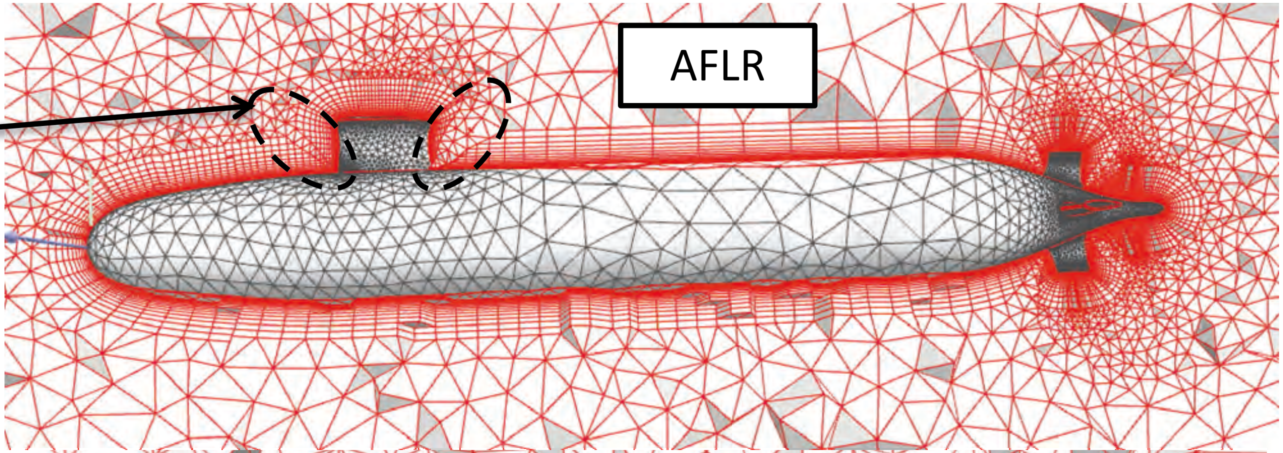
Capstone Architecture and Impact

- **Well abstracted reusable functional modules**
  - Three main modules: Geometry, Mesh and Attribution
    - Well defined APIs
  - Reusable Functions built on top of basic module APIs
    - Functions may be reused to build more high-level functionality
- **Extensible using plugins**
- **All the core capabilities accessed using the SDK**
  - Capstone frontend (GUI) itself uses the SDK
  - Foundation enabling other tools/solvers
    - CREATE-RF Sentri (Gen 2) solver embeds Capstone for geometry-driven analysis capabilities
    - Capstone is a key component of CREATE-Genesis and is the foundation for Genesis-Design component
    - CMB tools from ERDC-ITL embeds the Capstone SDK for geometry and mesh-generation capabilities

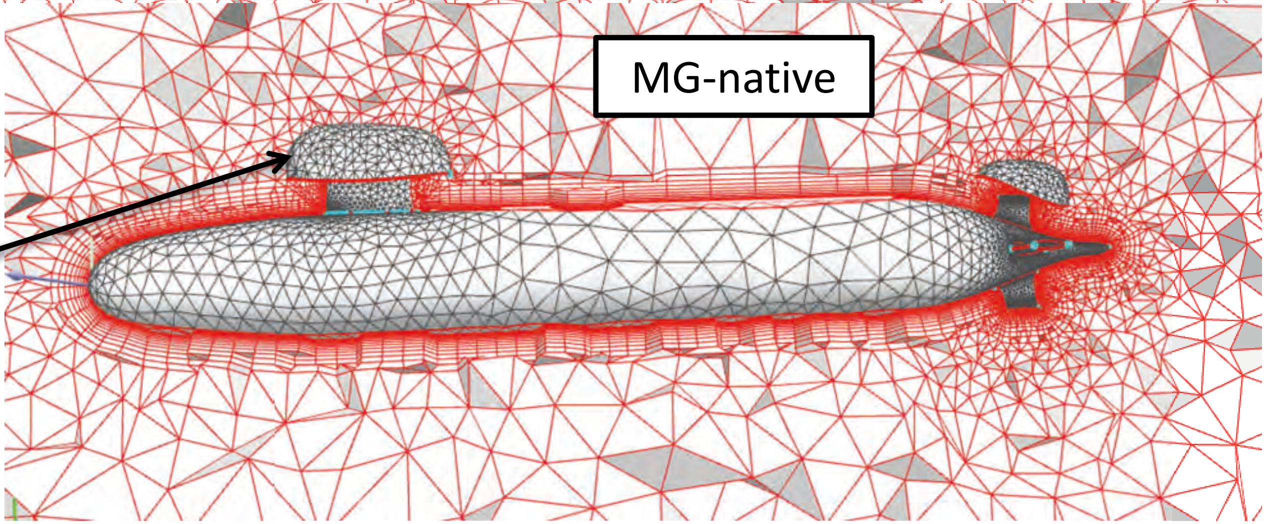
Capstone 7.0 Highlights

- **MG Native Volume Meshing**
  - Not required to exclusively use AFLR

- **BL 'unzipping'**
- **Euler-mesh creeps in**

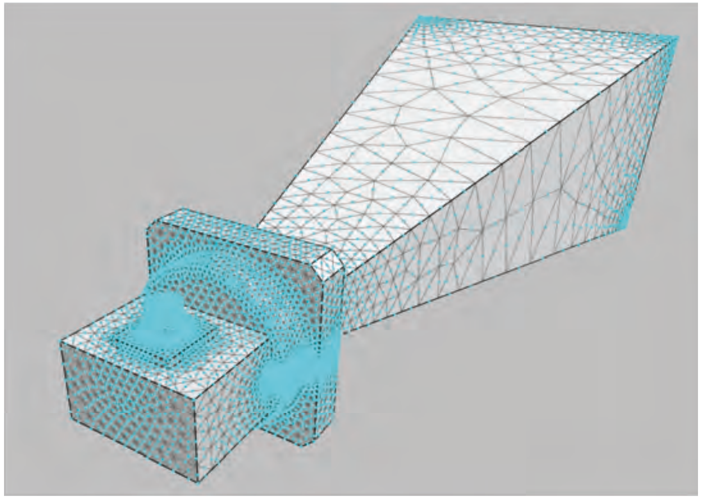


- **BL mesh grows correctly all the way**
- **Terminates with a smooth lifted surface**

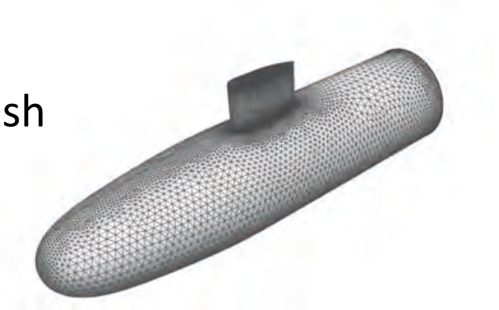


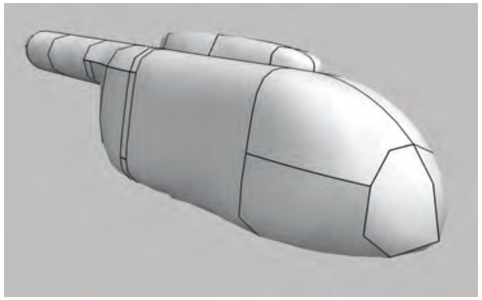
Capstone 7.0 Highlights

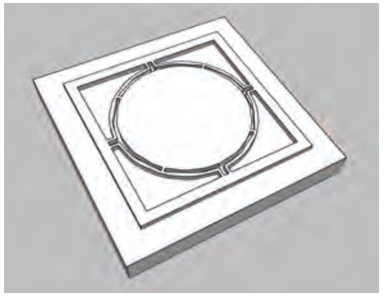
- **High-order curvilinear mesh generation**
  - Quadratic and cubic Lagrange mapping
    - successfully used by RF Sentri hp-version
  - Conformal to actual CAD geometry



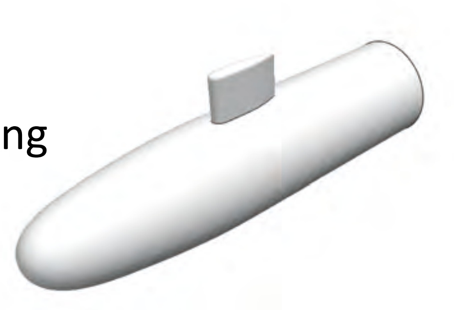
Linear mesh

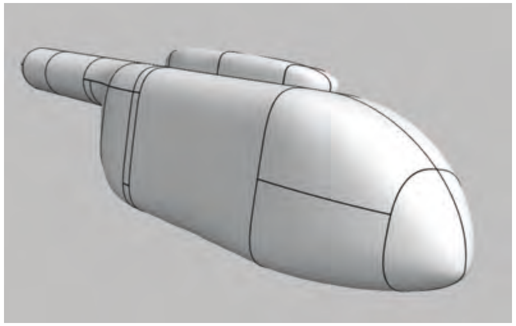


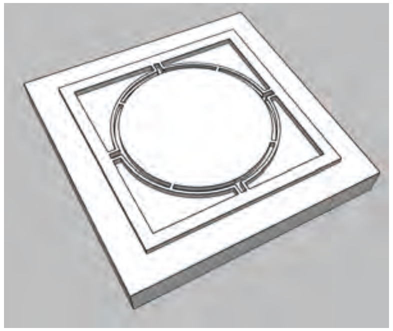




CAD-conforming mesh

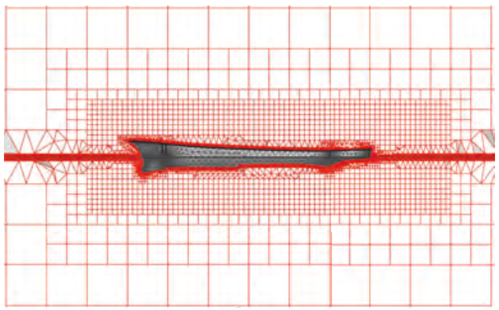


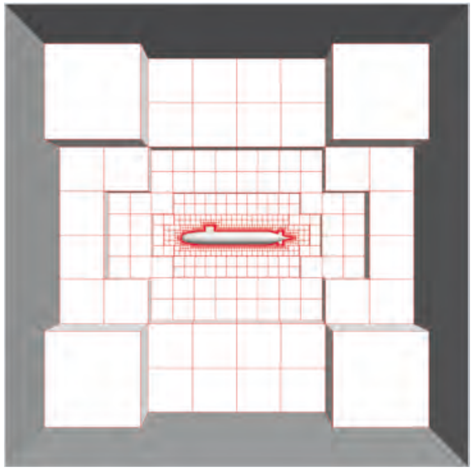


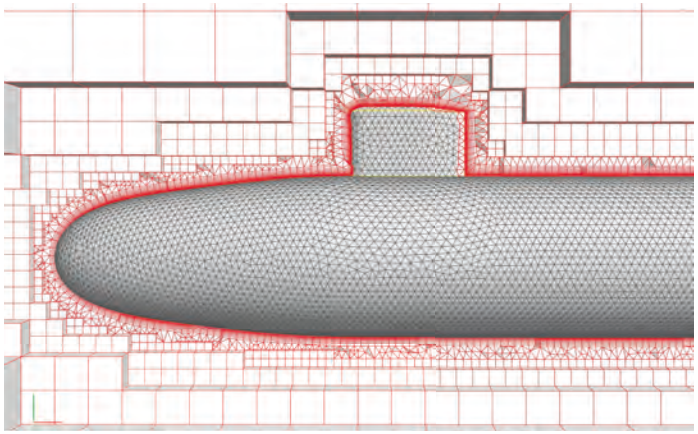


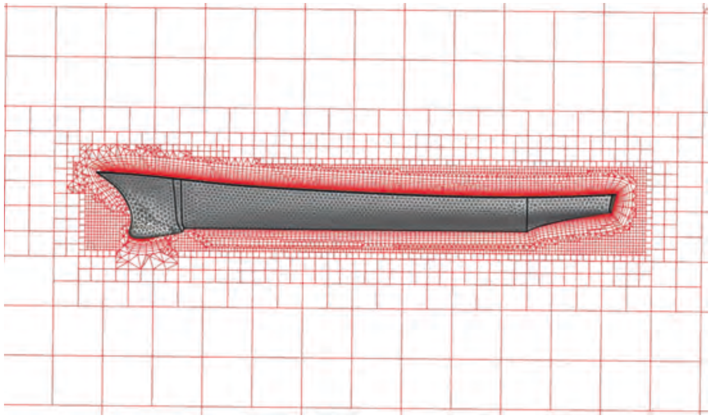
Capstone 7.0 Highlights

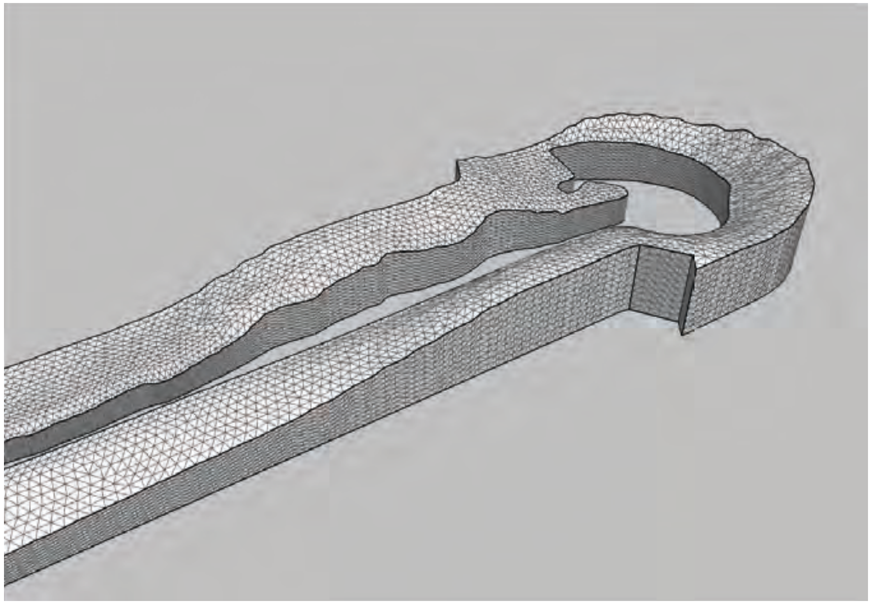
- **Hex-dominant and Extrusion-based Volume Meshing**



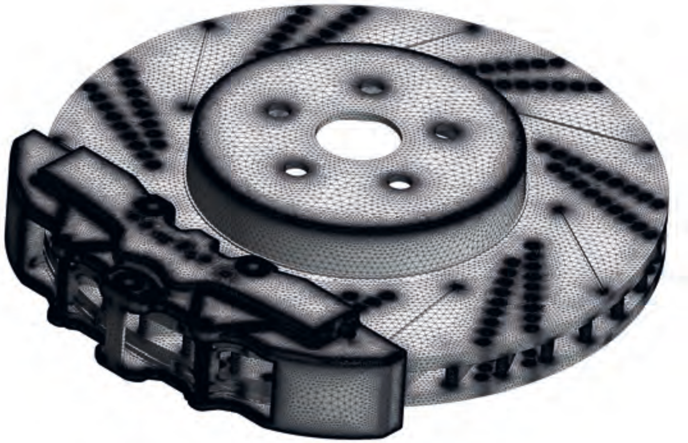


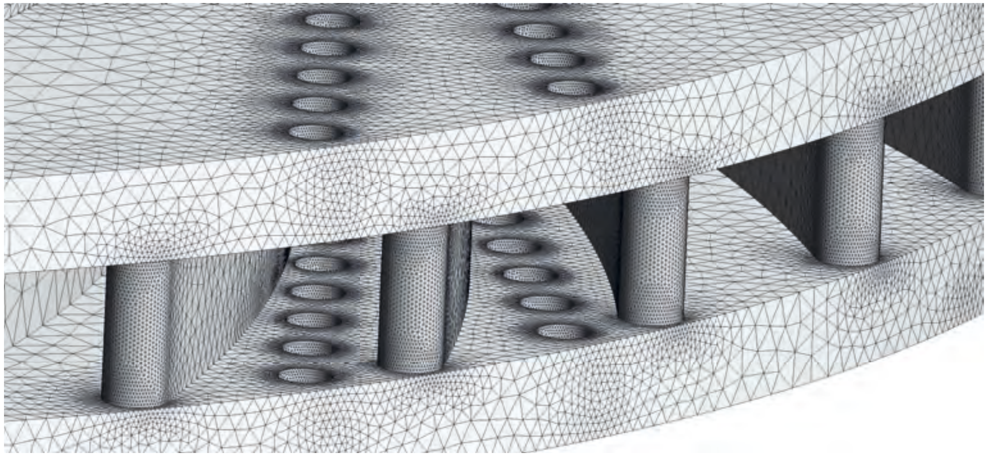


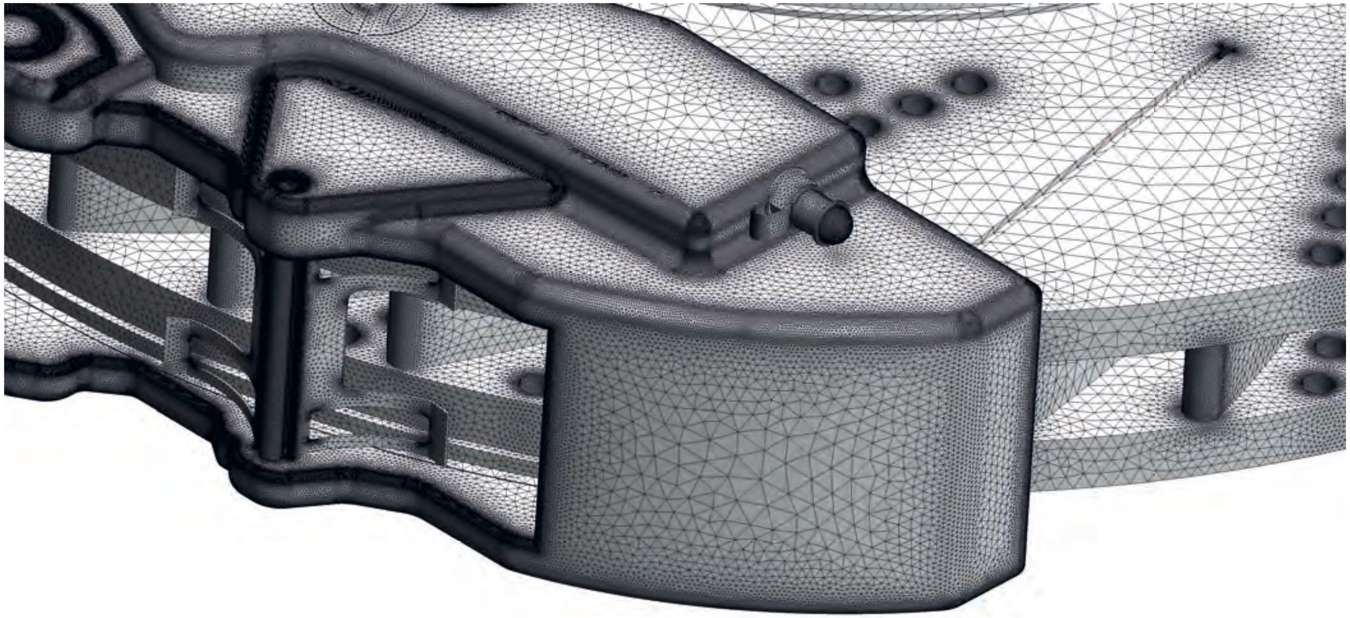




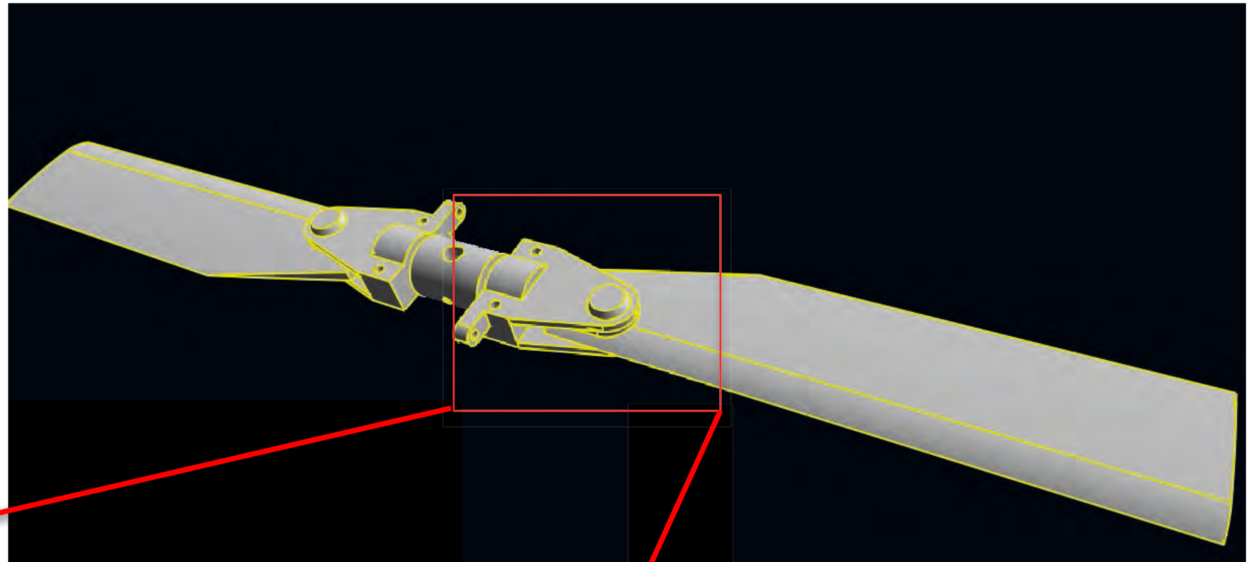
Surface mesh: Break disk

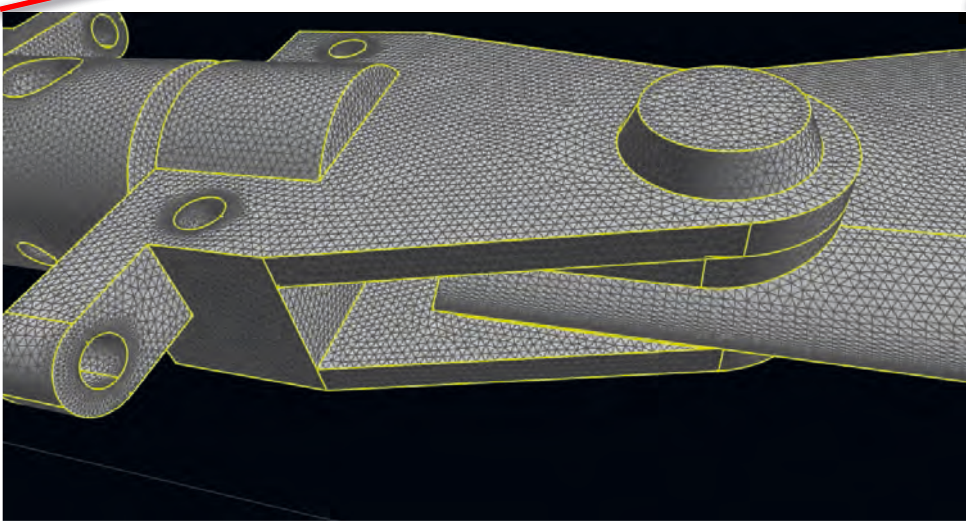




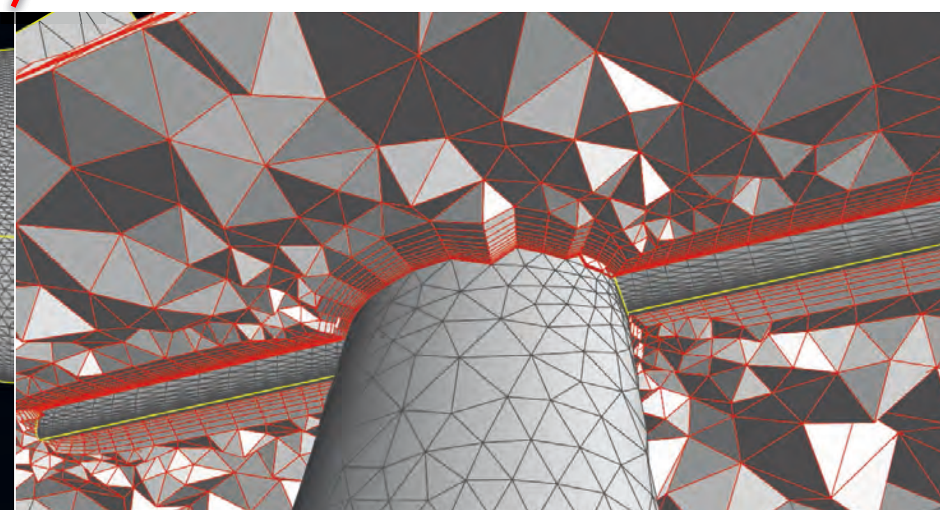


Anisotropic surface meshing





Anisotropic surface meshing



Combined surface and volume BL (crinkle-cut)

MG-Native Volume Meshing

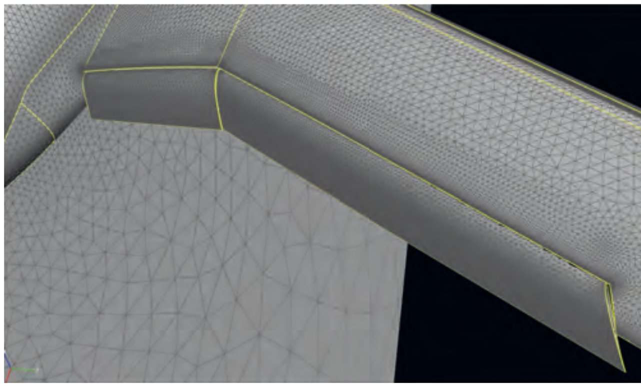
- **AIAA High-Lift Workshop Geometry**

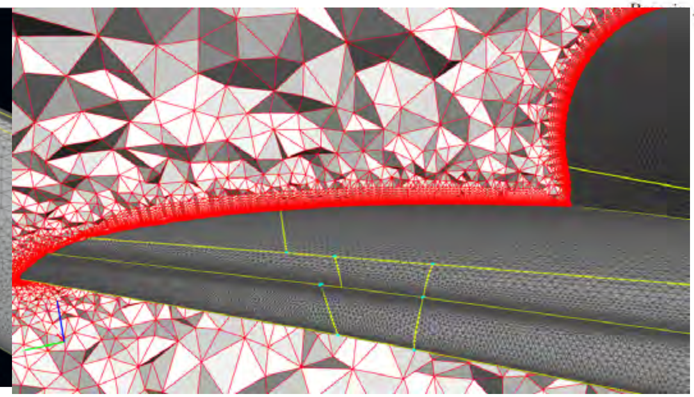
Mesh generation for high-lift aircraft geometry configurations

Saikat Dey*
US Naval Research Laboratory, Washington, DC, 20375, USA

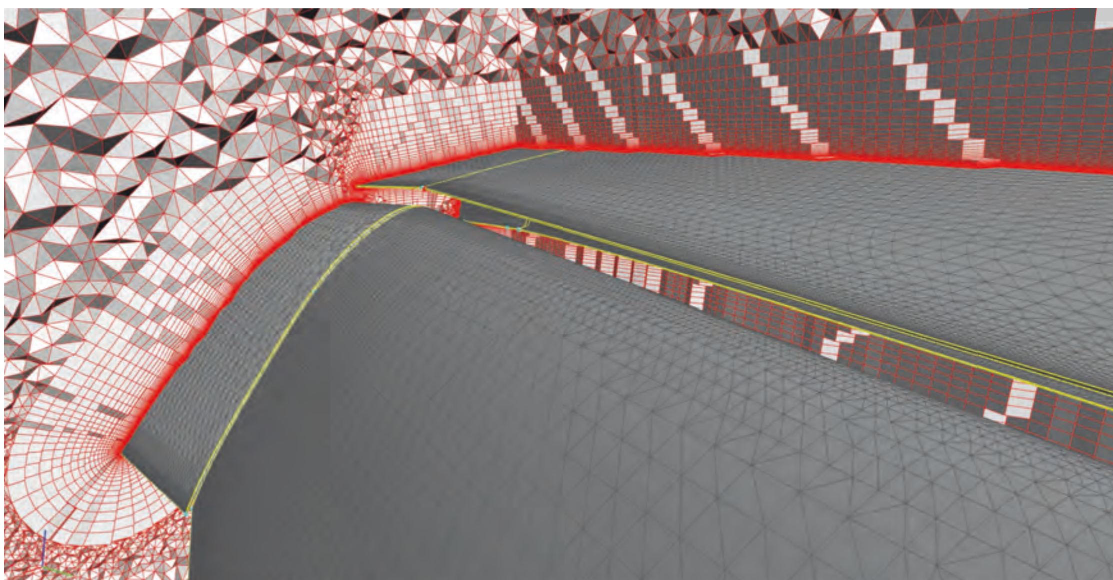
Aubry,† B. Kaan Karamete, Eric L. Mestreau and James L. Dean
Sotera Defense Solutions, Herndon, VA, 20171, USA

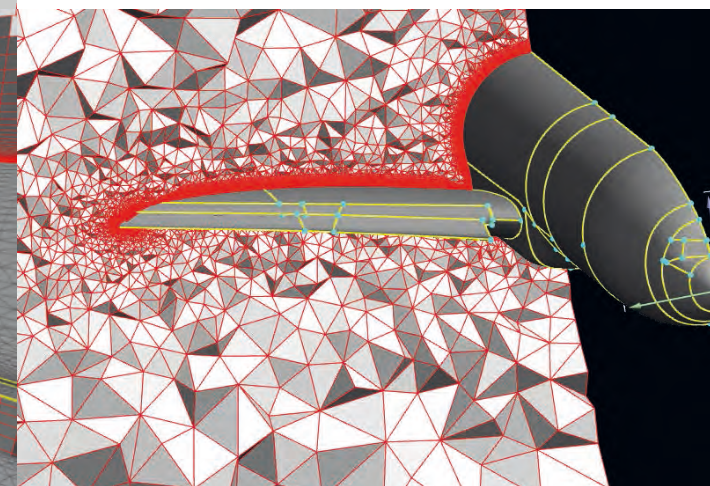
Mark Richardson
Elemental Technologies, American Fork, UT, 84003, USA



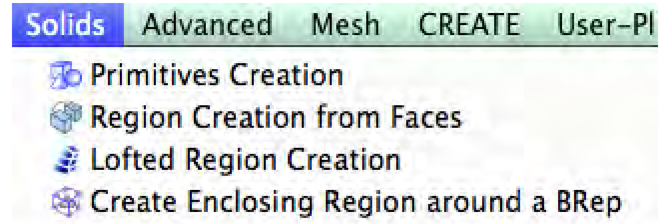


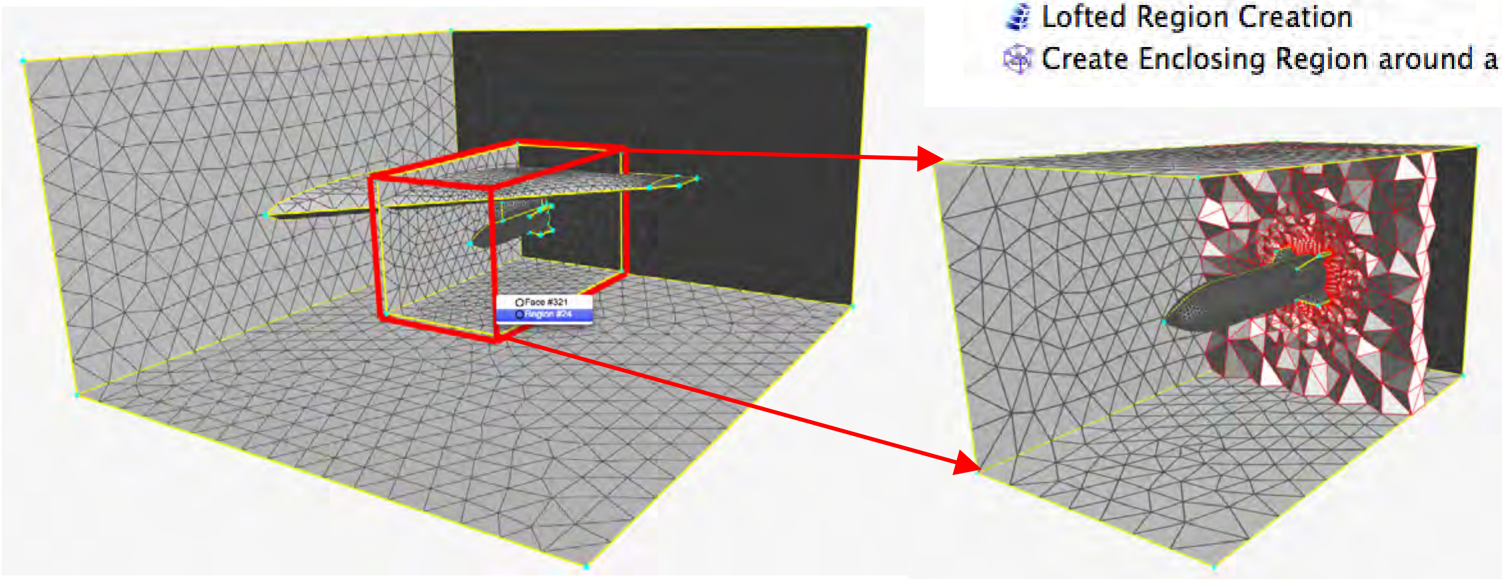
AIAA SciTech 2017
Jan 9-13,
Grapevine, TX



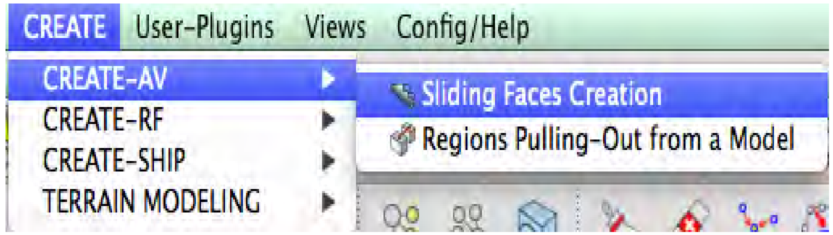


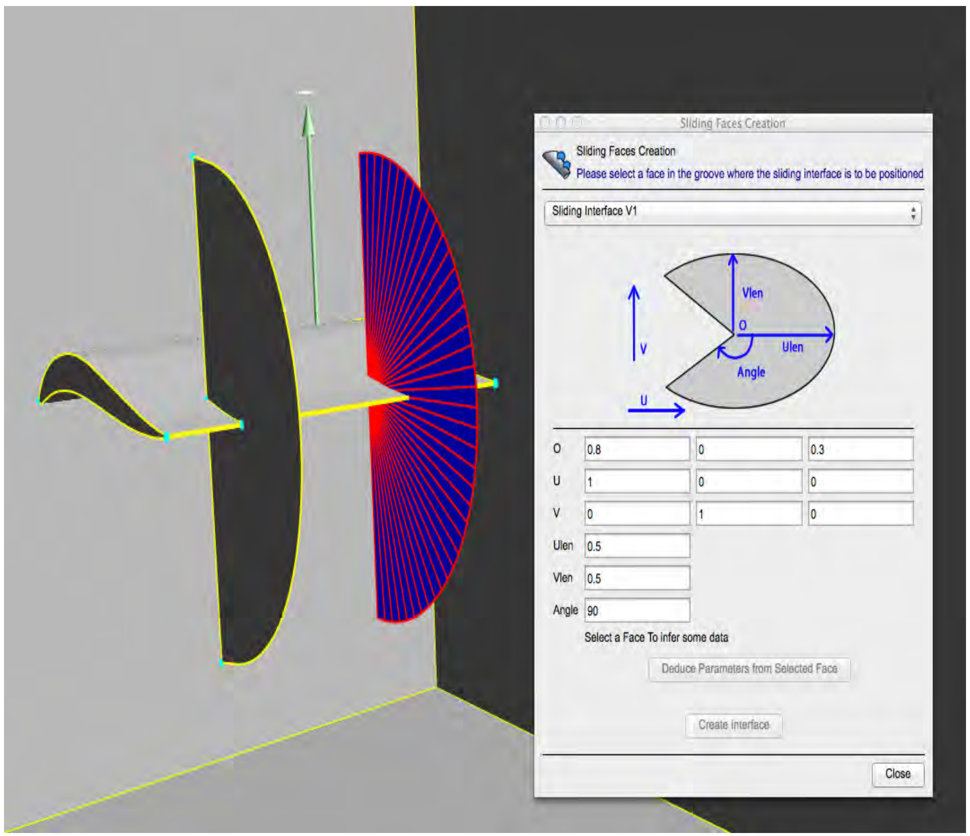
Multi-body meshing for store-separation analyses

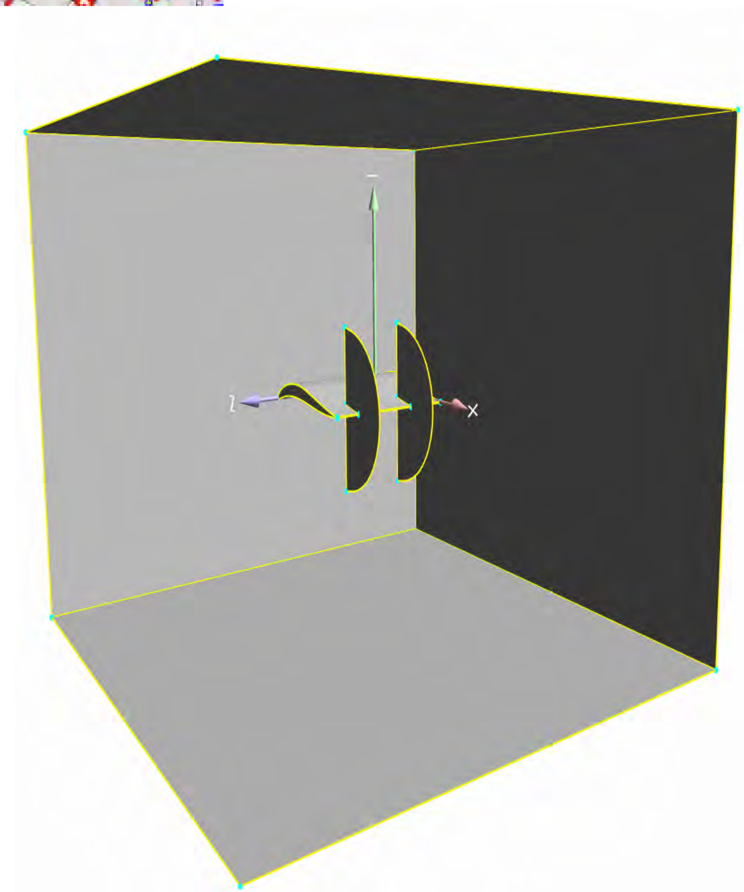




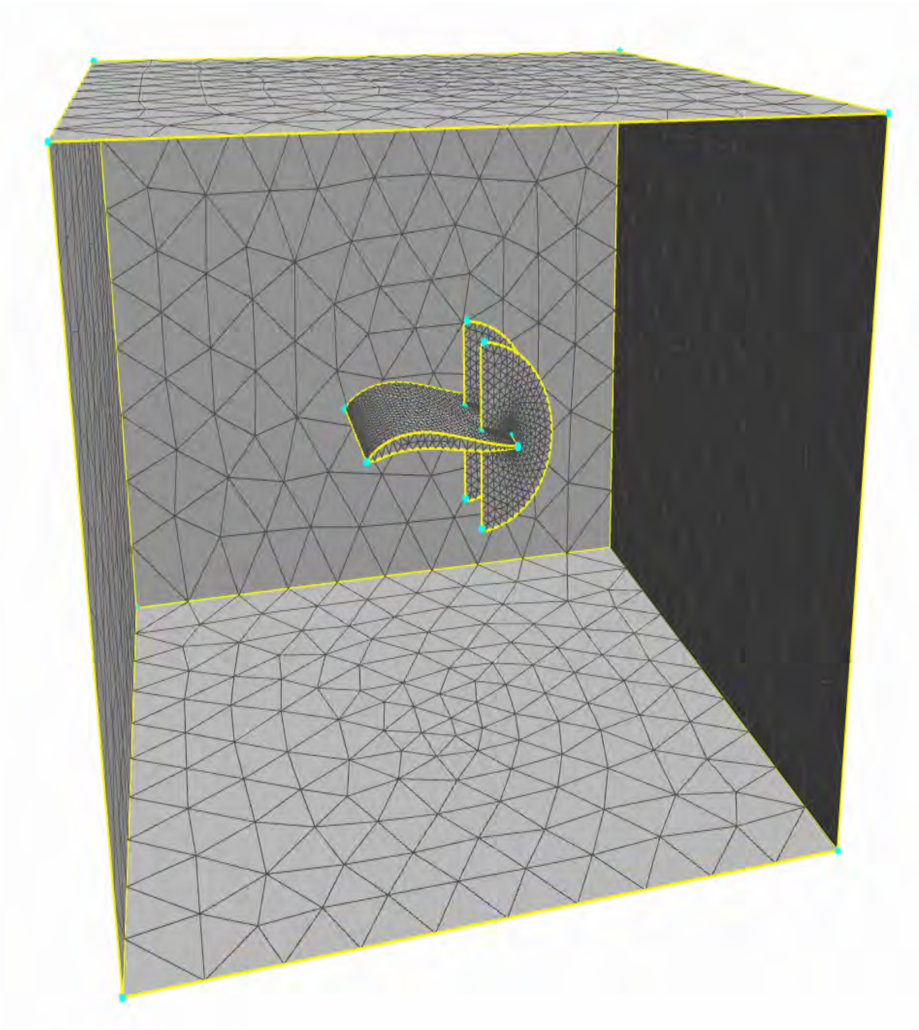
Sliding-Plane Boundary Layer Meshing

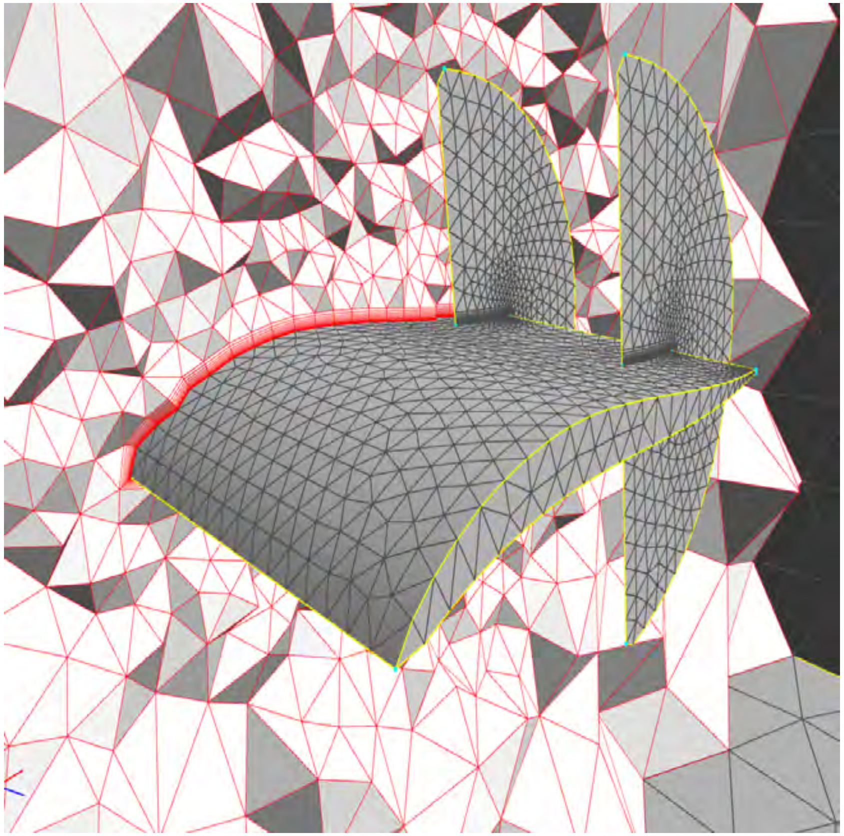






Sliding Plane Boundary Layer Meshing



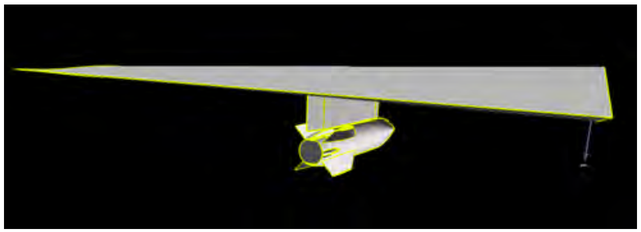


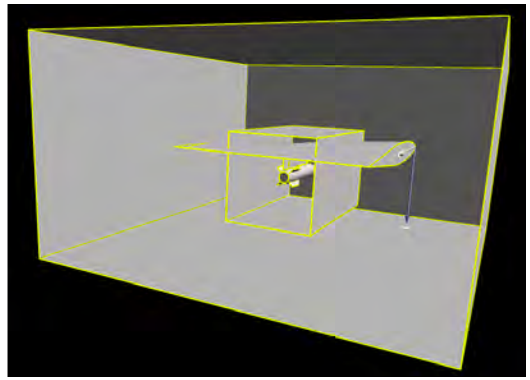
Improving turnaround time

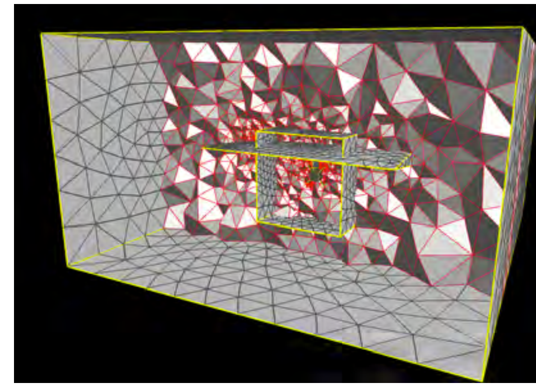
IGES Import (dirty)

Ready to mesh (clean)

BL Mesh

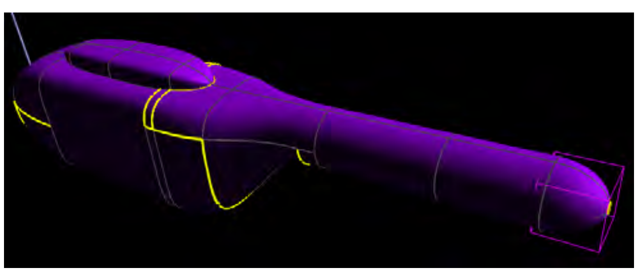


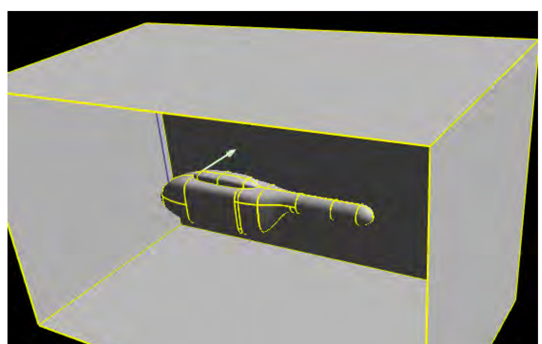


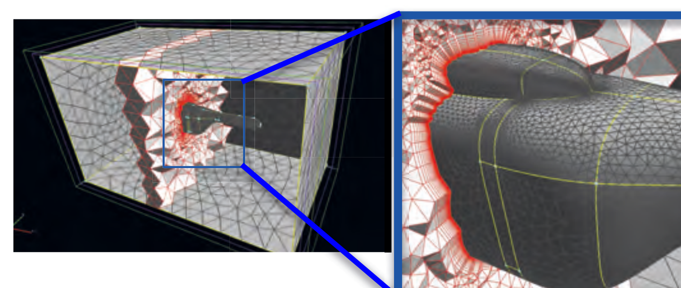


~5 min

~5 min

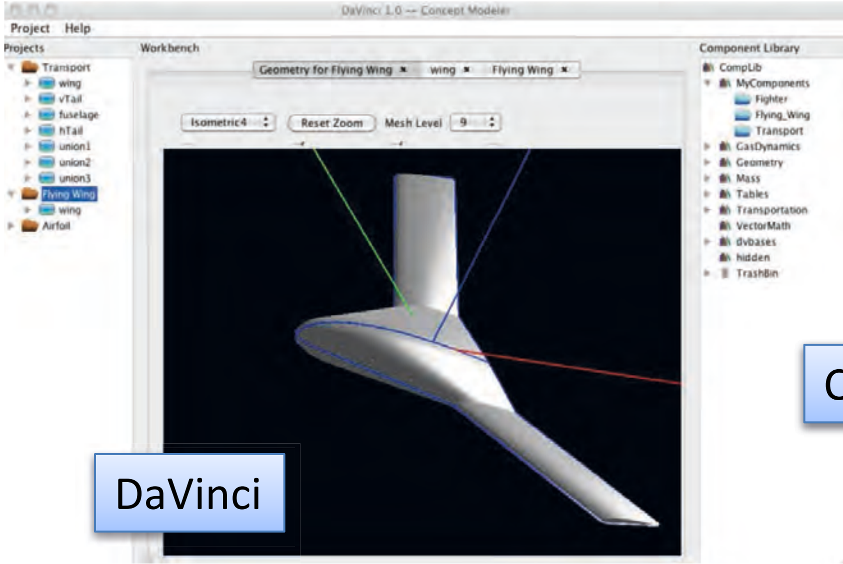


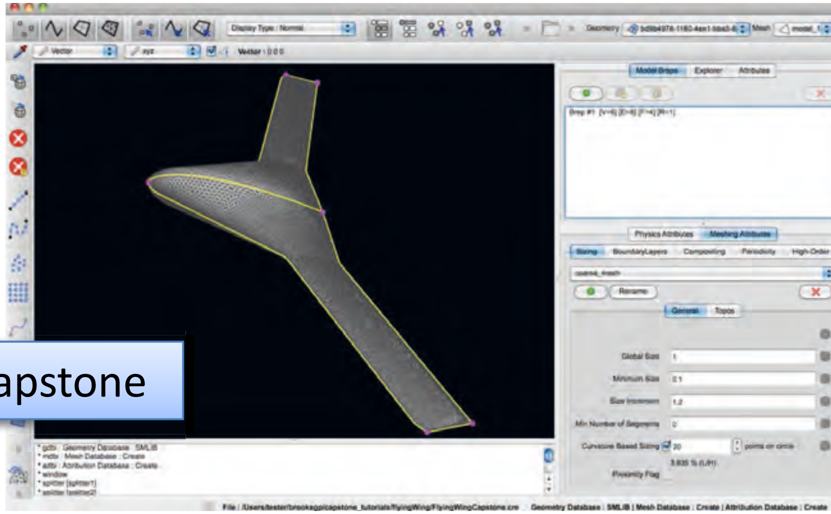


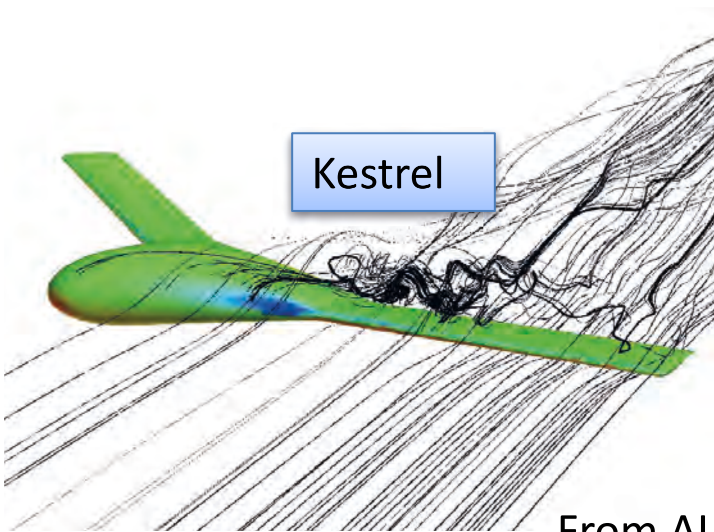


Capstone Impact: Design it better, faster and cheaper!

ASC Pilot Project





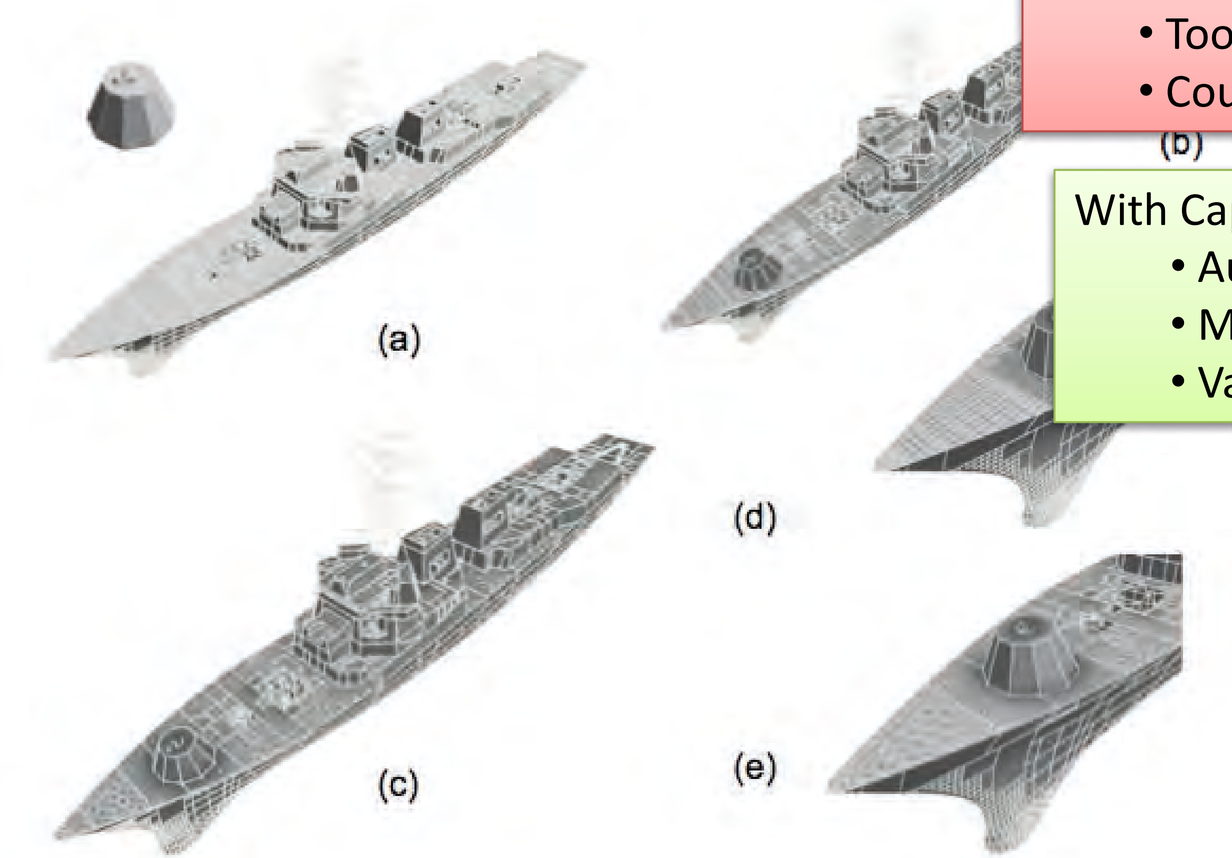


Capstone is enabling hi-fidelity physics-based analysis earlier in the design process

- Huge impact in avoiding cost later
- Recipe-based (kernel/CAD agnostic)

From AIAA paper by Greg Brooks (AV-Shadow Ops)

Capstone Impact: Automated Ship Modeling



Before Capstone:

- Manual
- Took 1 year
- Could produce invalid meshes

With Capstone:

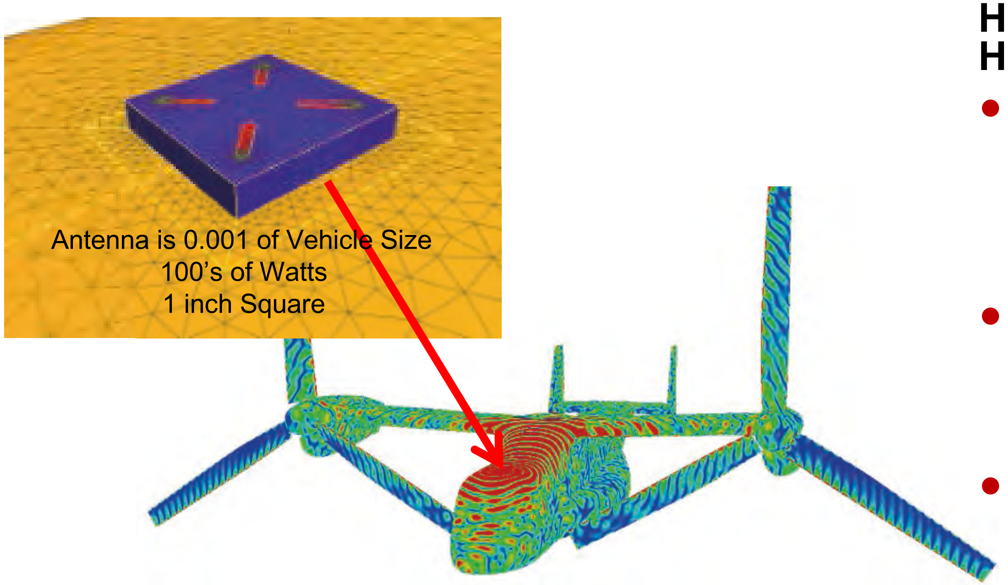
- Automated
- Month or less
- Valid

<u>Critical for enabling Computational Full Ship Shock Tests</u>

Huge improvement in turnaround time!

Weapon System Acquisition Kept on Track

In a recent Acquisition Program, the government review board found that, for one critical criterion, the contractor had neither the computational tools nor the skill set to perform the necessary design study. To avoid delay in the delivery of this system, government personnel stepped in and analyzed the device using HPCMP CREATE^{TM} RF SENTRi and Capstone software for multiple design configurations. SENTRi was also used to determine the range of input parameters that met the government's functional requirements. As a result, a design was chosen and the system was fielded on schedule.



Many Antennas per Vehicle
Cause Significant Interference

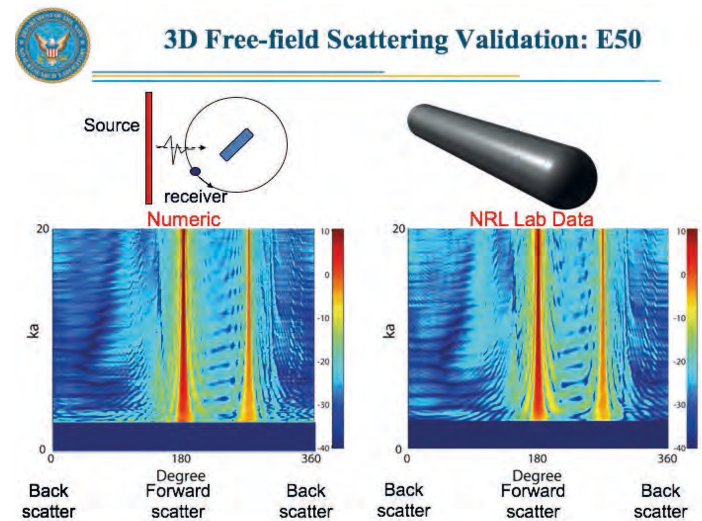
HPCMP CREATE^{TM} SENTRi software and HPCMP computer resources enabled:

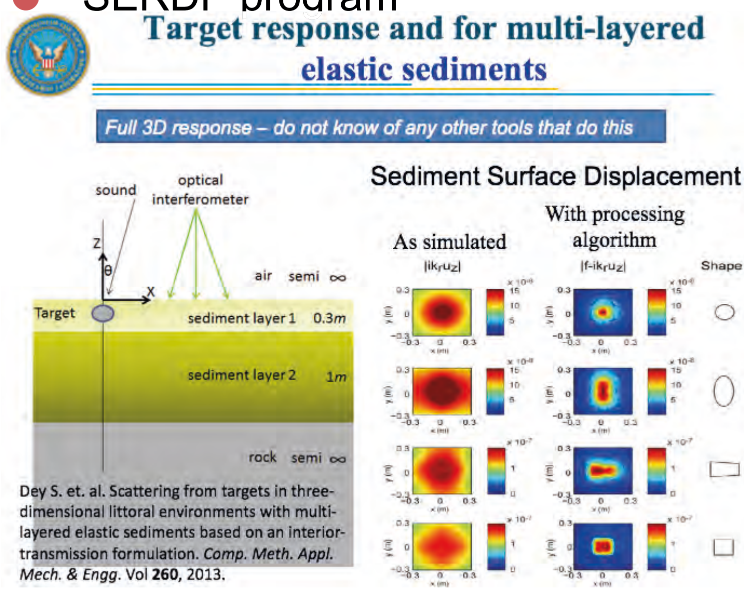
- **Virtual prototyping with SENTRi and Capstone enabled an appreciable reduction in time and expense (parametric physical model construction and testing would otherwise have been required).**
- **Project Chief Engineer stated: "The SENTRi supported study provided user command confidence in the acquisition of the device" allowing it to go to production**
- **The government analyst was nominated for Outstanding Programmatic Achievement.**

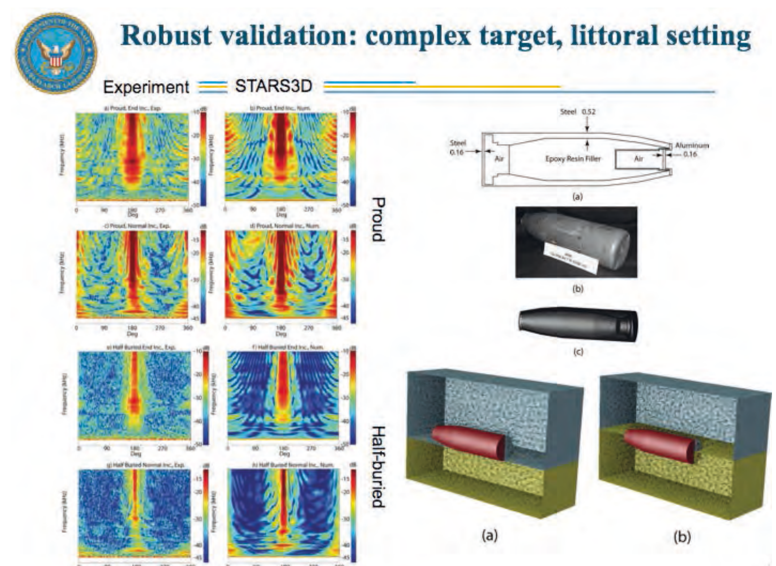
HPCMP CREATE^{TM} resources and expertise enabled the antenna to be fielded on schedule and meet its functional requirements.

Capstone Impact Beyond CREATE

- **NRL (Capstone+STARS3D)**
  - Low Frequency Broad Band (LFBB) Sonar simulations
    - Transitioned to <u>*Knifefish* littoral mine-hunting system (part of LCS Mine Counter Measure Mission Package)</u>
  - Unexploded Ordnance detection
    - SERDP program







Capstone used to generated numerical models of targets in exterior environments

Closing Remarks

- Effective use of computationally-based tools is a key to improving efficiency of research, development, and sustainment of defense systems
- Capstone provides geometry, meshing and attribution capabilities that are filling specific gaps
  - Significantly reduced time and effort for geometry preparation and meshing
  - Enable accurate and scalable geometry-based adaptive analysis
  - Provide a common geometry and meshing infrastructure for CREATE-developed solvers and design tools/environment
- Current release 7.1 provides significant capabilities that solve several use-cases of DoD interest
- Increasing adoption within DoD acquisition community
  - >350 exclusive/unique users of Capstone
  - >600 cumulative users with other CREATE-developed tools
- More information at : https://create.hpc.mil

The Role of CREATE^{TM}-AV in Realization of the Digital Thread

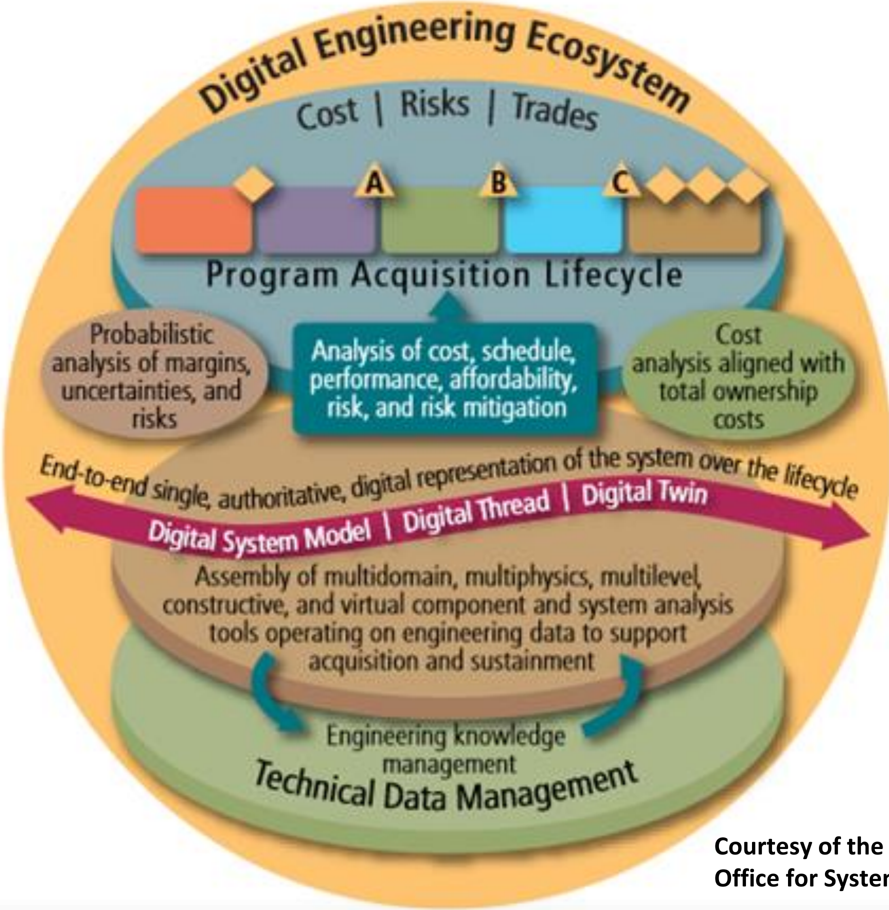
Dr. Ed Kraft
Associate Executive Director for Research
University of Tennessee Space Institute
October 25, 2017

Introduction

- The Aerospace & Defense Industry is investing heavily in Industry 4.0
- The AF in particular, and the DoD in general, are at the threshold of developing Digital Engineering Ecosystems in collaboration with Industry to take advantage of the Digital Revolution
- The HPC CREATE™ Program has evolved into an important source of high-fidelity, physics-based performance modeling tools with inherent capabilities enabling development of authoritative digital surrogate truth sources key to realization of a Digital Thread / Digital Twin

It is Time to Move From Abstraction to Realization in the Integration of Physics-Based Modeling into Digital Engineering Ecosystems

Digital Engineering Ecosystem

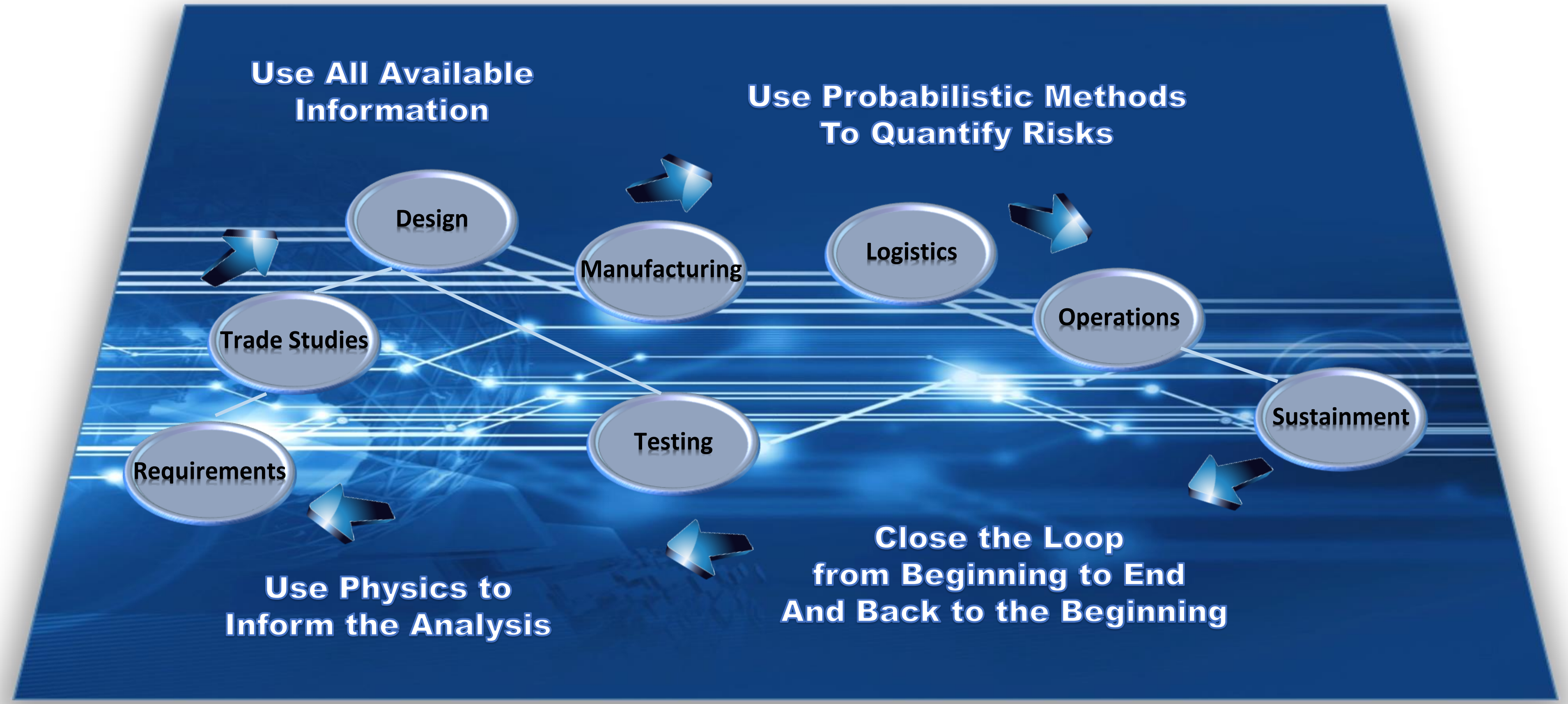


Courtesy of the Deputy Assistant Secretary of Defense Office for Systems Engineering

The interconnected infrastructure, environment, and methodology (process, methods, and tools) used to store, access, analyze, and visualize evolving systems' data and models to address the needs of the stakeholders.

Defense Acquisition Guide

Connected and Integrated Data
Digital Thread / Digital Twin



Make Informed Decisions Throughout the Lifecycle

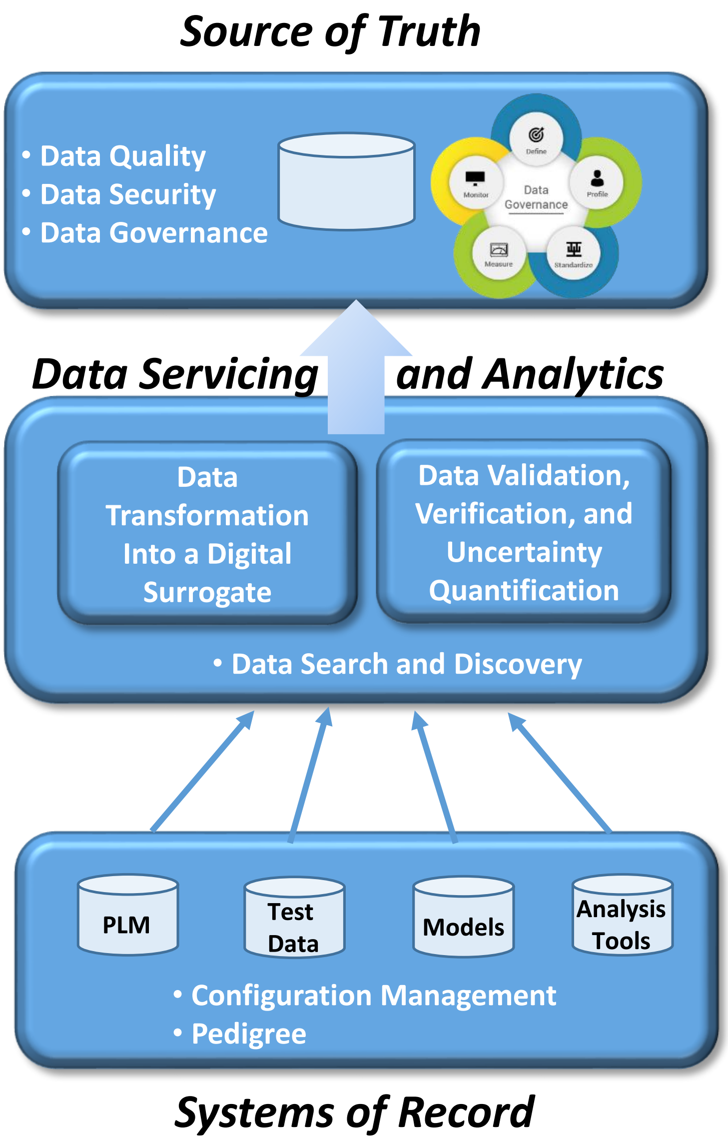
Tenets of the Digital Thread/Digital Twin

- Access to and ability to exercise data to understand performance and technical risks
- End-to-end system model – ability to transfer knowledge upstream and downstream and from program to program
- Single, authoritative digital representation of the system over the life cycle – the authoritative digital surrogate “truth source”
- Application of reduced order response surfaces and probabilistic analyses to quantify margins and uncertainties in cost and performance
- Preserve meta-data on decision processes and outcomes

It is Not Sufficient to Just Digitize Current Processes – We Need to Reinvent Processes Leveraging the Digital Connectivity of Trusted Data and Knowledge

A Single, Authoritative Digital Surrogate "Truth Source"

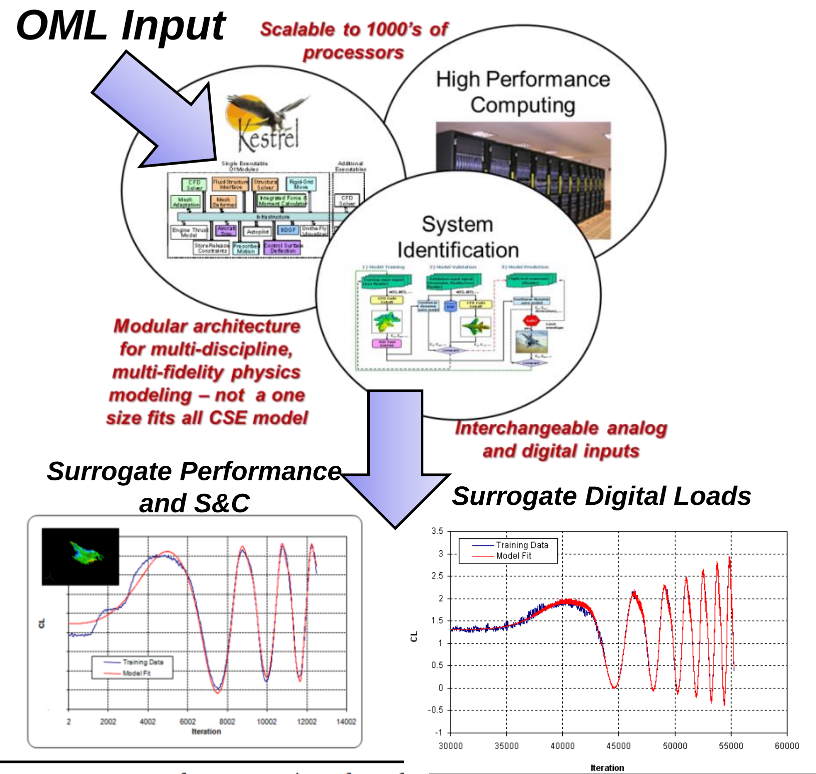
- A technical definition declares quality of a truth source to be "the state of completeness, validity, consistency, timeliness and accuracy that makes the data appropriate for a specific use"
- System of Record (SOR) – the authoritative data source for a given element or piece of information
- Source of Truth (SOT) – <u>trusted</u> data source that gives a complete picture of the data object as a whole
- Trusted data source connotes
    - An entity authorized by a <u>governing authority</u> to develop or manage data for a specific purpose
    - Shared by all stakeholders with all equities preserved



Opportunities for CREATE™-AV to Enable the Digital Thread

SPACE INSTITUTE

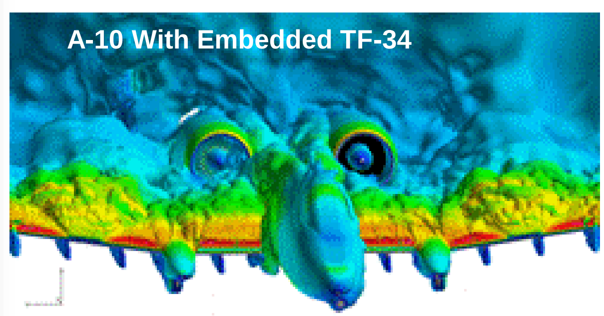
- Multi-discipline, multi-physics, multi-fidelity capability
- Ability to rapidly and efficiently generate **reduced order models for surrogate representations**
- Ability to address system integration issues during detailed design (fluid/structures, airframe/propulsion, airframe/weapons)
- Scalable to take advantage of high performance computing assets
- **Configuration management and Quality Control** critical to confidence in applications across multiple regimes.

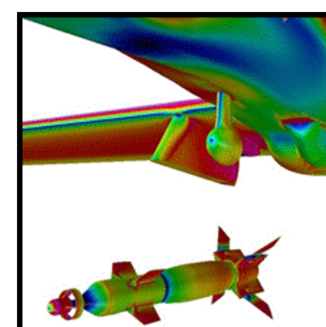


$$C_L(\alpha, q, \dot{q}) = C_0 + C_1\alpha + C_2 q + C_3 q^2\alpha + C_4\dot{q}\alpha + C_5 q^4 + C_6\dot{q}q^2 + C_7 q\alpha^2 + C_8\dot{q}q + C_9\alpha^3 + C_{10}\dot{q} + C_{11}\dot{q}^3 + C_{12}\dot{q}^2 + C_{13}q^2 + C_{14}q\alpha$$

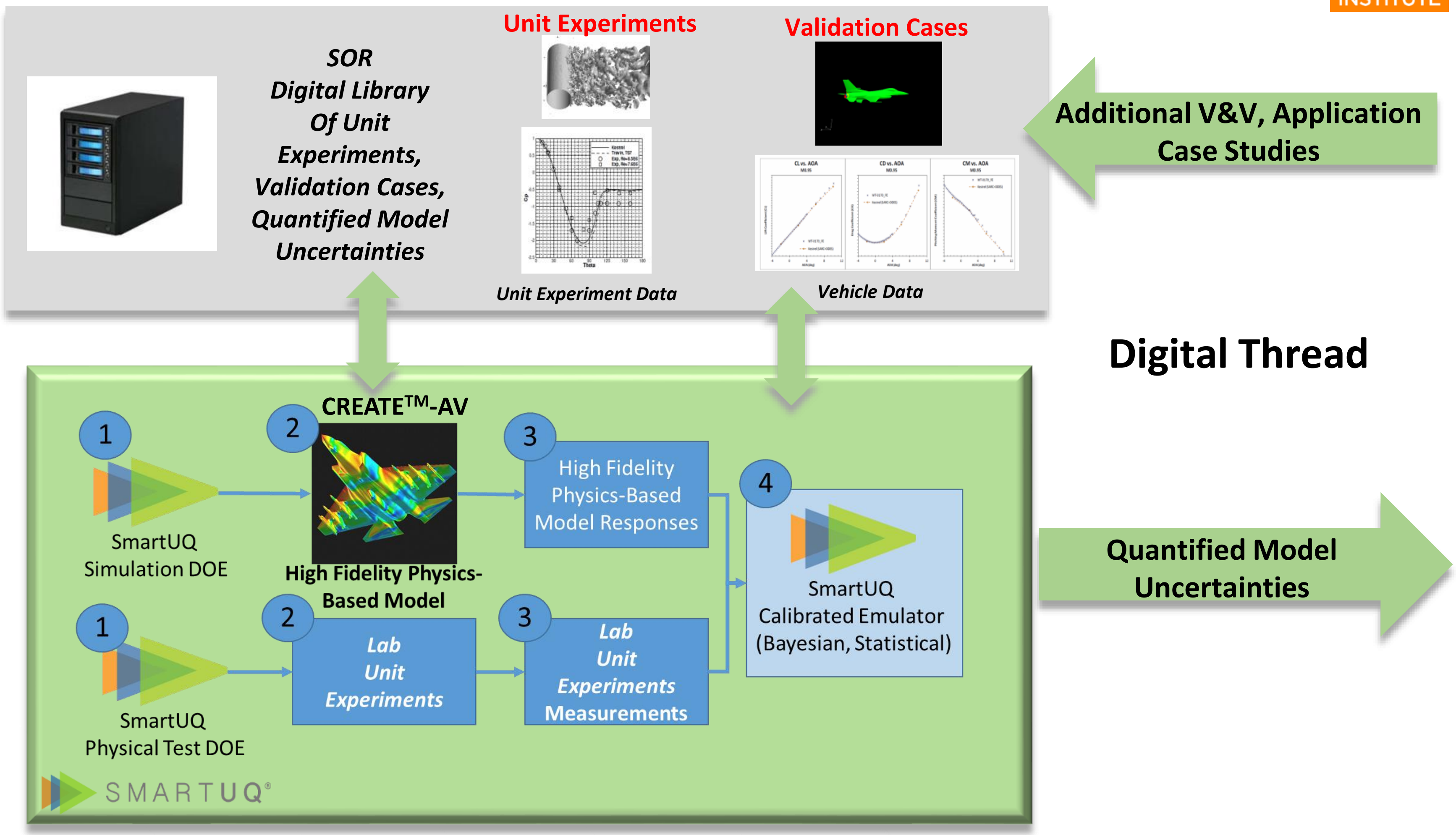
$$Loads = f(\overline{q}, M, \alpha, \alpha^2, q, \alpha q, \dot{q}^2, \ldots)$$

To Become an Integral Component of a "Truth Source" Requires a Pedigree, Transformation to a Digital Surrogate, Integration with Other Data Sources, and Uncertainty Quantification





Developing the Pedigree

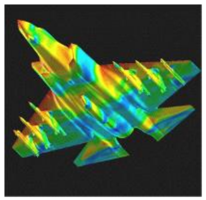


Library of Experimental Validation Data and V&V of Models Digitally Preserved as a System of Record Will Expedite a Digital Truth Source

Developing the Model-Based Digital Surrogate

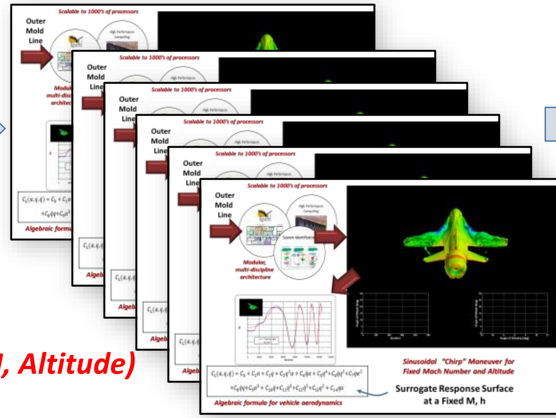
SPACE INSTITUTE

CREATE™-AV



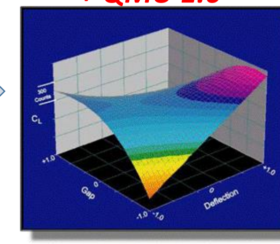
High Fidelity Physics-Based Models

Reduced Order Model Response Surface Generation Over Entire Operating Envelope



$C_X = f\,(M, Altitude)$

Model-Based Performance Response Surface 1.0 + QMU 1.0



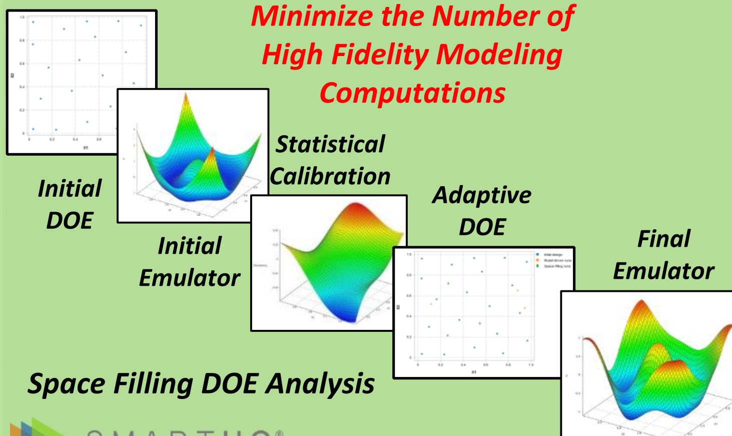
Digital Authoritative Truth Source

Digital Thread

Quantified Model Uncertainties

Additional V&V, Application Case Studies

Minimize the Number of High Fidelity Modeling Computations



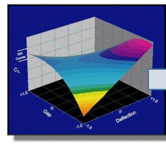
Modeling Efficiency, Scalability, and Optimized UQ Methods Will Be Required to Generate Comprehensive Model-Based Surrogates

Merging Model and Test Data

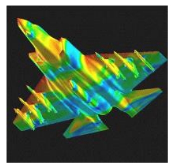
SPACE INSTITUTE

Digital Authoritative Truth Source →

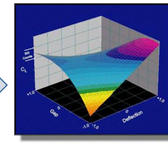
Response Surface 1.0 + QMU 1.0



Model Based

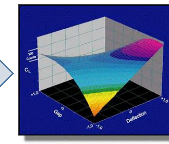


Response Surface 1.1 + QMU 1.1



Ground Test Based

Response Surface 1.2 + QMU 1.2



Flight Test Based

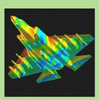
Digital Authoritative Truth Source →

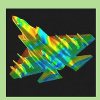
Digital Thread

CREATE™-AV
V&V'D Applied High-Fidelity Model

CREATE™-AV

Baseline + *Epistemic Delta* = *Correction*



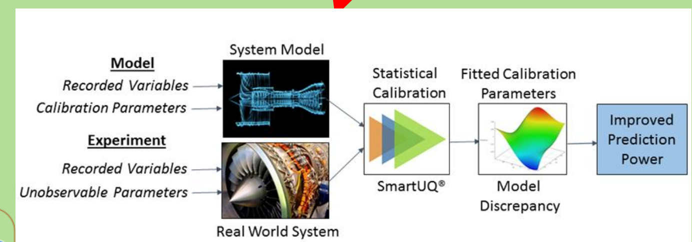


Identification of Source and Range of Epistemic Uncertainties

1. Modeled Assessment / Correction of Epistemic Uncertainty

Epistemic inputs sampling → Aleatory UQ ⟷ Emulator Evaluations

2. Combined Epistemic and Aleatory Analysis of Experimental Data



3. Merge of Experimental and Modeled Data into New Authoritative Truth Source with Quantified Uncertainties

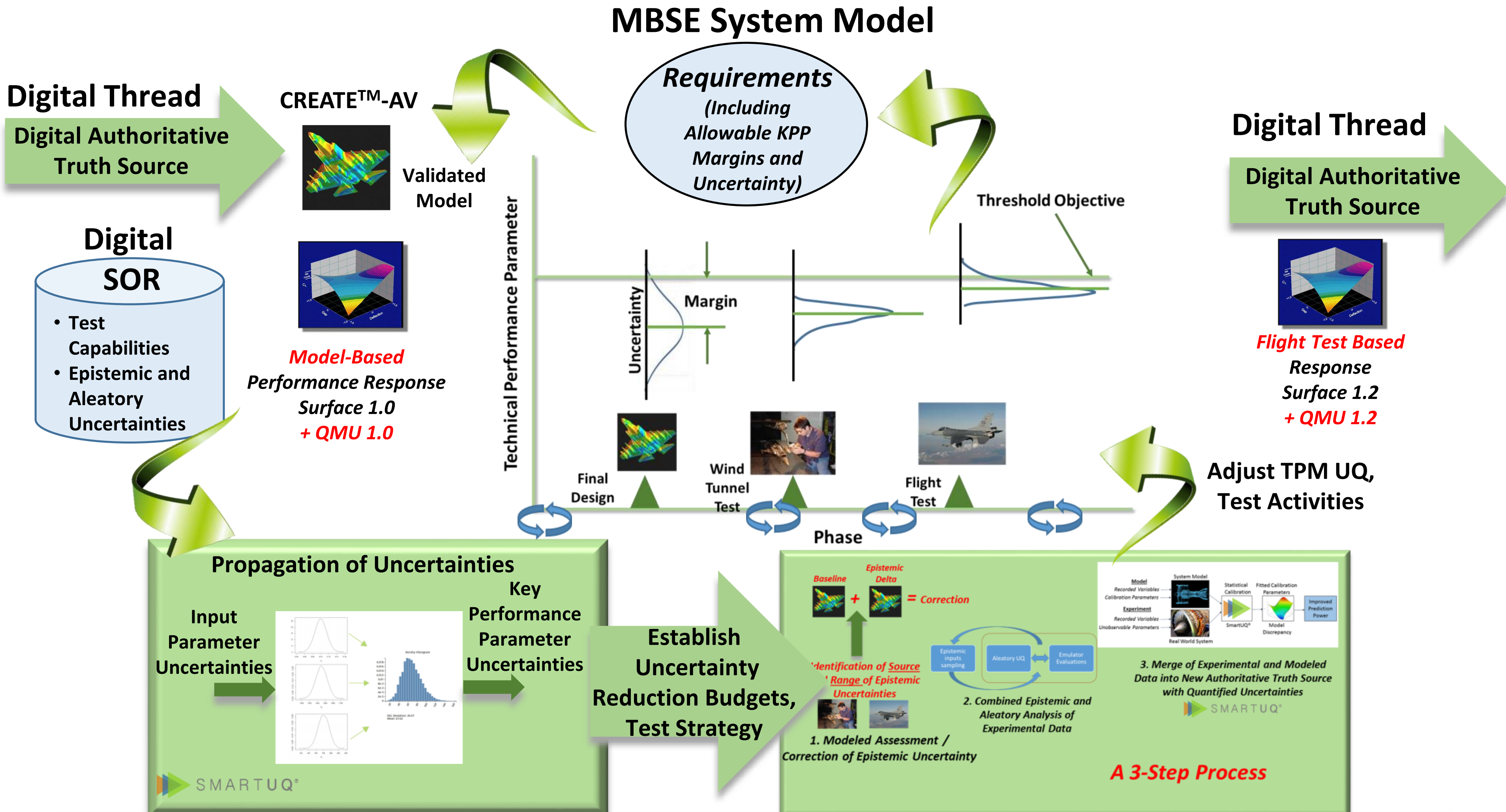
SMARTUQ®

Digital Thread

A 3-Step Process

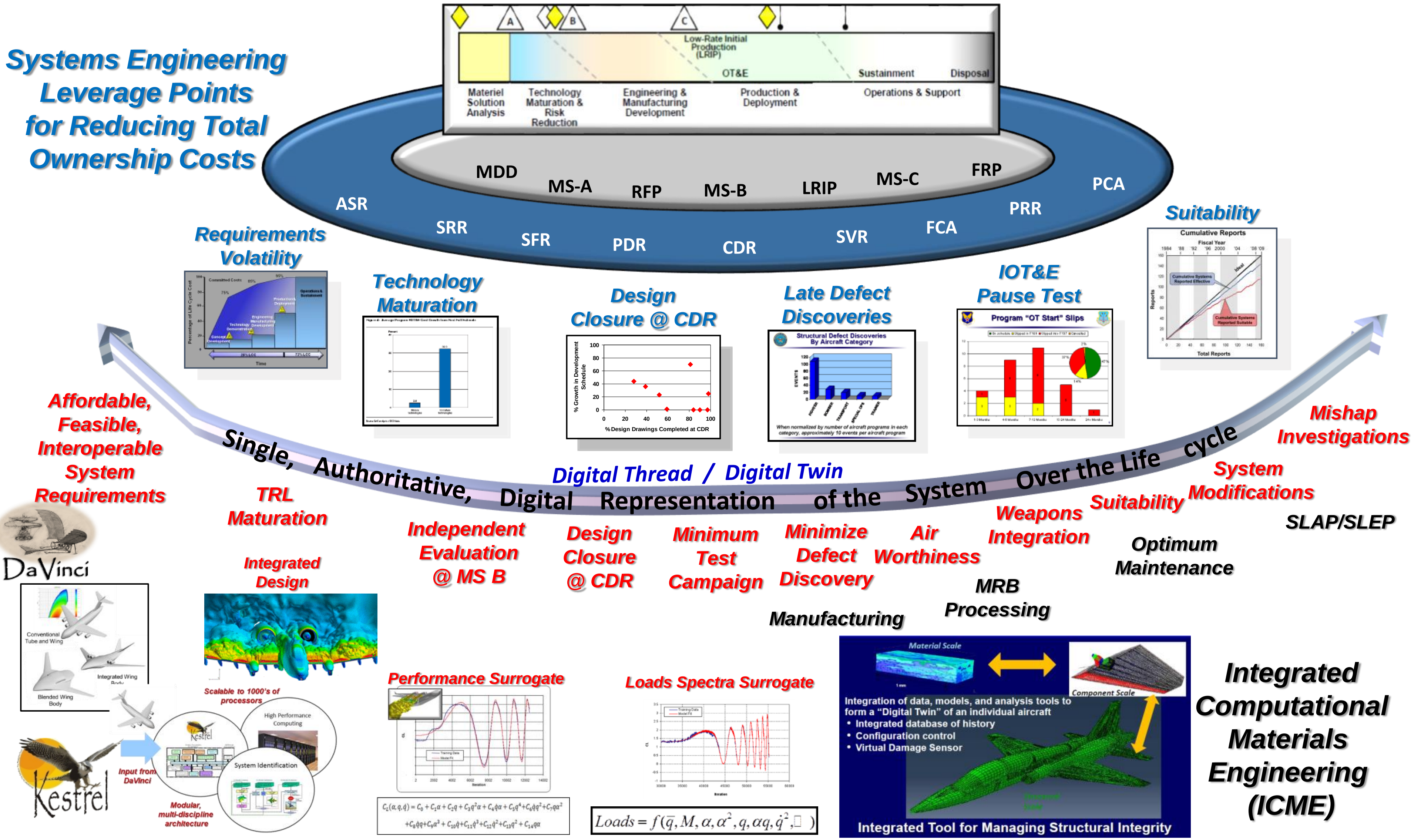
← **Additional V&V, Application Case Studies**

MBSE, MBE, UQ, and T&E – Transforming to a Digital Process



Moving Toward a "Digital TEMP" to Improve Quality of Performance Against Requirements and Reduce Cost and Schedule for T&E

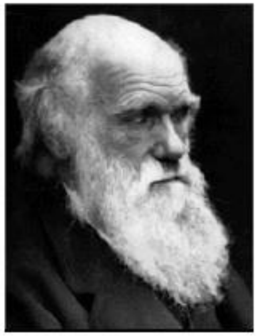
CREATE™-AV Lifecycle Impact as a Truth Source
A Vision Realized



Summary

SPACE INSTITUTE

- The Digital Revolution is reshaping the development and sustainment of aerospace and defense systems
- The DoD is moving forward with Industry to develop the architecture for a Digital Engineering Ecosystem
- The crucial elements for a Digital Ecosystem are
  - Identification and preservation of Sources of Record
  - Transformation of SOR data into digital surrogates
  - Quantification of the quality of the digital surrogates
  - Governance of the Authoritative Digital Surrogate Truth Source



Charles Darwin 1809-1882

"It is not the strongest of the species that survive, nor the most intelligent, but the ones most adaptable to change"

CREATE ™ -AV has inherent capabilities conducive to providing an authoritative digital surrogate truth source for air vehicle performance, but will require focused attention on establishing its pedigree and persistently quantifying uncertainties at each application phase over a system lifecycle

Dr. Edward M. Kraft

Associate Executive Director for Research

University of Tennessee Space Institute

411 B. H. Goethert Parkway

Tullahoma, TN 37388-9700

ekraft@utsi.edu

Office 931-393-7284

Mobile 931-434-2302

CREATE™

Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles (CREATE™-GV)

Abstract ID: 19704

DOD HPC MODERNIZATION PROGRAM

Mr. Jody D. Priddy
U.S. Army Engineer Research and Development Center (ERDC) 601-634-3015 jody.d.priddy.civ@mail.mil

CREATE™-GV

Scope

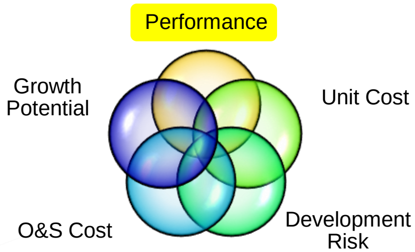
Develop physics-based, High Performance Computer (HPC) tools to enhance ground vehicle concept development, inform requirements development and provide requisite data for trade-space analysis to positively impact cost, schedule and performance with significant reduction in design risk for the acquisition community.

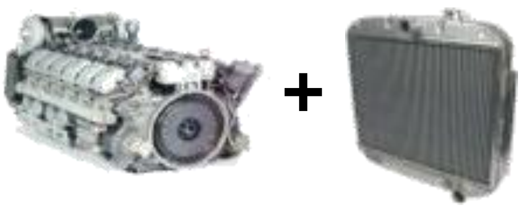
- **Ground Vehicle Interface (GVI)**
  - User interface to provide subject matter experts and power users with simplified and intuitive access to the analysis capabilities of the CREATE™-GV tools. The GVI does not require extensive knowledge of the underlying HPC M&S.
- **Mercury**
  - HPC physics-based co-simulation tool for M&S of terrain mechanics and vehicle systems and components. Incorporates suspension, tire and track, soil modeling, and powertrain simulation.
- **Mobility Analysis Tool (MAT)**
  - Computational tool for analyzing HPC physics data and producing mobility performance metrics required for trade exploration and systems engineering. Incorporates soil condition, vehicle performance and configuration, vegetation density, average surface roughness, average slope, etc.
- **Validation and User Transition**
  - Assist in capturing and integrating user requirements into CREATE™-GV.
  - Develop demonstrations and pilot projects to provide validation of products and processes.
  - Develop documentation and training – transition software products to users.

Early Detection of Design Flaws, Reduced Development Times, Enhanced Mission-Suitable Designs

CREATE-GV Focus is on <u>Performance</u>

Finding the sweet-spot among competing objectives (**<u>performance</u>**, unit cost, O&S costs, development risk, and growth potential) is a non-trivial task.





= ???

Ground vehicles are complex systems with many interrelated subsystems.

<u>Early decisions</u> have the largest impact on lifecycle cost and are made when knowledge is at a minimum.

Capability and Gaps Document

CRES-GV Capability and Gaps Document (May 16, 2013)

CRES-GV Capability and Gaps Document

High-Computational-Effort Tools for Ground Systems Design and Development

Dr. Robert E. Smith, TARDEC, rob.e.smith@us.army.mil
Mr. Randy Jones, ERDC, randolph.a.jones@usace.army.mil
Mr. Michael O'Neal, MCSC, Michael.oneal1@usmc.mil
Mr. Robert Huggins, MCSC, Robert.huggins@usmc.mil

Version: 3.27.2013

CRES-GV

Computational Research for Engineering and Science - Ground Vehicle

CRES-GV Capability and Gaps Document (May 16, 2013)

<u>Signatures, Effective Date and Version Control.</u> This document is effective on the date of the last signature below. The Joint Center for Ground Vehicles Governance Board signatures provides the required endorsement from the Army and Marine Corps Ground Vehicle Acquisition and Technology leadership in order to obtain the appropriate financial support for this effort. The Joint Enterprise Development Integration council will provide version control of this document. Minor updates will be presented to the JCGV Governance Board for approval and updated with a version control sheet indicating approved changes. Major updates will require a new release of the document and an updated signature page.

Signatures

MICHAEL D. VIGGATO
Deputy to the Commander
TACOM Life Cycle Management Command

JAMES H. SMERCHANSKY
Deputy Commander, Systems Engineering
Interoperability, Architectures & Technology
Marine Corps Systems Command

KEVIN FAHEY
Program Executive Officer Combat Support & Combat Service Support

WILLIAM E. TAYLOR
Program Executive Officer
Land Systems Marine Corps

See attached page
SCOTT J. DAVIS
Program Executive Officer
Ground Combat System

ASHLEY G. JOHNSON
Deputy Chief of Naval Research
Expeditionary Maneuver Warfare and Combating Terrorism

PAUL D ROGERS, Ph.D.
Director, Tank Automotive Research, Development and Engineering Center

REED L. MOSHER, Ph.D.
Director, Engineer Research and Development Center (ERDC)
Information Technology Laboratory

JOHN WEST
Director
High Performance Computing Modernization Program (HPCMP)

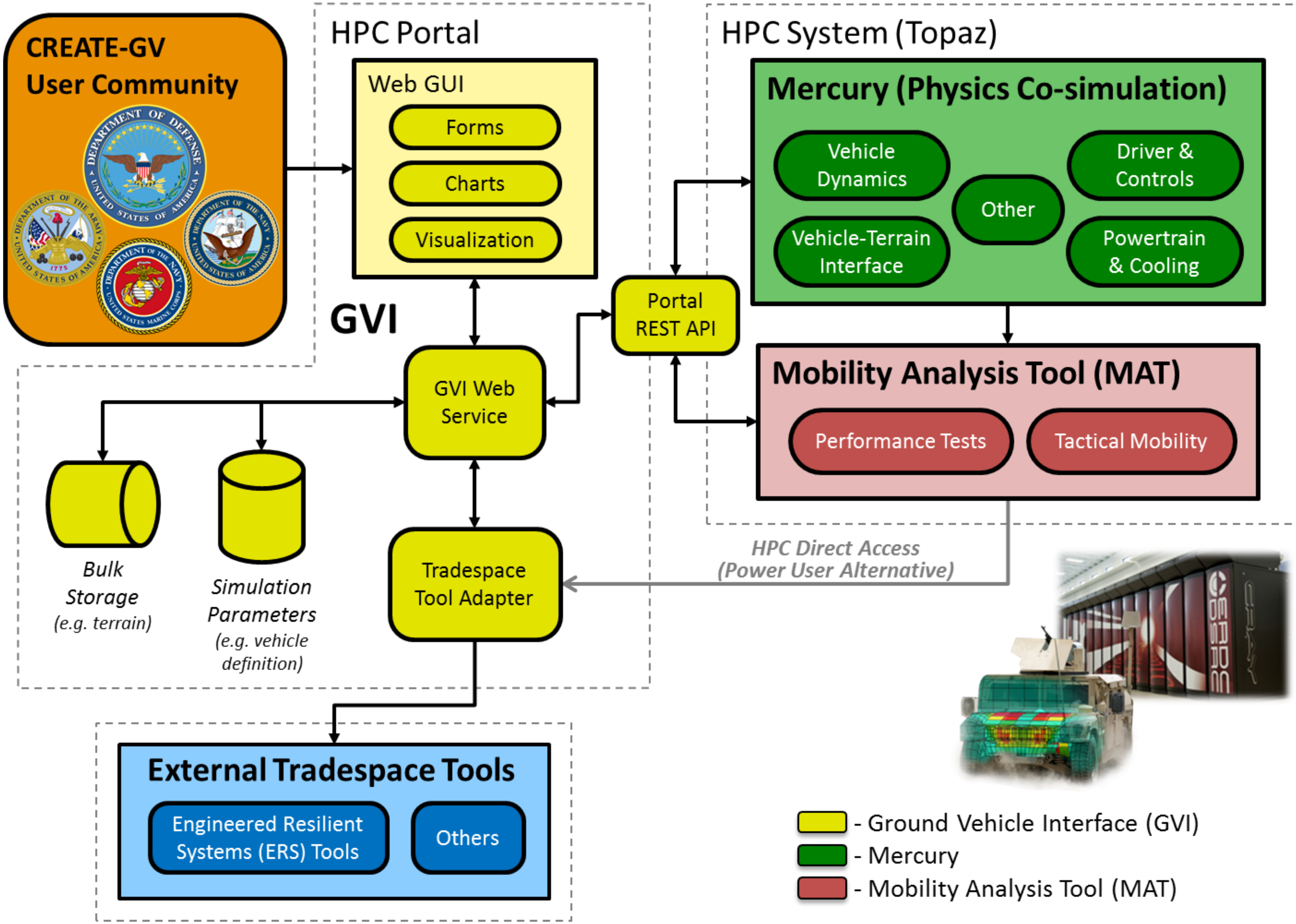
12

Starting Point for CREATE™-GV Requirements

Physics Domain Gaps from the GV Capability and Gaps Document

ID	Physics Domain	Brief Description	GV Capability
PD-001	Propulsion	Focus on Powertrain performance	PACE, Mercury
PD-002	Mobility and Vehicle Dynamics	Focus on vehicle dynamics, off- and on-road mobility test metrics, and mission-level analysis	Chrono, Mercury, MAT
PD-008	Under Hood Cooling and Crew Cooling	Focus on cooling point considerations in powertrain performance	PACE, Mercury
PD-009	Soldier Models for Occupant Centric Analysis	Focus on design impacts upon human performance limits	Chrono, Mercury, MSU-CAVS support

Current Architecture



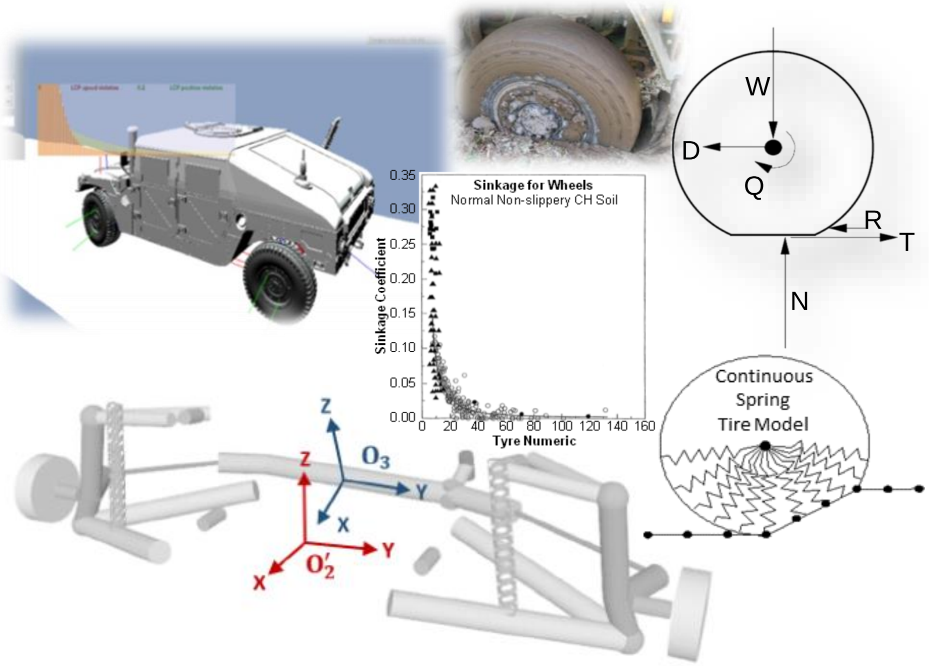
Key Computational Tools

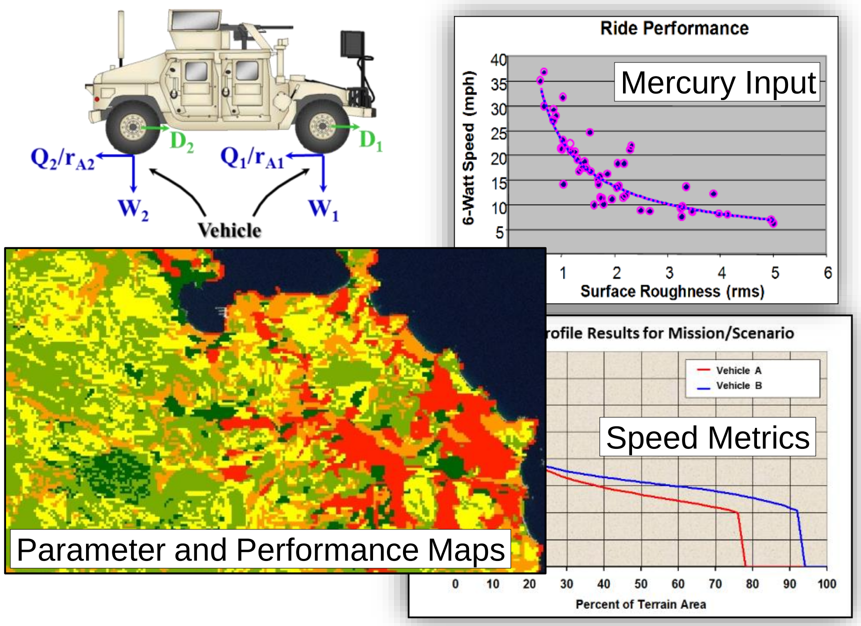
Mercury

- Simulates engineering performance tests of wheeled and tracked ground vehicles for proving-ground type developmental testing.
- Co-simulation framework for integrating physics domains.
  - Powertrain
  - Vehicle Dynamics (wheels and tracks)
  - Tire-soil & track-soil interaction

Mobility Analysis Tool (MAT)

- Converts vehicle performance metrics and terrain information into mission-based analysis of performance over large areas of terrain.
- Predicts multiple metrics currently used in acquisition processes.
  - % NOGO
  - Mission rating speeds

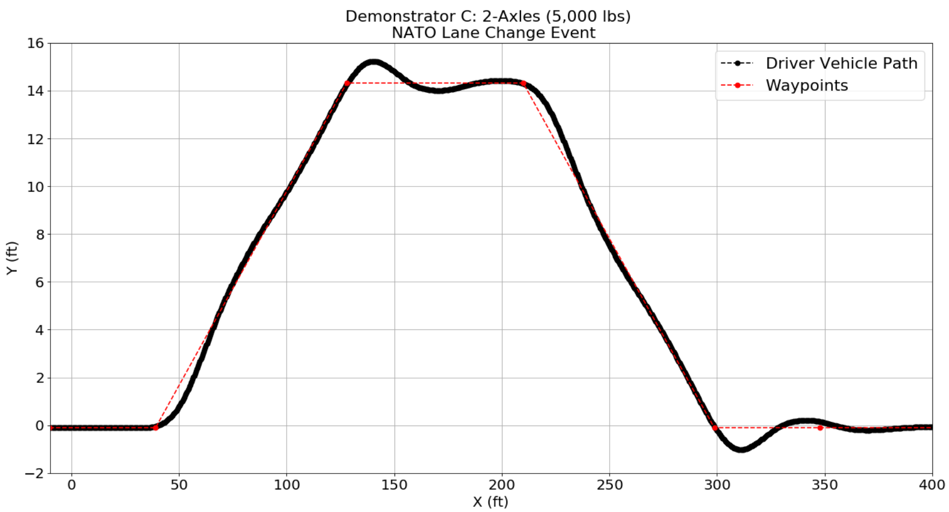


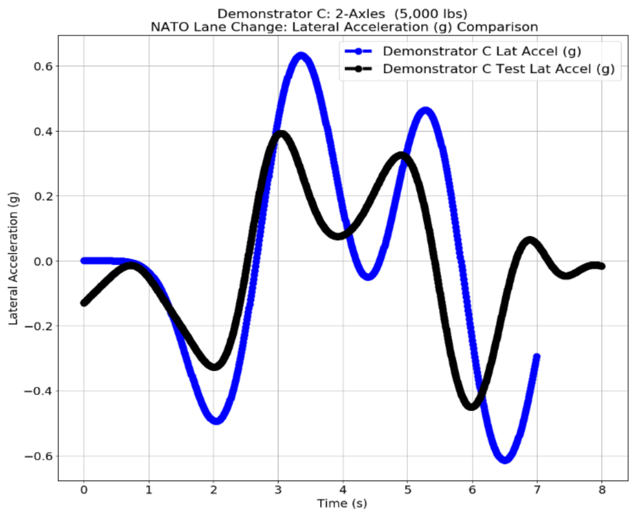


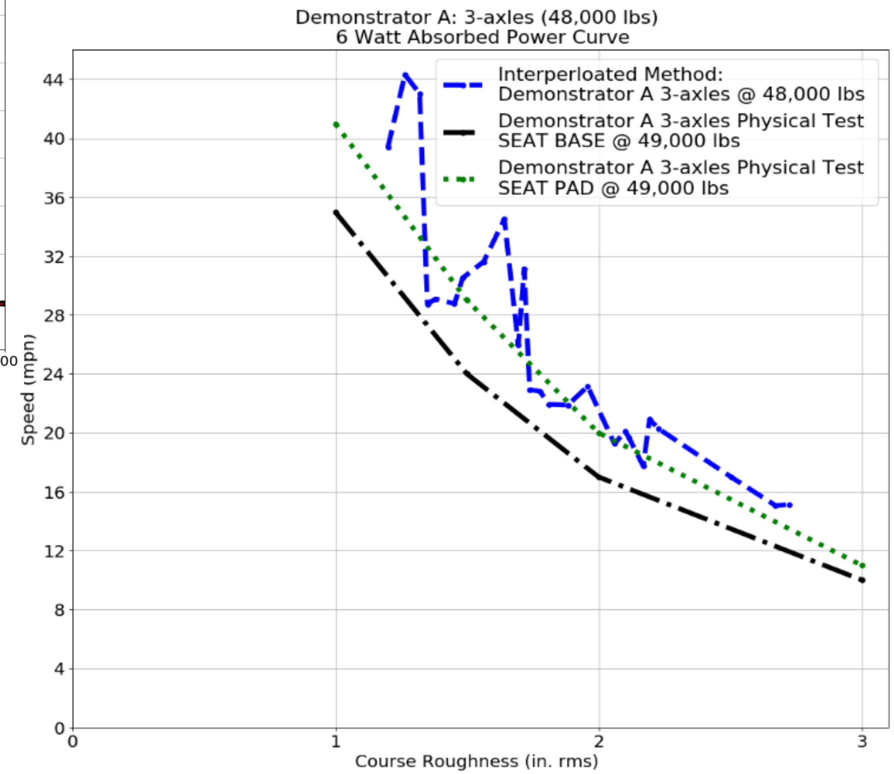
Validation and User Transition

Emphasis on validated and useful tools

- Ensure GV products provide credible results to users and key decision makers.
- Facilitate the transition from developers to the user community.







UNCLASSIFIED: Distribution Statement A. Approved for public release.

Development Partners

DOD HPC MODERNIZATION PROGRAM

ERDC
INNOVATIVE SOLUTIONS for a safer, better world

TARDEC

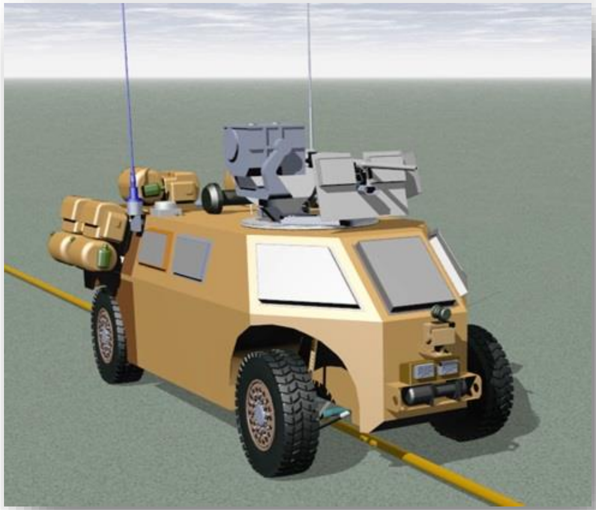
MISSISSIPPI STATE UNIVERSITY

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

CREATE-GV Impacts

Engineered Resilient Systems (ERS) – Light Reconnaissance Vehicle (LRV) Pilot Program

- The GV HPC tools GVI, Mercury and MAT have been integrated to provide S&T users a simplified capability to generate the requisite data for trade-space analysis.
- Over 65,000 unique LRV configurations have been analyzed for 5 key mobility performance parameters

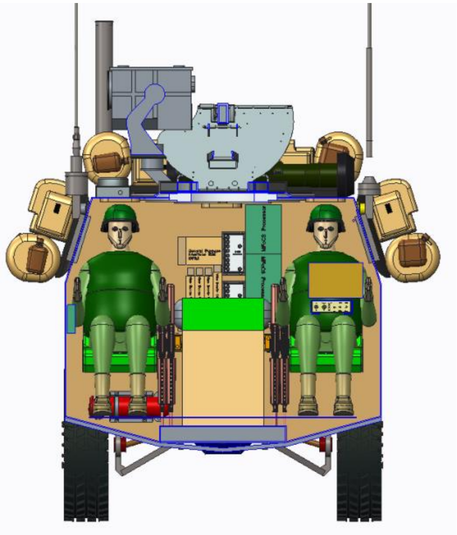


Future Users

- The limited early successes of the GV tools have initiated interest from various DoD users and from private industry. The tools are currently being deployed for use by key DoD government end-users with objectives for later industry use.

ERDC
INNOVATIVE SOLUTIONS
for a safer, better world

ERS
ENGINEERED RESILIENT SYSTEMS
DEPARTMENT OF DEFENSE



TARDEC

DOD HPC MODERNIZATION PROGRAM

DOD HPC MODERNIZATION PROGRAM

CREATE

Thank You

UNCLASSIFIED: Distribution Statement A. Approved for public release.

Presented to:

20^{th} Annual NDIA Systems Engineering Conference

Rotorcraft Acquisition: Development of Modeling and Simulation Procedures

DISTRIBUTION A. Approved for public release: distribution unlimited.

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Date: 25 October 2017

Presented by:

Dr. Marty Moulton

Chief, Aeromechanics Division

U.S. Army Aviation and Missile Research, Development, and Engineering Center

Army Aviation

Lifecycle Acquisition Support

- **Contractor development test**

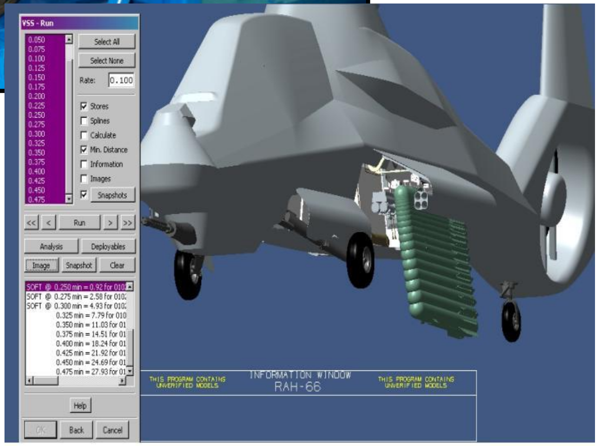
- **Formal inspection, design review, and safety assessment**

- **Component qualification test of performance under specified conditions and duration**

- **Formal contractor demonstrations**

- **Government testing**

- ***Engineering analysis, modeling and simulation (M&S)***



M&S VV&A Standard

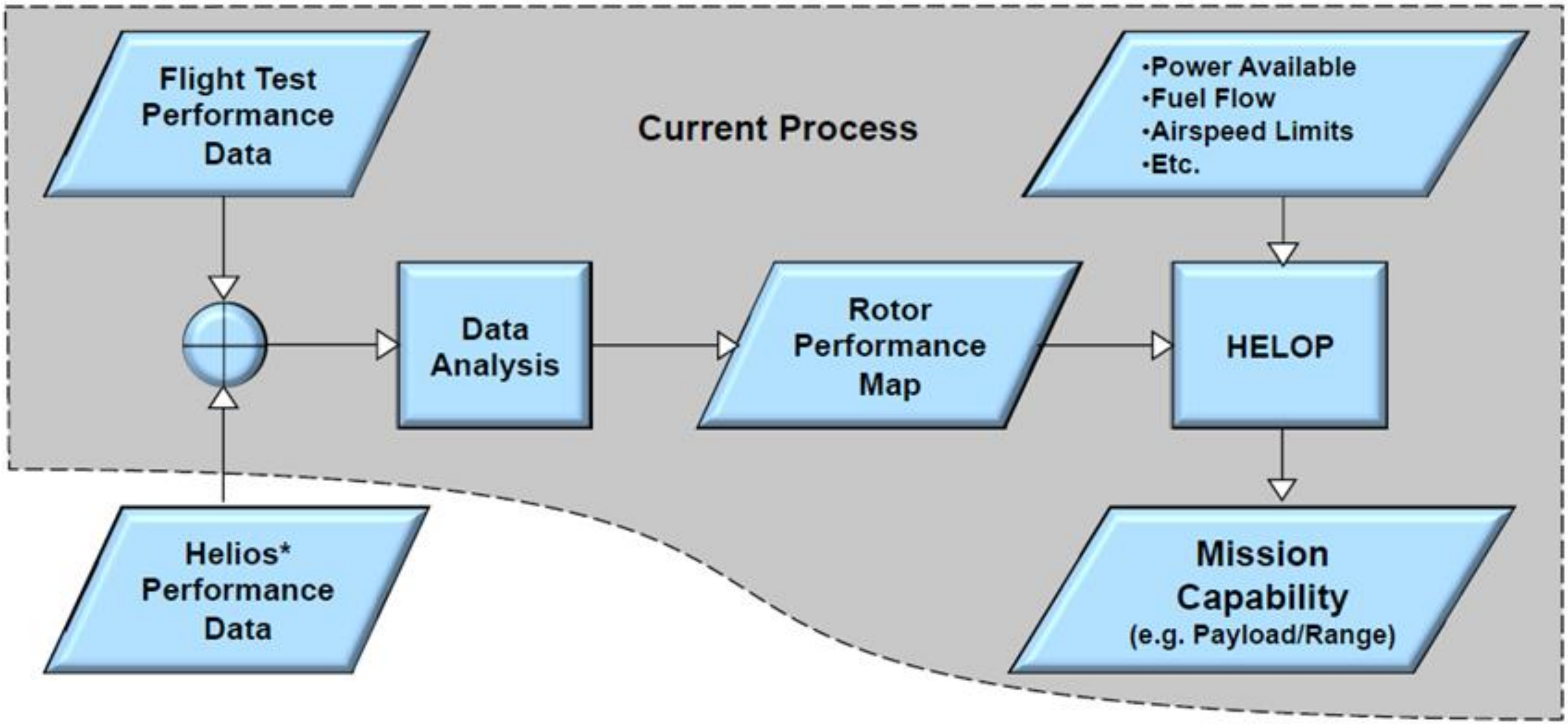
DoDI 5000.61 defines the minimum set of items to document as part of Verification, Validation & Accreditation (VV&A).

AR 5-11 requires VV&A of models.

DA PAM 5-11 gives procedures to assist the M&S developer, proponent, and application sponsor in conforming to the VV&A policies.

- VV&A establishes the credibility of M&S to effectively support Army decisions.
- All models, simulations, and associated data developed, made available, managed, or used by the Army to support Army or DOD processes, products, and decisions will undergo verification and validation throughout their lifecycles and be accredited for the intended use.
- Cargo PM identified a requirement for M&S IAW AR 5-11.
- Process development started with the CH-47 Block 2 efforts and continues to evolve.

Leveraging M&S for Acquisition
Flight Performance



* CREATE-AV Software Product: High-fidelity, full vehicle, multi-physics analysis tool for rotary-wing aircraft

CH-47 w/ACRB Blades Mission Analysis Prediction

U.S. ARMY RDECOM

AMRDEC

Objective

Predict mission performance for the CH-47 helicopter w/ACRB blades using Helios Engineering Model based rotor map.

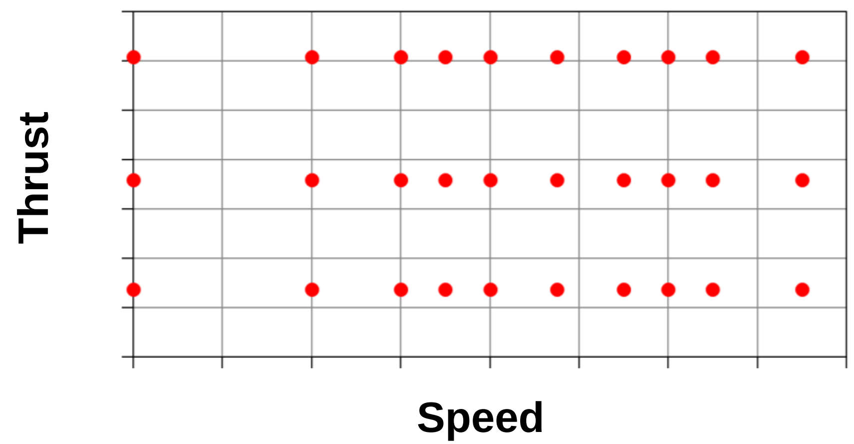
Software Basis

Helios v4.0

Evaluation Data

Will compare with flight test data when available.

Run Matrix



Schedule

Task ID	Task Name
4	CH-47F w/ ACRB Mission Analysis
4.1	Thrust Sweep - Hover
4.2	~~Thrust Sweep - 200 ft/min VROC~~
4.3	Speed Sweep - High Gross Weight
4.4	Speed Sweep - Mid Gross Weight
4.5	Speed Sweep - Low Gross Weight
4.6	Perform Mission Analysis
4.7	Report

Timeline: Q1 14 (J F M), Q2 14 (A M J), Q3 14 (J A S), Q4 14 (O N D), Q1 15 (J F M), Q2 15 (A M J)

Summary of Predictions

- Initial 2012 ACRB predictions based on SME experience (not a repeatable process)
- Final 2015 ACRB predictions based on modeling and simulation (repeatable process)
- M&S supported critical programmatic decision to proceed with acquisition

Positively Impacting Defense Acquisition Programs: CH-47 Steady State Flight Envelope

Opportunity: The Cargo PMO is developing a new rotor blade to increase flight performance, and the increase may impact dynamic component fatigue loads.

Project Objectives: Utilize Helios to develop and validate a model to predict dynamic component loads for rotor steady state operating conditions. Extend the validated baseline model to predict steady state dynamic component loads for the proposed rotor blade.

Potential Impacts:

- Enhance structural airworthiness assessments
- Provide capability for Flight Test Matrix Optimization through virtual test capacity
- Perform risk-reduction assessments of rotor design parameters on critical fatigue loads

Validation Challenges:

- Adoption of M&S into existing organizational processes
- Available test data not specifically obtained for validation
- Validation of the model near edge of aircraft envelope requires focused SME involvement

Definitions of VV&A

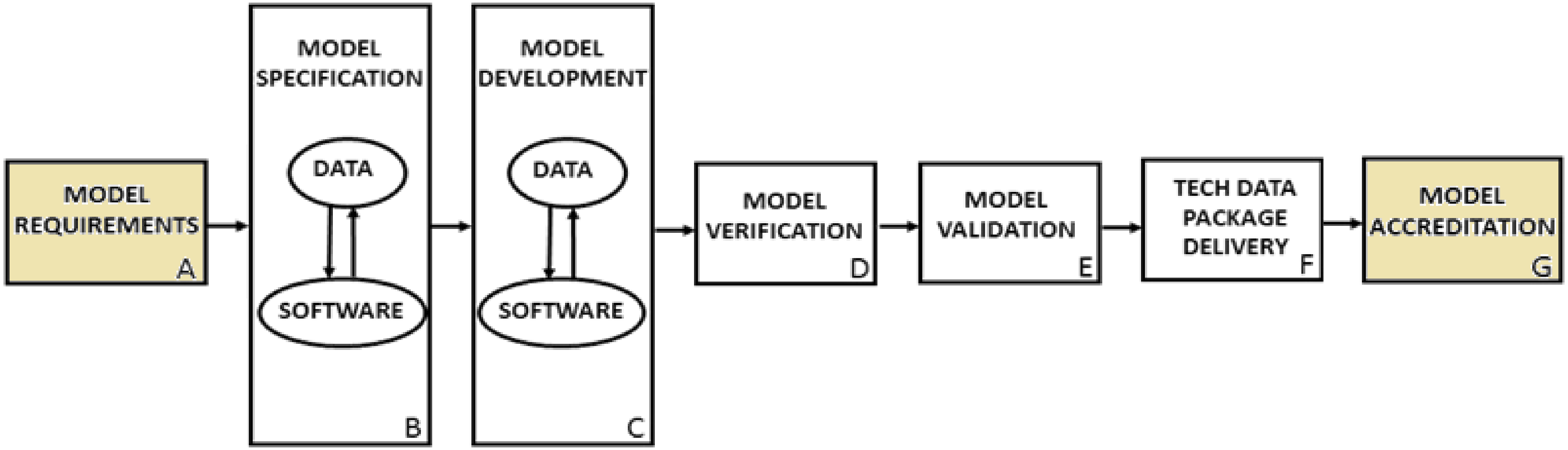
Definitions of verification, validation, and accreditation are as follows:

- Verification is the process of determining that an M&S accurately represents the developer's conceptual description and specifications. Verification evaluates the extent to which the M&S have been developed using sound and established software-engineering techniques.

- Validation is the process of determining the extent to that an M&S is an accurate representation of the real world from the perspective of the intended use of the M&S. *Validation methods include expert consensus, comparison with historical results, comparison with test data, peer review, and independent review.*

- Accreditation is the official determination that a model, simulation, or federation of M&S is acceptable for use for a specific purpose.

Generic Model Process



Accreditation Agent – The organization designated by the application sponsor to conduct an accreditation assessment for an M&S application including data.

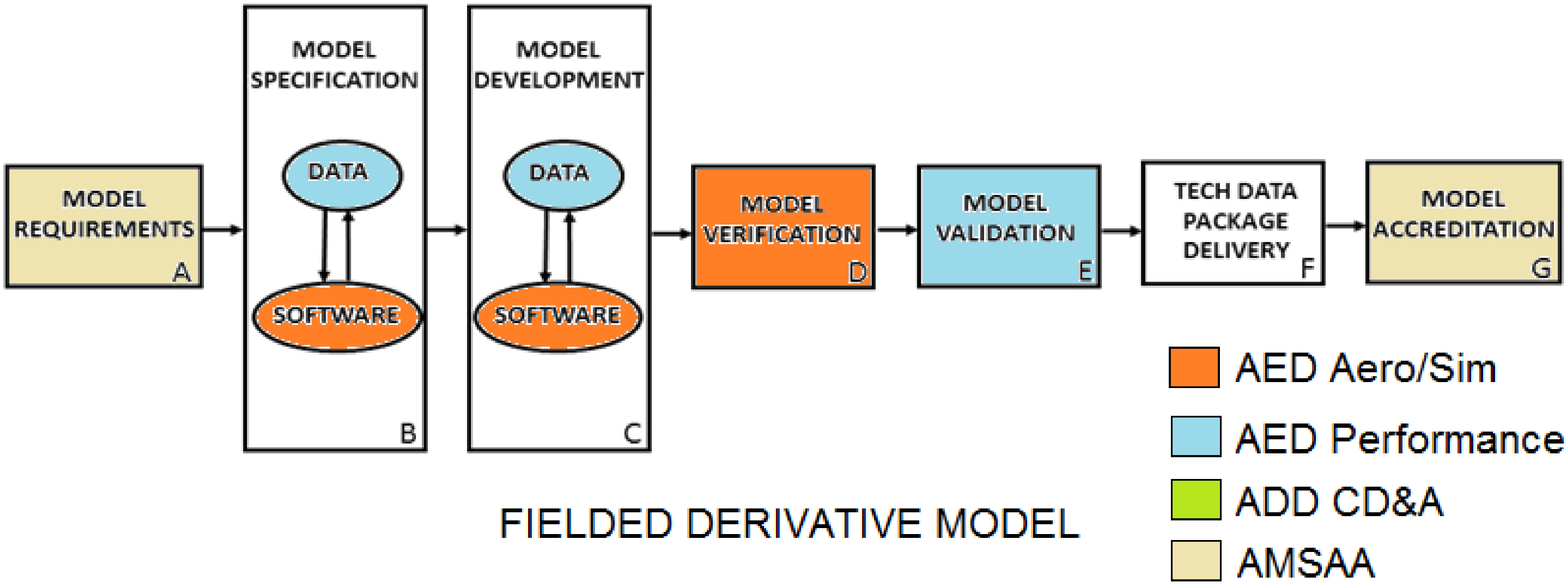
Roles and responsibilities are defined during accreditation planning for a *specific project and intended use*.

FVL Capability Set 3 AoA (Milestone A)

- AMSAA (Army Materiel Solution Analysis Activity) requires fielded aircraft data for baseline and alternative assessments.
- TRAC (TRADOC Analysis Center) requested to assess fielded and conceptual models in existing performance planning tools (CFPS/Falconview).
- IAW AR 5-11, *Management of Army Models and Simulations,* AMRDEC developed a VV&A process to wrap performance data in simplified engineering flight models to meet requirements.

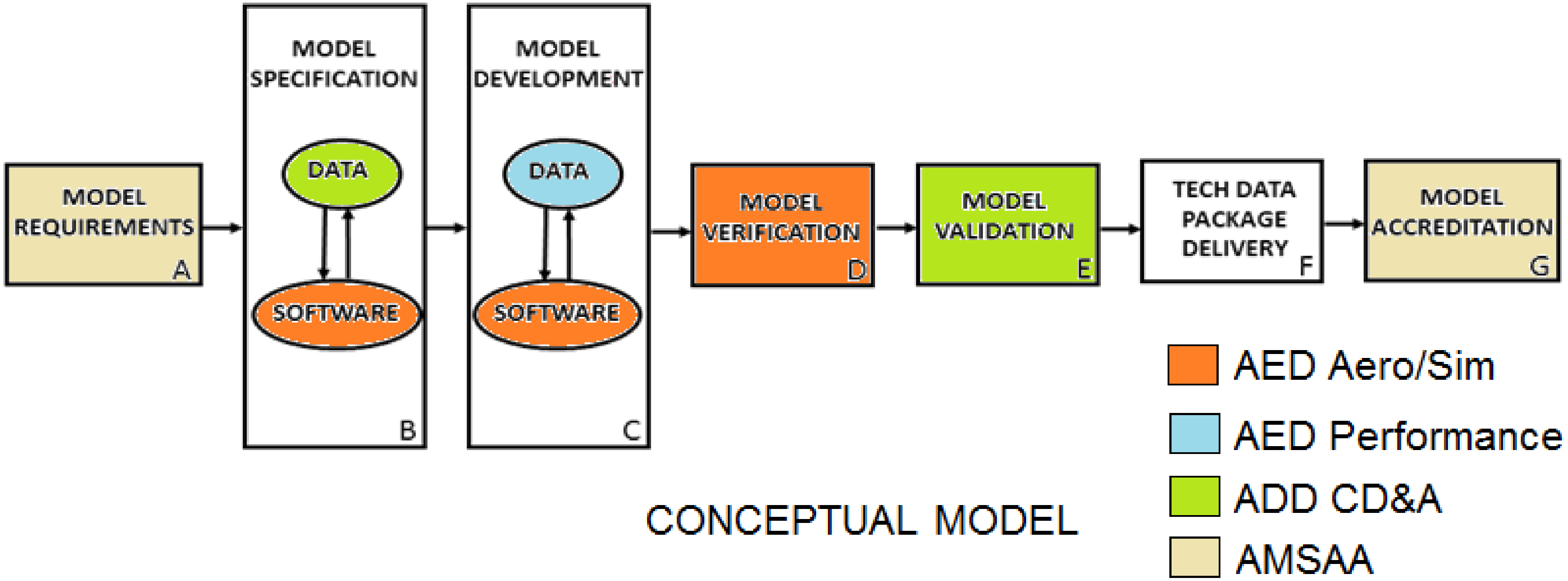
Study Baseline	Baseline Upgrade	COTS / GOTS	New Start Compounds	New Start Tiltrotors
Current relevant combat fleets including SLEP as necessary. Include currently programmed upgrades and modifications, and those in Service-level long-range resource requirement forecasts	Study Baseline + Additional viable modifications to legacy systems need substantially increase speed, range, and/or worldwide operational capability	Commercial-off-the-shelf or Government-of-the-shelf options that offer significantly improved speed, range, and/or worldwide operational capability	New start options in a compound-helicopter configuration. Variants representing "high" or "low" cases should be assessed if expected to provide significant differences	New start options in a tiltrotor configuration. Variants representing "high" or "low" cases should be assessed if expected to provide significant differences

Tailored Process



FIELDED DERIVATIVE MODEL

Tailored Process



Process Documentation

Model Production Process

	Flight Performance Specification (B)	Software 2 *.dll 1 *.res (C)	Model Verification Plan (D)	Model Validation Plan (E)	Software Version Description (F)	
Product Requirements Document (A)	Data Substantiation Report (B)	Data 14 .xls tables (C)	Software Verification Report (D)	Model Validation Report (E)	Data Delivery Memo (F)	Accreditation Memo (G)

Model Development Plan

Model Development plan was constructed specifically for the FVL AoA model effort to define process, roles and responsibilities.

Summary/Lessons Learned

- Credible lifecycle acquisition support that leverages modeling and simulation must provide a VV&A plan, including an accreditation agent, and subsequent documentation
- Lifecycle engineering support may require SME-based validation followed by test data-based validation
- Test plans must include requirements for M&S model development and validation
- Future Vertical Lift

JMR TD Configurations

Other Configurations

AMRDEC Web Site
www.amrdec.army.mil

Facebook
www.facebook.com/rdecom.amrdec

YouTube
www.youtube.com/user/AMRDEC

Twitter
@usarmyamrdec

Public Affairs
AMRDEC-PAO@amrdec.army.mil

NDIA #19693: Program Management in HPCMP-CREATE™ (A Family of Large-scale, Physics-based, System-of-Systems, Software Development Projects)

An Application of Risk-based Management Practices in Software Development

DOD HPC MODERNIZATION PROGRAM

Richard P Kendall, Ph.D. with
D.E. Post, L.G. Votta, P. A. Gibson, L. A. Park and S.M. Sundt
October 2017

Program Management in CREATE

If you were starting a new
- distributed,
- physics-based,
- system-of-systems
- HPC-capable
DoD software development project

How would you manage it for long-term success?

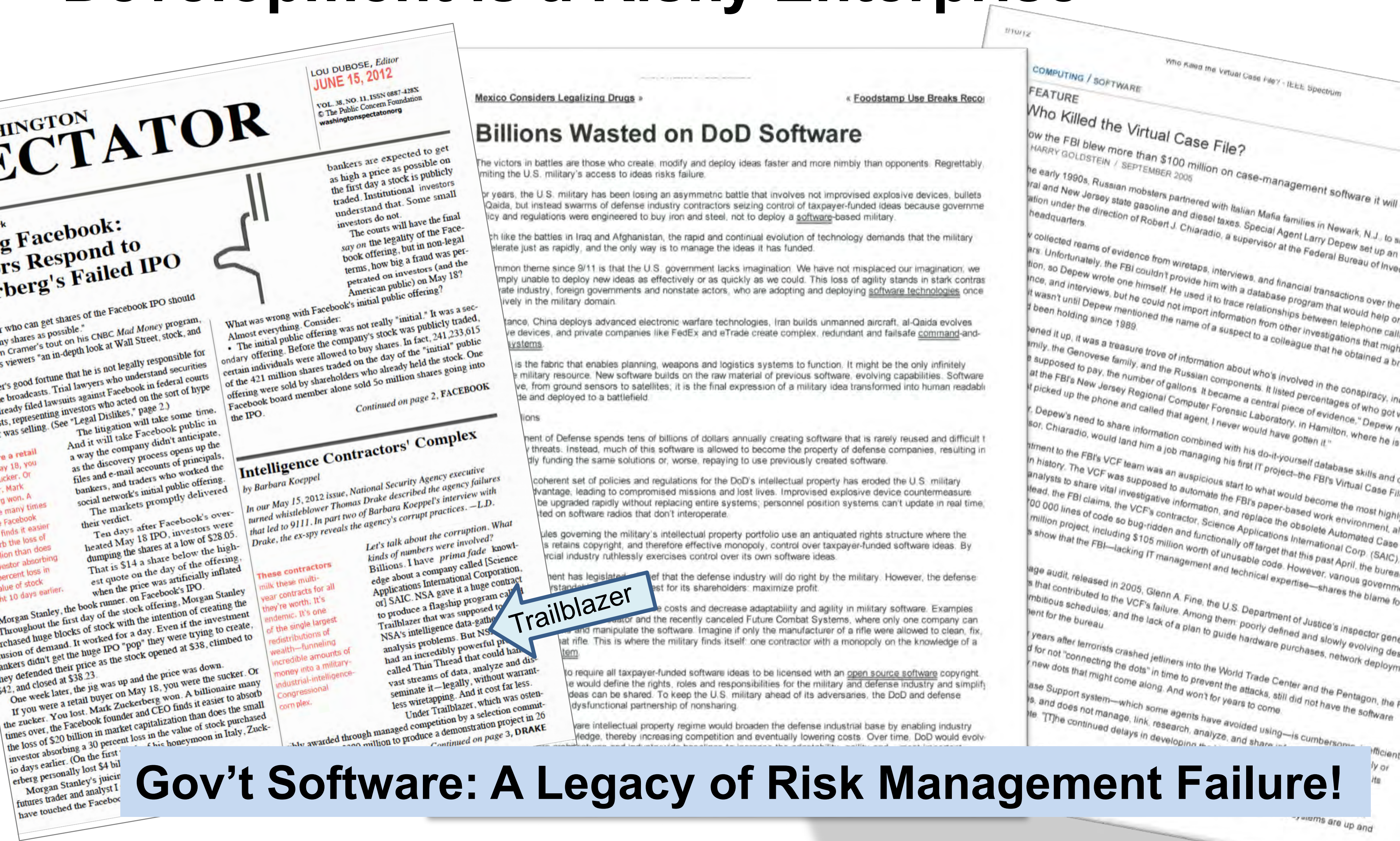
…based on the CREATE experience

Program Management in CREATE

Why should you have confidence in the staying power of CREATE?

Distribution A: Approved for Public release; distribution is unlimited.

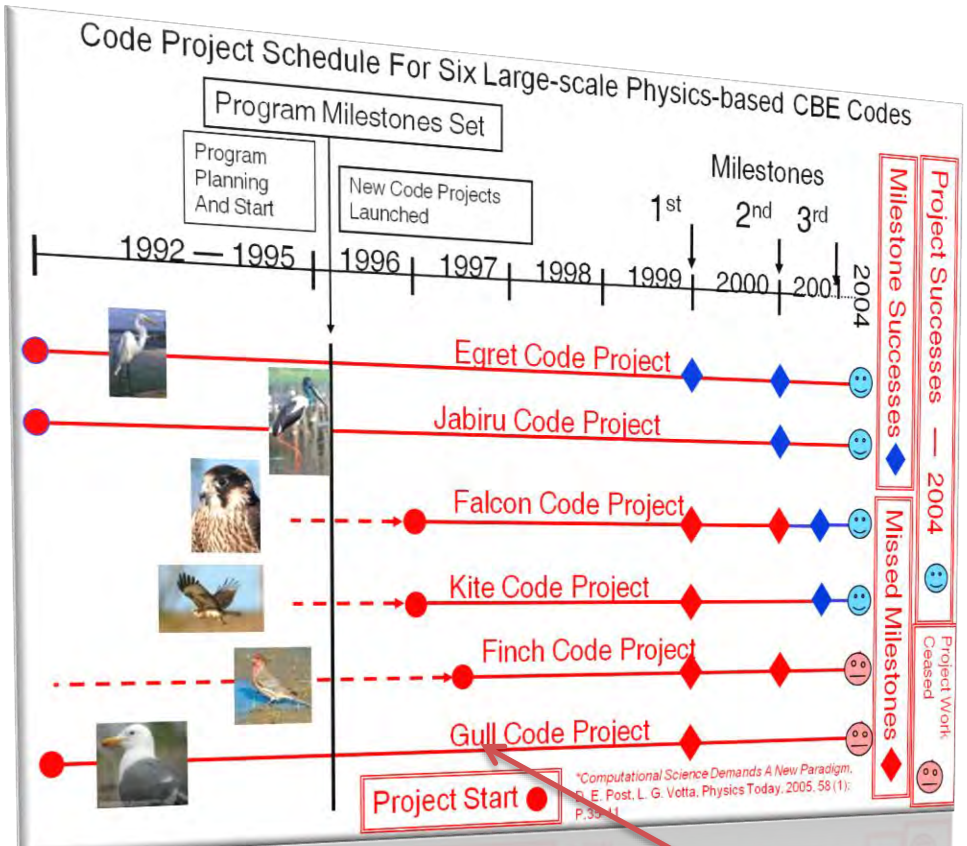
Start by Recognizing that Software Development is a Risky Enterprise



Gov't Software: A Legacy of Risk Management Failure!

Examples of Failure Similar to CREATE

- **DOE ASCI (Multi-Physics, HPC) < 50% Success**



SOFTWARE PROJECT MANAGEMENT AND QUALITY ENGINEERING PRACTICES FOR COMPLEX, COUPLED MULTIPHYSICS, MASSIVELY PARALLEL COMPUTATIONAL SIMULATIONS: LESSONS LEARNED FROM ASCI

D. E. Post
R. P. Kendall

LOS ALAMOS NATIONAL LABORATORY, LOS ALAMOS, NM, USA (POST@LANL.GOV)

Abstract

Many institutions are now developing large-scale, complex, coupled multiphysics computational simulations for massively parallel platforms for the simulation of the performance of nuclear weapons and certification of the stockpile, and for research in climate and weather prediction, magnetic and inertial fusion energy, environmental systems, astrophysics, aerodynamic design, combustion, biological and biochemical systems, and other areas. The successful development of these simulations is aided by attention to sound software project management and software engineering. We have developed "lessons learned" from a set of code projects that the Department of Energy National Nuclear Security Agency has sponsored to develop nuclear weapons simulations over the last 50 years. We find that some, but not all, of the software project management and development practices (rather than processes) commonly employed for non-technical software add value to the development of scientific software and we identify those that we judge add value. Another key finding, consistent with general software industry experience, is that the optimal project schedule and resource level are solely determined by the requirements once the requirements are fixed.

Key words: Software engineering, verification, validation, software project, management, computational science

Acknowledgments

The authors are grateful for discussions with and suggestions from Tom Adams, Marvin Alme, Bill Archer, Donald Burton, Gary Carlson, John Cerutti, William Chandler, Randy Christiansen, Linnea Cook, Larry Cox, Tom DeMarco, Paul Dubois, Michael Gittings, Tom Gorman, Dale Henderson, Joseph Kindel, Kenneth Koch, Robert Lucas, Tom McAbee, Douglas Miller, Pat Miller, David Nowak, James Rathkopf, Donald Remer, Richard Sharp, Anthony Scannapieco, Rob Thomsett, David Tubbs, Robert Weaver, Robert Webster, Daniel Weeks, Robert Weaver, Robert Webster, Dan Weeks, Don Willerton, Ed Yourdon, Michael Zika, and George Zimmerman.

The International Journal of High Performance Computing Applications, Volume 18, No. 4, Winter 2004, pp. 399–416
DOI: 10.1177/1094342004048534

1 Introduction

In the middle of 1996, the Department of Energy (DOE) launched the Accelerated Strategic Computing Initiative (ASCI) to develop an enhanced simulation capability for the nuclear weapons in the US stockpile. The Los Alamos National Laboratory (LANL) and Lawrence Livermore National Laboratory (LLNL) were tasked with developing this capability for the physics performance, and the Sandia National Laboratory (SNL) for the engineering performance of weapons systems. The ASCI program is now almost eight years old and now has been renamed to Advanced Simulation and Computing (ASC). It is an appropriate time to assess the progress and to develop "lessons learned" to identify what worked and what did not. This paper presents the "lessons learned" for successful code development during the ASCI project so far. The major points are summarized in Table 1.

In the absence of testing, improved nuclear weapons simulation capability is needed to sustain the US defensive capability. Following the fall of the Soviet Union and the cessation of testing nuclear weapons by both Russia and the US in the early 1990s, the US inaugurated the "Stockpile Stewardship" program to maintain its nuclear stockpile. Even though the Russian Federation poses a much reduced threat to the US compared to the Soviet Union, history, particularly the history of the twentieth century, has amply demonstrated that any nation that does not possess a strong defense based on modern military technology can – and often will – fall victim to an aggressor. The US and Russia have been in the process of reducing their stockpiles from the level of tens of thousands of warheads needed to counter a "first strike" to the thousands of warheads needed for deterrence. The nuclear weapons mission is to sustain and maintain the US reduced stockpile for the foreseeable future. The existing stockpile consists of weapons systems highly optimized for specific missions and for the maximum yield to weight ratio. They were designed for a 15–30 year shelf life with little consideration given to possible longer-term aging issues. The weapons program now has the challenge of adapting the existing warheads for different missions, and extending their lifetimes to 40 to 60 years without the ability to test the nuclear performance. The strategy developed for "Stockpile Stewardship" has four major elements:

CREATE-Scale Project Cancelled

CREATE Core Risks

10 Core Risks Identified in 2008

1. **Creating and inventing new, innovative software technologies** within the existing DoD program and project management structure.
2. **Loss of credibility due to defects** or insufficiently accurate models in the software that result in inaccurate results.
3. **Building and managing software development teams** that are embedded in, and part of, the DoD customer organizations.
4. **Significant losses of core development staff** and their corporate knowledge, due to severe funding reductions and other institutional turmoil.
5. **Program coordination within the diverse management cultures** especially security management—within different DoD organizations.
6. **Requirements creep and relevancy** over the project's major development phases.
7. **Rapidly changing computational and computer technologies** especially rapidly changing computer architectures and environments.
8. **Loss of DoD stakeholder and sponsor support** due to frequent turnover of senior DoD personnel.
9. **Loss of control of intellectual property rights** In the absence of domestic copyright protection.
10. **Supporting CREATE software users without impacting development.**

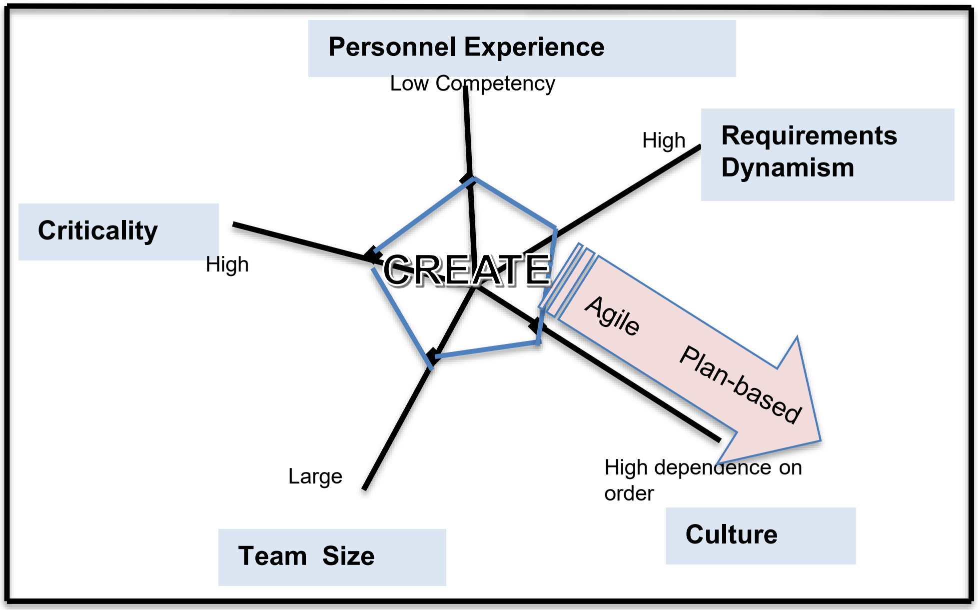
CREATE Risk Management Principles

Addressing the Core Risks

- Develop a compelling, credible vision and endeavor to communicate it.
- Develop a long-term strategic plan and define the essential processes required to execute it.
- Recruit the right team leaders and strong, multidisciplinary teams.
- Balance the need for development team empowerment with the need for accountability.
- Recognize that program management must extend to the risks most outside its control: stable funding, stakeholder support and deployment to customers.
- Protect the development effort from institutional turmoil.
- Implement a rigorous verification and validation program.

The CREATE Approach: Principles to Practices to Mitigate Risk

Development Environment Indicators

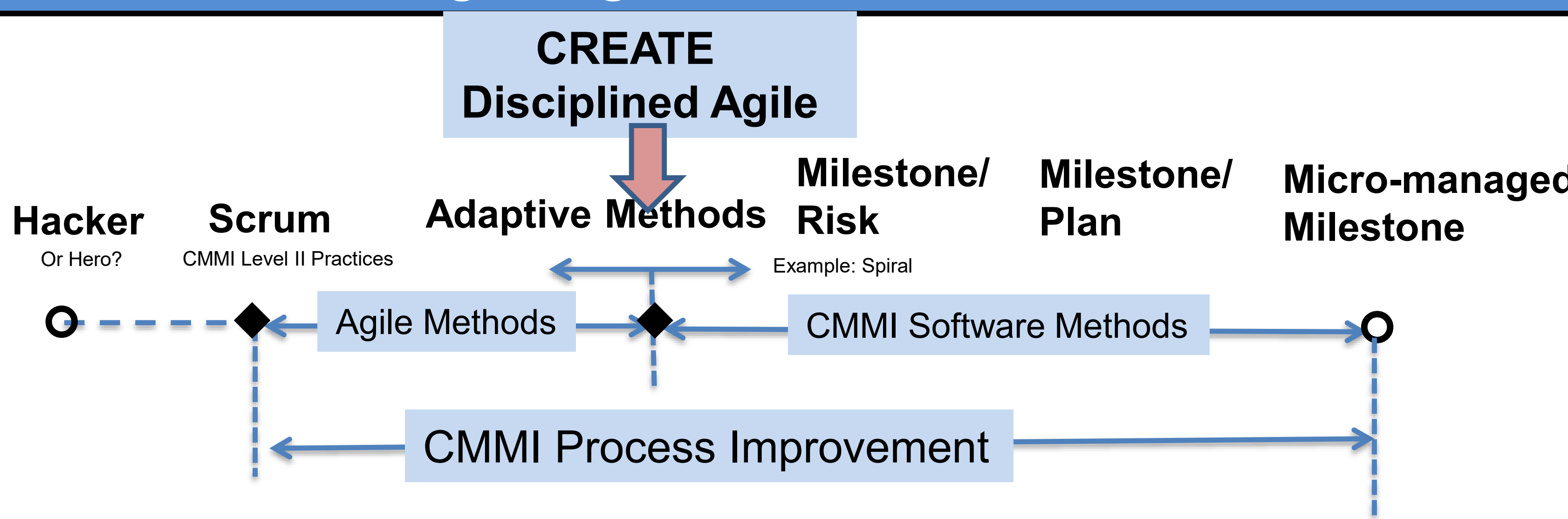


Notional Home Ground Chart for CREATE
after Boehm, Using Risk to Balance Agile and Plan-Driven Methods, IEEE Computer Society, 2003

"Principles" translated into shared "Practices", as opposed to "Processes", best fit the need for flexibility for CREATE operating within the three Armed Services

Risk 1: Challenge of developing new, innovative software within the DoD Program Management structure

- Mitigating Practice: Strive for flexible execution with risk-mitigating milestones



after Boehm, “Getting Ready for Agile Methods with Care”, IEEE Software, 2002

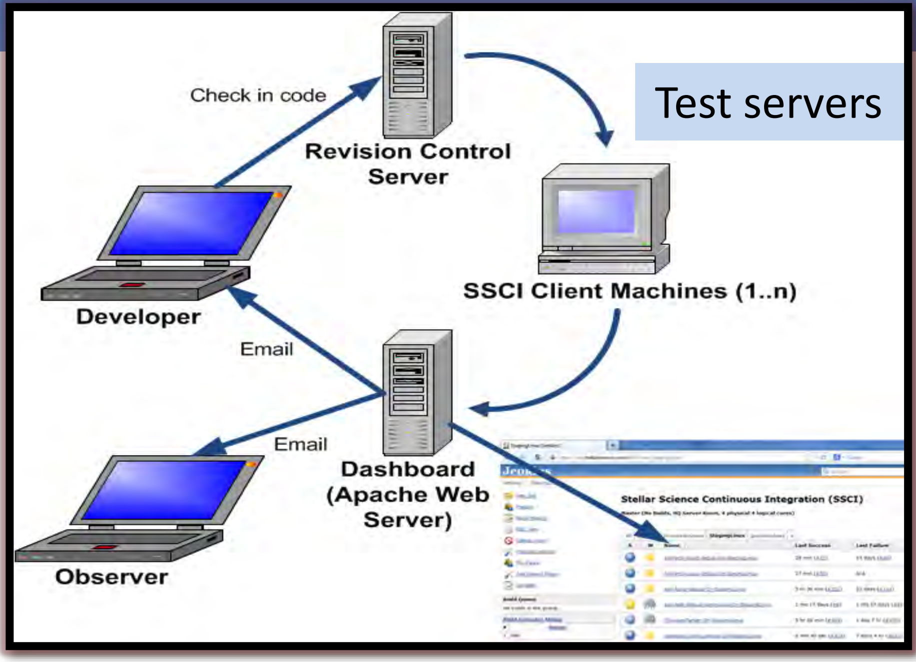
CREATE Development Approach: A Disciplined Agile Workflow Management Approach based on Scrum

Risk 2: Loss of credibility

due to software defects or inaccuracies

Mitigating Practice: *Implement a testing program compliant with National Research Council Guidelines; strive for continuous integration with automated regression tests for each commit, and test coverage measurements*

Regression testing after every commit



CREATE-RF Continuous Integration Platform

Discover problems before they are hard to fix

Risk 3: Difficulty building software teams

under DoD constraints

- Mitigating Practice: *Identify a principal developer within **customer** organizations (in CREATE's case, the Services)*
- Mitigating Practice: *Recruit lean (5 -15 member) development teams lead by technical experts (typically from the DoD S&T community)*

CREATE Product Teams
Create Program Associate Director

Ships
Project Manager
HPCMP, Lorton

NavyFOAM
NSWC, Carderock

Integrated Hydro Design Environment
NSWC, Carderock

Navy Enhanced Sierra Mechanics
NSWC, Carderock

Rapid Ship Design Environment
NSWC, Carderock

Air Vehicles
Project Manager
HPCMP, Lorton

Kestrel
46th Test Wing, Eglin AFB

Quality Assurance
NAVAIR, Patuxent River

Helios
Army AFDD, Ames

Genesis-DESIGN
HPCMP

RF Antennas Project
Sensors Directorate, AFRL, WPAFB

SENTRi
Sensors Directorate, AFRL, WPAFB

Mesh & Geometry
Capstone
Project Manager
Navy NRL

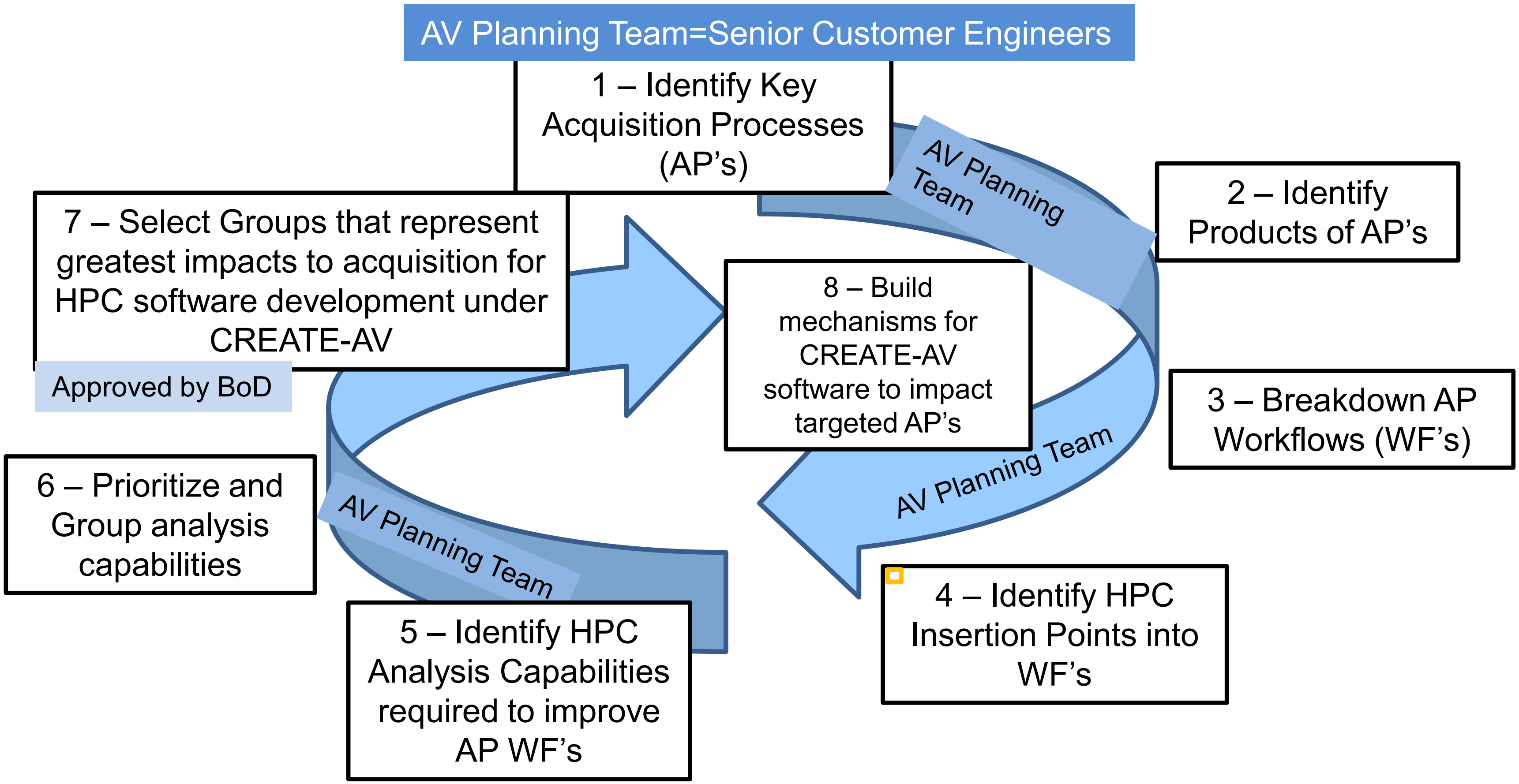
Ground Vehicles
Project Manager

Mercury
ERDC

MAT
TARDEC

Risk 4. Funding Reductions

- **Mitigating Practice:** ***Reach out to the customer with Pilot Projects that demonstrate value***

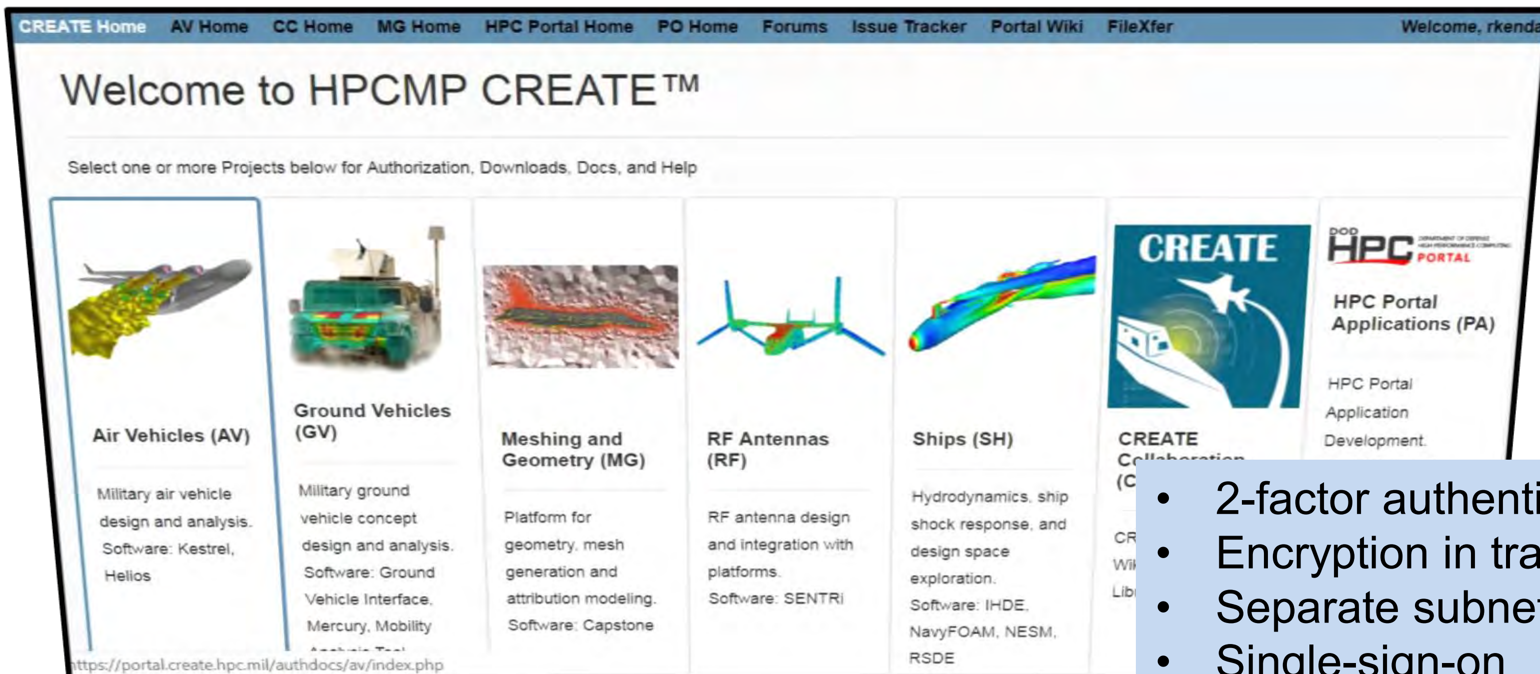


This helps demonstrate value and promotes customer commitment

Risk 5: Difficult program coordination

in an environment of diverse management cultures—especially security-related

- Mitigating Practice: *Establish browser access to CREATE software and support*



- 2-factor authentication
- Encryption in transit and at rest
- Separate subnet
- Single-sign-on

Secure access without downloading software

Risk 6: Requirements creep and product relevancy

Mitigating Practice. ***Express requirements as use-cases in language that customers and developers both understand.***

CREATE-Capstone Foundational[1] Capability Requirements

ID	Description
MG-00	Import Externally Generated Geometry (CAD,
MG-01	Create Parameterized Geometry
MG-02	Support Dependency-Based Associative Mod
MG-03	Repair Externally Generated (eg CAD) Geome
MG-04	Support De-featuring and Idealization of Geon
MG-05	Provide Robust Surface Meshing Algorithms
MG-06	Provide Robust Volume Meshing Algorithms
MG-07	Provide Geometry-based Mesh Generation an
MG-08	Support Multi-scale Models
MG-09	Support Legacy Component Integration
MG-10	Support Analysis Model Attribution
MG-11	Provide Accurate and Scalable Runtime Geom
MG-12	Core Framework (Internal requirements to suppo above)

MG-06 Use-Cases

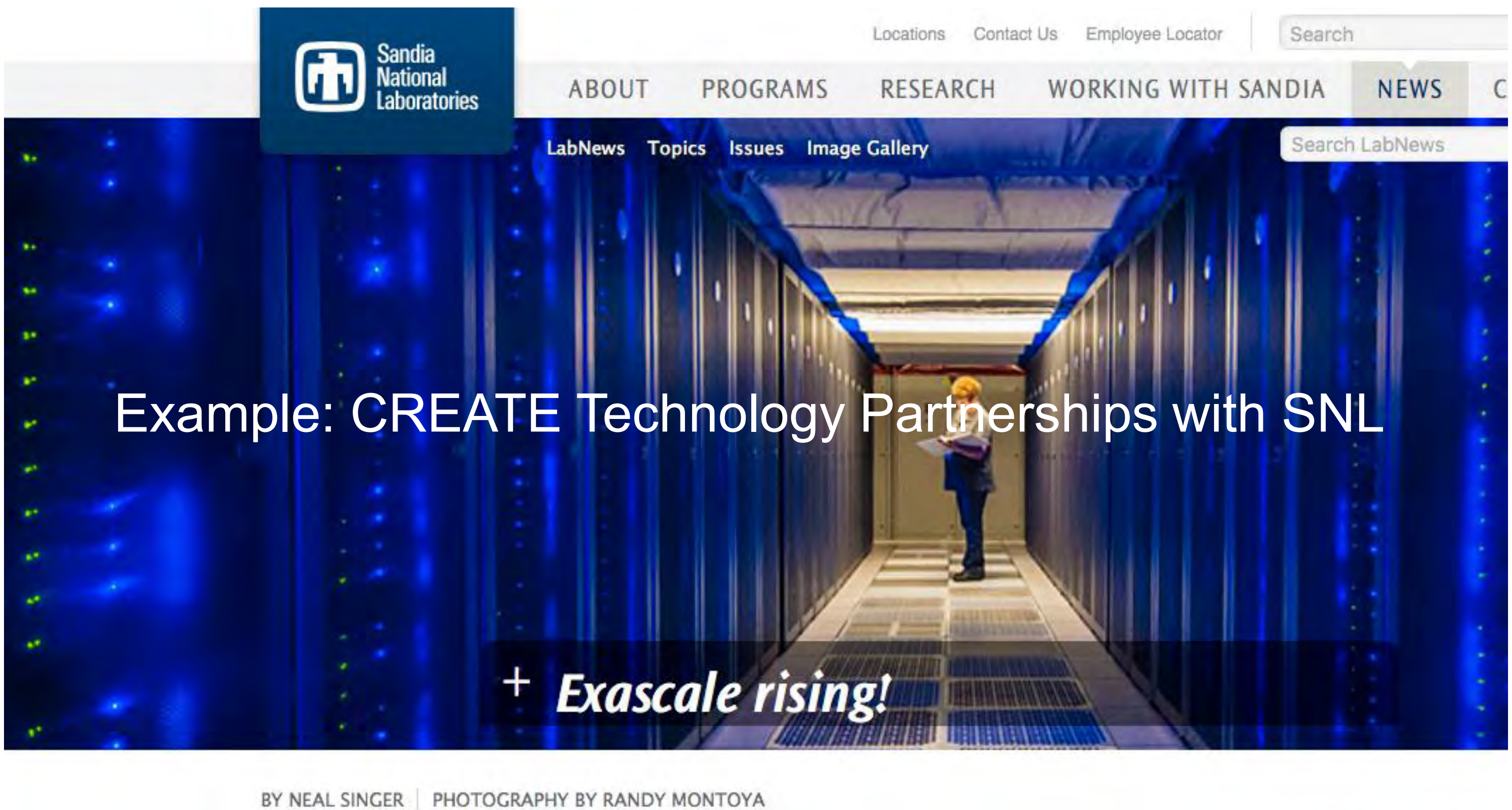
MG-06-UC-01	**Unstructured all-tetrahedral volume meshing**
MG-06-UC-02	**Unstructured hexahedral-dominated hybrid meshing**
MG-06-UC-03	**Boundary Layer meshing with triangular wedge elements in the viscous region transitioning to tet. No interference from other BL**
MG-06-UC-04	**MG07-UC04 with complex geometries and multiple intersecting boundary-layers**
MG-06-UC-05	**Boundary layer meshing with hex,prism in the viscous regin transitioning to hex/tet**
MG-06-UC-06	**MG06-UC05 with complex geometries & multiple intersections**
MG-06-UC-07	**Volume mesh handing for high order element (first approach)**
MG-06-UC-08	**Matching volume meshes for periodic boundary condition**
MG-06-UC-09	**Exterior volume meshing up to a given truncation boundary**
	sources
	for moving parts
MG-06-UC-12	**Support for 'strand-meshing' paradigm**

The focus is on shared understanding of requirements

[1] Established in 2008

Risk 7: Anticipating and responding to rapidly changing HPC environments

Mitigating Practice: *Ensure that the CREATE program maintains an awareness of evolving state of the art in high performance computing*



Example: CREATE Technology Partnerships with SNL

Risk 8: Loss of sponsor support

due to frequent turnover of senior DoD personnel

• Mitigating Practice: *Continually reach out to new senior- and middle-level members of the DoD acquisition engineering community.*

Examples of Outreach:

- 3 BAAs or CRADAs
- 60+ CREATE Pilot Projects
- Dozens of training courses
- 100’s of technical articles(45+ in 2016 alone)

Risk 9: Loss of control of IP rights

HPCMP CREATE™ Software
User Agreement

Authorized to U.S. Government agencies and their contractors in support of a current contract or technology transfer agreement with the U.S. Government

Distribution Control Number: 1313674496

Warning – This document refers to technical data, the export of which is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

1. Introduction

a. This Software User Agreement is made by and between the Department of Defense as represented by the High Performance Computing Modernization Program (hereinafter, "HPCMP") and the undersigned Software User Agreement Recipient

- Mitigating Practice: *Require a standard software distribution agreement (a license for use).*

Recipient has no right to receive, use or examine any source code or design documentation relating to the Product,except as specifically authorized by approved collaborative development and source code agreements. HPCMP retains all right, title and interest in the Product and any portion thereof and in all copies, modifications and derivative works of the Product and portions thereof including, without limitation, all rights the Government may have to patent, copyright, trade secret, trademark and other proprietary or intellectual property rights. Recipient has no rights, by license or otherwise, to use, disclose or disseminate the Product, in whole or in part, except as otherwise expressly provided herein. Recipient may not use any name, mark or designation of the Product except for the express purposes in this Software User Agreement.

c. Unless otherwise permitted by the HPCMP, Recipient shall utilize the Product exclusively to support United States Government programs. Recipient agrees that it shall not provide or allow access to this material to persons other than its employees or persons acting on its behalf in support of U.S. Government programs, without permission of the HPCMP.

2. Rights of Use

Rights to use this Product are granted under this Software User Agreement only for the intended use as determined by the HPCMP, and as documented in the Purpose section of this Software User Agreement. Requests for other uses must be submitted in writing to the HPCMP. The HPCMP has the sole right to approve such requests, and will do so in writing.

3. Restrictions

a. The Recipient shall not re-distribute, sell, or use the Product for any purposes not approved the HPCMP, in whole or in part. The Recipient may produce copies of the Product or portions of the Product for use solely by the Recipient, or for use by a U.S. contractor/sub-contractor organization authorized in writing by HPCMP. Recipient shall require each authorized U.S. contractor/subcontractor organization receiving a copy of the Product or portion of the Product to execute and enforce the terms and conditions of this Software User Agreement, and limit use of the Product to the specific purpose stated within this Software User Agreement. A copy of the authorized copy of the Product or portio User Agreement requirements. In addition all authorized U.S. contractors/subcontrac be responsible for compliance with the ter

b. The HPCMP may change the terms and co

c. The Recipient bears full responsibility controlled material in or related to the Pr The Product is subject to the Arms Expor Act of 1979, as amended, Title 50, U.S.C., App. 2401, et seq. Violations of these export laws are subject to severe criminal penalties.

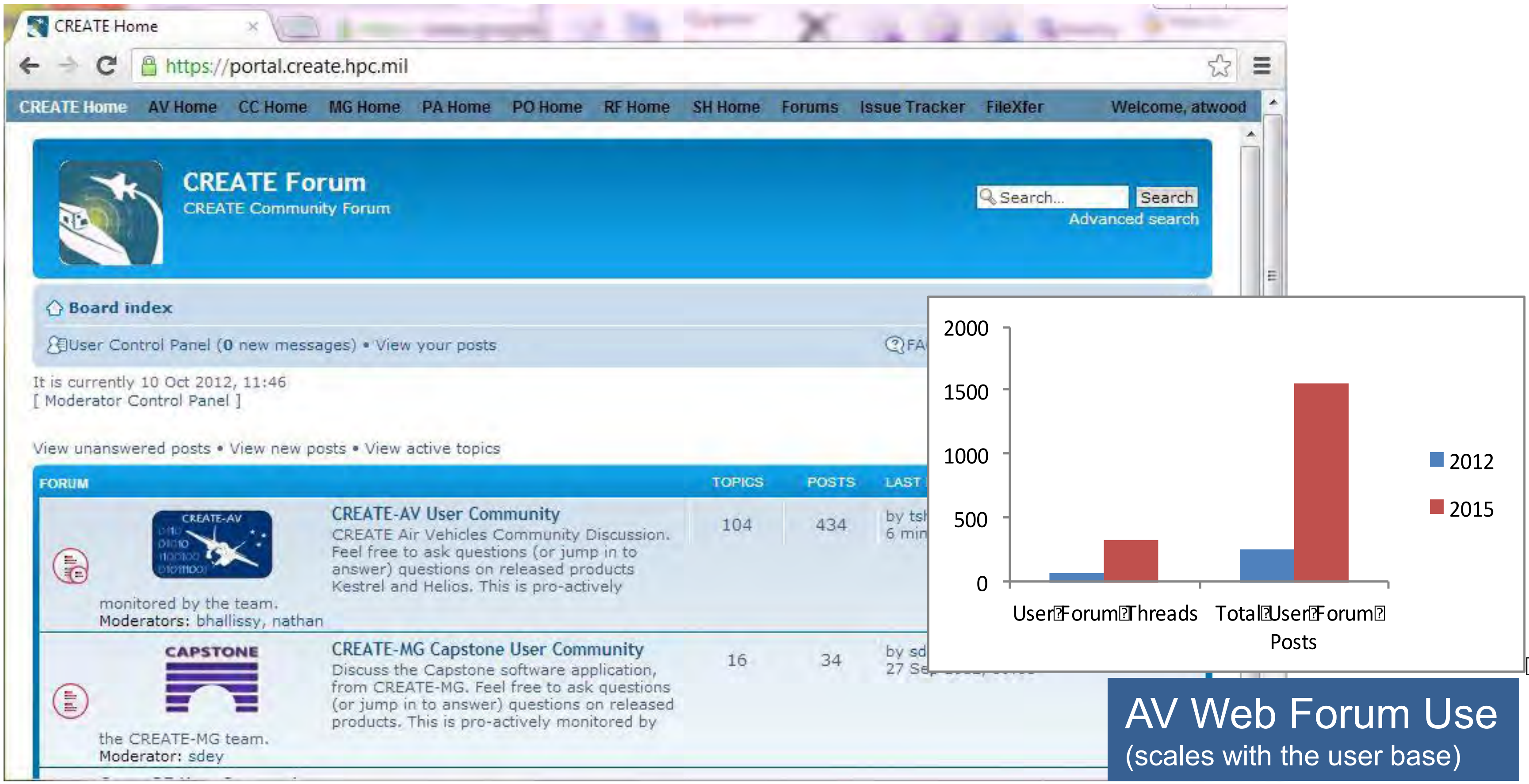
- Practice: Acquire the necessary rights (DFARs) in contracts and licenses.

d. The Recipient acknowledges that the Product may be controlled by the International Traffic In Arms Regulation (ITAR), 22 CFR Sections 121 through 128, and may require an export distribution agreement before assigning any FOREIGN NATIONAL or FOREIGN REPRESENTATIVE to perform work using the Product or before granting any FOREIGN NATIONAL or FOREIGN REPRESENTATIVE access to the Product, and/or technical data generated by the Product. Furthermore, such persons must be approved by the HQUSACE designated Foreign Disclosure Officer before beginning such

Risk 10: Supporting CREATE users

without impacting product development

- Mitigating Practice: *Look for scalable self-help solutions, like Web Forums*



AV Web Forum Use
(scales with the user base)

CREATE Program Management

What has made it work?

- Leadership beyond program management
- Balance between developer freedom and responsibility
- Embedded in CREATE's primary customer organizations
- Customer-defined use-cases
- Frequent product releases
- Browser-based access and Customer Forums

NDIA #19693

Richard P. Kendall, Ph.D.

Software Engineering Consultant
DoD High Performance Computing Modernization Program
(505) 660-0976
Richard.p.kendall4.ctr@mail.mil

Improving Efficiency in Assembly, Integration, and Test

Jeff B. Juranek
Corporate Chief Engineer's Office

25 October 2017

Approved for public release. OTR-2017-01044.

Abstract

The Aerospace Corporate Chief Engineer's Office (CCEO) conducted an Assembly, Integration & Test (AI&T) Efficiency Study to gain insight and an understanding of why AI&T routinely suffers significant schedule delays related to inefficient operation. The study was undertaken as a result of customer concerns related to recent space vehicle AI&T activities that drove major schedule slips and cost increases on the program critical path. This effort was focused on studying Class A selected programs since 2000. Five areas of research were conducted, including: 1) defining what constitutes assembly, integration, and test for space vehicles; 2) a data analysis of space vehicle AI&T cycle time durations, 3) a comprehensive literature search on AI&T methods; 4) a benchmarking study of other industries to learn what innovative best practices companies use to become more efficient in their assembly and test operations; and 5) defining what drives AI&T efficiency /inefficiency.

Acknowledgments

The Corporate Chief Engineer's Office would like to acknowledge the co-author and lead technical contributor for the AI&T Efficiency Study: Charles P. Wright; *Environments and Test Assessment Department; Engineering Technology Group*.

This work was funded by The Aerospace Corporation's Corporate Chief Engineer's Office in support of its mission to develop, codify, and promulgate best practices, tools, and processes across national security space.

Outline

- Introduction
  - *Why We Test*
  - *Key Terminology*
  - *Defining Assembly, Integration, and Test*
- Key Observations
  - *Program Schedule Analysis*
  - *Contributors to Schedule Slips: Design*
  - *Contributors to Schedule Slips: Workmanship*
  - *Contributors to Schedule Slips: Space Vehicle Accessibility*
  - *Contributors to Schedule Slips: Late Deliveries*
  - *Contributors to Schedule Slips: Late Cycle Escapes Detected in AI&T*
  - *Embedded Waste in AI&T*
- Summary of Key Observations
- Summary of Key Recommendations

Introduction

Improving Efficiency in Assembly, Integration, and Test

Why We Test

- Demonstrate requirements have been meet
- Demonstrate flightworthiness by detecting and correcting anomalous behavior before flight
- Ensure survival of launch and operating environments
- Decrease mission risk
- Test Strategies
  - *Development (Proof of design concept + Development of manufacturing processes)*
  - *Qualification (Demonstrate 6σ design margins)*
  - *Protoqualification (Demonstrate 3σ design margins)*
  - *Acceptance (Demonstrate workmanship, functionality and performance)*
  - *Flightproof (Protoqualification levels + Acceptance durations for dynamics)*
- Common Test Objectives
  - *Design verification (Qualification and Protoqualification testing)*
  - *Margin demonstration*
  - *Workmanship screening*
  - *Performance to specification*
  - *Acceptance test validation*

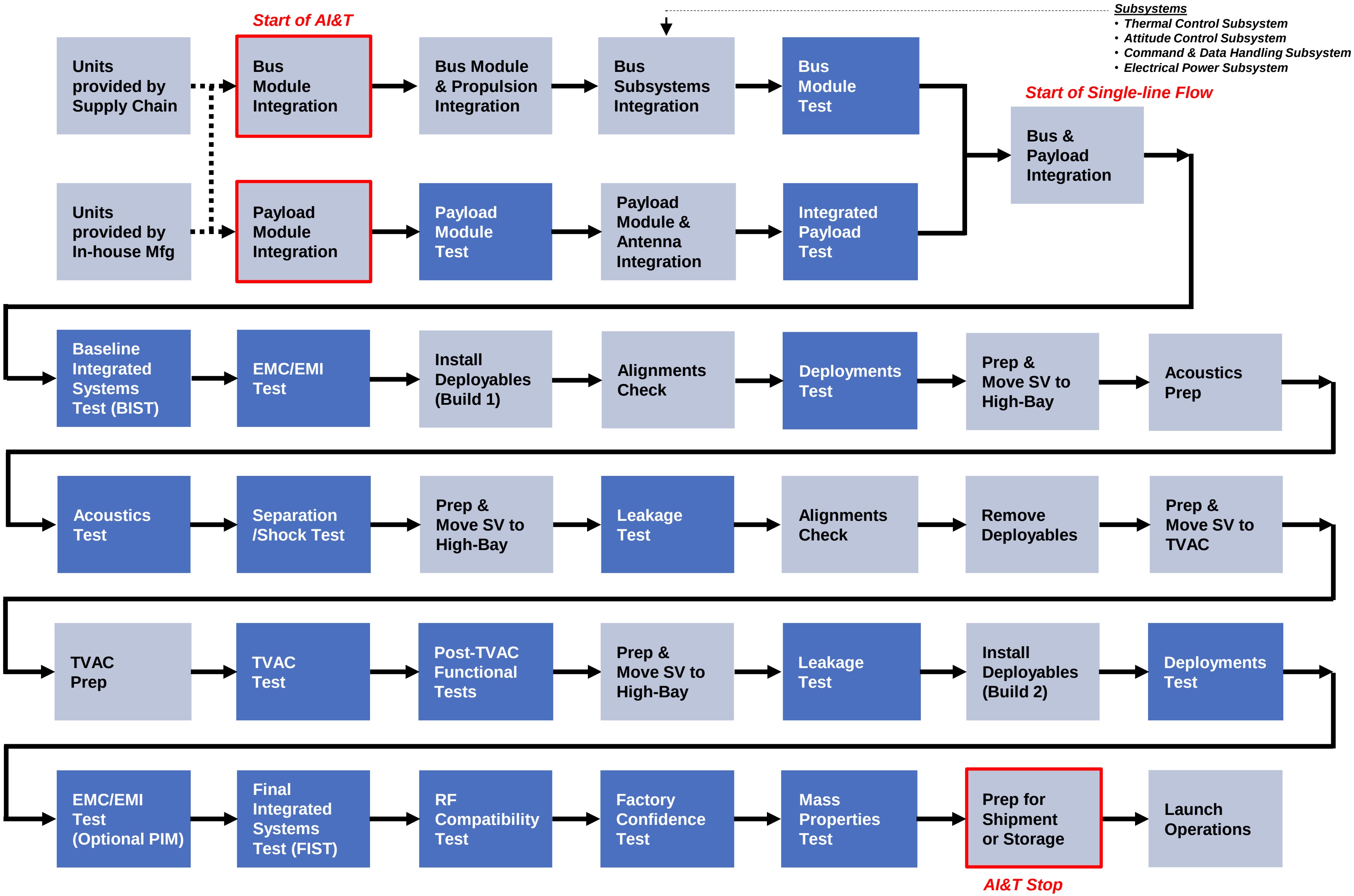
Effective testing is key to program and mission success

Key Terminology

- Definition of assembly, integration, and test (AI&T):
  - *Start of AI&T is when a completed bus structure and/or payload structure is assembled together, harnesses installed, and ready for unit integration*
  - *Conclusion of AI&T is shipment of the space vehicle to storage or to launch site*
- Efficiency: A measure of the ratio of actual hours worked compared to the total hours worked.
- Value Stream: All of the process steps, both value-added and non-value added, required to complete a product from beginning to end. Value stream mapping (VSM) is a Lean technique used to document, analyze and improve the flow of information or materials required to produce a product for a customer. VSM documents the current state and future state of a process after the process flow has been improved by eliminating the inherent waste in both non-value added and value-added steps.
- Waste: Any activity, task, or time element which does not add value to the product and creates inefficiency in the system. The 7 traditional wastes are: 1) defects; 2) excess inventory; 3) over-production; 4) waiting; 5) excessive motion; 6) transportation; and 7) over-processing.
- Value (from the customer's perspective): Performing a build or verification task one-time.

No consistent definition for the Start of AI&T; and no consistent definition of Value

Defining Assembly, Integration, and Test (AI&T)



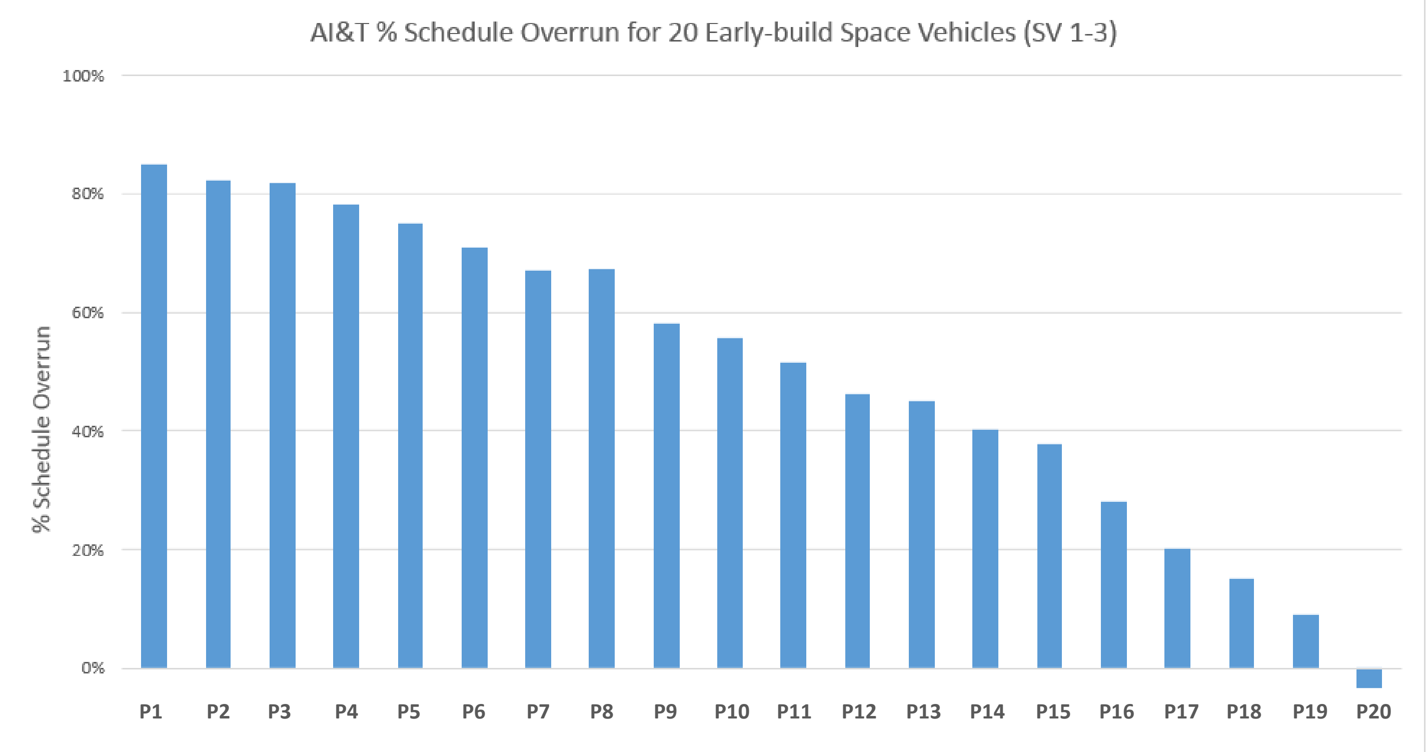
EMI/EMC – Electromagnetic Compatibility/Interference PIM – Passive Intermodulation RF – Radio Frequency TVAC – Thermal Vacuum

Key Observations

Improving Efficiency in Assembly, Integration, and Test

Program Schedule Analysis

- Perception exists that "AI&T is inefficient" and "AI&T is the major cause leading to cost overruns"



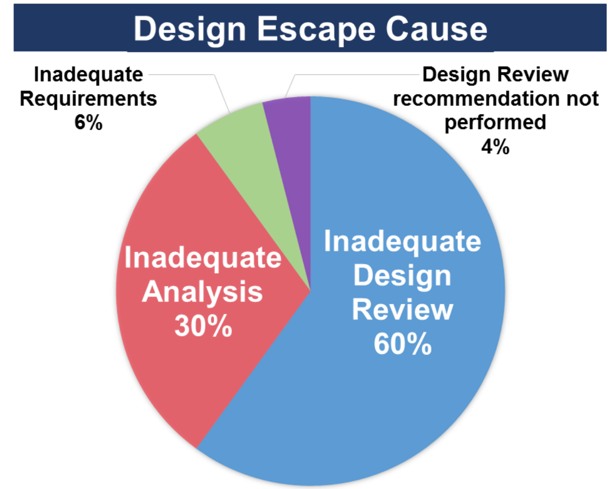
Note: Start dates based on planned schedule at critical design review (CDR); completion dates are actuals.

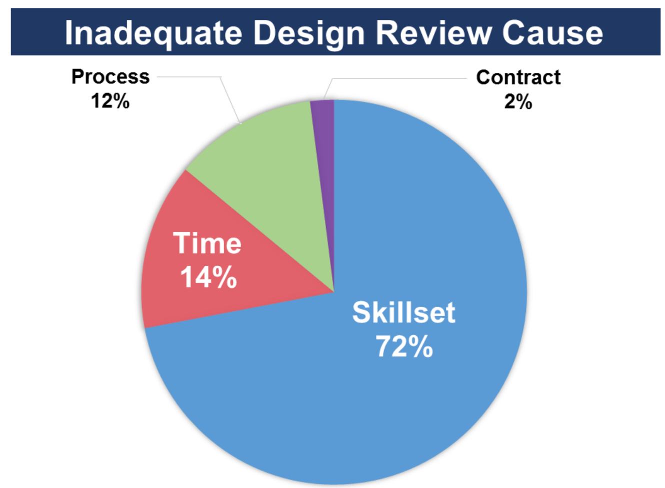
Source: AI&T Efficiency Study, TOR-2015-01412, 9 January 2017

Greater than 50% of the vehicles experienced more than 2X their planned AI&T duration

Contributors to Schedule Slips: Design

- Root cause of design escape varies
  - *Inadequate design review (60%)*
  - *Inadequate analysis (30%)*
- In 19 of 21 test cases that didn't have a fully-tested Engineering Model (EM), the designers indicated that issue would have been found had they utilized a fully-tested EM
  - *Provides the most robust validation method to flush-out inadequate analysis and packaging issues*
  - *A fully tested EM prior to CDR drives early discovery, demonstrates compliance while maturing the Design Review data products*
- Reviewer skillset implicated in cause of inadequate design reviews (72%)
  - *Not getting help; not the right persons; not raising issues*
  - *Mixed technology units require multi-discipline SMEs*
  - *Skillset of Government team should be supplemented with FFRDC oversight*

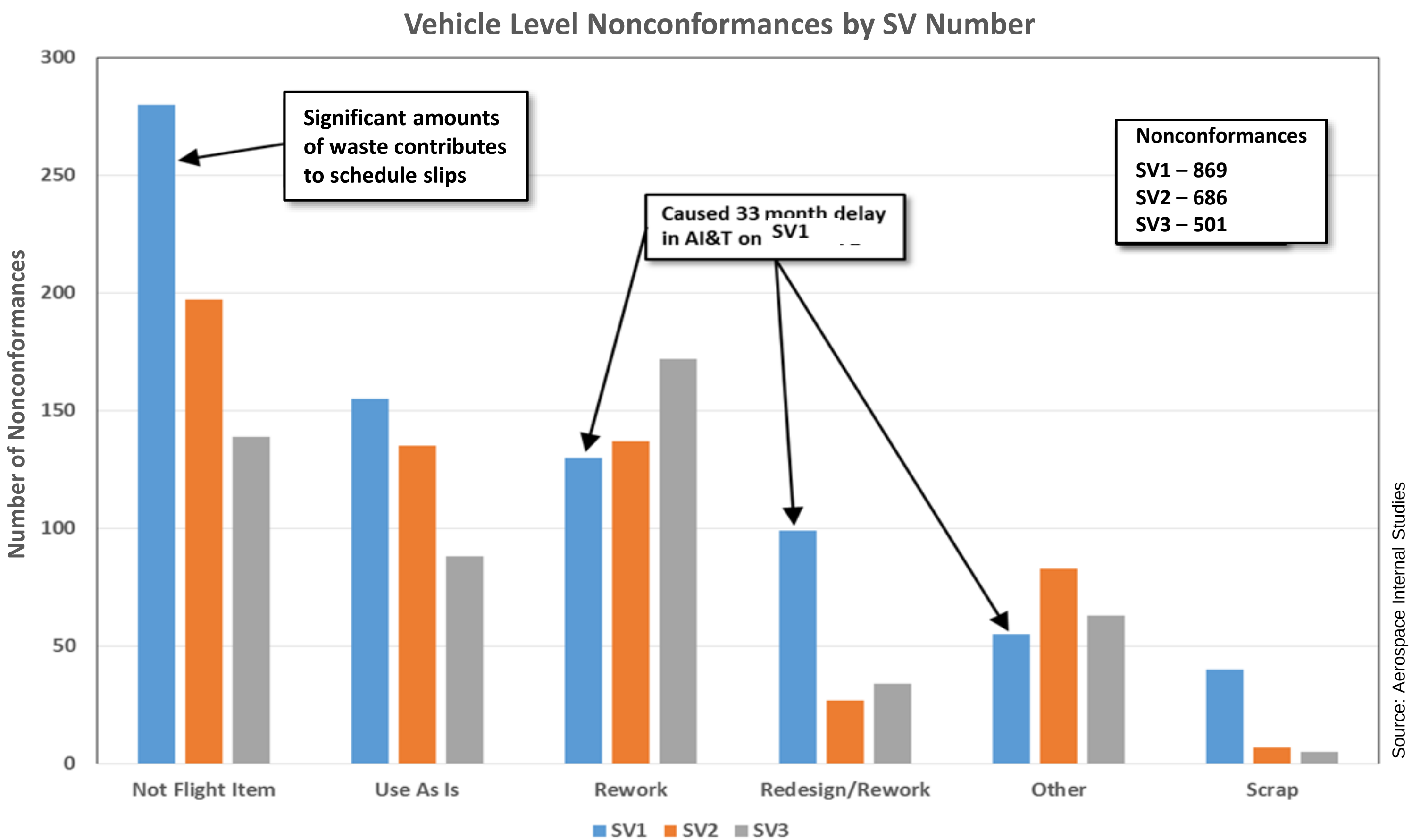




Source: Design Review Improvement Recommendations, TOR-2015-02545, 29 May 2015

Many design escapes are preventable with the right set of reviewers and having a robust design review process with incremental reviews

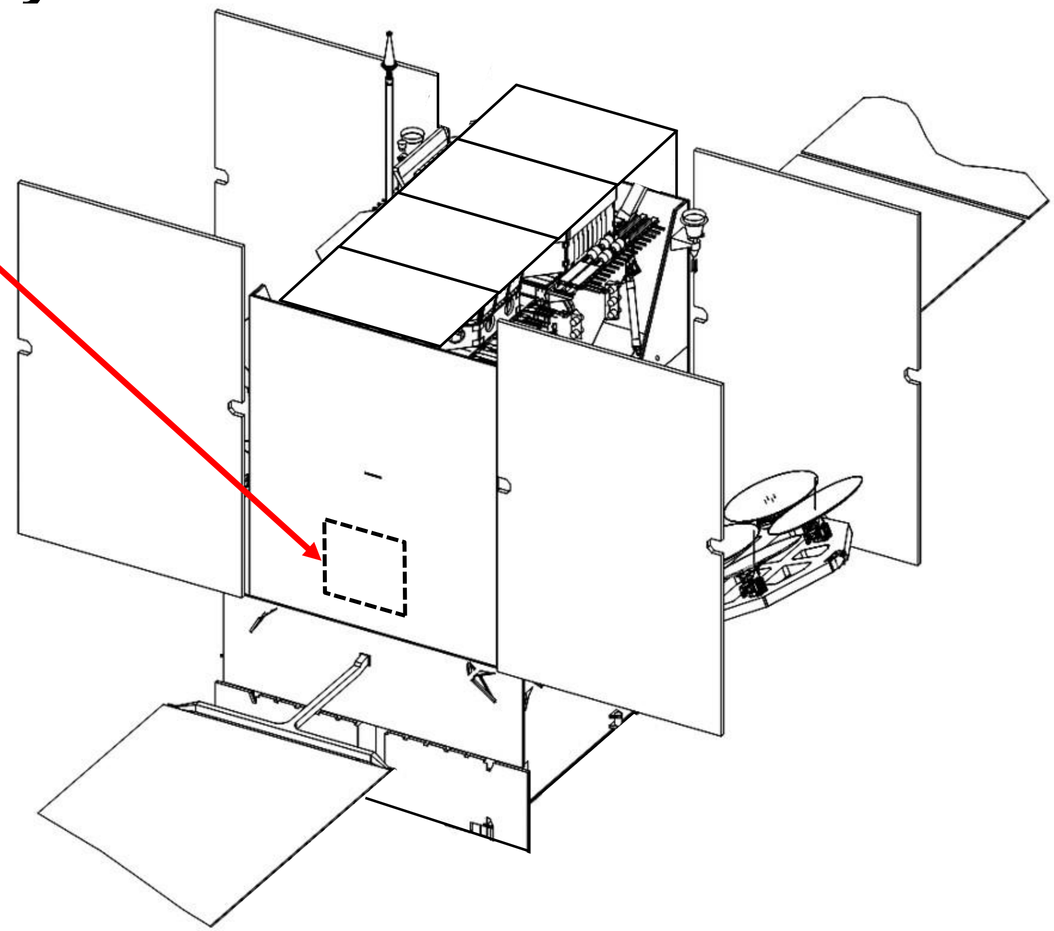
Contributors to Schedule Slips: Workmanship



Anomalies during AI&T contributed to a 33-month schedule slip on SV1

Contributors to Schedule Slips: Space Vehicle Accessibility

- Failed components at space vehicle-level required access hole to be cut in load-bearing structural panel to remove and replace (R&R)
- This is what poor *Design for Accessibility* looks like – no way to access electronic components
- Space vehicle design created access constraint

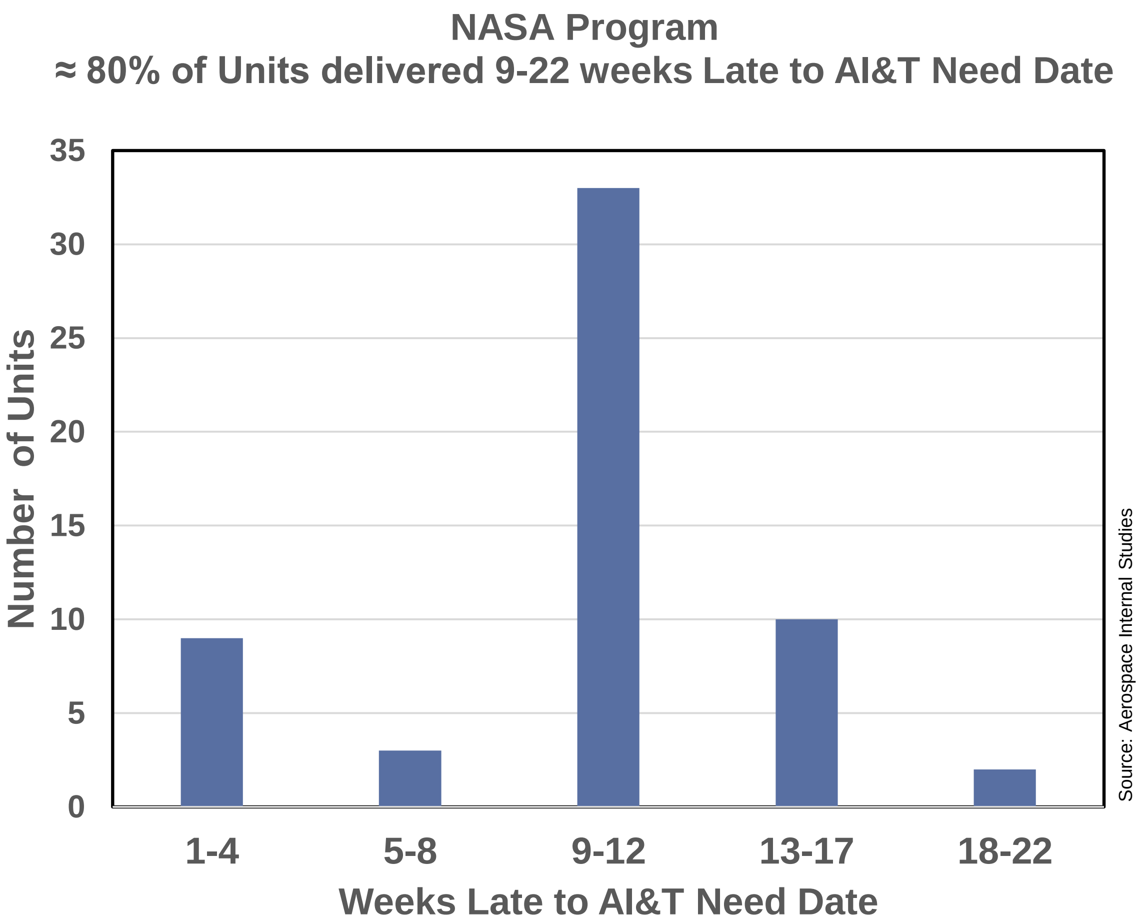


Notional Space Vehicle
(Access hole depicted is representational not actual)

***Example of Design for Accessibility Requirement*:**
"The spacecraft shall be designed such that remove and replace of any unit does not require disassembly of the primary structure, removal of harnesses, or removal of other units."

Poor space vehicle accessibility resulted in 6-month slip in AI&T

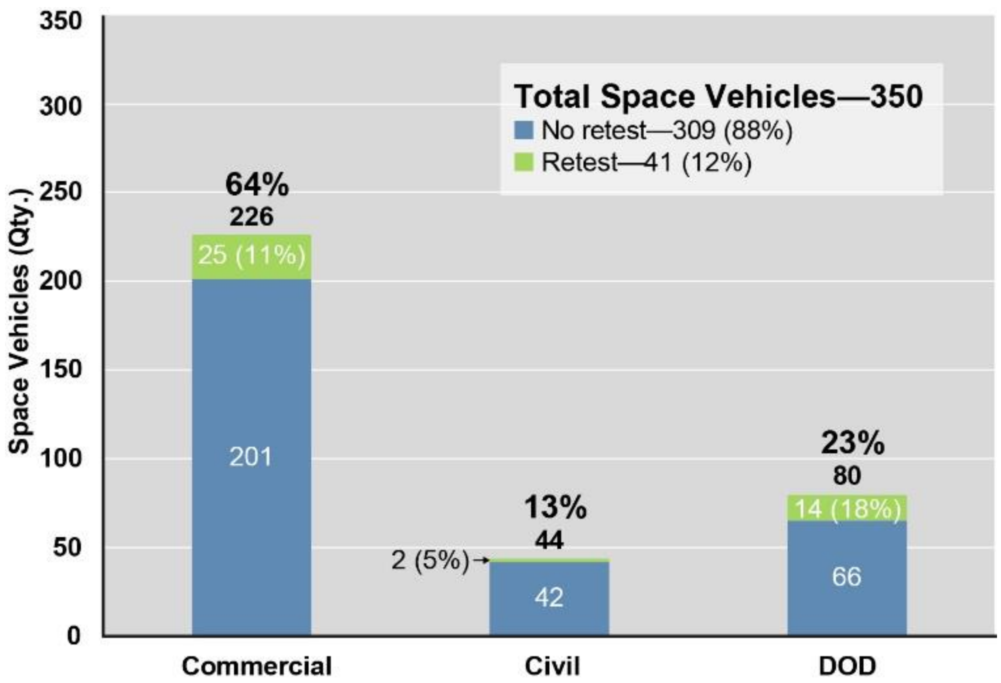
Contributors to Schedule Slips: Late Deliveries



Units delivered late to AI&T cause planned schedules to "go out the window"

Contributors to Schedule Slips: Late Cycle Escapes Detected in AI&T

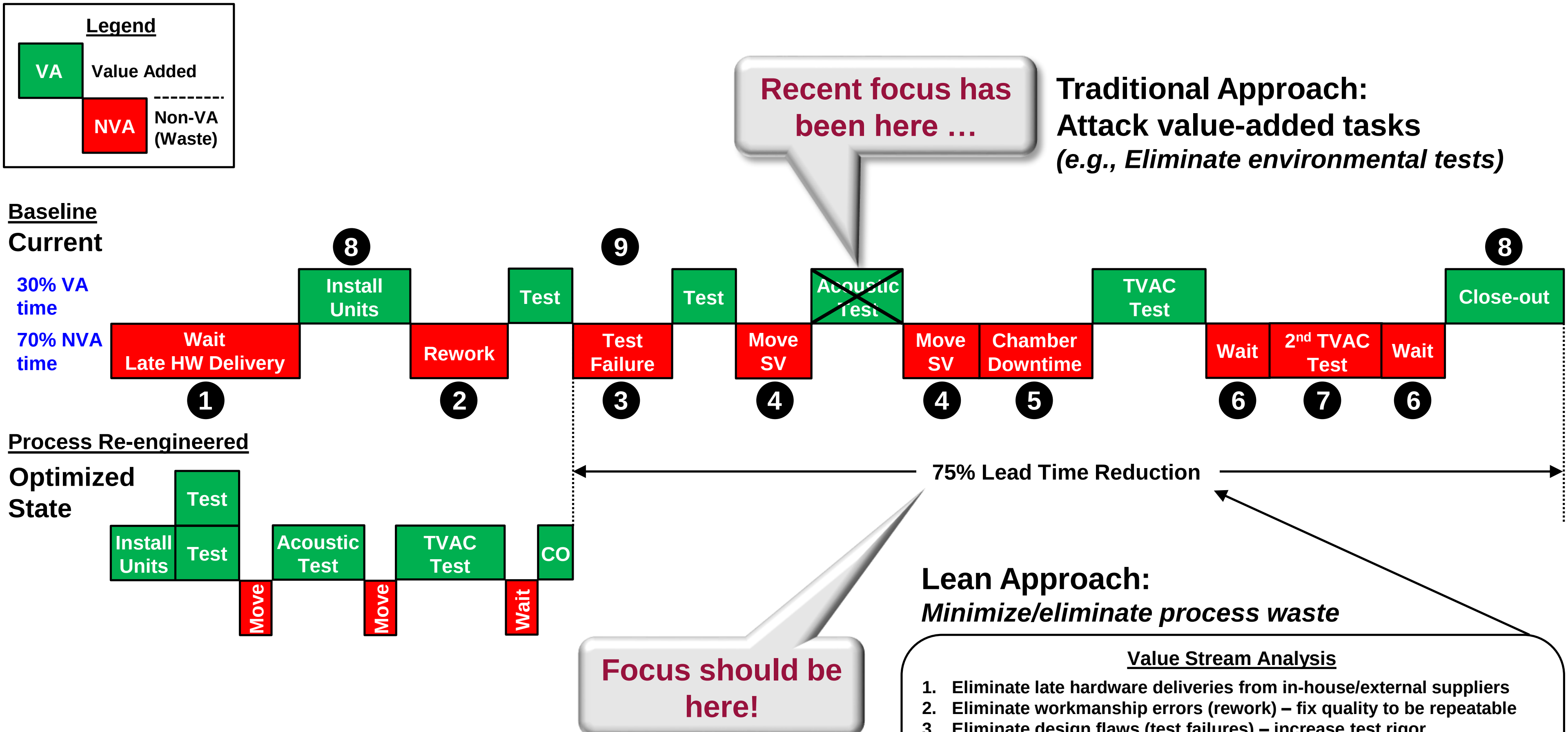
- Study of 350 space vehicles since 2000 showed 12% see thermal vacuum (TVAC) retest



Source: Mission Assurance Implications of Space Vehicle Thermal Vacuum Retest, TOR-2017-01693, 5 June 2017

Eliminating TVAC retests rests on stronger Unit design and screening

Embedded Waste in AI&T



Value Stream Analysis

1. Eliminate late hardware deliveries from in-house/external suppliers
2. Eliminate workmanship errors (rework) – fix quality to be repeatable
3. Eliminate design flaws (test failures) – increase test rigor
4. Minimize SV moves – collocate activities outside chamber/work cell
5. Eliminate chamber downtown-time – increase preventive maintenance
6. Minimize wait times
7. Eliminate TVAC retest (2nd TVAC)
8. Reduce installation and close-out steps durations
9. Perform tests in-parallel with other tests (whenever safely possible)

Lean Metrics

- % Reduction in Lead Time
- % VA time vs. NVA time
- Spaghetti Diagram (travel distances)
- Facility Space (square footage)

This is how you Lean …

Baseline – Current
⮤ **Process Improvement – Improved State**
⮤ **Process Re-engineering – Optimized State**
⮤ **Ideal State**

Key Observations and Key Recommendations

Improving Efficiency in Assembly, Integration, and Test

Key Observations

- Six significant issues associated with schedule overruns during assembly, integration and test (AI&T) phase:
  1. *AI&T schedules at critical design review (CDR) are routinely unexecutable – flawed baseline schedule is used to measure later schedule performance*
  2. *Flight hardware design escapes detected in AI&T strongly drive schedule slips*
  3. *Flight hardware workmanship issues detected in AI&T strongly drive schedule slips*
  4. *Late delivery of flight hardware/software/GFE/GSE strongly drives AI&T schedule slips*
  5. *Thermal vacuum retest – 12% of studied vehicles see more than one TVAC test*
  6. *Significant amounts of waste exists (errors in procedures, test set-up/facility, test SW database errors, etc.)*

GFE – Government Furnished Equipment   GSE – Ground Support Equipment   TVAC – Thermal Vacuum

Key Recommendations

- Require schedules in the RFP response and at CDR account for AI&T inefficiencies to improve realism
- Strengthen design and review processes to minimize escapes into AI&T
  - *Require frequent incremental design reviews in addition to milestone reviews*
- Require “Design for Accessibility” as a key design requirement to reduce delays due to lack of space vehicle accessibility
- Fix design, workmanship, and software problems in manufacturing and in the supply chain (NOT in AI&T) to eliminate late deliveries
- Strengthen unit and lower level test programs to screen-out problems before delivery to AI&T to minimize impact of late cycle escapes
  - *Add board/slice thermal pre-conditioning*
  - *Use highly accelerated life testing (HALT) on new development units*
- Increase focus on the identification and elimination of waste – require value stream mapping and Lean metrics

RFP – Request for Proposal CDR – Critical Design Review

References

1. "*Design Review Improvement Recommendations*," TOR-2015-02545, The Aerospace Corporation, 29 May 2015.
2. "*Assembly, Integration, and Test (AI&T) Efficiency Study*," TOR-2016-01412 (Restricted access), The Aerospace Corporation, 9 January 2017.
3. "*Mission Assurance Implications of Space Vehicle TVAC Retest*," TOR-2017-01693, The Aerospace Corporation, 5 June 2017.

Biographies

Mr. Juranek has more than 32 years of experience working on Air Force, IC, MDA, NASA and commercial space programs. He is currently a Project Leader Sr. in the Corporate Chief Engineer's Office at The Aerospace Corporation. Prior to working at The Aerospace Corporation, Mr. Juranek worked as a Department Manager in Systems Engineering and as a Section Manager of Space Reliability Engineering at Raytheon Space & Airborne Systems. Additionally, he also spent part of his career at Boeing Satellite Systems (formerly Hughes Space and Communications) where he gained experience as both a production manager and an IPT Lead for xenon ion propulsion systems power supply manufacturing and test. During this time he also worked in Product Effectiveness, and spent time working with parent company General Motors/Delco Electronics to assist in bringing the Lean production philosophy to satellite manufacturing. Mr. Juranek started his aerospace career at Hughes Aircraft Radar Systems Group in 1985 working as a manufacturing engineering planner, and was a graduate of the Hughes Manufacturing Technology Rotation Program. Mr. Juranek holds a B.S. in Industrial Technology from Iowa State University, as well as a M.S. in Quality Assurance from California State University, Dominguez Hills.

CARDEROCK DIVISION

Network Surface Combatant RSDE Pilot Study

NDIA Systems Engineering Conference
25 October 2017

NAVSEA WARFARE CENTERS

Presenter: Dr. Douglas Rigterink
Code: 823

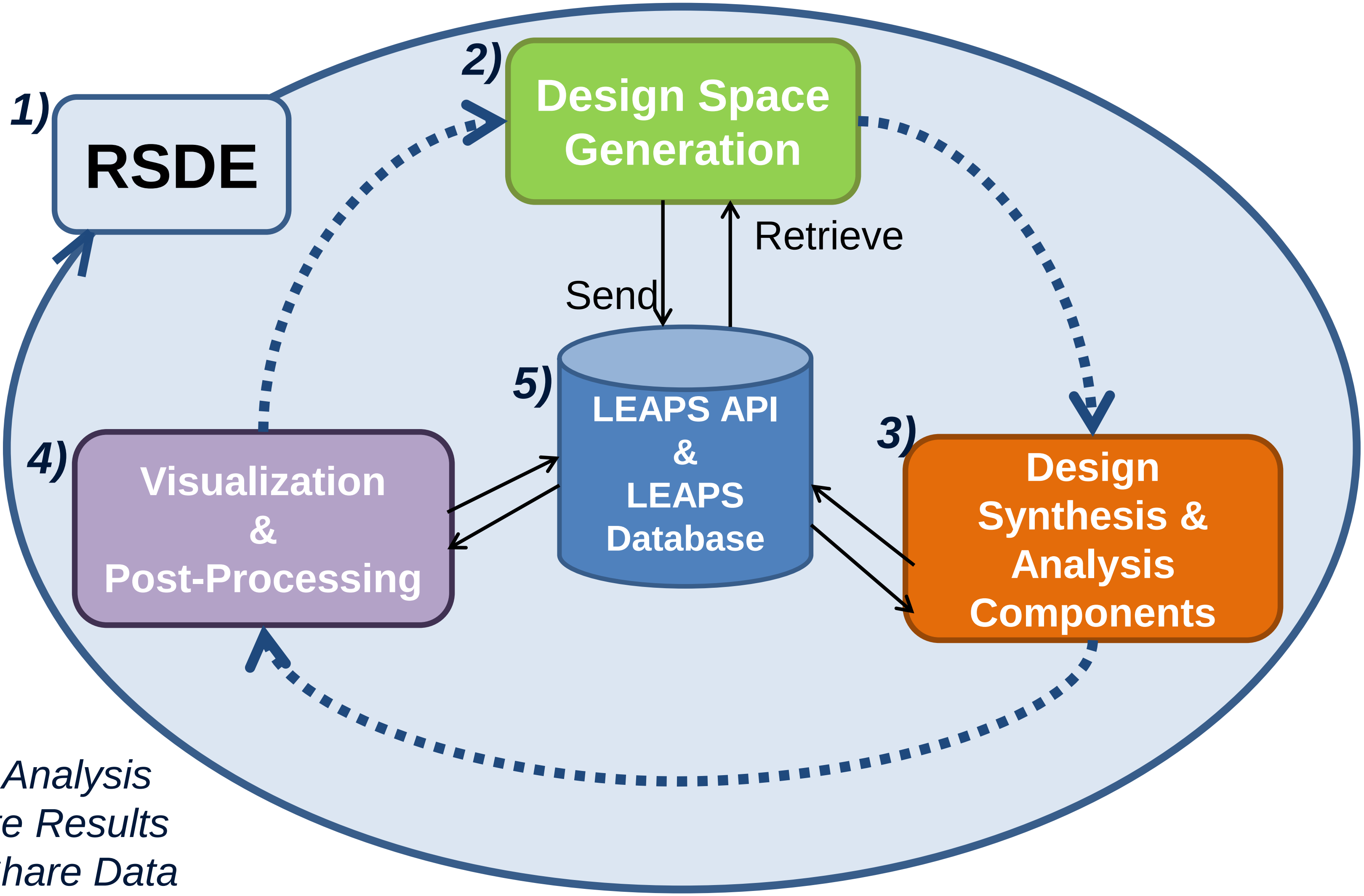
douglas.rigterink@navy.mil | 301-227-5886

Study Objectives

- **Inform the setup of Future Surface Combatant AoA studies.**
  - Baseline designs from FSC wargame studies,
    trading reduced sensing capabilities for weapon systems
- **Familiarize NSWCCD Code 824 Future Ship and Submarines Concepts Branch with the use of RSDE for future studies and provide feedback to improve the software.**

CREATE
Computational Research & Engineering Acquisition Tools & Environments

RSDE Functional Product Architecture



1) *Interface*
2) *Sampling*
3) *Design & Analysis*
4) *Investigate Results*
5) *Store & Share Data*

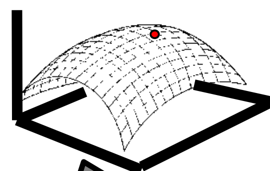
Distribution Statement A: Approved for public release, distribution is unlimited.

Design Space Exploration

Run **RSDE**

Designers provide **Baseline** + **Ranges** of inputs. Requirements, etc. {min,max}

Sample Point

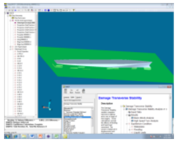


***Included* Analyses:**

IHDE

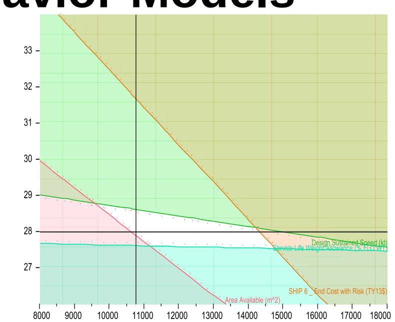
SHCP-L

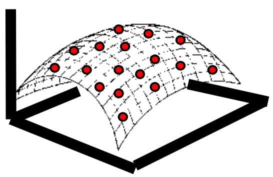
Etc…



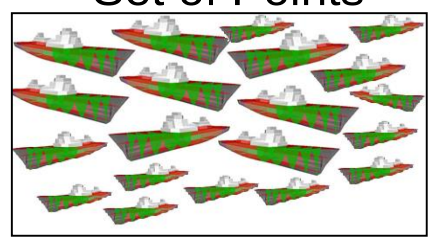
Automatically Re-samples for additional design points

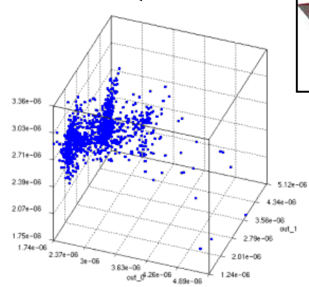
Visualizations & Behavior Models

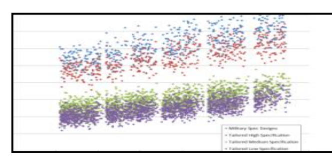




Set of Points







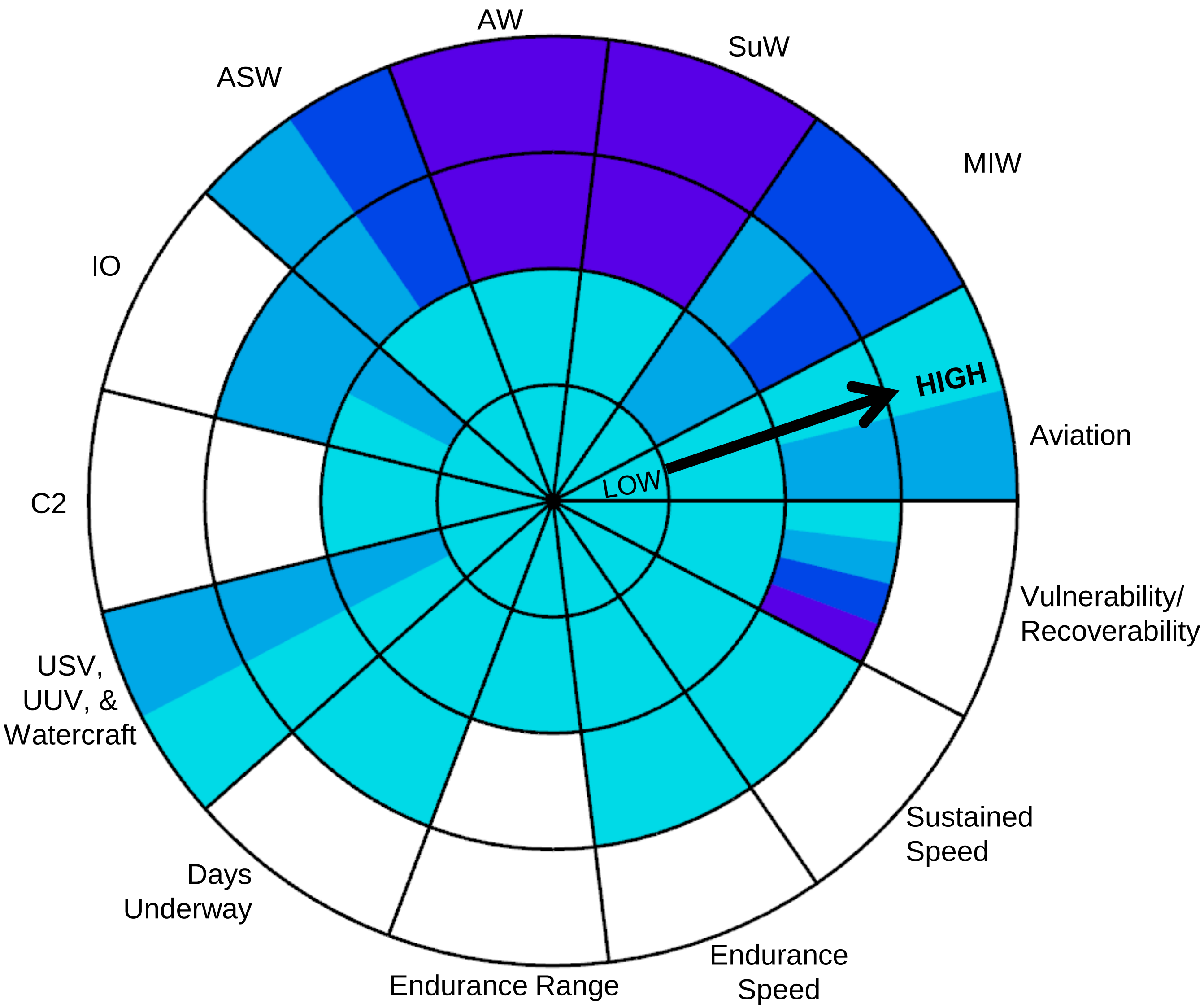
Output

Designs & Analyses

In LEAPS

Distribution Statement A: Approved for public release, distribution is unlimited.

Operational Design Space



Capability Source

- Standalone Capability
- Onboard UXV/Aviation
- Interface with Advanced/Deployed UXV
- Networked Track Received
- Outside of Design Space

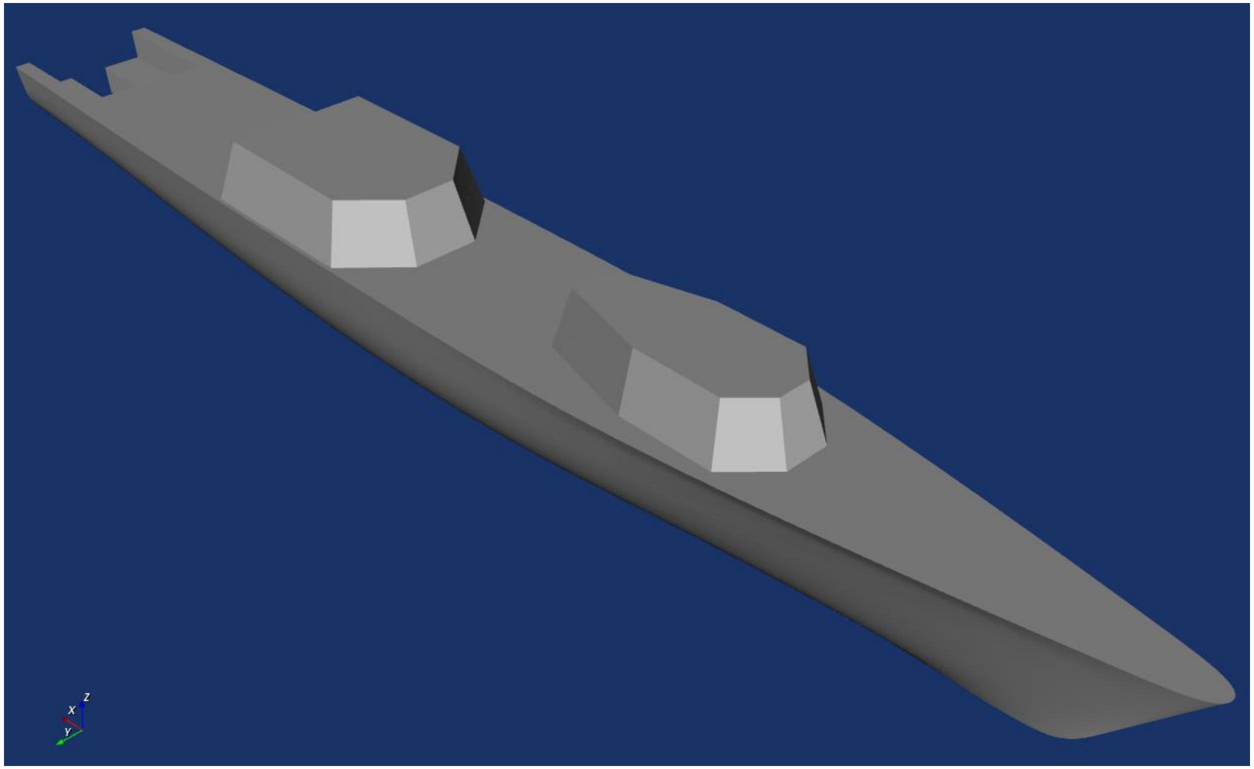
Major Study Trade-offs

- **Combat System Major Trade-offs:**
  - Fixed array vs. rotating array radar
  - Number of VLS cells (16 to 96)
  - Main gun size
  - Sonobouy system
- **Embarked Systems Trade-offs:**
  - Number of manned and unmanned aviation units
  - Number and size of small boats/equivalent USV & UUVs
  - Boat launch location
- **Naval Architecture Trade-offs:**
  - Length
  - Propulsion system type – mechanical vs. IPES
  - Engine separation – survivability
  - Auxiliary propulsion unit – survivability

Low Magnitude DSE Concepts

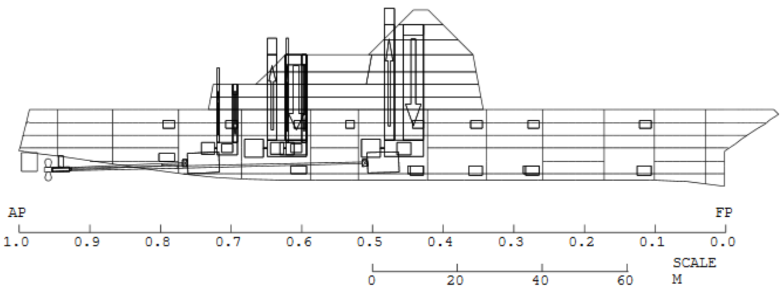
Description FAST Study Variant	**Length Waterline**	**Propulsion**	**Engine Room Separation**	**VLS Cells**	**Relative CSEL Weight/Elec**	**Helo**	**UAV**	**Boats/USV/UUV**
NSC Analog Patrol 1 Combatant	130m	2 shaft CODAG	No	32	Baseline	1	2x TERN UAV	2x 11m RHIB equivalent, stern launch
Euro Style Combatant Patrol 2 Combatant	123m	2 shaft CODAG	Yes	16	0.91 / 1.02	1	2x TERN UAV	2x 11m RHIB equivalent, side launch
IPES Small Surface Combatant Patrol 2 Combatant	117m	1 Shaft IPES + APU	No	16	0.91 / 1.02	1	2x TERN UAV	2x 7m RHIB equivalents, side launch
Small Destroyer Battle Group Escort Variant 5 w/ downsized radar	148m	2 shaft, 4 COGAG	Yes	96	1.71 / 3.04	1 or 2	3x TERN UAV	2x 11m RHIB equivalent, side launch
APU Destroyer Battle Group Escort Variant 6	155m	2 shaft IPES + APU	No	96	1.73 / 3.17	2	3x TERN UAV	2x 11m RHIB equivalent, launch method under evaluation
IPES Surface Combatant Patrol 1 Combatant	136m	2 shaft IPES	No	32	1 / 1	1	2x Tern UAV	2x 7m RHIB equivalents, side launch
1 Shaft Destroyer Battle Group Escort Variant 5 w/ downsized radar	141m	1 shaft GT + APU	No	96	1.71 / 3.04	2	3x TERN UAV	2x 11m RHIB equivalent, side launch

National Security Cutter Analog

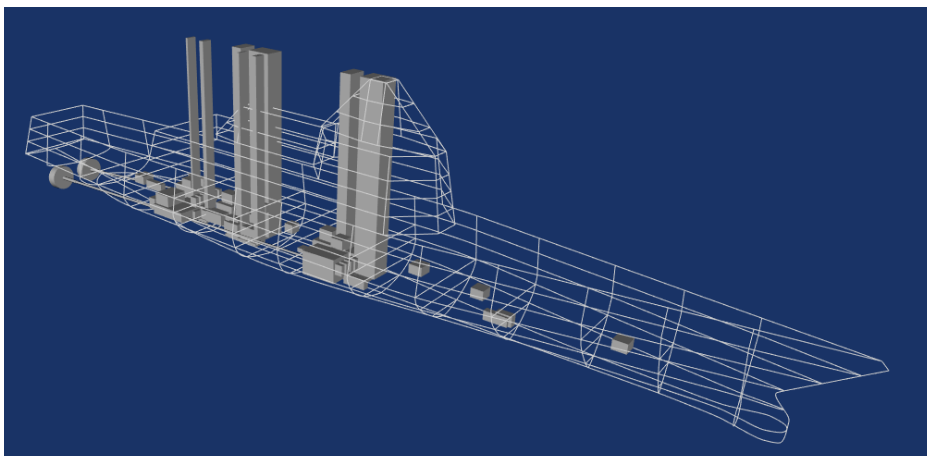


FAST Study Design Variant	Length Waterline	Propulsion	Engine Room Separation	VLS Cells	Helo	UAV	Boats/USV/UUV
Patrol 1 Combatant	130m	2 shaft CODAG	1 bulkhead separation	32	1	2x TERN UAV	2x 11m RHIB equivalent, stern launch

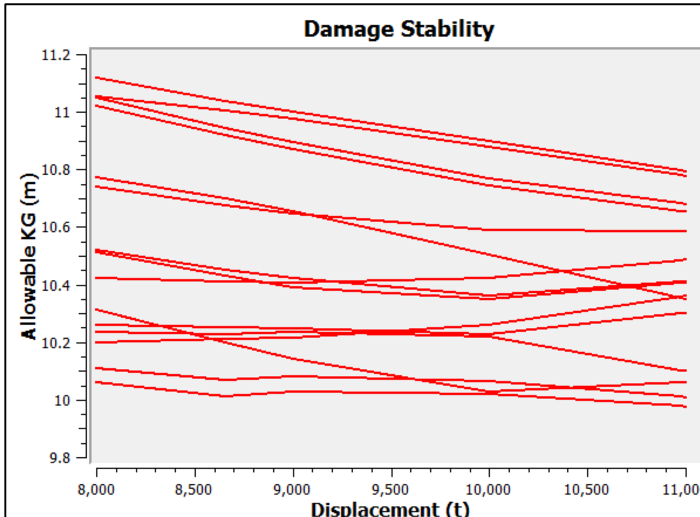
Automated Damage Stability



ASSET 6.3



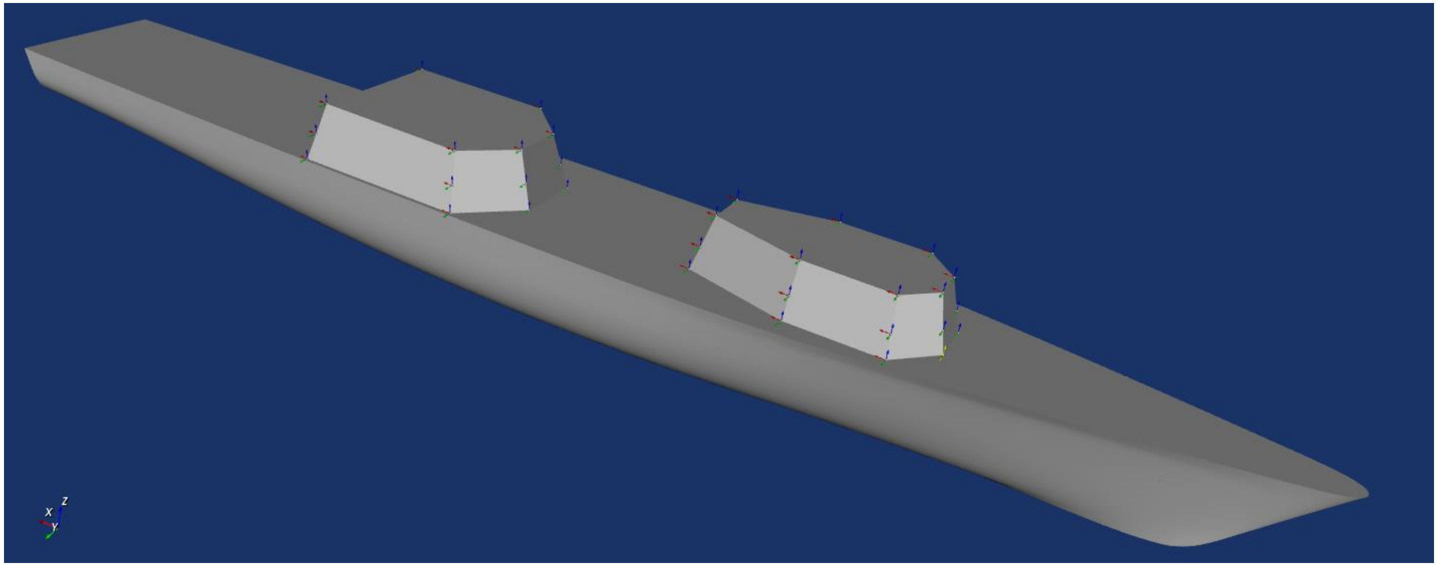
RSDE 3.0



	Flooding Scenario	isplacemer	Allowable KG	Limiting Criteria	Calc Status
1	STBD, Centered at x = -7.604	8000.0	11.054	Area Ratio	VALID
2	STBD, Centered at x = -7.604	8658.1	11.005	Area Ratio	VALID
3	STBD, Centered at x = -7.604	9000.0	10.975	Required GZMax-GH	VALID
4	STBD, Centered at x = -7.604	10000.0	10.879	Required GZMax-GH	VALID
5	STBD, Centered at x = -7.604	10977.7	10.780	Required GZMax-GH	VALID
6	STBD, Centered at x = -7.604	11000.0	10.777	Required GZMax-GH	VALID
7	STBD, Centered at x = 4.246	8000.0	11.118	Area Ratio	VALID
8	STBD, Centered at x = 4.246	8658.1	11.037	Required GZMax-GH	VALID
9	STBD, Centered at x = 4.246	9000.0	11.000	Required GZMax-GH	VALID
10	STBD, Centered at x = 4.246	10000.0	10.901	Required GZMax-GH	VALID
11	STBD, Centered at x = 4.246	10977.7	10.796	Required GZMax-GH	VALID

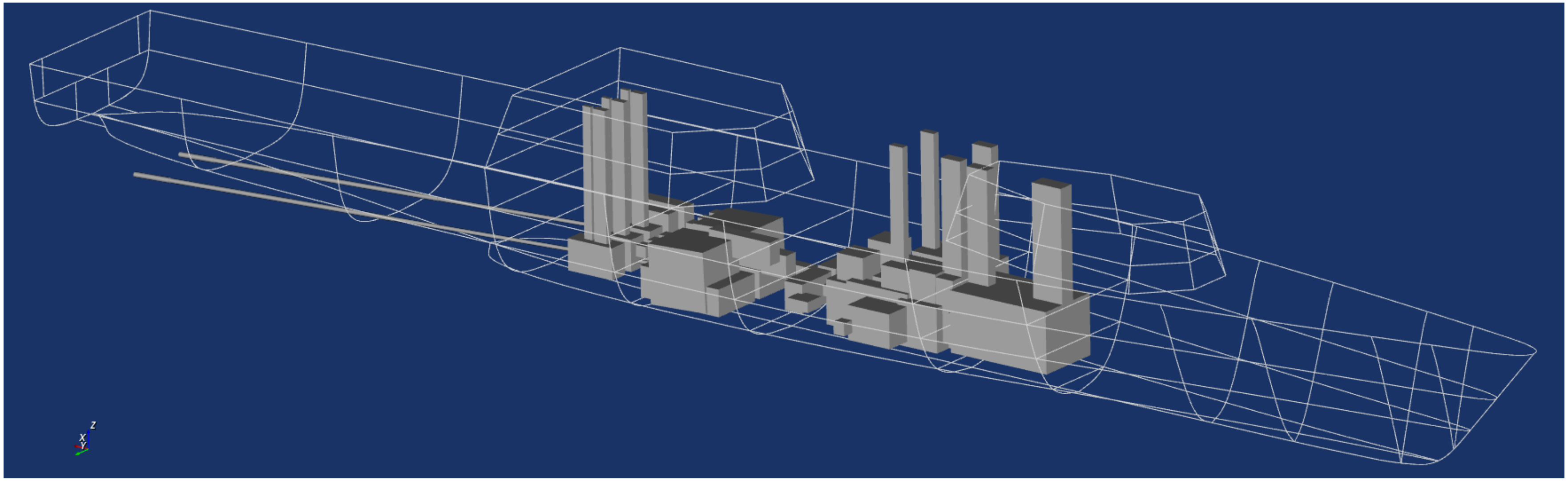
Automated 15% LBP Damage Scenario Analysis

Deckhouse Modeling



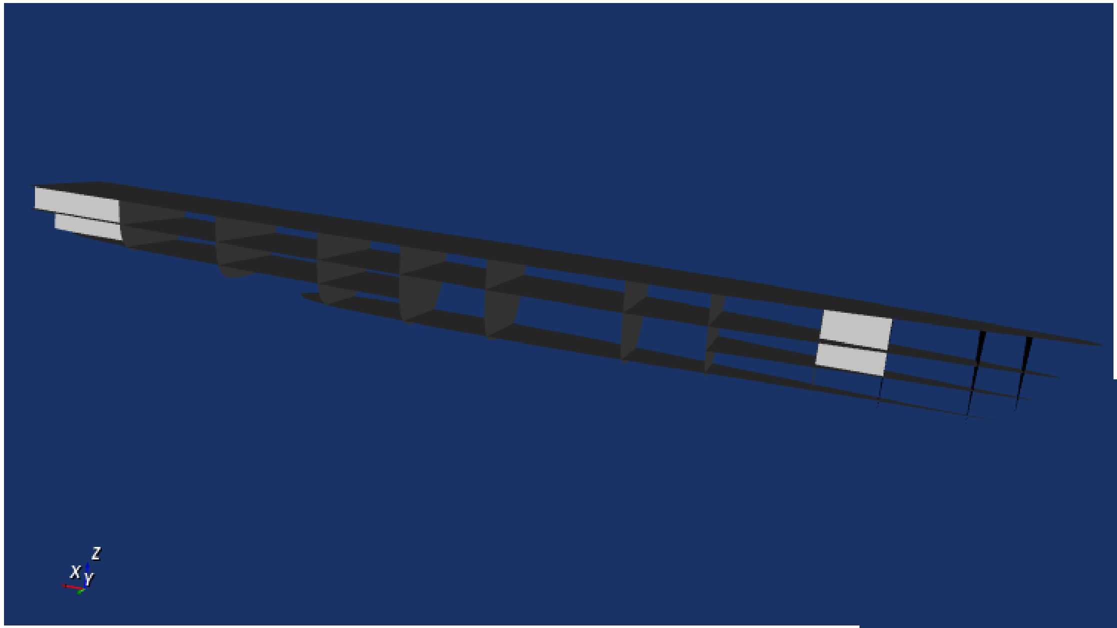
- **Deckhouses created based on constraint points**
- **Constraint points tied to design features e.g. the intersection of a deck and bulkhead or other constraint points**
- **Constraint points will be variables in RSDE 3.1 Design Space Explorations**

Ship Systems Arrangements

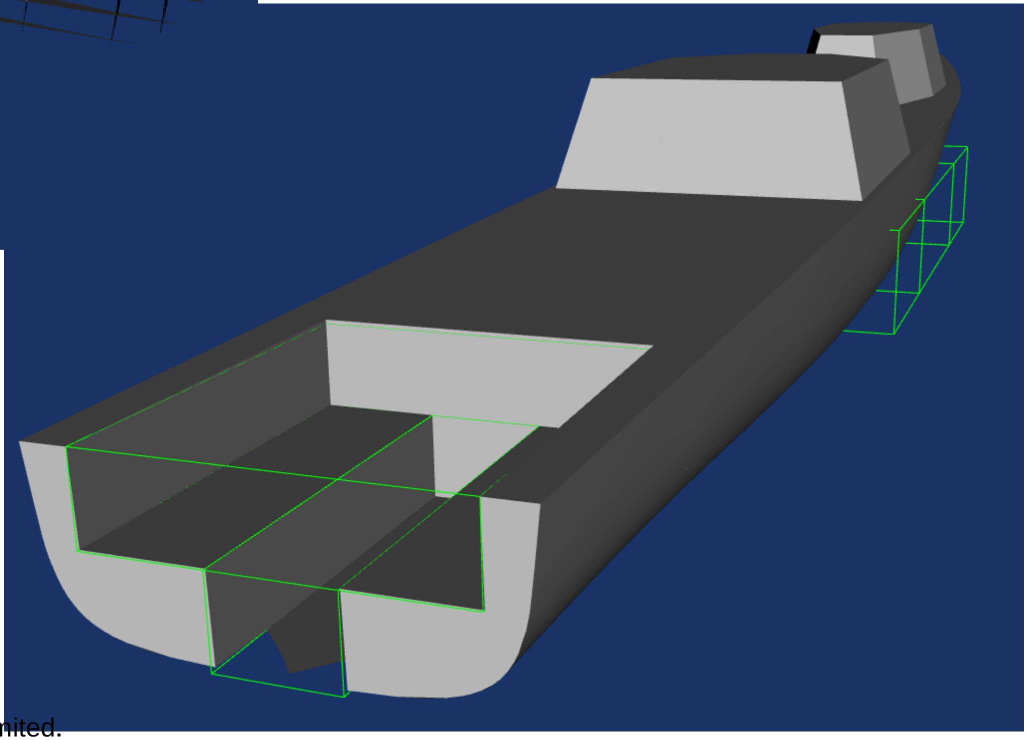


- **Machinery arrangement shown above is <u>NOT</u> representative of actual engine room arrangement**
  - Developing & documenting process for modeling machinery arrangements that are beyond scope of RSDE machinery theory
  - Large set of machinery components are represented in model
  - Increased control over placement of components

Structural Arrangement Flexibility

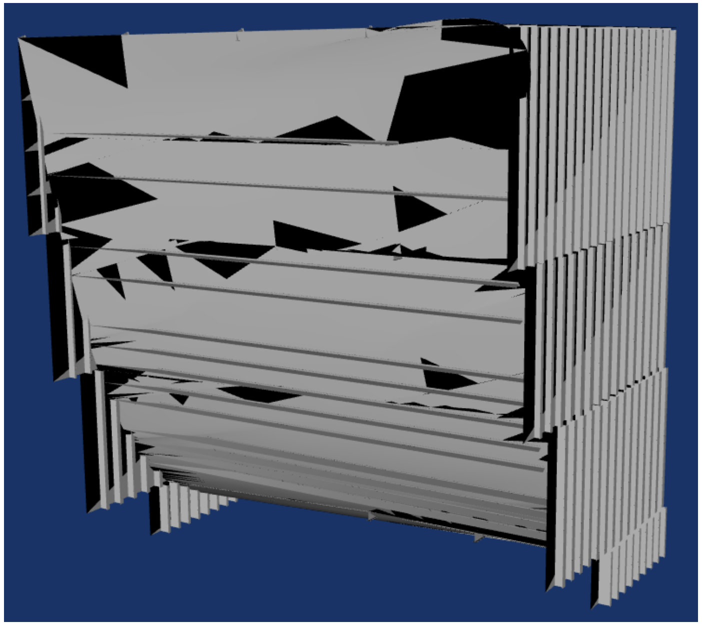


Simplified placement and removal of transverse and longitudinal bulkheads

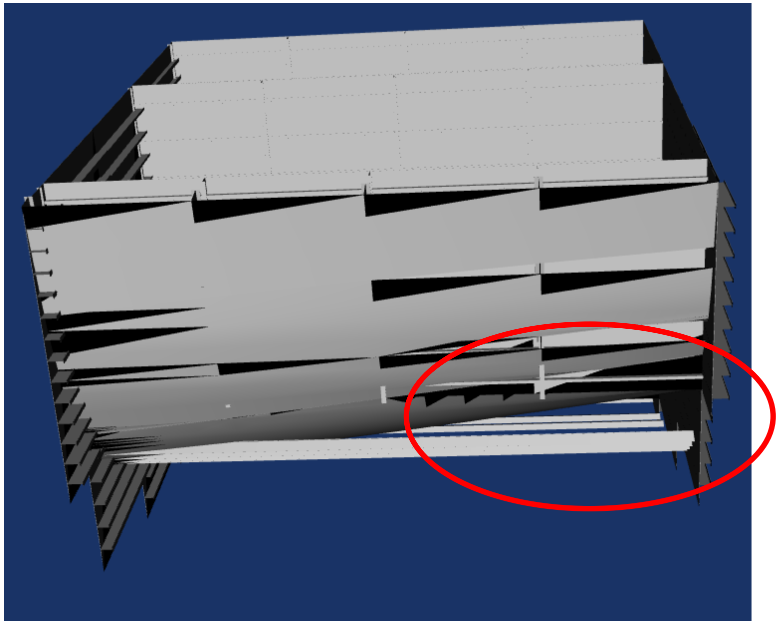


Ability to remove hull shell structural members to model stern launch areas

3D Structural Models



3D structural models are now used for weight estimation



Structural theory assumes linear stiffeners, leading to gaps

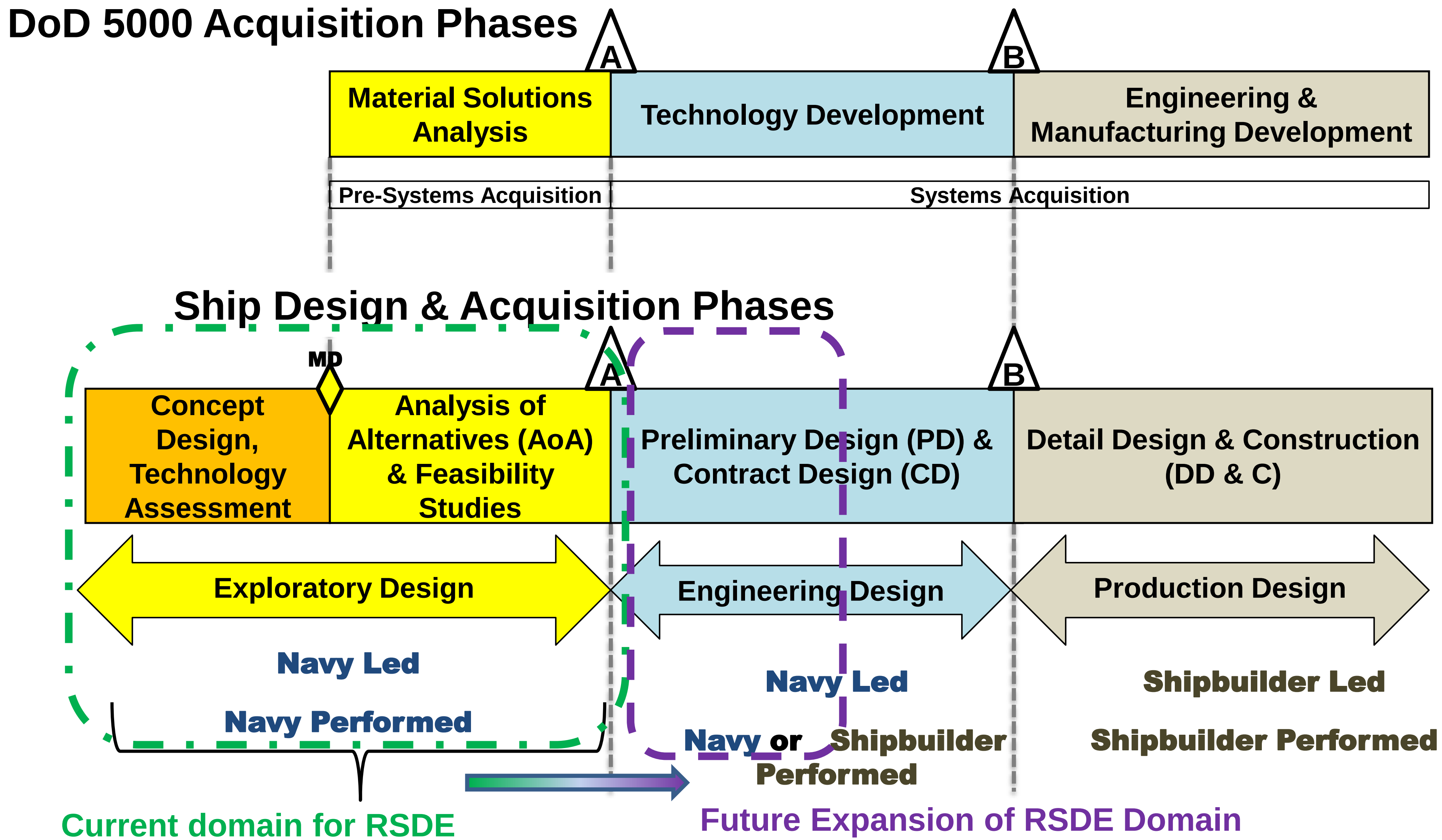
Findings: Design Perspective

- **Mission requirements as defined in capability concept wheel appear to be feasible**
  - Modeling mission systems to the level of detail that is necessary for mission effectiveness analysis is challenging
  - Traditional Naval Architectural disciplines are strengths of RSDE
- **Initial damage stability analysis shows smaller hulls will have issues with meeting damage stability flooding criteria due to large engine room and weapons systems spaces within the hull**
  - Embedded SHCP-L damage stability module allows designers to design to damage stability requirements at beginning of design rather than test against requirements at end of design
- **Adding unmanned vehicles has a significant impact on manning**
  - 1 UAV can require up to 7 additional crew
- **Impact of different RHIB launch locations has not be studied yet, but can be analyzed using embedded Ship Motions Program module**

Findings: Tool Perspective

- **The initial learning curve of using the new RSDE software was steep but as new training materials and software updates have become available the process has rapidly improved.**
- **Near term updates to RSDE allow for reuse of information between models streamlining the model development process.**
- **The study has familiarized members of NSWCCD Code 824 Future Ship and Submarines Concept Branch with RSDE for use in future studies and has provided the RSDE Development Team (Code 823) useful feedback for improving the software.**
    - Dr. Alexander Gray (823) – RSDE Product Lead
    - Pedro Muslera (823) – RSDE Implementation Team
    - Drake Platenberg (824) – FSC Baseline Development Task
    - James Lovenbury (824) – UUV Design Tool Development
    - Nick Mullican (823) – RSDE Development Team
    - Mark A. Parsons (823) – Ph.D. Student at Virginia Tech researching Concept Effectiveness and Vulnerability Analyses with Dr. Alan Brown

The Future of RSDE



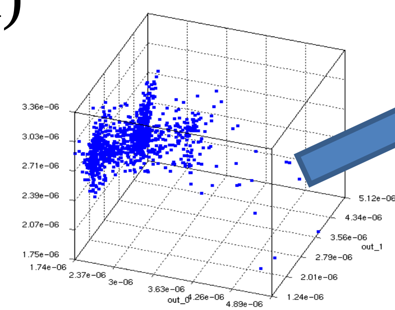
Future Expansion of RSDE Domain

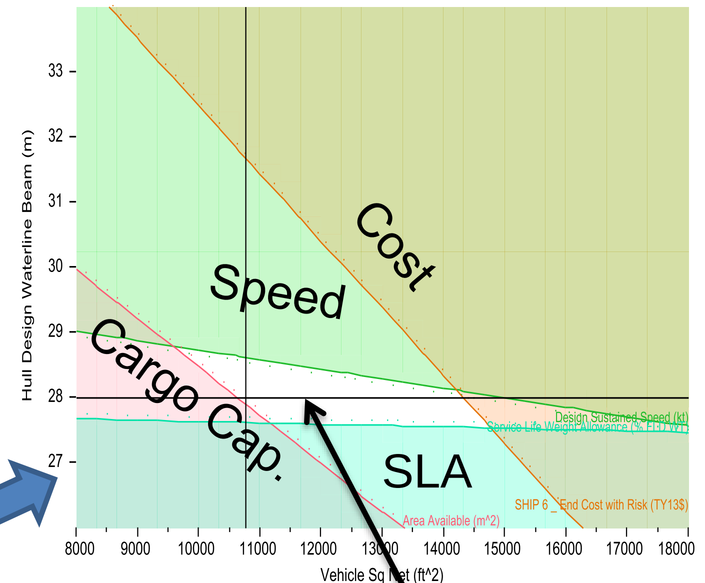
The Future of RSDE: Near Term

RSDE v3.1 - Release Dec. 2017

- ***Improved*, High Magnitude DSE (monohull)**
  - Rapidly generate 1000’s of ship concepts
  - Now with *SHCP & IHDE* integrated
- **Multi-hull hullform study DSE**
  - Rapidly generate and analyze resistance & seakeeping of multi-hull hullforms (catamaran & trimaran)

High Magnitude





White space shows feasible region

RSDE: Long Term

- **Roadmap developed to 2025, planned development:**
  - Submarine Design Space Exploration
  - Systems Design (Machinery, Distribution, CPES)
  - Topside Design
  - Automated Costing
  - Arrangements (Manual & Automated)
  - Damage Stability Enhancements (Downflooding)
  - Predictive Structural Loads
  - Generative Structures
- **Constant emphasis on Decision Support, Visualization, and Data Analysis Capabilities and Tool Flexibility Improvements**

CARDEROCK DIVISION

Network Surface Combatant RSDE Pilot Study

NDIA Systems Engineering Conference
25 October 2017

NAVSEA WARFARE CENTERS

Presenter: Dr. Douglas Rigterink
Code: 823

douglas.rigterink@navy.mil | 301-227-5886

19697 – Environment, Safety, and Occupational Health (ESOH) Risk Management

NDIA Systems Engineering Conference
Wednesday, October 25, 2017

Mr. David Asiello
Office of the Assistant Secretary of Defense (Energy, Installations & Environment)

Outline

Acquisition Environment, Safety, and Occupational Health (ESOH)

- **Role of OASD(EI&E)/ESOH**
- **Acquisition ESOH Policy**
- **Comparing and Contrasting Risk, Issues, and Opportunity (RIO) Management & ESOH Risk Management**
  - Risk Assessment
  - Risk Tracking
  - Risk Acceptance
- **Summary**

Cleared by DOPSR for open publication

DoD Mission and Acquisition ESOH

DoD Mission:

The mission of the Department of Defense (DoD) is to provide the military forces needed to deter war and to protect the security of our country

Acquisition ESOH supports the DoD's mission during non-combat activities by:

- **Preventing loss of life or serious injury**
- **Avoiding damage to facilities or equipment**
- **Preventing harm to the environment and the surrounding community**
- **Avoiding system failures and impacts to mission capability or mission operability**

OASD(EI&E) – ESOH Role in Acquisition

- **Defense Acquisition Board Advisor for ESOH considerations**
  - Oversight of ACAT 1D, IAM, and Special Interest programs
  - Provides ESOH subject matter experts to DASD(SE)-led Program Support Assessments
- **Member of Defense Acquisition Policy Working Group (DAPWG)**
  - Focus on DoDI 5000.02 -- ESOH in acquisition policy
  - Identify OSD ESOH “expectations” in the Defense Acquisition Guidebook (DAG)
  - Provide guidance for policy implementation on the Acquisition Community Connection (ACC)
- **Provide ESOH input to Chairman of the Joint Chiefs of Staff Instruction CJCS 3170.01, *Joint Capabilities Integration and Development System (JCIDS)***
- **Chair of DoD Acquisition ESOH Integrated Product Team (IPT)**
  - Component consensus on ESOH policy and guidance

Acquisition ESOH Policy Requirements

➢ **DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, Enclosure 3 (Systems Engineering (SE))**

- Integrate ESOH risk management into the overall SE process for all engineering activities throughout the system's life cycle
- As part of risk reduction, eliminate ESOH hazards where possible and manage ESOH risks where hazards cannot be eliminated
- Use methodology in MIL-STD-882E, *Standard Practice for System Safety*
  - Includes a process that requires assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware
  - Document hazards with a closed-loop Hazard Tracking System (HTS) and specifies required data for tracking

Cleared by DOPSR for open publication

Acquisition ESOH Policy Requirements, Cont.

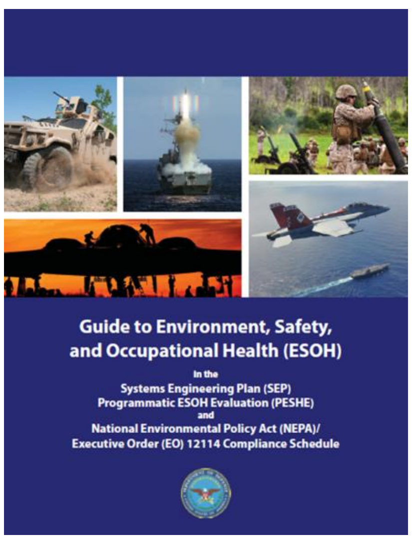
- **DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, Enclosure 3 (Systems Engineering (SE))**
  - Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, document that the associated risks have been accepted by the delineated acceptance authorities
  - The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle of the system and will provide formal concurrence prior to all High and Serious risk acceptance decisions
  - Address the status of ESOH risks and acceptance decisions at technical reviews
  - Address the status of all High and Serious ESOH risks at acquisition program reviews and fielding decisions

Acquisition ESOH Guidance and Resources

- **DAG SE Chapter [https://dag.dau.mil]**

- **Acquisition Community Connection (ACC) ESOH Community of Practice**

ACC Website:
[https://acc.dau.mil/esoh]



- ***Guide to ESOH in the Systems Engineering Plan (SEP), Programmatic ESOH Evaluation (PESHE), and NEPA/EO 12114 Compliance Schedule*** **[https://acc.dau.mil/CommunityBrowser.aspx?id=683547&lang=en-US]**

Comparing Risk, Issue, and Opportunity (RIO) & ESOH Risk Management

RIO Management

- Focus is on impacts to program cost, schedule, and performance
  - Can drive ESOH risks
- Aims to manage uncertainty and increase predictable outcomes in delivering capability to the warfighter
- Most important decisions to control risk are made early in a program’s life cycle
- Less emphasis on RIO Management in Operations and Support Phase
- Issue is a realized risk

ESOH Risk Management

- Focus is ESOH risks
  - Can drive cost, schedule and performance risks
- Aims to eliminate hazards or minimize ESOH risks to people, equipment, or the environment
- Most important decisions to eliminate hazards or mitigate risk made early in a program’s life cycle when they impact system design
- ESOH risks identified and tracked throughout life cycle – key sustaining engineering activity
- Mishap is a realized ESOH risk

Opportunities have potential future benefits to the program’s cost, schedule, and/or performance baseline.

Assessing “ESOH” and “Program” Risks

RIO Management

- DoD RIO Management Guide for Defense Acquisition Programs
- Identify the “future event” that could occur and the potential impact to the program's ability to meet cost, schedule, and performance
- Determine consequence of impact to program's ability to meet cost, schedule, or performance objectives
- Determine, qualitatively or quantitatively, likelihood the future event could occur and cause negative consequences

ESOH Risk Management

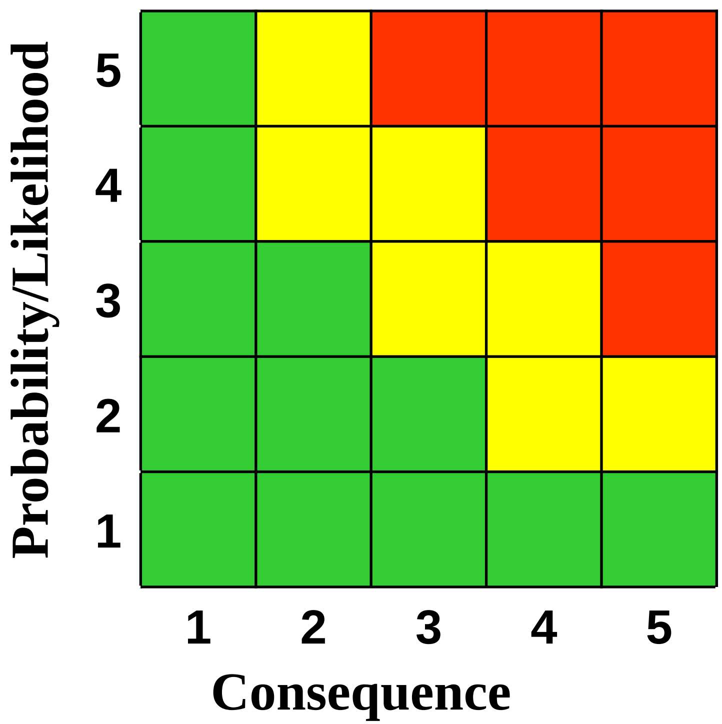
- MIL-STD-882E methodology
- Identify the hazard and potential mishaps that could harm people, equipment, or the environment
- Determine severity of the consequences of the mishap occurring
- Determine, qualitatively or quantitatively, probability that the hazard could result in a mishap

Process is fundamentally the same for cost, schedule, and performance risks and ESOH risks.

Assessing “ESOH” and “Program” Risks

RIO Management

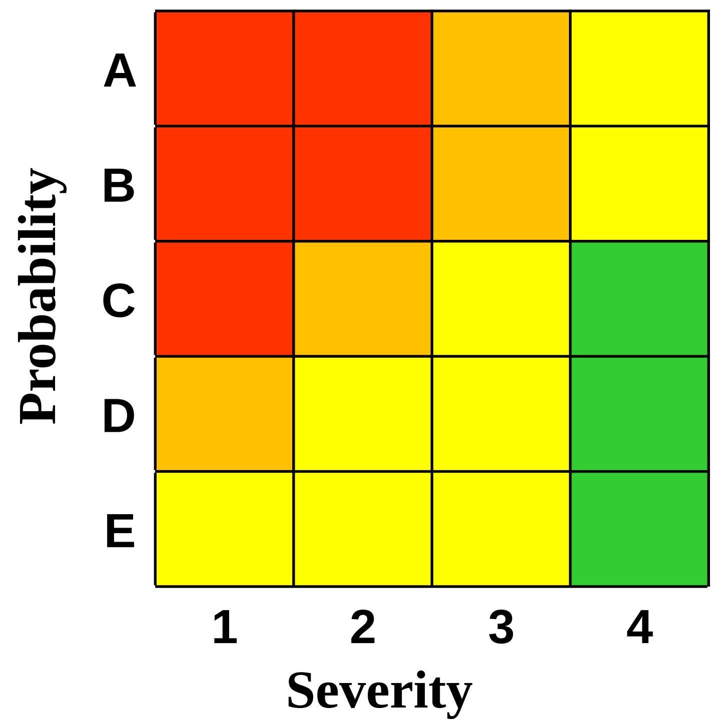
- 5 x 5 Matrix



Red = High Risks
Yellow = Medium Risks
Green = Low Risks

ESOH Risk Management

- 5 x 4 Matrix



Red = High ESOH Risks
Orange = Serious ESOH Risks
Yellow = Medium ESOH Risks
Green = Low ESOH Risks

RIO Consequence Criteria

SAMPLE CONSEQUENCE CRITERIA			
Level	**Cost**	**Schedule**	**Performance**
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining Precludes program from meeting its APB schedule threshold dates	Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success 2 Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4 Significant Impact	5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk Fielding of capability to operational units delayed by more than 6 months	Degradation impairs ability to meet a KSA. 2 Technical design or supportability margin exhausted in key areas Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives
3 Moderate Impact	1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC Manageable with PEO or Service assistance	Can meet APB objective schedule dates, but other non- APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks
2 Minor Impact	Costs that drive unit production cost (e.g., APUC) increase of <1% over budget Cost increase, but can be managed internally	Some schedule slip, but can meet APB objective dates and non-APB key event dates	Reduced technical performance or supportability; can be tolerated with little impact on program objectives Design margins reduced, within trade space
1 Minimal Impact	Minimal impact. Costs expected to meet approved funding levels	Minimal schedule impact	Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires

MIL-STD-882E Severity Categories

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than$10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

RIO Likelihood / Probability Levels

Typical Likelihood Criteria		
Level	**Likelihood**	**Probability of Occurrence**
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%

MIL-STD-882E Probability Levels

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.

Tracking and Communicating ESOH Risks & Program Risks, Issues, and Opportunities

RIO Management

- Risks tracked in a risk register
- Risk register may include the following information for each risk:
  - Risk category
  - Risk statement
  - Likelihood
  - Consequence
  - Planned mitigation measures
  - Risk owner
  - WBS/IMS linkage
  - Expected closure dates and documentation of changes, where applicable
- Risks communicated at Risk Management Boards
- Risks communicated at Program Reviews

ESOH Risk Management

- ESOH risks must be tracked in a hazard tracking system (HTS)
- HTS has <u>required</u> fields for each ESOH risk
  - Identified hazards
  - Associated mishaps
  - Risk assessments (initial, target, event(s))
  - Identified risk mitigation measures
  - Selected mitigation measures
  - Hazard status
  - Verification of risk reductions
  - Risk acceptances
- ESOH risks must be communicated at Technical Reviews
- High & Serious ESOH risks must be communicated at Program Reviews

Example for Communicating ESOH Risks Using RIO Management Guide Matrix

RIO Management Guide

Probability/Likelihood					
5		4A		2A	1A
4		4B	3A 3B 3C	2B	1B
3		4C	3D 3E	2C	1C
2		4D		2D 2E	1D
1		4E			1E
Consequence	1	2	3	4	5

MIL-STD-882

Probability				
A	1A	2A	3A	4A
B	1B	2B	3B	4B
C	1C	2C	3C	4C
D	1D	2D	3D	4D
E	1E	2E	3E	4E
Severity	1	2	3	4

Cleared by DOPSR for open publication

ESOH Risks and Program Risks are Linked

- **ESOH risks can drive Program Risks**
  - <u>ESOH Risk</u>: Far Field Noise emissions from the system exceed the requirements detailed in the Air Installation Compatible Use Zone for planned basing/training locations
  - <u>Resultant Schedule risk</u>: Program had to stop using aircraft as intended and could not field systems as planned
- **Program risks can drive ESOH Risks**
  - <u>Schedule Risk</u>: Testing site will no longer be available six months from now as originally planned; to avoid schedule slip, program testing will be done earlier
  - <u>Resultant ESOH risk</u>: Because now there was not enough time to conduct National Environmental Policy Act analysis/documentation requirements for testing

Comparing ESOH & Program Risk Acceptance

RIO Management

- There is no formal "acceptance" of risks
- It is implicit that risks are "accepted" when briefed at Program Reviews

ESOH Risk Management

- Appropriate authority must formally accept ESOH risks
- User representative must concur before risks accepted
- Risk acceptance must occur before exposing people, equipment, or the environment to known hazards
- Risk acceptance is linked to specific event and system configuration (e.g., Developmental Test)
  - Thus, ESOH risks may need to be accepted at multiple times during the program

ESOH Risk Acceptance Authorities

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	1A	2A	3A	4A
Probable (B)	1B	2B	3B	4B
Occasional (C)	1C	2C	3C	4C
Remote (D)	1D	2D	3D	4D
Improbable (E)	1E	2E	3E	4E
Eliminated (F)	Eliminated			

Risk Assessment Code	Risk Level	Risk Acceptance Authority
IA, IB, IC, IIA, IIB	High	Component Acquisition Executive
ID, IIC, IIIA, IIIB	Serious	Program Executive Officer-level
IE, IID, IIE, IIIC, IIID, IIIE, IVA, IVB	Medium	Program Manager
IVC, IVD, IVE	Low	Program Manager

Summary

- **Two approaches for managing risk in Acquisition**
  - RIO management
  - ESOH risk management
- **Approaches for RIO and ESOH management essentially the same**
  - Risks are assessed using severity of consequence and probability criteria
  - Risks are depicted in risk matrices
  - Risks need to be tracked and communicated
- **ESOH risk management has some unique features**
  - MIL-STD-882E methodology must be followed
  - DoDI 5000.02 lists specific requirements for briefing ESOH risks
  - ESOH risks must be formally accepted by the appropriate risk acceptance authority
  - ESOH risks must be managed throughout the system's life cycle
- **ESOH and cost, schedule, and performance risks are linked**

OASD(EI&E)/ESOH

Mr. David Asiello
Acquisition ESOH Lead
david.j.asiello.civ@mail.mil

Cleared by DOPSR for open publication

20028
Joint Software Systems Safety Engineering Handbook Implementation Guide

Robert E. Smith, CSP
Booz Allen Hamilton

20th Annual NDIA Systems Engineering Conference
Springfield, VA

25 October 2017

BLUF

- **System Safety, to include <u>Software Safety</u>, is required for acquisition programs IAW DoDI 5000.02 and MIL-STD-882E**
- **Detailed guidance for software safety is provided in the Joint Software Systems Safety Engineering Handbook (JSSSEH) Version 1.0 published 27 August 2010 as referenced in MIL-STD-882E**
  - Comprehensive handbook, although lengthy at 344 pgs
  - Acquisition Programs unfamiliar with software safety find it difficult to extract software safety techniques and processes in order to satisfy MIL-STD-882E Software Level of Rigor (LOR) requirements
  - Programs typically re-state the LOR table from MIL-STD-882E, Table V in their Safety Plans and do not identify and specify the artifacts and Objective Quality Evidence (OQE) to be produced for all LOR tasks
  - Could result in not performing a comprehensive software safety program and therefore not fully characterizing software’s contribution to system risk
- **Joint Boards recognized this concern and developed a JSSSEH Implementation Guide on 1 April 2016 to further assist programs, and was endorsed by the Joint Services Weapon Safety Review (JSWSR) Boards on 29 June 2016**
- **Revised Implementation Guide (Rev A) issued 17 October 2017**

Software Safety Requirements

- **Software Safety is required for acquisition programs**
  - DoDI 5000.02, Enclosure 3, Para 11 – SOFTWARE "…The SEP should address the following: software unique risks; inclusion of software in technical reviews; identification, tracking, and reporting of metrics for software technical performance, process, progress, and quality; **software safety** and security considerations; and software development resources."
  - DoDI 5000.02, Enclosure 3, Para 16 - ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH) "The Program Manager will integrate ESOH risk management into the overall systems engineering process for all engineering activities throughout the system's life cycle. As part of risk reduction, the Program Manager will eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. **The Program Manager will use the methodology in MIL-STD-882E**..."
  - MIL-STD-882E, Section 4.4 Software contribution to system risk. "The assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability….. Therefore, **another approach shall be used for the assessment of software's contributions to system risk** that considers the potential risk severity and the degree of control that software exercises over the hardware."

Common Approaches to Software Safety

- **MIL-STD-882E references the JSSSEH and Section 4.4.2 includes a note to "Consult the Joint Software Systems Safety Engineering Handbook and AOP 52 for additional guidance on how to conduct required software analyses."**
- **The JSSSEH is a lengthy document making it difficult for programs not familiar with software safety activities to extract detailed LOR tasks and tailor for particular program needs**
- **Programs often default to only referencing or reusing the LOR table from MIL-STD-882E (i.e., Table V) as their software safety approach in their System Safety Management Plans (SSMPs) and/or System Safety Program Plans (SSPPs)**
- **May result in not performing the specific LOR tasks that comprise a comprehensive software safety program, resulting in failure to assess software's contribution to system risk(s)**

MIL-STD-882E, Table V, Software Safety Criticality Matrix

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

High Level, overarching LOR tasks

MIL-STD-882E, Table V, Level of Rigor Tasks

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

- **Note that the LOR tasks table contains no details on the specific tasks, artifacts and Objective Quality Evidence (OQE) to be produced for LOR (e.g., requirements analysis, architecture analysis, design analysis, safety-specific testing, and code analysis)**
- **The JSSSEH includes these details, but not in a specific location**
- **Challenge is getting Acquirers (Customer) and Developers (software developers) to specify how they will turn the objectives of MIL-STD-882E and the JSSSEH "guidance" into actual Software System Safety Engineering (SSSE) Requirements**

Implementation Guide Overview

- **Developed by the Joint Services – Software Safety Authorities (JS-SSA) Sub-Working Group in support of the JSWSR Boards on 1 April 2016 - endorsed by the JSWSR Boards on 29 June 2016**
- **Titled "Software System Safety Implementation Process and Tasks Supporting MIL-STD-882E With Joint Software System Safety Engineering Handbook References"**
  - Short name – "Implementation Guide"
- **Provides implementation guidance for Software System Safety program requirements specified in MIL-STD-882E and guidance detailed in the JSSSEH**
- **Updated in 2017 to address identified errors, Service comments and create more direct alignment with the Tasks in MIL-STD-882E**
- **Released as "Revision A" on 17 October 2017**

Implementation Guide Outline and Methodology

- The implementable process task requirements are presented as a decomposition of parent and children activities, similar to a Work Breakdown Structure (WBS)
- Parent tasks are graphically represented depicting inputs to the tasks and the products that the task would typically produce
- Tasks identified as MIL-STD-882 requirements are coded in the graphics using an extreme bold border of the task box
- Task decomposition is to the level necessary for a basic understanding of the process, the tasks that implement the process, and the products the tasks would likely produce
- The requirements derived that apply to each task are specified and cross referenced to both the applicable MIL-STD-882E requirements and JSSSEH sections and paragraphs that provide guidance on meeting the requirements

Process Tasks (2016 Guide)

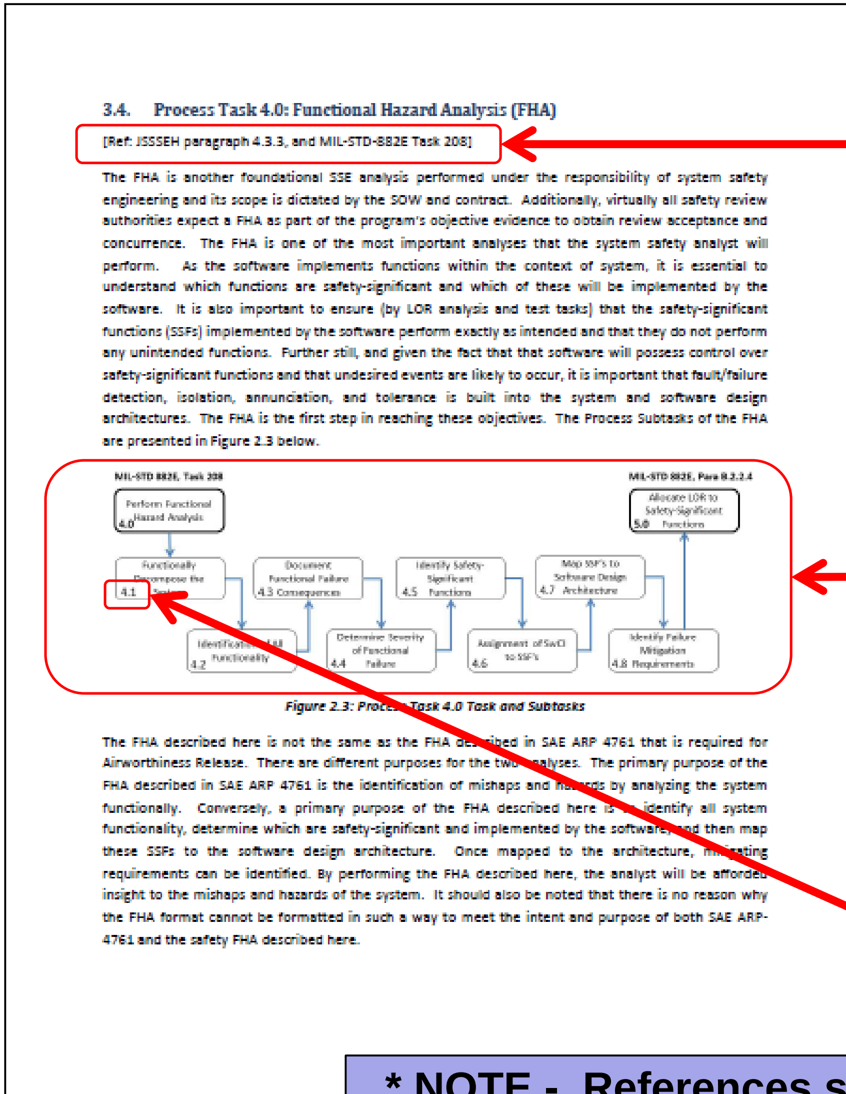
- **14 Process Tasks identified in the Implementation Guide**
  - Process Task 1.0: Prepare the System Safety Management Plan (SSMP)
  - Process Task 2.0: Prepare System Safety Program Plan (SSPP)
  - Process Task 3.0: Preliminary Hazard Analysis
  - Process Task 4.0: Functional Hazard Analysis (FHA)
  - Process Task 5.0: LOR Allocations to Safety-Significant Functions
  - Process Task 6.0: Preliminary Safety Requirements Analysis (SRA)
  - Process Task 7.0: Perform In-Depth Hazard Analysis
  - Process Task 8.0: Perform Detailed Safety Requirements Analysis
  - Process Task 9.0: Perform Safety Requirements Traceability
  - Process Task 10.0: Perform Code-Level Safety Analysis
  - Process Task 11.0: Perform Software Test Planning
  - Process Task 12.0: Monitor Safety-Significant Software Testing
  - Process Task 13.0: Perform Residual Safety Risk Assessment
  - Process Task 14.0: Participate in Life-Cycle Management and Support
- **Each Process Task has Process Subtasks to amplify details and/or additional steps associated with each Task**

Process Tasks (2017 Guide)

- **13* Process Tasks identified in the Implementation Guide**
  - Process Task 1.0: Prepare the System Safety Management Plan (SSMP)
  - Process Task 2.0: Prepare System Safety Program Plan (SSPP)
  - Process Task 3.0: Preliminary Hazard Analysis
  - Process Task 4.0: Functional Hazard Analysis (FHA)*
  - Process Task 5.0: Initiate Safety Requirements Hazard Analysis (SRHA)*
  - Process Task 6.0: Perform System and Subsystem Hazard Analyses*
  - Process Task 7.0: Finalize SRHA*
  - Process Task 8.0: Perform Final Safety Requirements Traceability*
  - Process Task 9.0: Perform Code-Level Safety Analysis
  - Process Task 10.0: Perform Software Test Planning
  - Process Task 11.0: Monitor Safety-Significant Software Testing
  - Process Task 12.0: Perform Safety Risk Assessment*
  - Process Task 13.0: Participate in Life-Cycle Management and Support
- **Each Process Task has Process Subtasks to amplify details and/or additional steps associated with each Task**

*** Changes in 2017: Titles of tasks revised and previous Task 5.0 combined into Task 4.0, and SRA is now System Requirements Hazard Analysis (SRHA)**

Process Tasks 4.0 – FHA [Partial Example]



3.4. Process Task 4.0: Functional Hazard Analysis (FHA)

[Ref: JSSSEH paragraph 4.3.3, and MIL-STD-882E Task 208]

The FHA is another foundational SSE analysis performed under the responsibility of system safety engineering and its scope is dictated by the SOW and contract. Additionally, virtually all safety review authorities expect a FHA as part of the program's objective evidence to obtain review acceptance and concurrence. The FHA is one of the most important analyses that the system safety analyst will perform. As the software implements functions within the context of system, it is essential to understand which functions are safety-significant and which of these will be implemented by the software. It is also important to ensure (by LOR analysis and test tasks) that the safety-significant functions (SSFs) implemented by the software perform exactly as intended and that they do not perform any unintended functions. Further still, and given the fact that that software will possess control over safety-significant functions and that undesired events are likely to occur, it is important that fault/failure detection, isolation, annunciation, and tolerance is built into the system and software design architectures. The FHA is the first step in reaching these objectives. The Process Subtasks of the FHA are presented in Figure 2.3 below.

Figure 2.3: Process Task 4.0 Task and Subtasks

The FHA described here is not the same as the FHA described in SAE ARP 4761 that is required for Airworthiness Release. There are different purposes for the two analyses. The primary purpose of the FHA described in SAE ARP 4761 is the identification of mishaps and hazards by analyzing the system functionally. Conversely, a primary purpose of the FHA described here is to identify all system functionality, determine which are safety-significant and implemented by the software, and then map these SSFs to the software design architecture. Once mapped to the architecture, mitigating requirements can be identified. By performing the FHA described here, the analyst will be afforded insight to the mishaps and hazards of the system. It should also be noted that there is no reason why the FHA format cannot be formatted in such a way to meet the intent and purpose of both SAE ARP-4761 and the safety FHA described here.

References* to specific sections in JSSSEH and MIL-STD-882E

Process flow diagram* provided

Process Task / Subtask referenced for each step

*** NOTE - References still the same in 2017 Guide. Flow diagrams altered as appropriate.**

Process Tasks 4.0 – FHA [Partial Example]

3.4.1. Process Subtask 4.1: Functionally Decompose the System

The information contained in the FHA reflects the same level of maturity as the design architecture. This is expected, and reinforces that the FHA must be kept current through all phases of the development lifecycle, to include functional, physical, and contractual changes made under configuration control. Frequency of updates to the FHA should be specified within the SOW and contract. However, SSSE should update the software inputs to the FHA IAW the SW development process and schedule. The format of the FHA should reflect that which will provide the analysis "answers" required by the analyst and criteria of the contract.

The first step of the analysis is to decompose the system. If the system is mature enough, this first step may be a physical decomposition of the system. If the system has not yet been allocated to specific pieces of hardware, this decomposition will be functional. The system must be analyzed functionally from the perspective of both "what the system is documented to do functionally", and "what you think the system can do functionally". The former is an assessment of documented functionality from the functional specifications and the latter is assessed by analyzing the functionality of the physical components of the system. The analysis of the physical attributes of the system is likely to provide insight to "hidden" or undocumented functionality. This is especially true for systems heavily using COTS components.

FUNCTIONAL HAZARD ANALYSIS								
System Decomposition	Individual Functional Descriptions	Functional Failure Modes	Consequences of Each Failure Mode	Severity of Consequences of Failure Modes	Safety-Significant Functions	Assessment of SCC and LOR	Map to Software Design	Failure Mitigation Requirements
Process Subtask 4.1	Process Subtask 4.2	Process Subtask 4.3	Process Subtask 4.3	Process Subtask 4.4	Process Subtask 4.5	Process Subtask 4.6	Process Subtask 4.7	Process Subtask 4.8

Figure 2.4: Example FHA Format

Figure 2.4 provides an example of a FHA format that will provide the analyst with the most basic of information required by the analysis. If the analyst (or the Acquirer) requires more than this simple example format can provide, add the appropriate columns to the format to identify and track the information required. The decomposition of the system is documented in Column one. System decomposition can be done in a WBS-like structure which may aid in structure, flow, traceability and assignment of responsibilities. For instance, on large, complex programs such as an Aircraft (Refer: Figure 2.2) the hazard "Loss of Engine" may be completely under the control of the Engine Integrated Product Team (IPT). The Engine IPT is more likely to support safety if the FHA can readily show the IPT which parts it is responsible for.

3.4.2. Process Subtask 4.2: Identification of All Functionality

Column two of the example FHA format in Figure 2.4 depicts where the system functionality is documented. For the initial FHA, the functionality may be "higher level" functions that haven't yet been decomposed to lower level functionality. For an initial FHA this is sufficient for this level of analysis maturity as lower-level functionality will likely take on the same criticality as their parent higher-level

15

Process Task / Subtask described in detail in subsequent paragraphs

Appendix A – LOR Task Table [Partial]

Legend:
PR: Prerequisite Requirement – Required regardless of LOR or required in order to assess and determine LOR
R: Required for assigned LOR
AD: As directed by Customer/Contract
IV&V: Independent Verification and Validation
N/A: Not Applicable for this program or LOR

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-of-Rigor → Baseline	4	3	2	1	Representative Artifacts Produced
Required System Safety Tasks to Support Software System Safety Per MIL-STD-882E								
SSE-1: Document the Developer plans and processes to meet the requirements of the System Safety and Software System Safety programs. Section 3.0 Process and Process Tasks for Software System Safety MIL-STD-882E, Task 102	Developer System Safety Manager Developer Software Safety	Developer Program Manager Developer Hardware and Software Design Engineering Developer Software Design Architect Developer Configuration Management	PR					System Safety Program Plan (SSPP) and Software System Safety Program Plan (SwSSPP). SOW, CDRL Acquirer Approved SSPP/SwSSPP
SSE-1.1: Define the safety-related terms (and the definitions) to be used on the program Section 3.1, Prepare the SSPP; Subsections 3.1.1-3.1.2 [Best Practice]	Acquirer System Safety Manager Developer System Safety Manager Developer Software Design Architect	Developer System Safety Acquirer SSWG Review and Approval	PR					Documented Program-Specific Terms and Definitions. MIL-STD-882E definitions and terms are required unless approved by appropriate authorities Acquirer Approved SSPP
SSE-1.2: Detail within the SSPP/ SwSSPP, how the SwSS tasks will be accomplished within the specific software development life-cycle for the project. Section 3.1.3 Prepare the SSPP MIL-STD-882E, Task 102	Developer Software Safety Developer Software Development	Acquirer SSWG Review and Approval	PR					SOW, CDRL. SSPP/SwSSPP Acquirer Approved SSPP/SwSSPP
SSE-1.3: Develop safety entry/exit criteria for each program phase of the software development life cycle to include concept refinement, requirements, preliminary and detailed design, coding, Test V&V, software release and support). [Best Practice]	Developer Software Safety Developer Software Development and Test Configuration Mgmt	Acquirer SSWG Review and Approval	PR					
SSE-1.4: Develop (or update) the Software Control Category (SCC) Definitions to be used on the program Section 3.1 Prepare the SSPP	Developer Software Safety Developer Software Development	Acquirer SSWG Review and Approval	PR					

Legend:
- PR: Prerequisite Requirement – Required regardless of LOR or required in order to assess and determine LOR
- R: Required for assigned LOR
- AD: As directed by Customer/Contract
- IV&V: Independent Verification and Validation
- N/A: Not Applicable for this program or LOR

LOR 1 Example [Partial]

- **Table indicates required (“R”) LOR activities for LOR 1, 2, 3, and 4**
- **E.g., Design Practice (DP)-11: Analyze all safety functional threads…**
  - Required only for LOR 1
  - One of many LOR 1 activities required (“R”) for LOR 1
  - Appendix A specifies the LOR activity, primary and support activities, applicable LOR, and artifact(s) to be produced

Level of Rigor (LOR) Activity	Primary Responsibility	Support Responsibility	Level-Of-Rigor					Representative Artifacts Produced
			Baseline	4	3	2	1	
DP-7: Create traceability from all safety-significant requirements to the system and software architecture Section 3.5 Section 3.8 [Best Practice]	Developer Software Design Architect	Developer Software Safety		R	R	R	R	Safety Requirements-to-design Traceability
DP-8: Functionally partition all implementations of high LOR requirements from lower LOR requirements in the design [Best Practice]	Developer Software Design Architect	Developer Software Safety				R	R	Functionally Partitioned Design in Design Documentation Artifacts
DP-9: Assess design's stress tolerant (i.e., memory, processing through-put, timing, etc). Make appropriate recommendations to update requirements for stress tolerant design. [Best Practice]	Developer Software Design Architect	Developer Software Safety Developer Software Requirements and Design				R	R	Stress Tolerant Design
DP-10: Perform Design Interface Analysis to evaluate internal and external interfaces of safety-critical units to ensure functional and physical compatibility across the interface.	Developer Software Design Architect	Developer Software Safety				R	R	Verification that the design controls the functional and physical interfaces with safety-significant functionality
DP-11: Analyze all safety functional threads to ensure that all paths lead to their desired outcomes and that there is no dead/unused code, unused/undesired entry/exit points into/out of the software thread [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Safety (functional) Thread Analysis
DP-12: Verify that every variable and functional statement in safety-critical modules of code have a predefined behavior that fulfill the criteria of the functional objective [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Safety-specific Behavioral Review Results for Safety-Critical Modules of Code
DP-13: Independent Safety Review of Requirements-to-Design for Safety Coverage	Someone Other Than System Safety Team	Independent Software Safety Independent Software Design	IV&V, AD					Independent Safety Review of Requirements-to-Design Coverage Artifact

DP-11: Analyze all safety functional threads to ensure that all paths lead to their desired outcomes and that there is no dead/unused code, unused/undesired entry/exit points into/out of the software thread [Best Practice]	Developer Software Design Architect	Developer Software Safety					R	Safety (functional) Thread Analysis

Change Management

- **JS-SSA meets twice annually**
- **Approved path for changes:**
  - Any user can submit comments
  - Comments collected from 4th QTR FY until end of 2nd QTR FY (comments, corrections, additions, deletions, etc.)
  - **Submit comments to JS-SSA Chair**
  - Proposed changes adjudicated between the Service JS-SSA Implementation Guide (IG) IPT
  - Changes approved by the JS-SSA Sub-group will then be integrated into the Implementation Guide and a new revision released in time for the Fall meeting (or end of year)
- **100+ proposed changes submitted during the FY2017 review period**
- **Proposed changes were adjudicated via email and in a face-to-face meeting April 2017**
- **Draft JS-SSA IG update distributed to Working Group and approved in August 2017**
- **Release of 2017 Guide Update (Rev A) on 17 October 2017**

2017 Summary of Changes

- **Numerous changes between 2016 Guide and 2017 Guide**
- **Two "Critical" changes to the Implementation Guide**
  - Less emphasis and more controls on tailoring of LOR table by contractors (Section 2.0)
    - Changed from: "The LOR table should be tailored for any given program as agreed to by the Acquirer and Developer."
    - To: "The LOR table should be assessed for tailored implementation for any given program, and tailoring is permitted as long as the tailored LOR tasks are approved by both the Acquirer and Developer."
  - Allows risks to be carried over, if appropriate, from one contractual activity to another following a reassessment (Section 3.2.4.2)
    - Changed from: "Risk accepted in one contractual activity should never be carried over as the baseline for the next contractual activity."
    - To: "Risk acceptance performed in one contractual activity should be reassessed for the next contractual activity."

2017 Summary of Changes (cont.)

- **Four "Significant" changes to the Implementation Guide**
  - SSMP tasks added to the LOR table in Appendix A as "Acquirer" activities
  - Removed requirement that Contractors must comply with future versions of DODI 5000.02 and MIL-STD-882, just the versions under contract
  - Clarified purpose of document as defining the processes and tasks needed to implement a MIL-STD-882E compliant SSSE program
  - Made the current Process Task 5.0 "LOR Allocations to Safety-Significant Functions" a subtask of draft Process Task 4.0 "FHA"
- **Majority of remaining changes are relatively minor and designed to resolve known inconsistencies and improve alignment with MIL-STD-882E**
  - Primarily changes to the process flow figures and associated paragraphs detailing the subtasks for the analyses/reports (PHA, SRA, etc.) to better define tasks and processes
  - Many editorial and administrative corrections
- **Changed "Hazard Risk Index" to "Risk Assessment Code"**
- **Changes to the LOR table in Appendix A**

2017 Summary of Changes – Appendix A

- **Seven new Baseline LOR SSE-related activities detailing Acquirer (i.e., "ACQ-#") responsibilities**
- **Some activity descriptions updated and enhanced, but overall, no other new activities added**

Level-Of-Rigor Activity / Task Type	2016 IG	2017 IG	Change
Acquirer (ACQ-#.#)	0	7	+7
System Safety Engineering (SSE-#.#)	22	22	-
Requirements Phase (RP-#)	11	11	-
Design Phase (DP-#)	13	13	-
Implementation (Coding) Phase (IP-#)	15	15	-
Test Phase (DP-#)	23	23	-
Life Cycle Support Phase (LC-#)	12	12	-
TOTAL ACTIVITIES / TASKS	**96**	**103**	**+7**

2017 Summary of Changes – Appendix A (cont.)

- **Several activities now required to be performed at lower LOR to align with MIL-STD-882E Table V LOR requirements**

Level-Of-Rigor	2016 IG	2017 IG	Change
Baseline	42	49	+7
1	54	54	-
2	47	49	+2
3	35	38	+3
4	20	27	+7
TOTAL ***(LOR 1 + Baseline)***	96	103	+7

Conclusion

- **Software Safety is required for acquisition programs IAW DoDI 5000.02 and MIL-STD-882E**
- **Additional guidance for software safety is provided in the JSSSEH Version 1.0 published 27 August 2010 as referenced in MIL-STD-882E**
- **Joint Boards developed a JSSSEH Implementation Guide on 1 April 2016 to further assist program perform software safety, and was endorsed by the JSWSR Boards on 29 June 2016**
- **2017 Implementation Guide Update (Rev A) release on 17 October 2017**
- **Implementation Guide will be updated annually, as required**

Implementation Guide assists in performing a comprehensive software safety program to fully characterize software's contribution to system risk

Resources (location of documents)

- **DAU Acquisition Community Connection Site, ESOH Community**
  - https://acc.dau.mil/ESOH

    ---or---
  - https://www.dau.mil/cop/esoh/Pages/Default.aspx
  - look under the “Resources” section

- **DoD Joint Software System Safety Engineering Handbook, 2010**
  - https://www.dau.mil/cop/esoh/DAU Sponsored Documents/SOFTWARE SYSTEM SAFETY HDBK 2010.pdf

- **Software System Safety Implementation Process and Tasks Supporting (a.k.a. “Implementation Guide”)**
  - https://www.dau.mil/cop/esoh/DAU%20Sponsored%20Documents/JSWRBs%20Endorsement%20JS%20SSA%20Software%20System%20Safety%20Implementation%20Guide%2029JUN2016.pdf

JSSSEH IG 2016

JSSSEH IG 2017 Rev A

Questions?

Robert E. Smith
Lead Associate

Booz | Allen | Hamilton

Booz Allen Hamilton
1550 Crystal Dr, Suite 1100
Arlington, VA 22202
Tel (703) 412-7661
smith_bob@bah.com

Ricks 19755

Agile Dynamics at Scale

A MITRE Innovation Program Research Project

NDIA 20th Annual Systems Engineering Conference

Presenting author:

Aleksandra Markina-Khusid amk@mitre.org

MITRE

Outline

- Project Description
- Modeling Agile Dynamics at Scale
- Simulating a Real Project

Acknowledgement

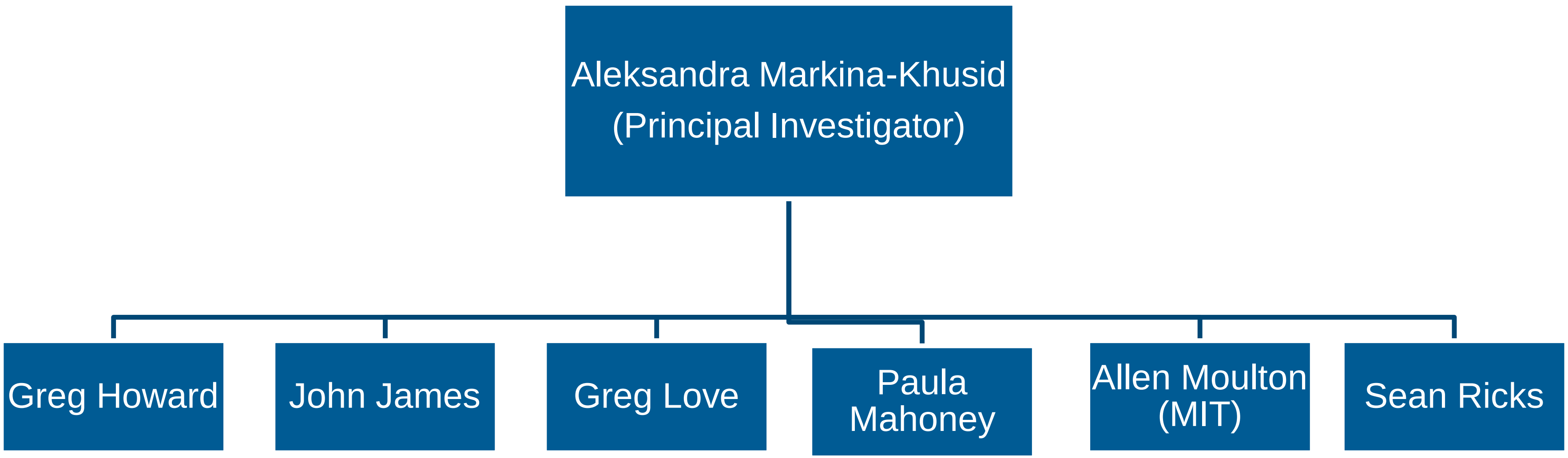
Disciplined Agile copyright material used with permission. All rights reserved.

Managed Agile Delivery copyright material used with permission. All rights reserved.

Scaled Agile Framework copyright material used with permission. All rights reserved.

Project Description

Team Members
A joint MITRE-MIT Research Project



Lean-Agile Methods

Systems Dynamics, Modeling and Simulation

Goals

1. **Use modeling to study how scaled Lean-Agile methods would enable Agile software development to integrate into a heavily plan-driven and risk averse enterprise such as the Air Force and DOD.**
2. **Perform virtual experimentation with scaled Lean-Agile methods by capturing those methods in a model (or models).**
3. **Provide expanded knowledge about Lean-Agile and a virtual experimentation resource for use by MITRE staff in engagements.**
4. **Develop a baseline for a model that can enable MITRE staff to test alternative management structures on projects they support.**
5. **Build a model that can make relative projections, not precise predictions.**
   - The models built in segments to test hypotheses but with a plan for integration at a later point. Each segment will provide value and contribute to Goal #1.

Perspective User Stories

- **Program Systems Engineer**

  Systems engineers use models to define, understand, communicate, assess, interpret, and accept the project scope; to produce technical documentation and other artifacts; and to maintain "ground truth" about the system(s).

  \- DoD Acquisition Modeling And Simulation Working Group

  – As a Program Systems Engineer I need to understand the engineering variables* and trades in order to develop the Program's Systems Engineering Plan (SEP).

  – As a Program Systems Engineer and given a SEP, I need to identify risk and opportunities.

**The Agile Genome*

1. Story/feature driven
2. Iterative-Incremental
3. Refactoring
4. Micro-Optimizing
5. Customer Involvement
6. Team Dynamics
7. Continuous Integration

- **Acquisition and Program Manager**

  – As a Program Manager I need to understand the SE variables impact on cost (development cost curve).

  – As a Program Manager I need to understand the SE variables impact on schedule (backlog burn down and project end).

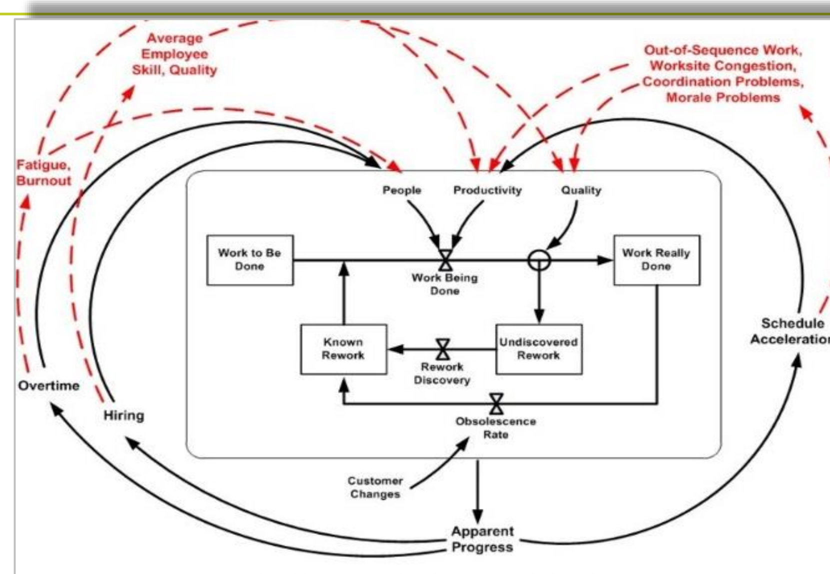
  – As a Program Manager I need to understand the SE variables impact on performance (defect rate).

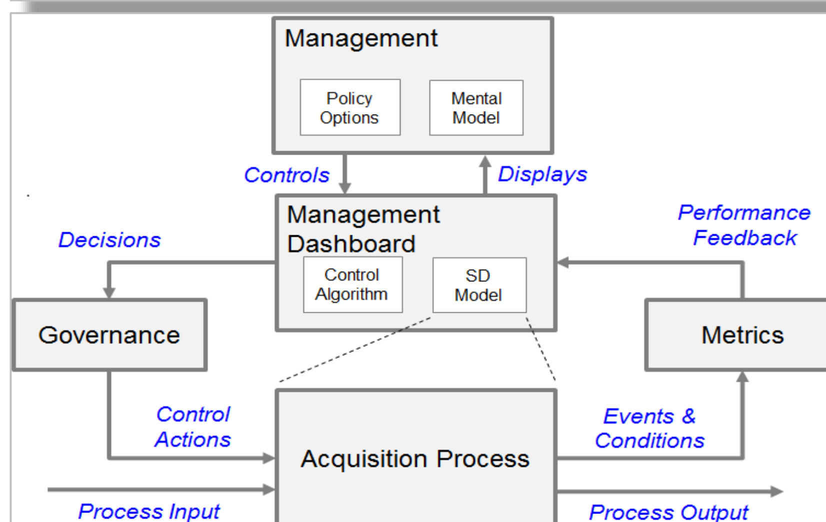
  – As a Program Manager I need to understand the impact on cost, schedule and performance when introducing new technology into the agile development cycle.

Research Idea

Decision Support for Acquisition Professionals and Managers

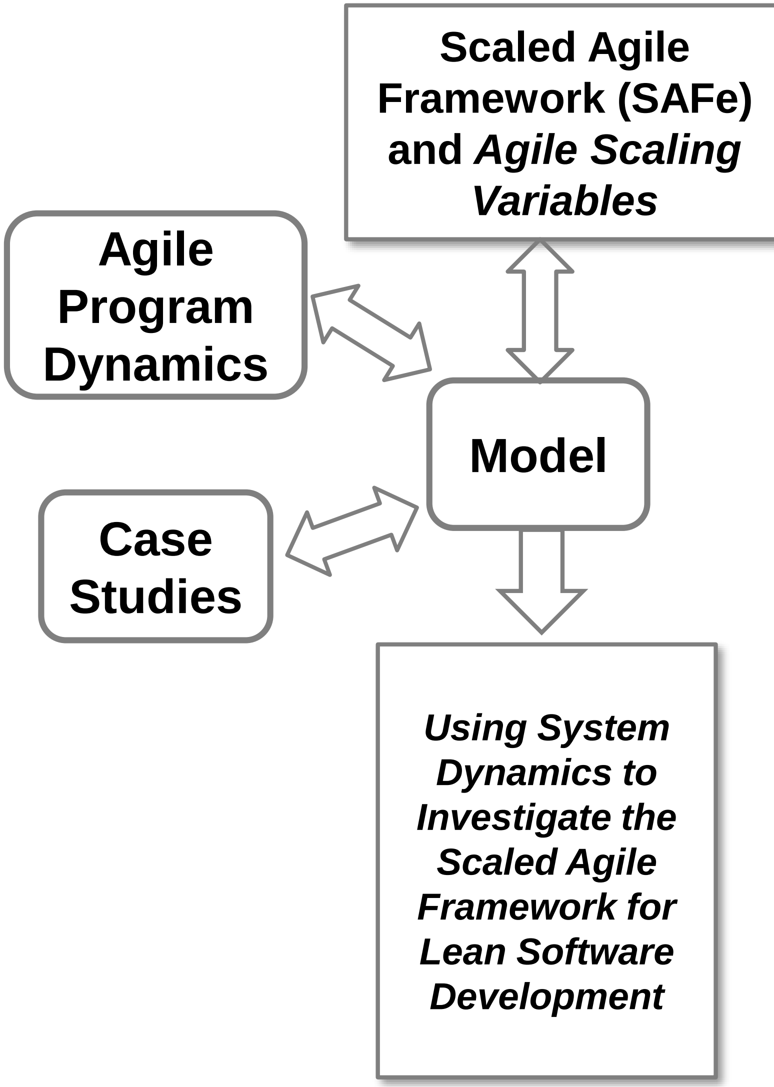
- **Model the dynamics of Lean-Agile methods for large scale efforts on:**
  - Program acquisition
  - Project management
  - Systems development
- **Incorporate range of structural cause-and-effect feedback loops and factors that drive nonlinear project behaviors that impact:**
  - Cost, Schedule, Performance
  - Risk
  - Value delivery
- **Provide dashboard tools:**
  - Predictive analytics for acquisition outcomes
  - Exploration of policy and governance options





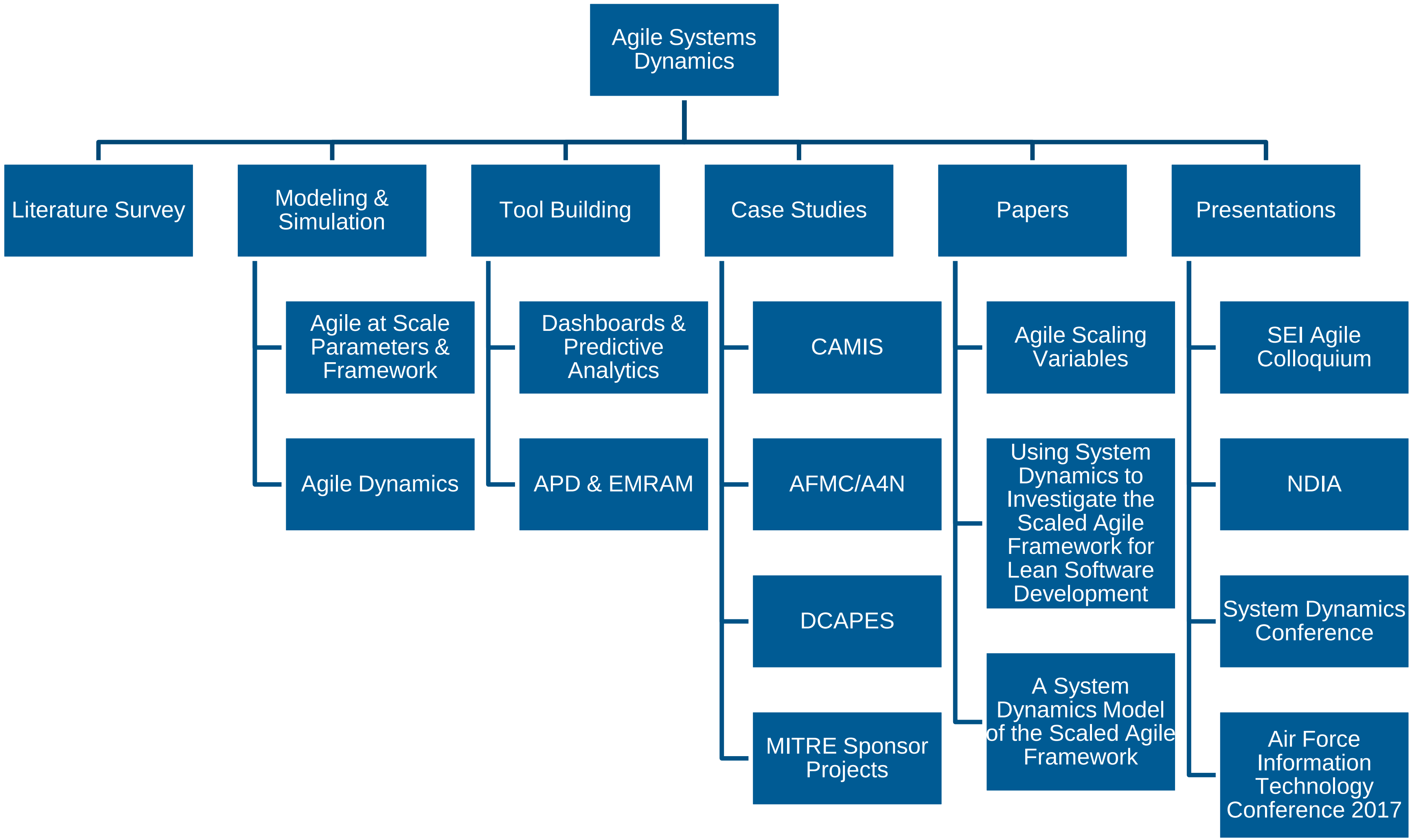
Research Methodology

- **Builds on MIT Agile Program Dynamics model (APD)**
  - Modeled an Agile Team
  - Models **Undiscovered Rework** – a decline in quality not immediately recognized that eventually adds **to Known Work**
- **Adding SAFe and the *Agile Scaling Variables* representing Lean-Agile principles, methods and practices.**
- **Model is validated/updated with case study real world results**
  - Case studies provide and highlight the areas of modeling
- **Show that adjusting variables produce expected effects**
  - Find unexpected behavior
- **Model provides source for conference papers**



MITRE

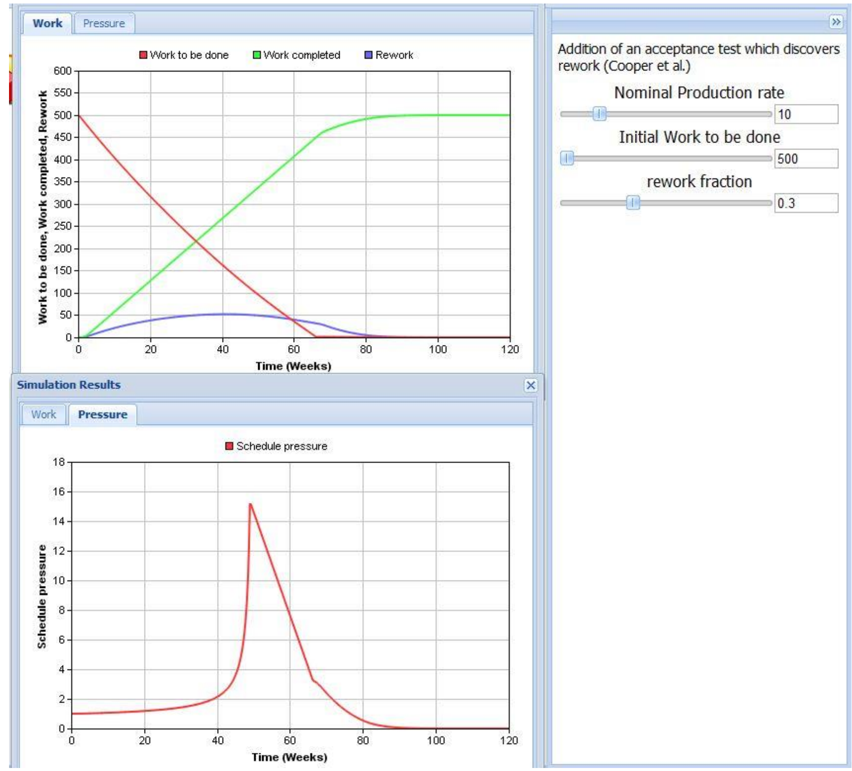
Project Structure



Modeling Agile Dynamics at Scale

Purpose

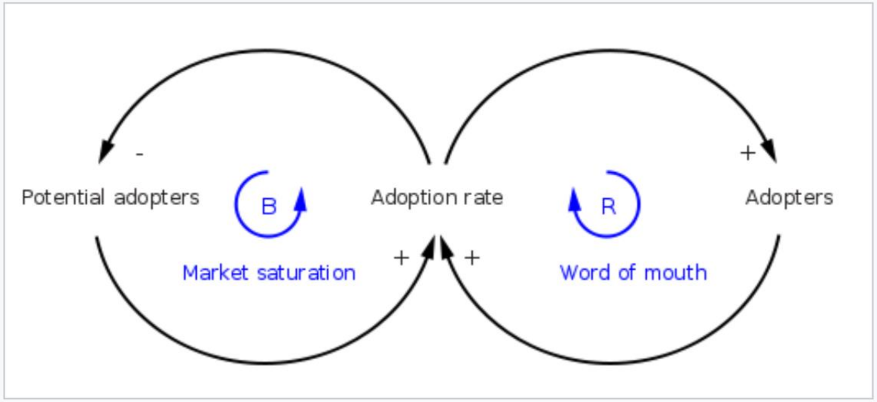
- **The rate of work completion depends on…**
  - Team size
  - Number of teams
  - Team experience
  - Sprint duration
  - Number of sprints per Program Increment (PI)
  - Automated testing
  - Frequency of demos
  - Continuous Integration (CI)
  - Etc.



Provide a tool to identify important dynamic relationships and trends and facilitate a conversation on process improvement.

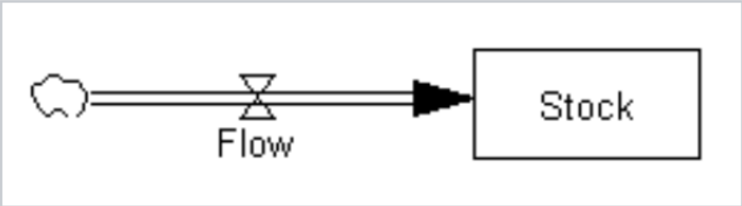
Systems Dynamics

- **A method to understand the dynamic behavior of complex systems**
- **A system's behavior is determined by:**
  - Individual components, and
  - ***The many circular, interlocking, sometimes time-delayed relationships among components***



Causal loop diagram of *Adoption* model, used to demonstrate systems dynamics

The causal loop diagram visualizes how different variables in a system are interrelated



A flow is the rate of accumulation of the stock

Source: Wikipedia

System Dynamics

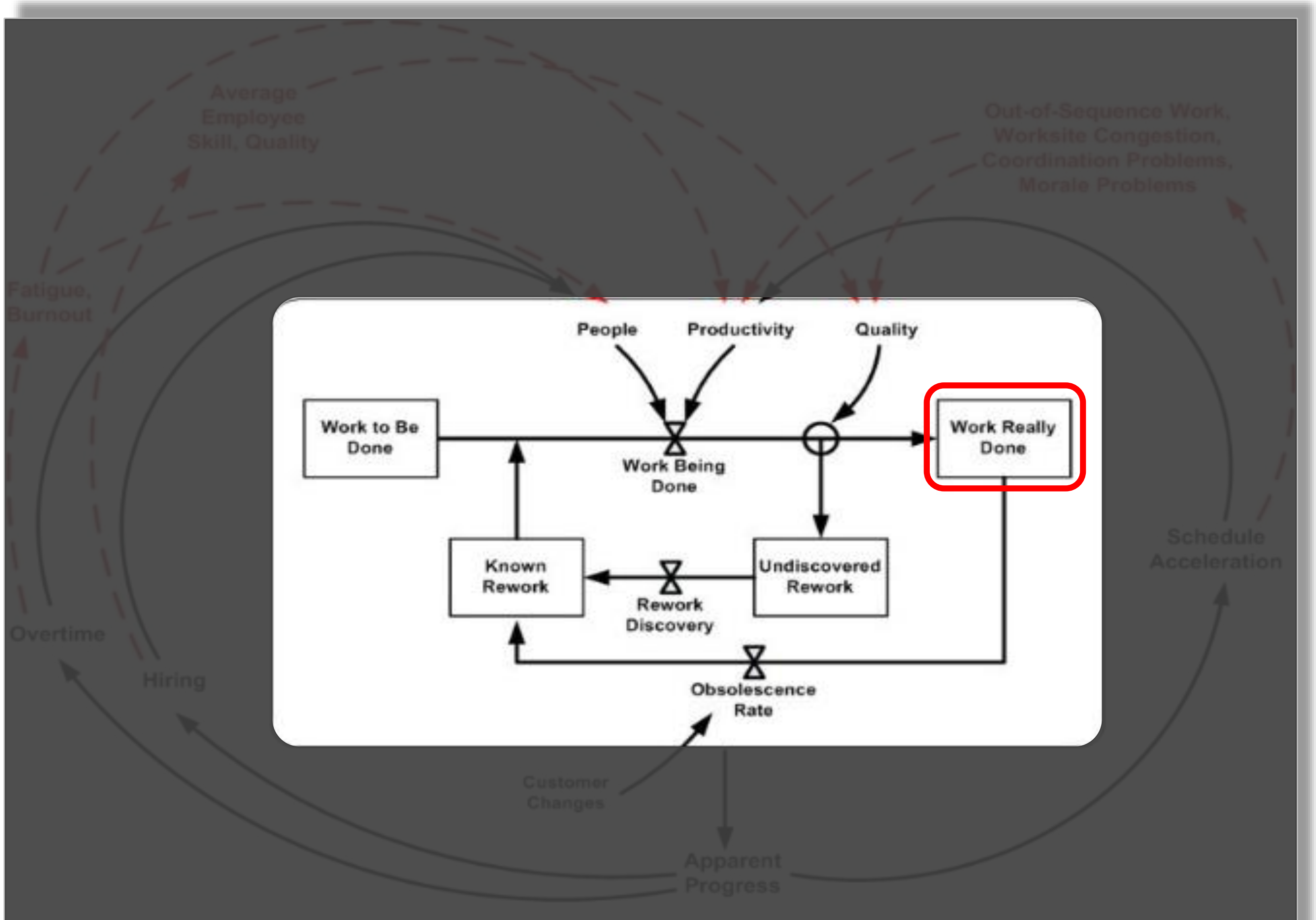


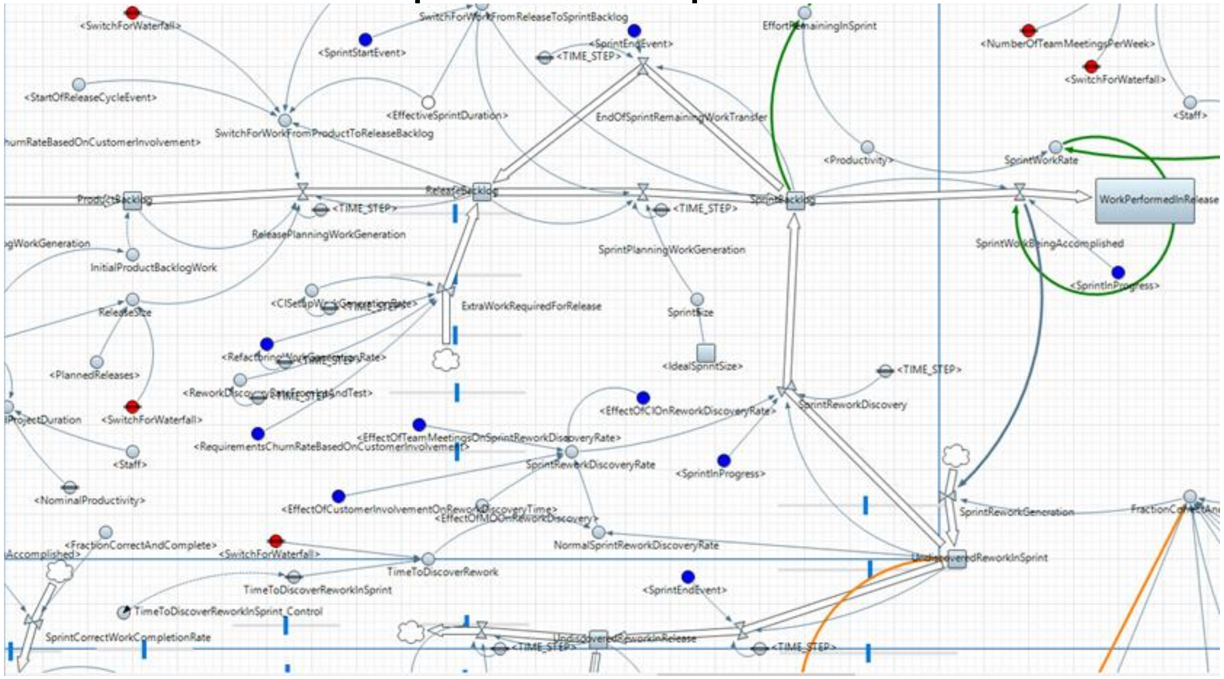
Figure 2 - Some Sample Project Dynamics

Source: Wikipedia

MITRE

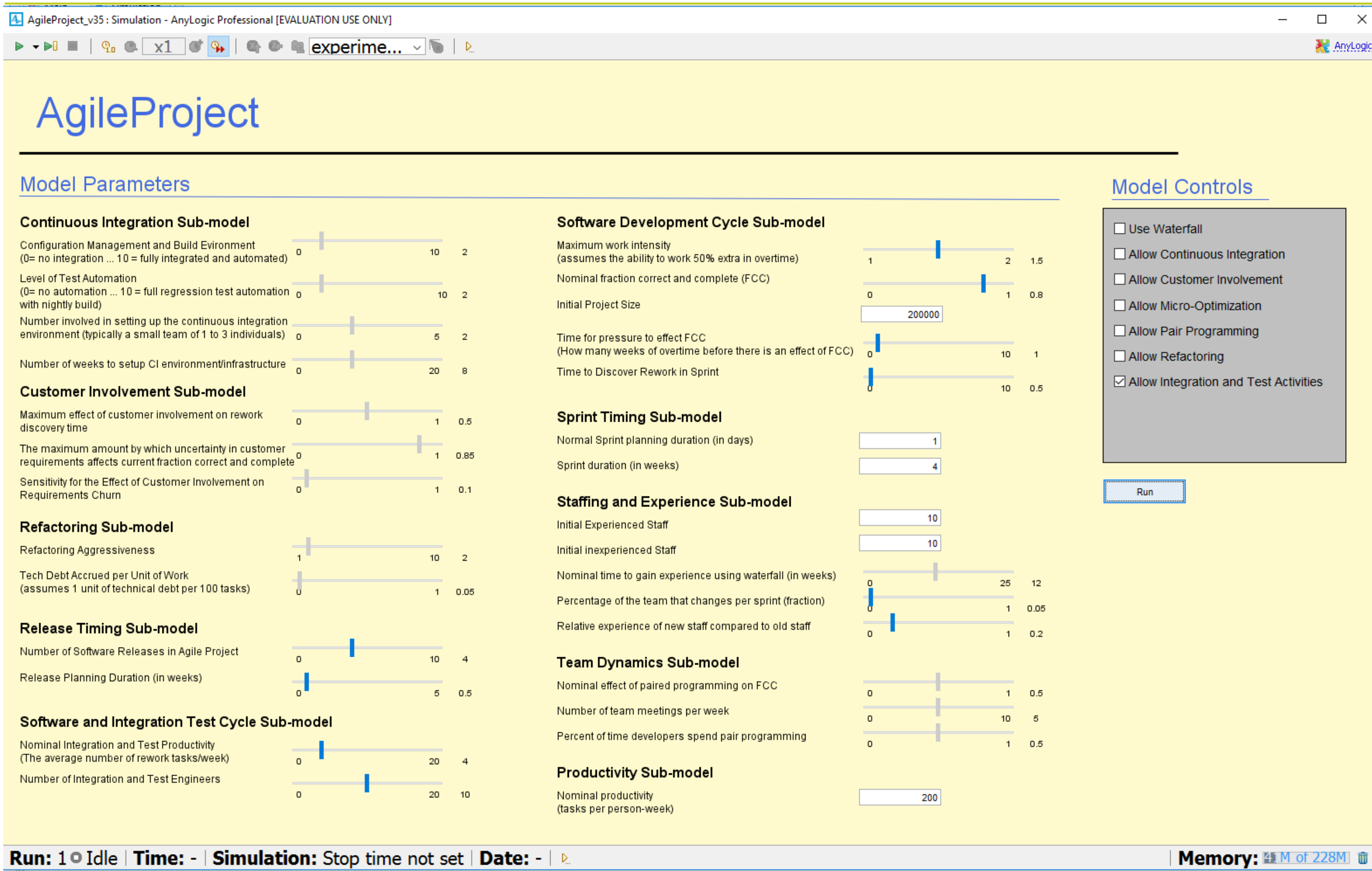
Prior Work

- **Agile Project Dynamics:**
  - MIT effort, Firas Glaiel
  - Model of a single agile development team
  - Product > Release > Sprint > Completed



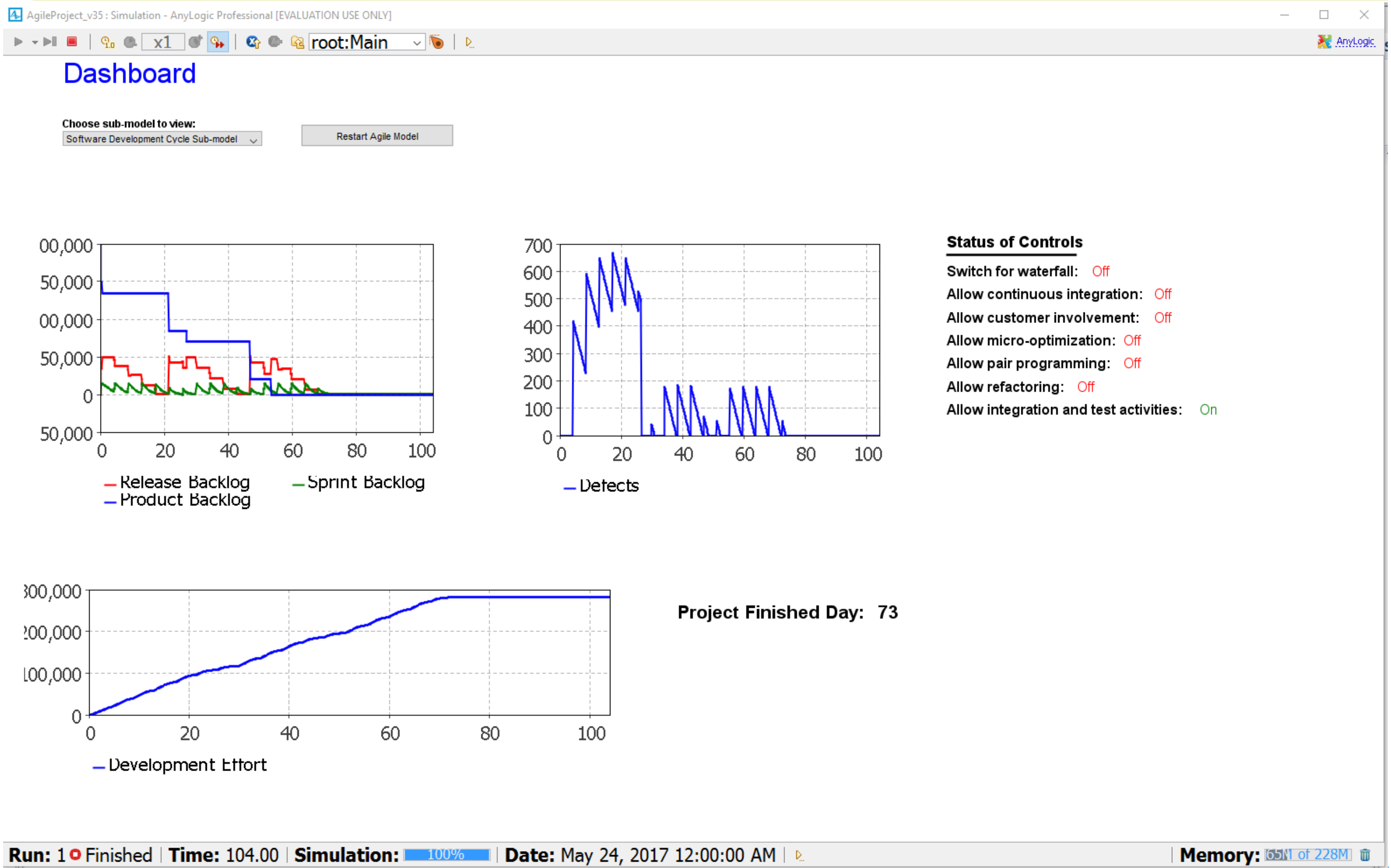
Glaiel, F. (2012). Agile Project Dynamics: A Strategic Project Management Approach to the Study of Large-Scale Software Development Using System Dynamics. Unpublished MIT SDM Thesis. Working Paper CISL# 2012-05.

Prior Work



MITRE

Prior Work

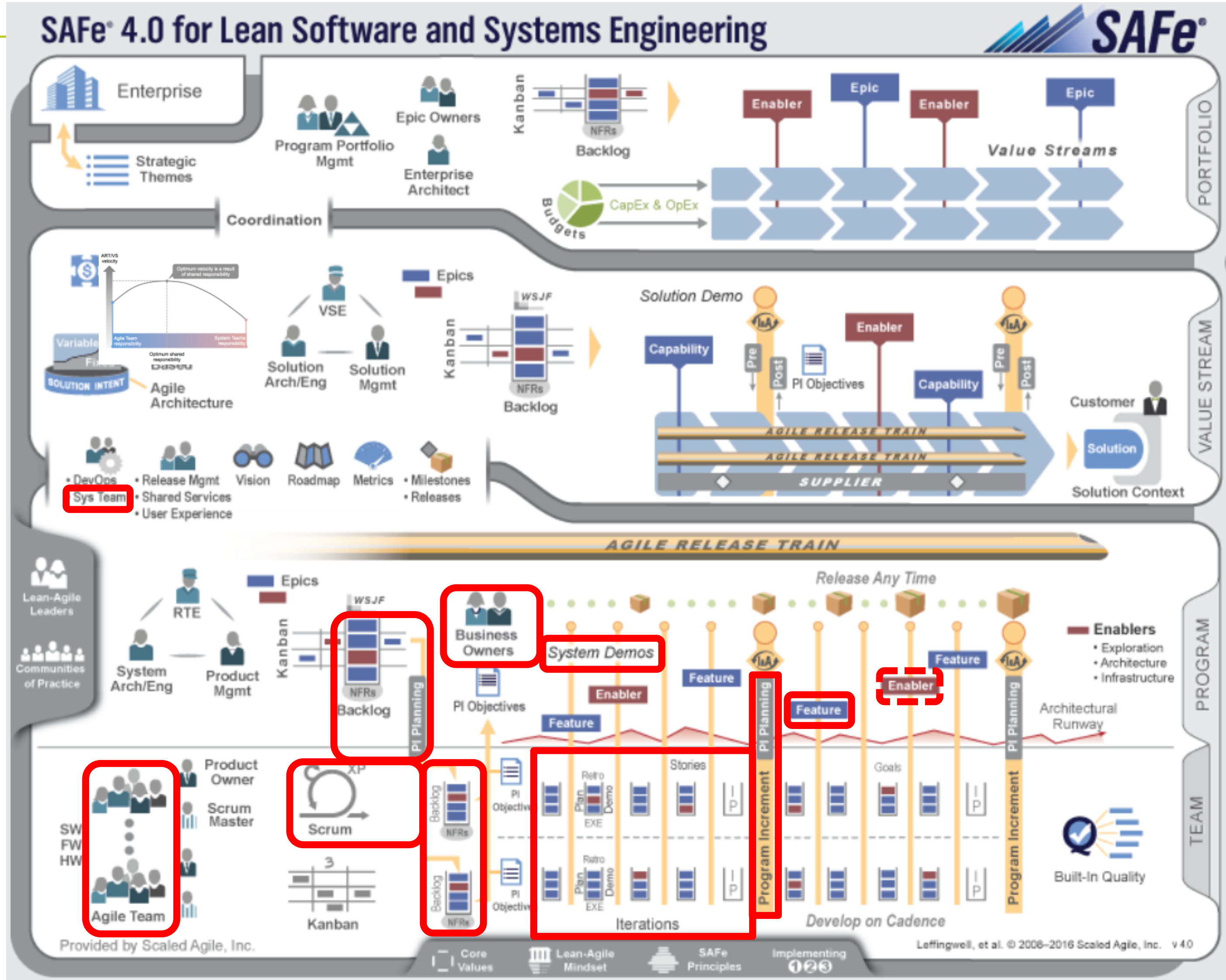

AgileProject_v35 : Simulation - AnyLogic Professional [EVALUATION USE ONLY]
x1
root:Main
AnyLogic
Dashboard
Choose sub-model to view:
Software Development Cycle Sub-model
Restart Agile Model
Release Backlog
Sprint Backlog
Product Backlog
Defects
Status of Controls
Switch for waterfall: Off
Allow continuous integration: Off
Allow customer involvement: Off
Allow micro-optimization: Off
Allow pair programming: Off
Allow refactoring: Off
Allow integration and test activities: On
Development Effort
Project Finished Day: 73
Run: 1 Finished
Time: 104.00
Simulation: 100%
Date: May 24, 2017 12:00:00 AM
Memory:

Our Work

- **Applied to Scaled Agile Framework (SAFe)**
- **Higher level dynamics of team interactions**
- **Extended development cycle to include integration and demos**
- **Distinguish between different types of rework**
  - Defects
  - Integration errors
  - Requirements errors

MITRE

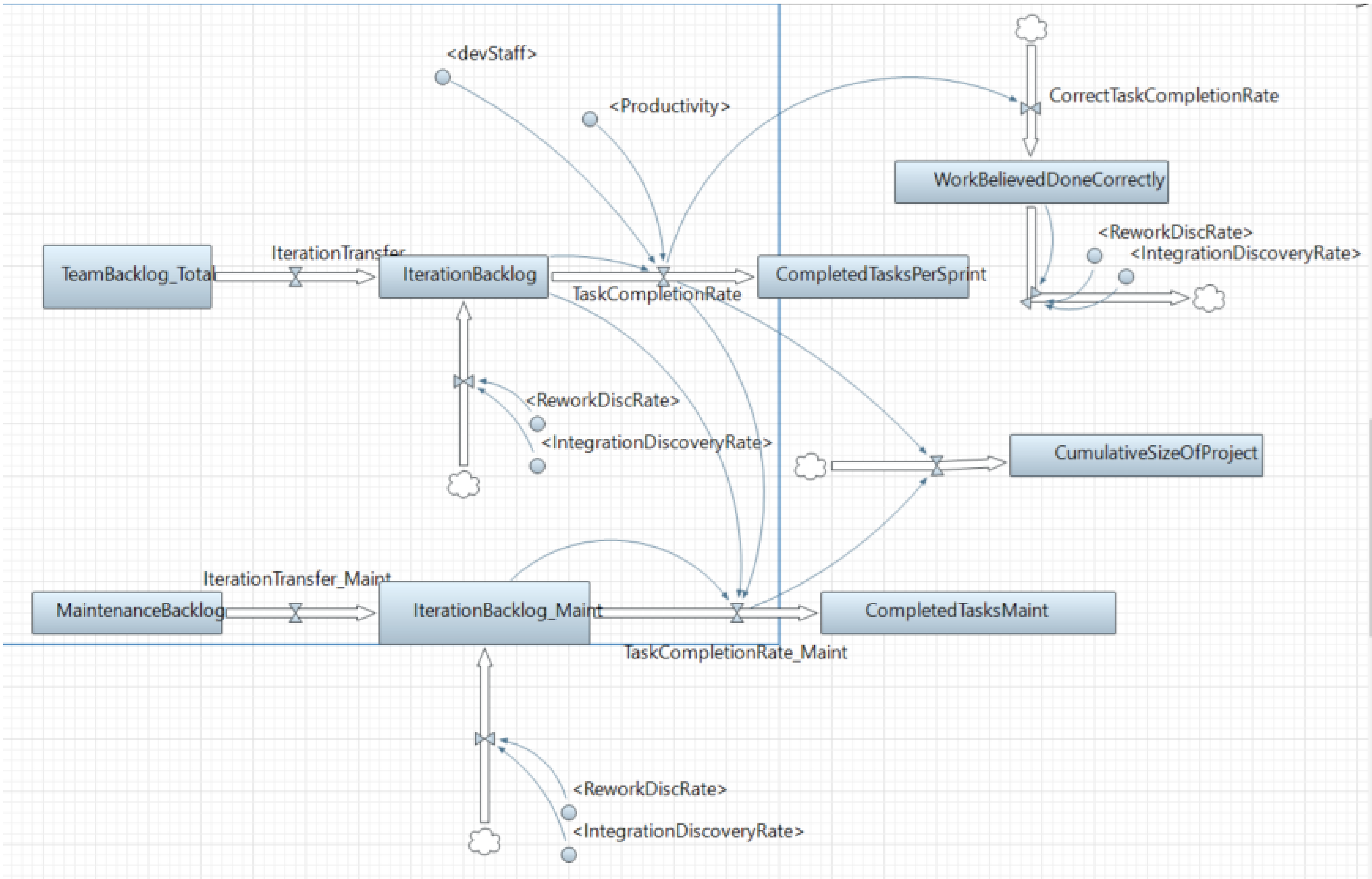
SAFe Elements



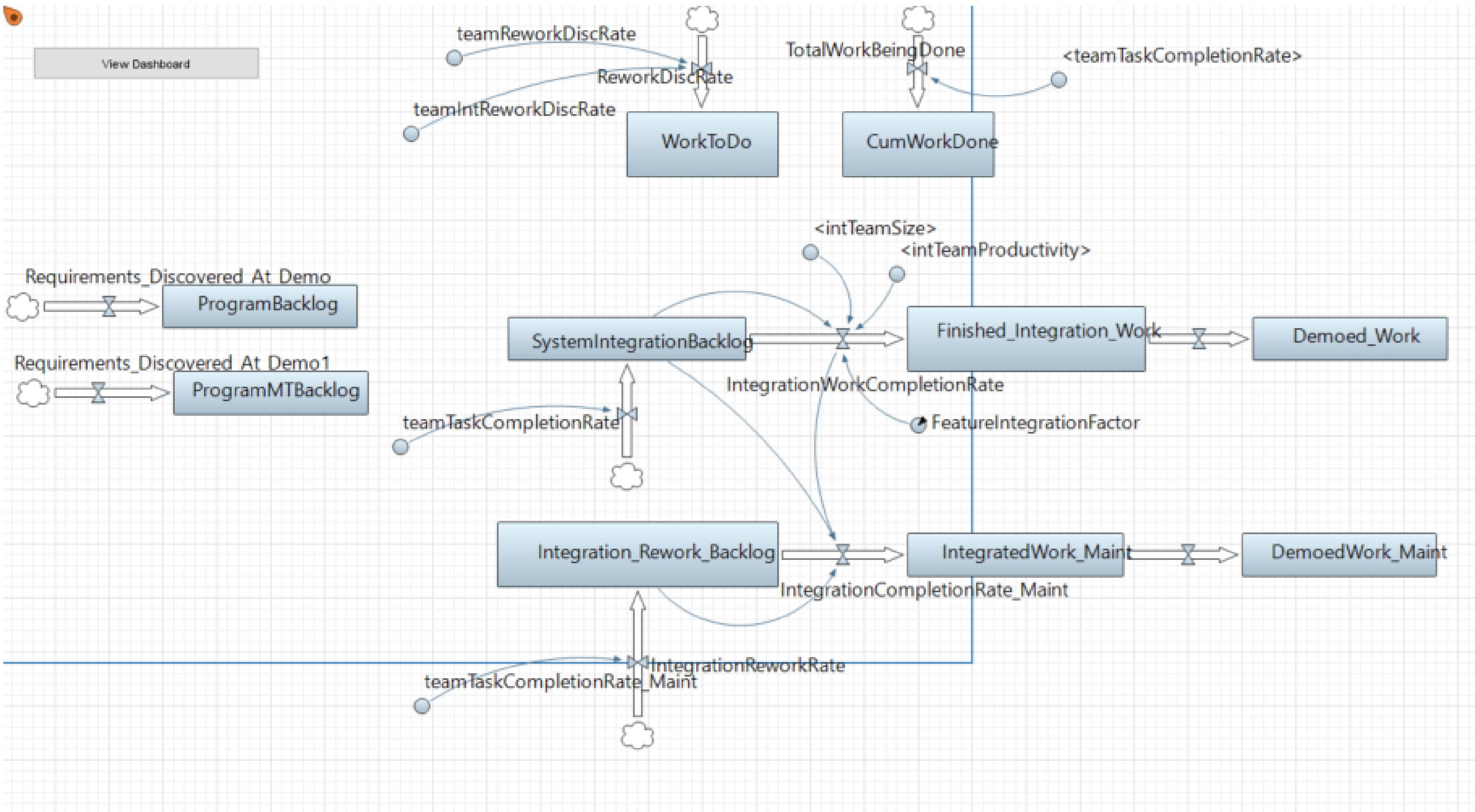
Scaled Agile Framework copyright material used with permission

MITRE

Team Work

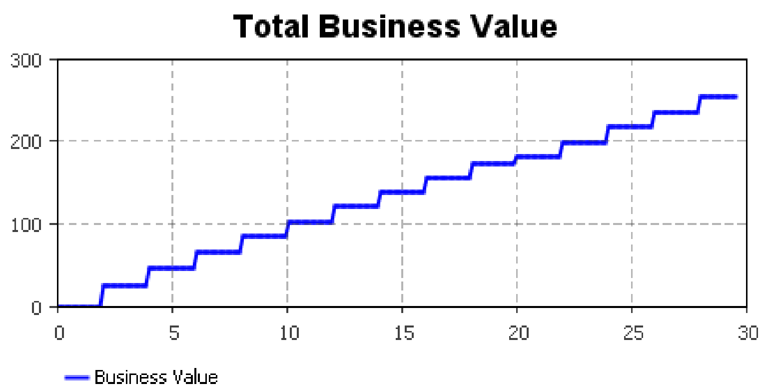

<devStaff>
<Productivity>
CorrectTaskCompletionRate
WorkBelievedDoneCorrectly
<ReworkDiscRate>
<IntegrationDiscoveryRate>
TeamBacklog_Total
IterationTransfer
IterationBacklog
TaskCompletionRate
CompletedTasksPerSprint
<ReworkDiscRate>
<IntegrationDiscoveryRate>
CumulativeSizeOfProject
IterationTransfer_Maint
MaintenanceBacklog
IterationBacklog_Maint
CompletedTasksMaint
TaskCompletionRate_Maint
<ReworkDiscRate>
<IntegrationDiscoveryRate>

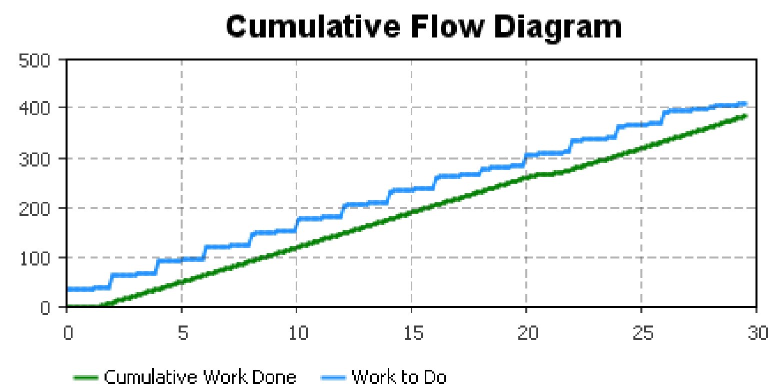
Program Work

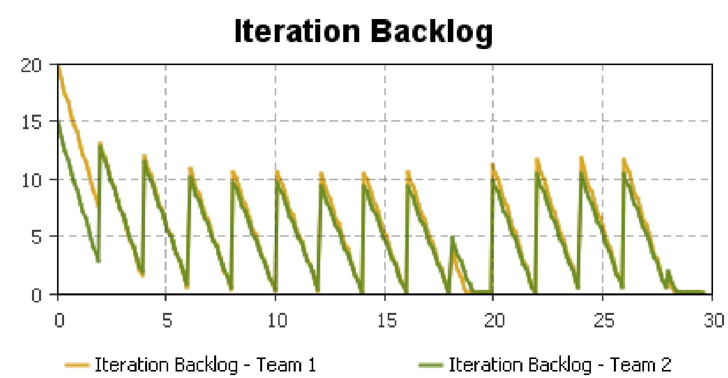


Output

View Model







Team 1

Team 2

Simulating a Real Project

Case Project Description

- **Tailored from SAFe 2.0**
  - Most team and program elements
  - 4 development teams
  - 2 weeks per Sprint, 4 Sprints per Program Increment
  - No enablers
  - No dedicated system team, continuous integration
    - The 4th Sprint is used as a development buffer and a time for development teams to do testing and integration work
- **Observations**
  - Large amounts of defects discovered in Sprint 4 leading to delays, cutting into planning sessions, and creating carryover problems for the next Sprint

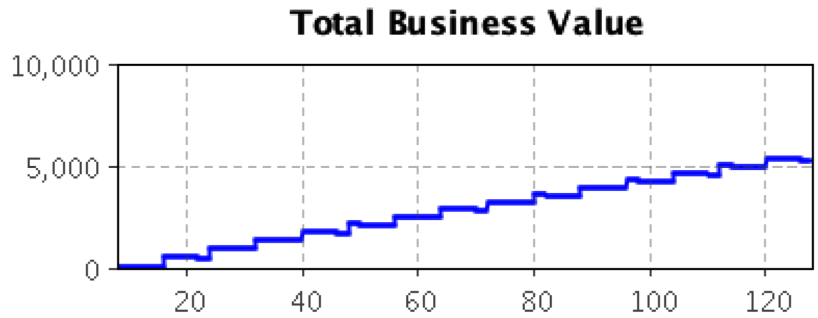
MITRE

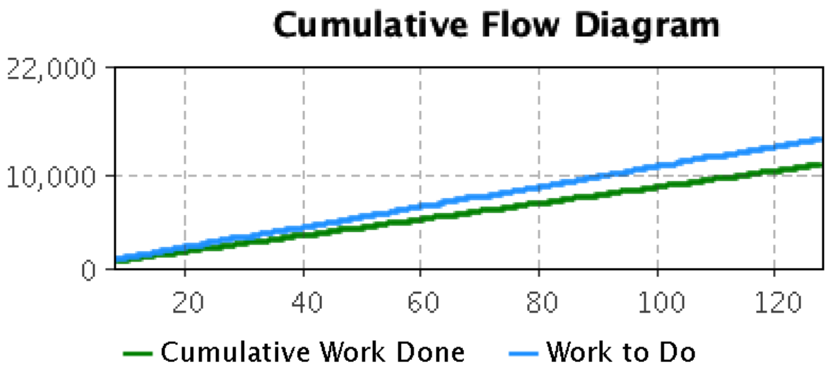
Simulation Description

- **Without CI (baseline)**
  - 4 dev teams of 10 each
  - No dedicated system team
  - 4 * 2-week Sprints per PI
  - Developers do integration during 4^{th} Sprint
  - 16 PIs simulated
- **With CI**
  - 4 dev teams of 9 each
  - Dedicated system team of 4
  - 4 * 2-week Sprints per PI
  - All Sprints used for development
  - 16 PIs simulated

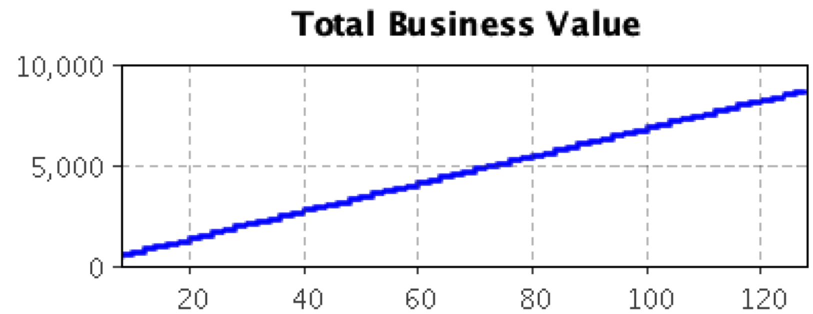
Results

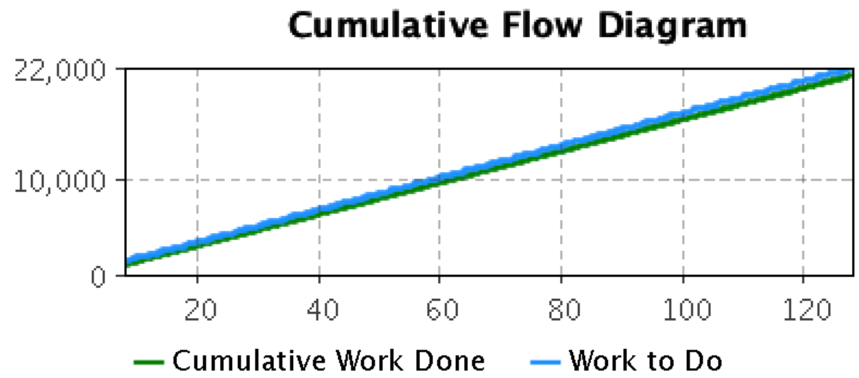
- **Without CI (baseline)**





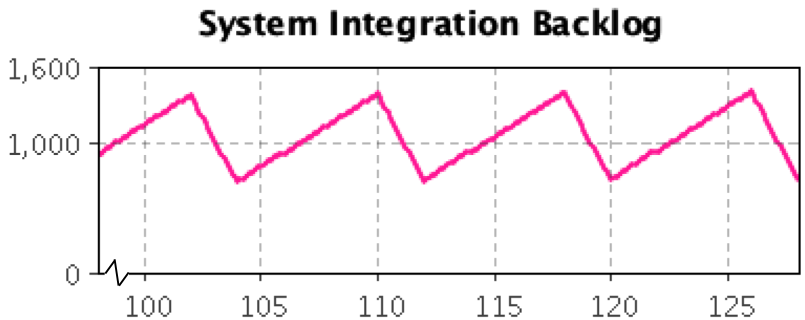
- **With CI**

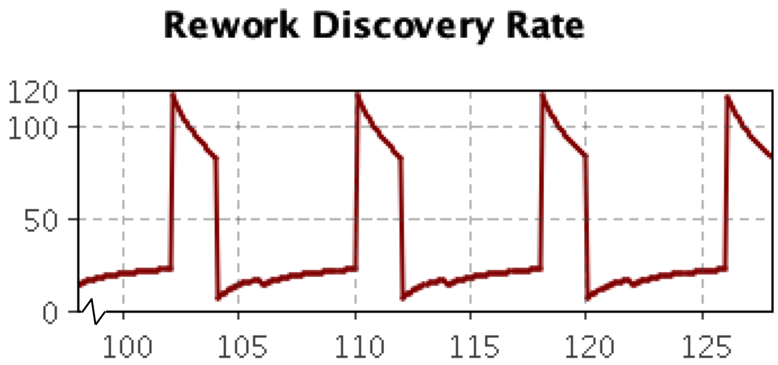




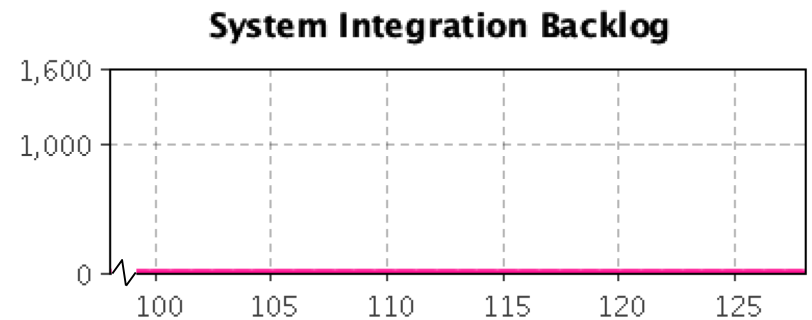
Results

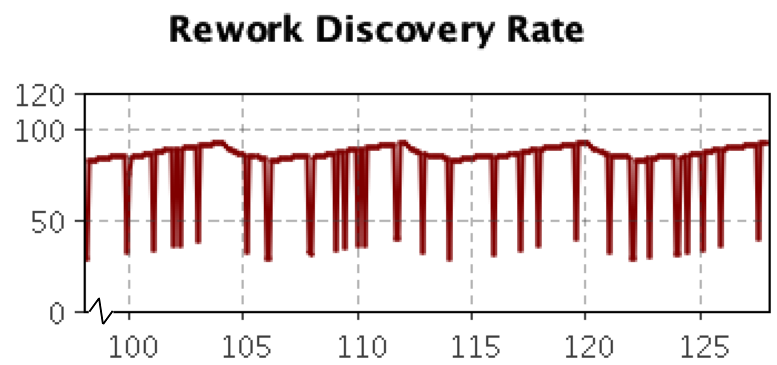
- **Without CI (baseline)**





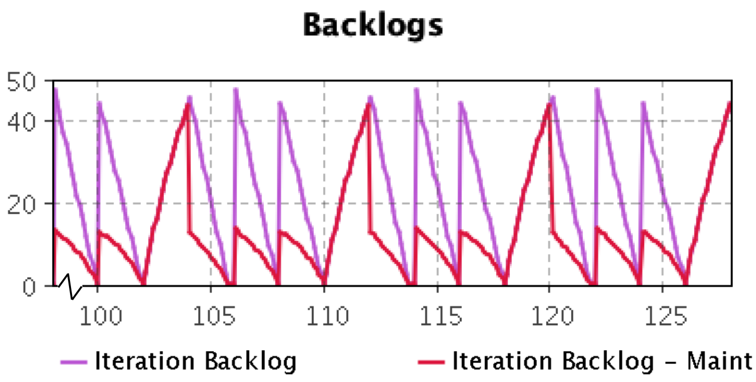
- **With CI**

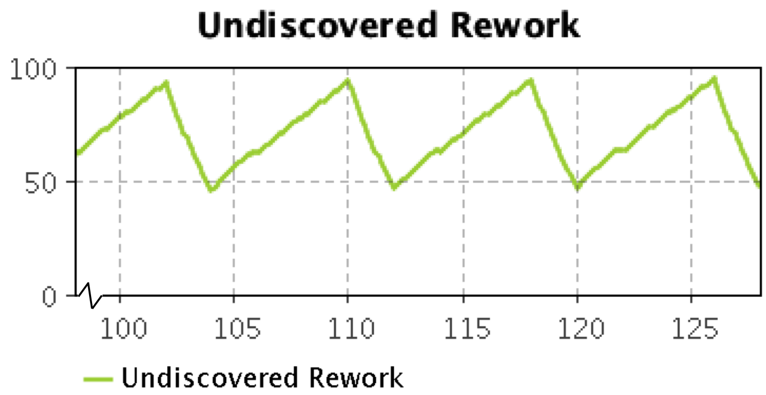




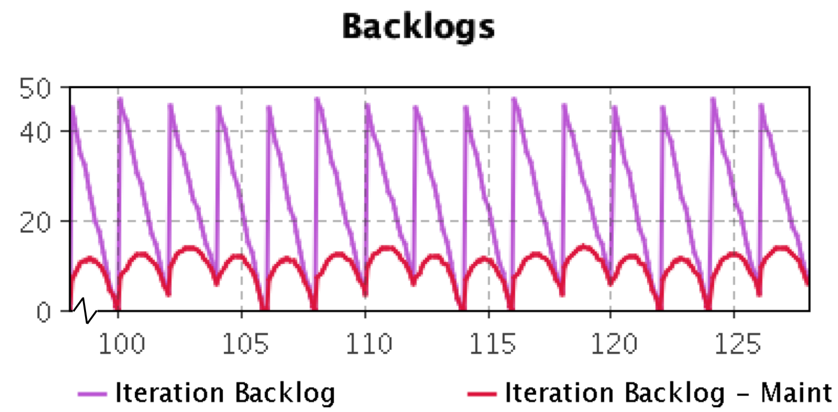
Results (Team 1)

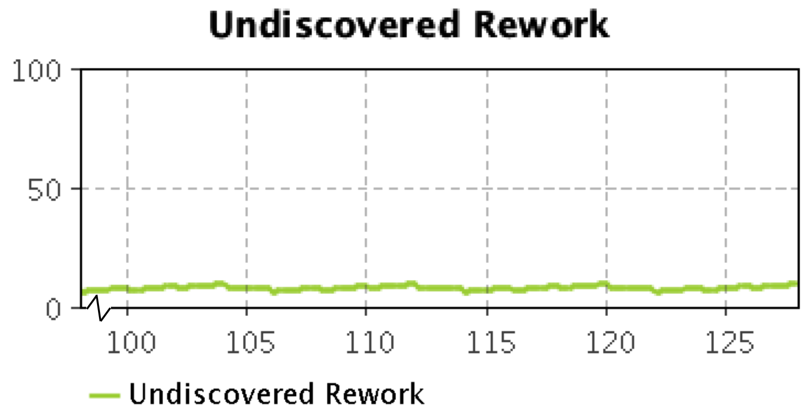
- **Without CI (baseline)**





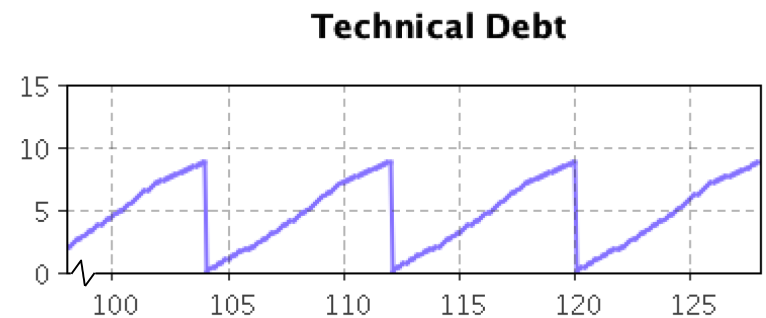
- **With CI**

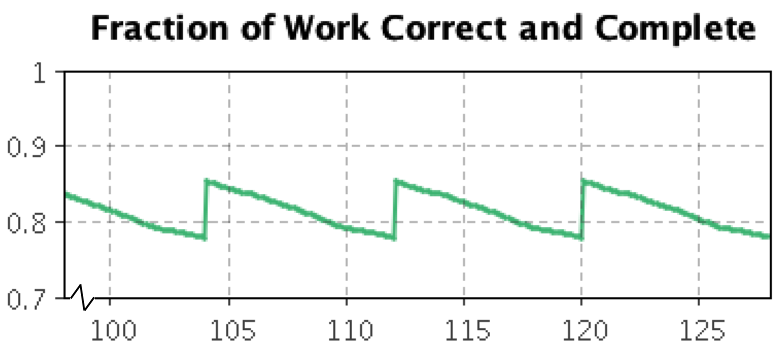




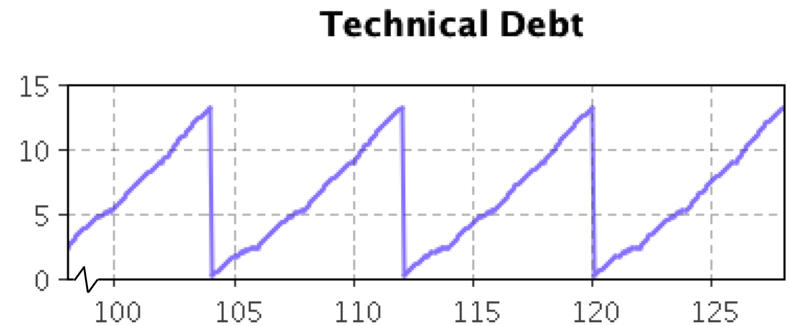
Results (Team 1)

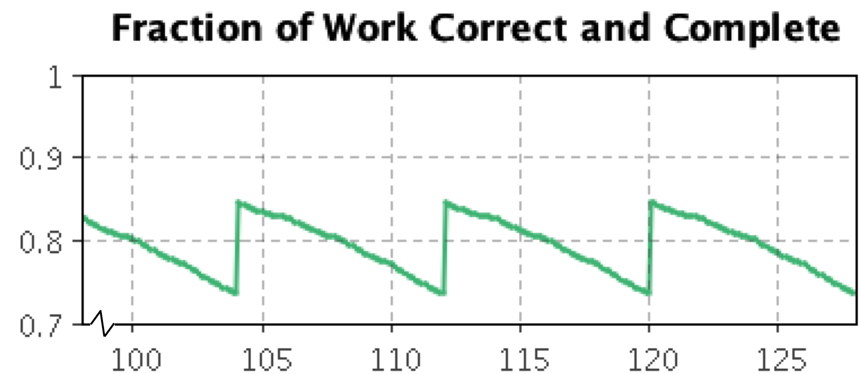
- **Without CI (baseline)**





- **With CI**





MITRE

Results

- **Without CI (baseline)**
  - TBV: 5706
  - Average team velocity: 50
  - Average undiscovered rework (bugs): 65
  - Average FCC: .81
- **With CI**
  - TBV: 8787
  - Average team velocity: 49
  - Average undiscovered rework (bugs): 8
  - Average FCC: .78

Doing integration continuously rather than waiting until the 4th sprint resulted in 54% more valuable work accomplished in the same amount of time with 88% fewer bugs in the code.

Limitations

- **SAFe or similar programs**
- **Homogenous stocks**
  - Stories and Features
  - Weighted shortest job first (WSJF)
- **Instantaneous meetings**

Future work

- **Improving the model**
  - Generalization
  - Effects of planning sessions
  - Effects of enablers
  - Communication/coordination overhead
- **Verification/Validation**
  - Case studies
  - Sensitivity analysis
- **Management flight simulator**

Conclusion

- Research builds on work begun at MIT
- Identified Agile scaling variables
- System dynamics techniques used to model the behavior of complex systems over time
- Begun building model for SAFe
- Model will provide a decision support tool

MITRE

Agile Dynamics at Scale
A MITRE Innovation Program Research Project

Questions

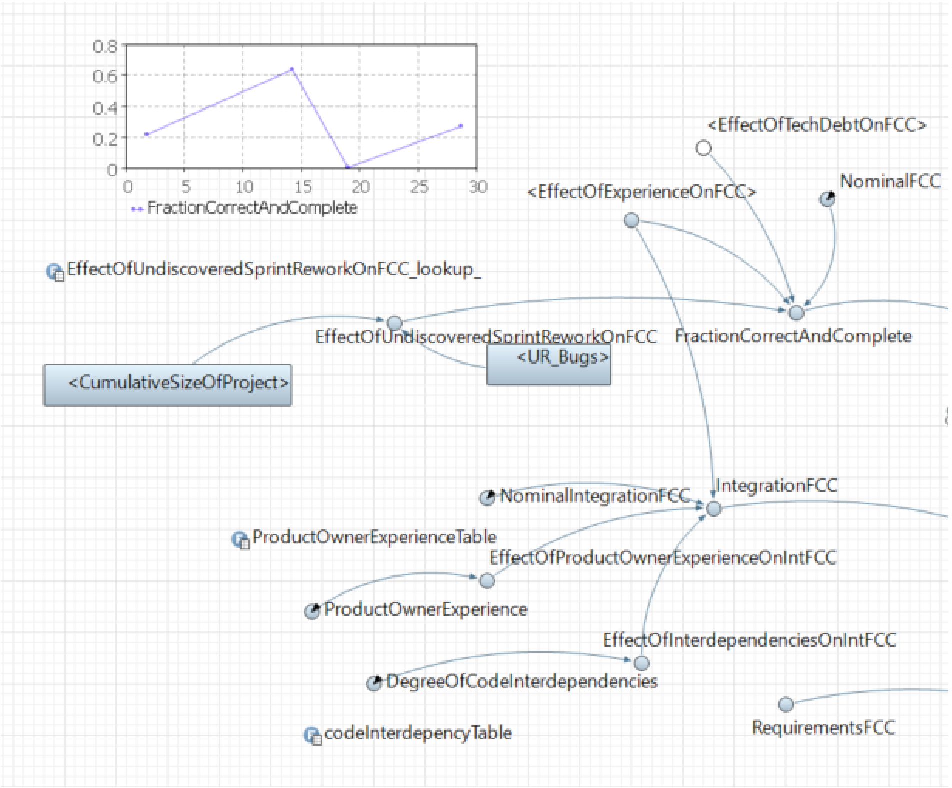
Thank You!

Aleksandra Markina-Khusid amk@mitre.org
Sean Ricks stricks@mitre.org

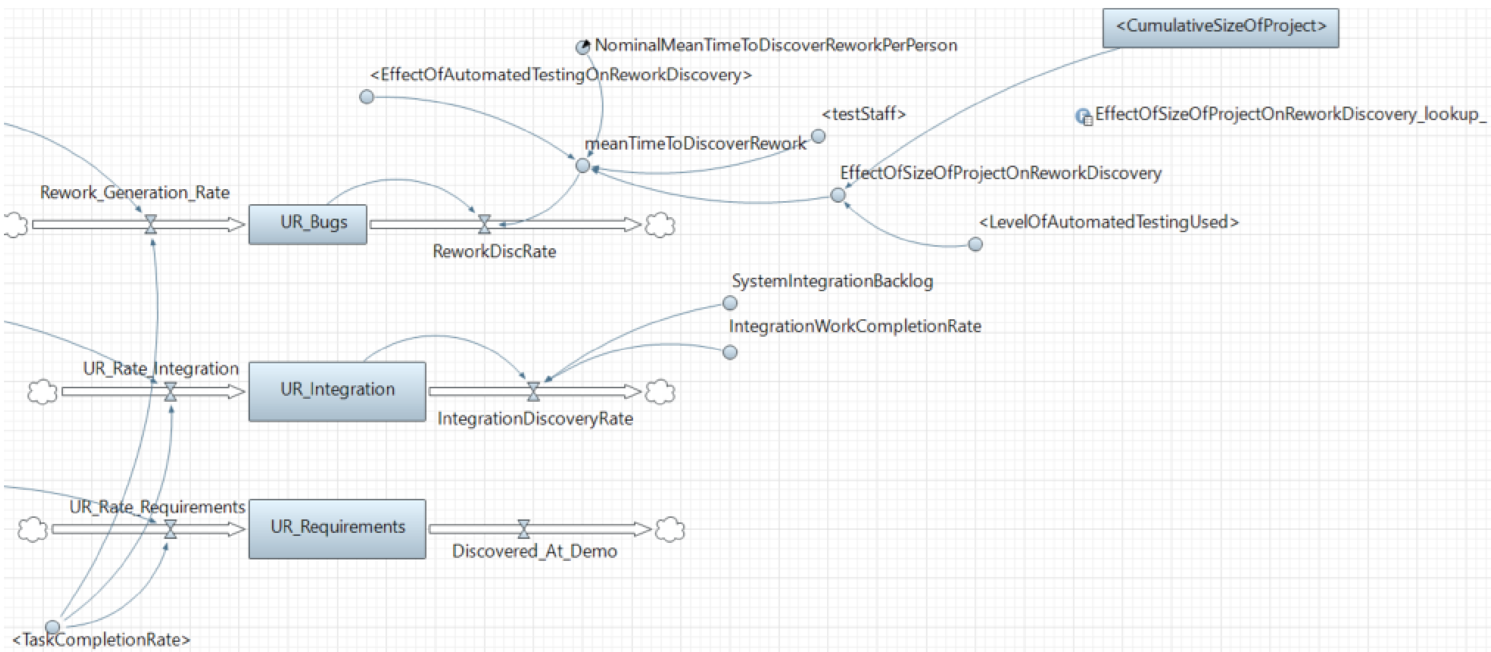
MITRE

Backup

Fraction Correct and Complete

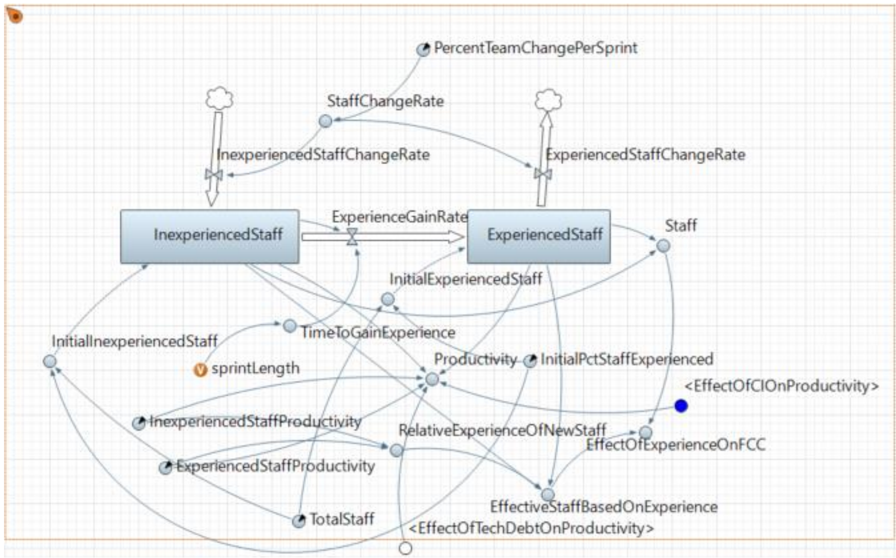


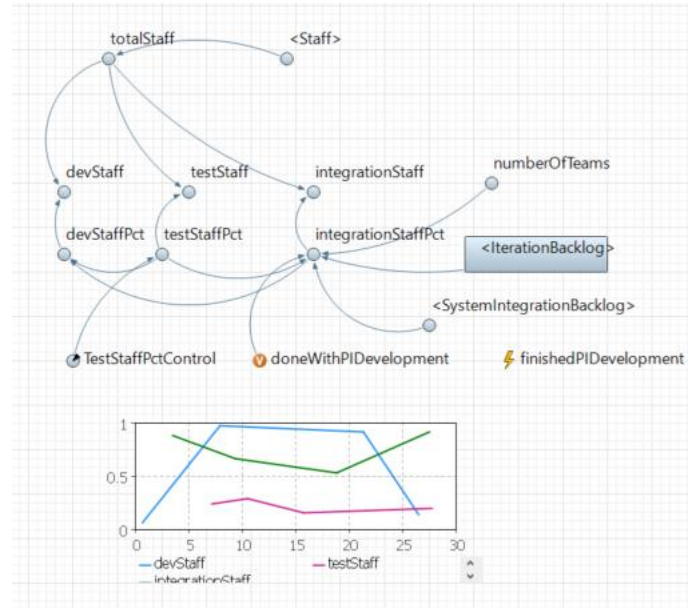
Rework Creation and Discovery

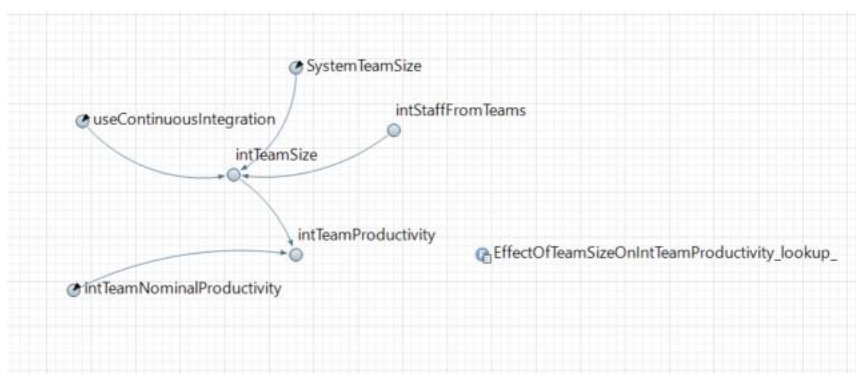


MITRE

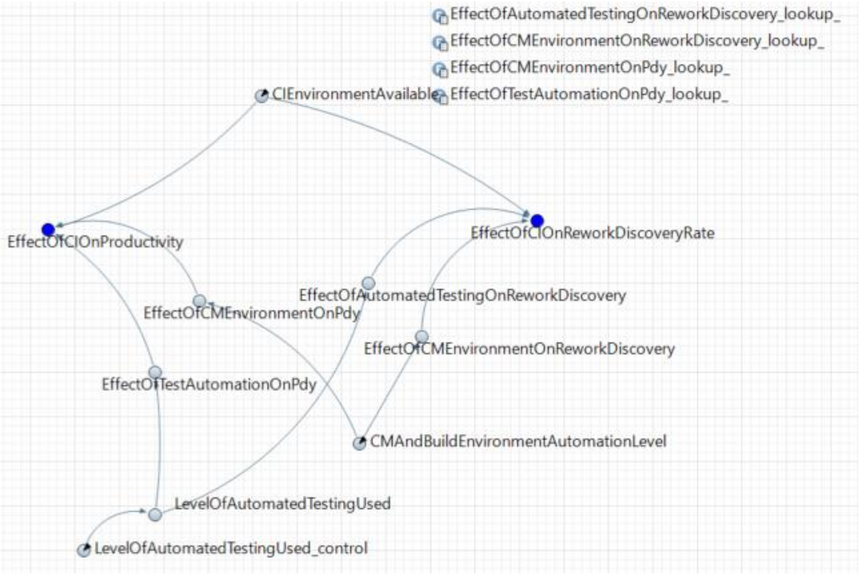
Human Resources and Staff Allocation

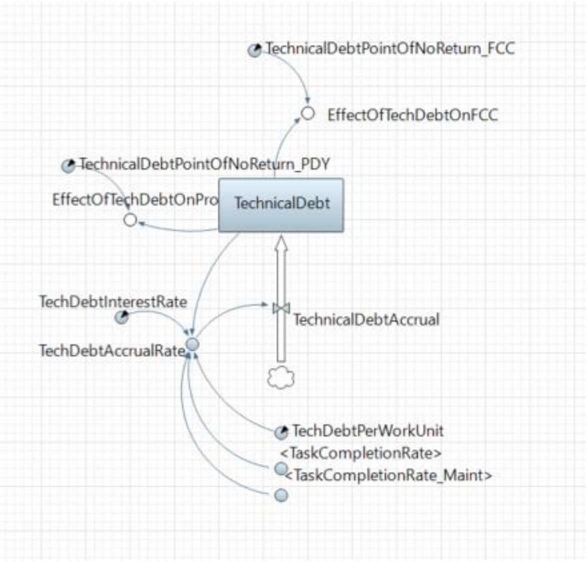






Effects of Automation and Tech Debt





MITRE

Acronyms

MIT	Massachusetts Institute of Technology
DOD	Department of Defense
APD	Agile Project Dynamics
SAFe	Scaled Agile Framework
EMRAM	Enterprise Modernization Risk Assessment Model
CAMIS	Cadet Administrative Management Information System
AFMC/A4N	Air Force Materiel Command, System Integration Division
DCAPES	Deliberate and Crisis Action Planning and Execution Segments
SEI	Software Engineering Institute
NDIA	National Defense Industry Association
MDA	Milestone Decision Authority
COR	Contracting Office Representative
PM	Project Manager
FFRDC	Federally Funded Research and Development Center
SME	Subject Matter Expert
SEP	System Engineering Plan
SE	System Engineering
SD	System Dynamics
ALCM	Agile Lifecycle Management
PI	Program Increment
CI	Continuous Integration
TBV	Total Business Value
FCC	Fraction Correct and Complete
WSJF	Weighted Shortest Job First
GOAA	Government Organization Agility Assessment
AiDA	Acquisition in the Digital Age
AF	Air Force

MITRE

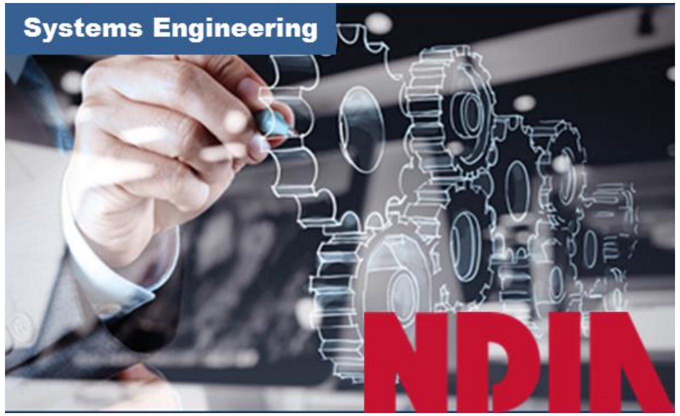
DEFENSE CONTRACT MANAGEMENT AGENCY

DCMA

One team, one voice delivering global acquisition insight that matters.

Assessing the impacts of Amended Toxic Substances Control Act (TSCA) to the DoD Mission and the Defense Industrial Base (DIB)

DIB Mission Assurance and IB Risks Posed by Chemical Regulation



Presented by:
Shane Esola
Technical Lead, Industrial Base Assessment
DCMA Industrial Analysis Group

NDIA Systems Engineering 23-26 Oct 2017

Outline

- Introduce the Industrial Analysis Group (IAG)
- Problem Statement (DIB sector perspective)
- Pilot Assessment Results
- Degrees of Potential Market Collapse Due to Regulation
- National Security Exemptions

Industrial Analysis Group (IAG) Mission

Mission Statement:

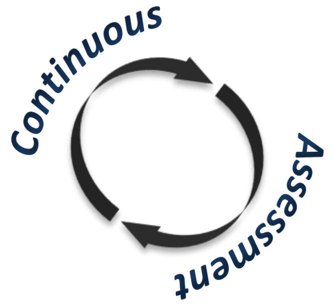
- Deliver actionable acquisition insight to DCMA, DoD senior leadership, and the national critical infrastructure community by continuously ***analyzing industrial capabilities*** and ***identifying strategic risks*** with recommended solutions through a ***Mission Assurance (MA) framework*** in order to ensure **Defense Industrial Base (DIB)** industrial capabilities are available to provide the most ***critical goods and services needed by the warfighter***.
- ***Lead*** the execution of DCMA's regulatory responsibility for **national *DIB Sector Mission Assurance***.

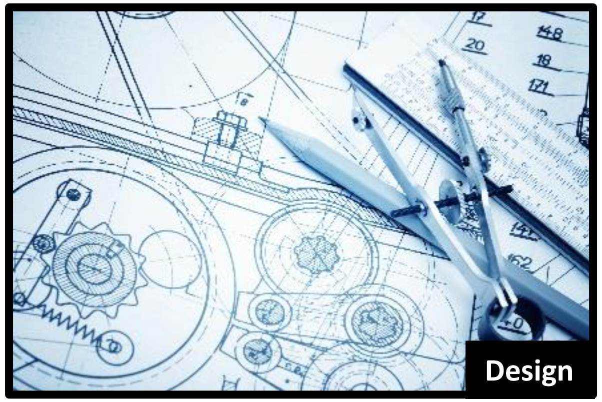
★ **Acquisition Strategy requires Industrial Analysis considerations prior to milestone decisions.**

Major Milestones

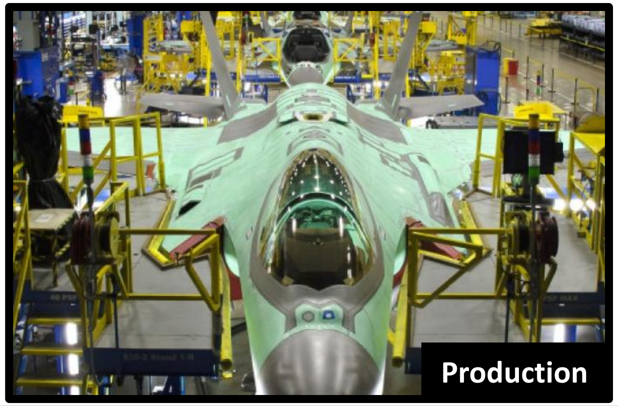
A B C LRIP **FRP** **IOC** **FOC**

Pre-Concept	Materiel Solution Analysis	Technology Maturation & Risk Reduction	Engineering & Manufacturing Development	Production & Deployment	Operations & Support




Design

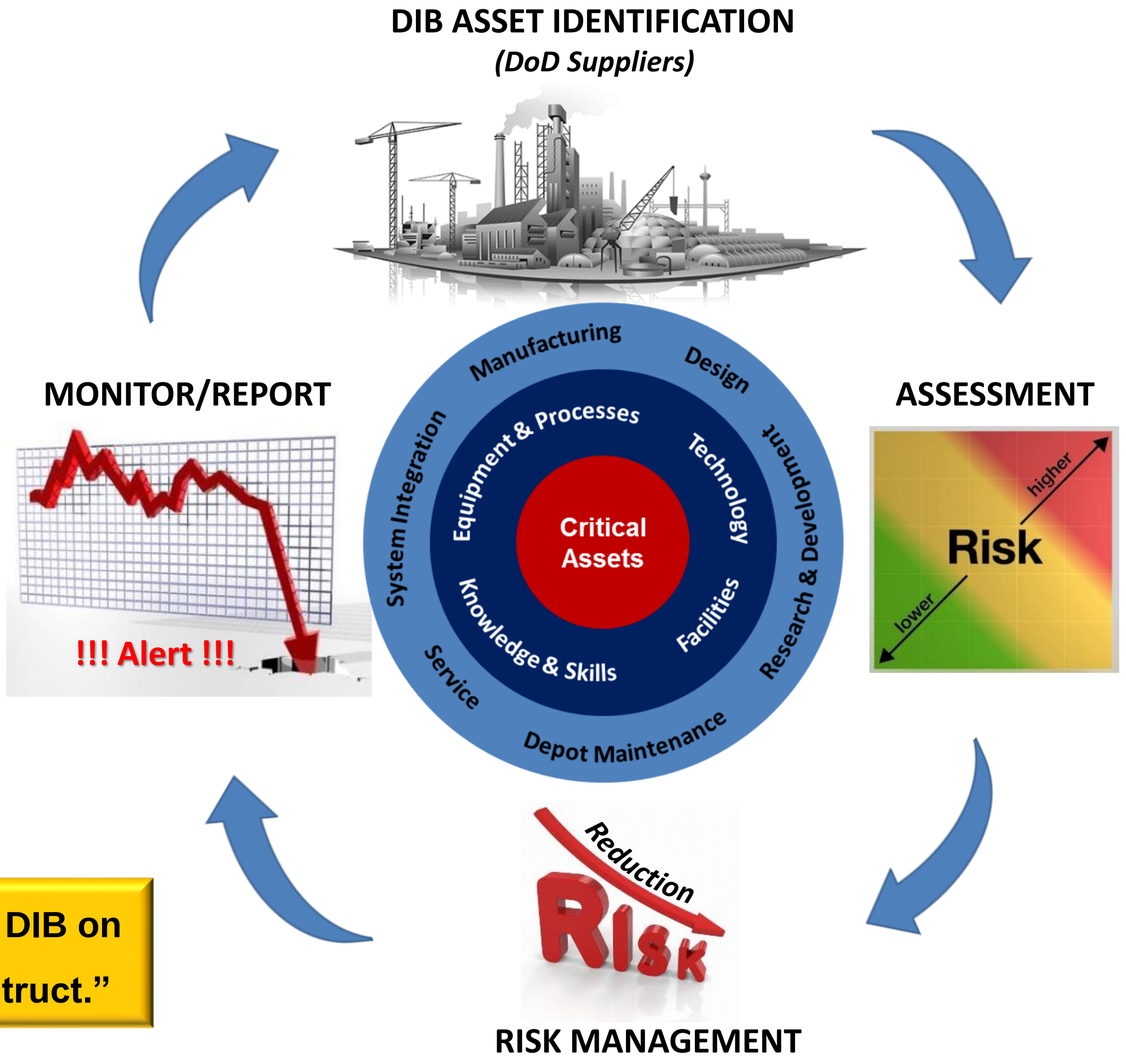

Development


Production


Sustainment

Industrial Analysis Group Mission Impacts

	What IAG Does For DoD
1	DCMA is the lead DoD component for the DIB sector. **Ensures DIB industrial capabilities are available to provide the most critical goods and services needed by the Warfighter.**
2	Executes industrial base assessments in support of statutory and regulatory acquisition program requirements (e.g. **supports Milestone Decisions**). **Feeds DIB MA Process**.
3	**Shares industrial base intelligence** among DCMA, DoD Enterprise, and National Critical Infrastructure community to assist in understanding the DIB, build collective knowledge, assess/manage risk, maintain readiness, and prioritize workload/funding



"Director, DCMA executes assigned national sector responsibilities for the DIB on behalf of the SECDEF and synchronizes these activities with the MA Construct."

~ From DRAFT DoD Instruction 3020.45, "Mission Assurance Construct" (May 2017) ~

Industrial Base Assessments (IBA)

Industrial Base Assessment
(Key Analysis Data Sets)

- Company Profile
- Business Profile
- Product Profile
- Industrial Capabilities
- Critical / Key Sub-tier Suppliers
- Alternate Sources of Supply
- Program Risk (e.g. QA)
- Financial Risk
- Industrial Base Capability Risk

Objective – Determine IB Risk

1. **How important is a capability to DoD (criticality)?**
2. **How likely is it that the capability will be disrupted (fragility)?**

Survey Industry & Gather Data

Manage & Store DIB Data

Analyze & Assess Industrial Capability Risk

Report to Senior Leaders

Why is the Chemical/Material Sector Important?

UNSEEN RISK - these risks are buried within a complex, global supply chain

- ❑ Can be enablers of Key Performance Parameters (KPPs) and U.S. Military strategic advantage
- ❑ Fundamental ingredients - higher probability of impacting a greater number of programs
- ❑ May enable a wide variety of industrial and maintenance processes
- ❑ Chemical sector accounted for 2% of GDP in 2016 (largest contributor in manufacturing)

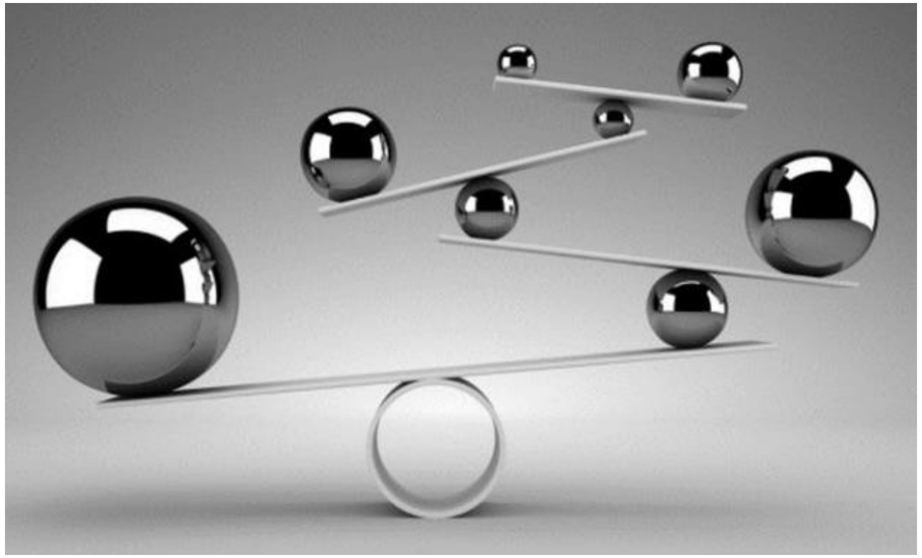
What Risks Can Result from Legislation/Regulation?

MARKET COLLAPSE and Unavailability of Chemical/Material

- ❑ Increased burden on industry
- ❑ Limit competition by increasing barriers to entry
- ❑ Suppress innovation by decreasing design choice
- ❑ Foreign supplier dependency
- ❑ Increased cost of goods & services
- ❑ Program schedule delays
- ❑ Performance issues due to unmanaged substitution

→ Operational readiness impacts

What Can Be Done to Manage Potential Risk?



BALANCE human health risk management with industrial base and mission risk

- ❑ Monitor pending regulatory and statutory changes
- ❑ Proactive industrial base assessment
  - Industry participation is essential
- ❑ Exemptions
  - Support with data (Gov & Industry) to make case
  - DIB capabilities sustained under certain conditions
- ❑ Alternative chemicals/materials or methods
  - Tradeoffs
- ❑ Risk acceptance
- ❑ Develop organic industrial capability

Pilot Assessment Results

OBJECTIVES

- Investigate NMP and MeCl chemical form, DoD purchase quantity, DoD customers, and end users
- Determine supplier fragility and assess criticality for NMP, MeCl, and alternatives
- Evaluate the market impact of the proposed TSCA regulation
- Project the market effect of a national security exemption

POPULATION

61 suppliers surveyed

American Chemistry Council

SELECT FINDINGS

- Air Force is dominant user of MeCl; Air Force and Navy top users of NMP
- Most common purchase form is a mixture containing MeCl or NMP
- At least 17 MDAPS supported; aviation heavy
- Common defense applications: paint removal, cleaning, coating reapplication
- Market impact if TSCA restrictions are put in place:
  - Some indicated they'd be out of business (incl. dominant DoD source)
  - DoD sales are insufficient to maintain overall business
  - Some indicated they would exit market (incl. dominant DoD source)
  - Others (perhaps more diversified) indicated minimal to no impact

CONCLUSIONS

- Industry participation was poor
- DoD demand is minimal compared to overall NMP/MeCl production
- Current industrial capability risk is LOW (there are many active suppliers)
- Alternatives exist, but are less effective and Services are hesitant to adopt. Recommend Joint, comprehensive trade-off assessment
- TSCA regulation likely to result in market correction and immediate DoD impacts; formation of defense unique niche market dependent on foreign market viability
- National security exemption might not prevent market collapse in this situation due to commercial demand dominance

Degrees of Potential Market Collapse Due to Regulation

Defense Unique Niche Market Stabilized by Foreign Demand

- DoD demand is small fraction of commercial demand
- Exemption is in place to allow U.S. defense uses of chemical
- *Foreign markets have less regulation and remain profitable*

IMPACT: Supplier market correction, but capabilities will remain. May see off-shoring of industrial capabilities.

Defense Unique Niche Market

- DoD demand is small fraction of commercial demand
- Exemption is in place to allow U.S. defense uses of chemical
- *Foreign markets are not profitable*

IMPACT: Major supplier market correction. Capabilities will be sustained by Government investment. Limited number of suppliers (IB risk).

Market Collapse

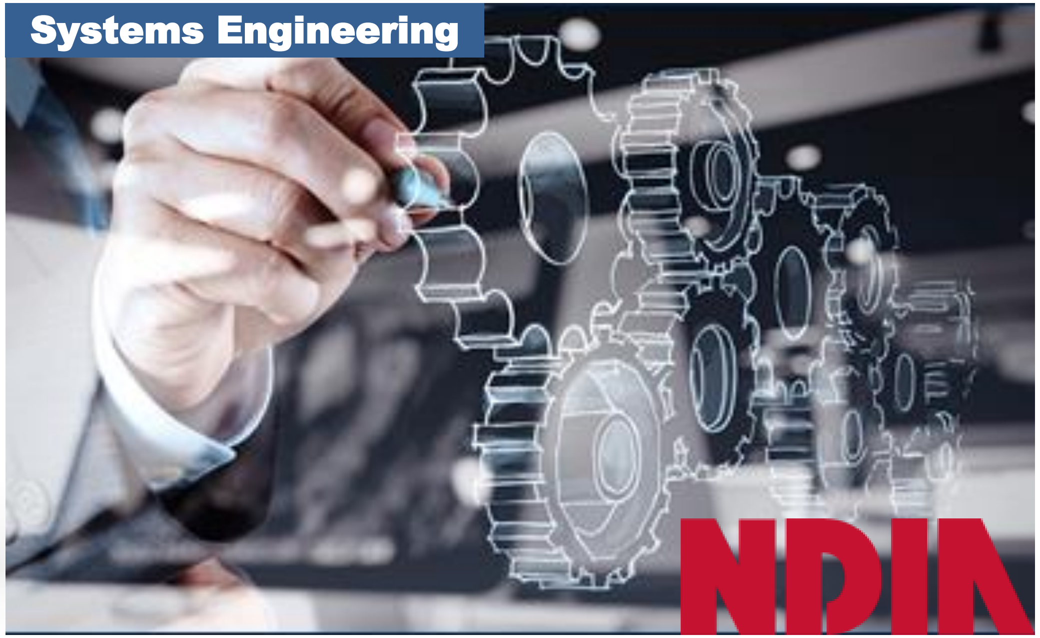
- DoD demand and Government investment is not incentive enough
- Domestic and Foreign markets are not profitable

IMPACT: Capability loss (operational risk)

When Is a National Security Exemption Effective?

Potential Conditions for Stabilizing Industrial Capability Using an Exemption:

- ❑ Criticality
- ❑ Minimum Sustainment Rate (MSR)
- ❑ Product diversity
- ❑ Defense vs. commercial demand distribution
- ❑ Competition
- ❑ Foreign market viability
- ❑ Timeline
- ❑ Alternative solution



Thank You

Air Force Materiel Command

Software Development Challenges in AFMC (Agile Software Development and Data Rights)

Abstract # 19902

25 Oct 2017

Dr. Marc Shaver, HQ AFMC/ENS
Mr. Andrew Jeselson, HQ AFMC/ENS
Mr. Curtis Jefferson, AFLCMC/EZAS

Breaking Barriers … Since 1947

Outline

- Introduction (Dr. Marc Shaver)
- HQ AFMC/EN ASD Questionnaire Results (Mr. Andrew Jeselson)
- AFLCMC/EN-EZ Agile Software Development (ASD) Workshop (Mr. Curtis Jefferson)
- AFLCMC/EN-EZ SW Data Rights Strategy Process (Mr. Curtis Jefferson)

Introduction

- **The Air Force Engineering Enterprise led efforts identifying knowledge, skills, and process gaps within the workforce**
- **Two software related topics were:**
  - **Awareness of Agile, Flexible SW Development & Sustainment Methodology to include Agile SW Development (ASD)**
  - **Software Data Rights Strategy process**
- **AF Life Cycle Management Center (AFLCMC), with AF Materiel Command (AFMC) support, leading efforts to address these topics**
- **A key initial outcome of these efforts is the requirement to develop education and training for the engineering workforce**
  - **Education will capitalize on existing DAU and other courses providing basic understanding of ASD and Data Rights**
  - **Focus on AF unique practices, processes, and tools**
  - **Initial concepts under development**

Background

- **ASD**
  - **Well understood and widely used commercially and, in DoD Information Technology (IT) and Business System applications**
  - **DoD weapon system acquisition now moving to apply ASD**
    - **No standard DoD weapon system specific ASD methodology or training**
  - **AFMC Engineering Council tasked AFMC/EN to study ASD to define scope and types of ASD employed and associated training**
  - **AFLCMC also interviewed programs to gather ASD lessons learned and best practices**
  - **AF pursuing weapon system specific ASD education addressing:**
    - **Implementation approaches, barriers and enablers, weapon system specific ASD challenges/problems/successes, and other management considerations**

Background (con't)

- **Software Data Rights Strategy**
  - **Data rights vital for life cycle management**
  - **Programs need to carefully consider appropriate Software Data Rights, especially related to sustainment, early in program's lifecycle**
  - **AFLCMC/EN-EZ developed a standard process for producing an Intellectual Property (IP) Strategy for Weapon System Software**
  - **Repeatable process that produces SW Data Rights strategy**
    - **Provides consistent approach for identification, justification, and documentation of the program's SW data rights; and assures persistence of the software data rights procured over program life cycle through early and continuous participation of government organic SW support agencies**
  - **AFLCMC has codified the SW Data Rights Strategy as a standard process**

Agile Software Development (ASD) Questionnaire

Background

- ASD has existed for decades for commercial and some DoD IT and Business System applications -- commercial training is available
- DoD weapon system acquisition and sustainment efforts are now applying ASD, however, there is no weapon system specific ASD training available to address unique DoD ASD applications

Issues

- ASD Training Action Item was assigned at 25 Feb 16 AFMC Engineering Council (EC) to:
  - ID programs/efforts that are using ASD Methodologies
  - ID ASD Training Needs & Gaps
- Stood-up cross-Center ASD SME team: EC members assigned SMEs for their Center
- ASD Questionnaire sent to cross-Center ASD SME team

Bottom Line

- 17 Nov 16 EC: Received ASD Training Questionnaire responses from cross-Center ASD SME team members. HQ AFMC/ENS and AFIT/LS personnel reviewed, consolidated, and analyzed the responses. The results indicate there is a pervasive need for ASD, and especially SCRUM training. The responses helped determine ASD Training Needs/Gaps and support development of Air Force ASD Training Plan.

- Upon your request, the ASD Questionnaire can be delivered to you
  - Contact Mr. Andrew Jeselson, HQ AFMC/ENS, andrew.jeselson@us.af.mil

HQ AFMC/EN ASD Questionnaire
Samples of Data Collected

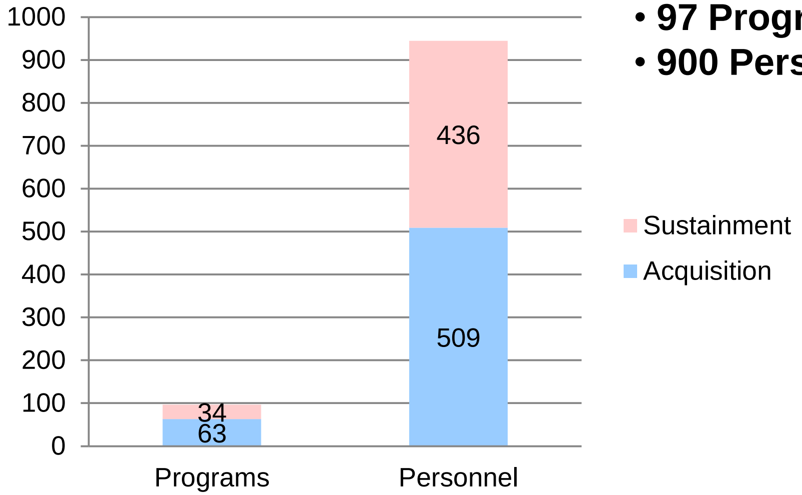
Data Collected

- Program identification data
- Type of ASD employed
- Current training expenditures
- Future training requirements

Center	Program Name	Kind of Program	Program Phase using ASD: MSA	TD	EMD	PD	OS	Type of ASD	Total # Personnel	Training Offered	Training Needed	Current Expenditures
[illegible]	JWS	Business/IT					X	Scrum	0	N	Y	
	F-22	ACWS					X	Safe	20	Y	Y	
	[illegible]	[illegible]					X	Scrum	?			
	B-2	ACWS					X	Cont Integration	?			
	CRH	Weapon System			X			Scrum	?			
	[illegible]	ACWS					X	Scrum	[illegible]			
AFSC 76 SMXG Tinker AFB	[illegible] Mission Planning	Development/Maintenance					X	Scrum	[illegible]	Y	N	$ 5,000
	B-1 Mission Planning	Development/Maintenance					X	Scrum	12			
	76 SMXG Tools	Development/Maintenance					X	Scrum	21			
AFTC/[illegible]	TBA-FAAB	Business/IT application program					X	SCRUM	4	Y	N	$ 13,000
	TBA-[illegible]	Business/IT application program					X	SCRUM	4			
	TBA-FMR	Business/IT application program					X	SCRUM	4			
	TBA-JM[illegible]	Business/IT application program					X	SCRUM	[illegible]			
	COOL	Operations center program					X	SCRUM	3			
	TBA-MRTFB	Business/IT application program					X	SCRUM	4			
AFRL/ RX	ICE – Integrated Collaborative Environment	Laboratory Program – for internal use	X					Scrum, RUP, Kanban, Extreme Programming	3	N	Y	

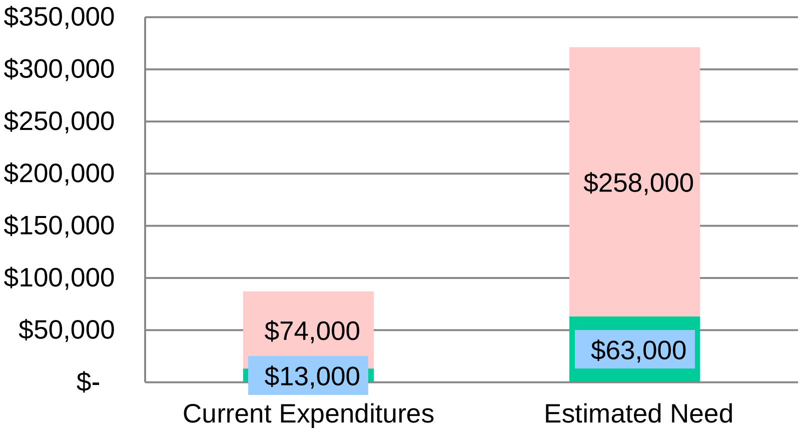
HQ AFMC/EN ASD Questionnaire Results

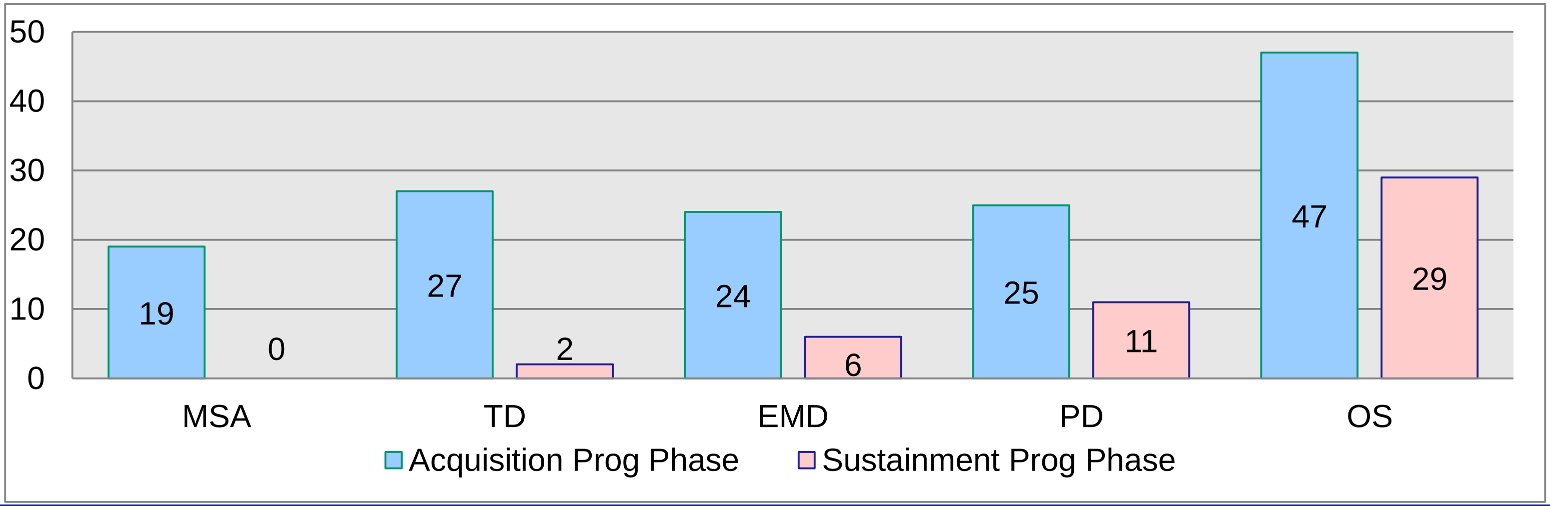
Personnel and Programs



- 97 Programs
- 900 Personnel (Est)

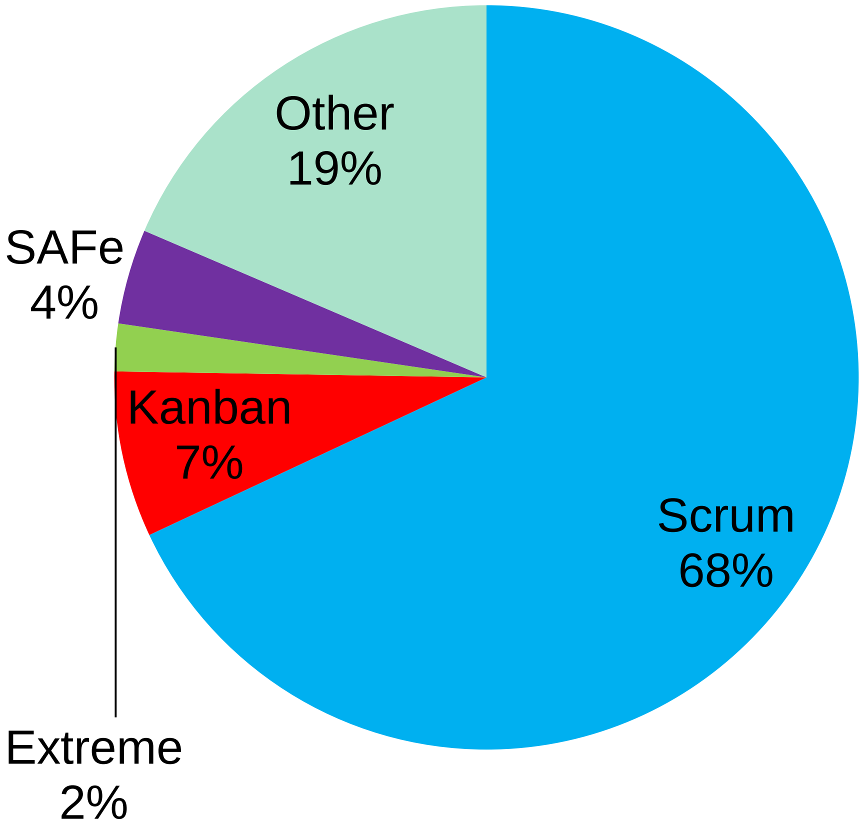
Agile Training Reported Funding





HQ AFMC/EN ASD Questionnaire Results (con't)

ASD Techniques in Use



Assessment:

- Many Air Force organizations are pursuing their own education
- AFMC has a need for enterprise level agile education
- AFIT/LS assisted with gap analysis and ASD course development
- More educational gap analysis is required; however, some tailored courses are likely to be needed
  - SMC/EN funds a Software Engineering Institute (SEI) ASD for Government programs course for SMC ASD training
  - AFLCMC/EN-EZ is developing an ASD workshop

AFLCMC/EN-EZ Agile Software Development (ASD) Workshop

Guidance For Agile Avionics SW Development

How do I apply software engineering in an ASD environment?

How do can I support the PM's needs?

How can I track development progress in terms of functionality (Value!)?

How can I handle early discovery of issue?

How should I communicate with the contractor

How can I include the customer (e.g. war fighter, flight test, operational test, etc.)

How can I track development progress in terms of SWE (e.g., moving data throughout the SW system)?

Metrics!

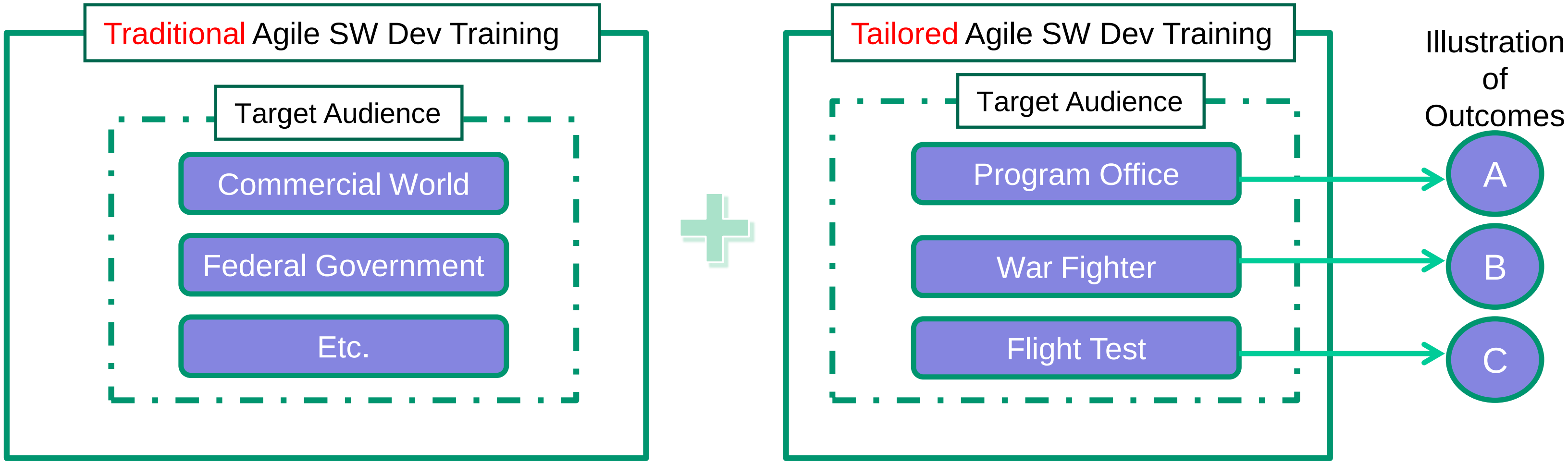
Guidance For Agile Avionics SW Development

- **Issue**
  - **Lack of guidance to help AF POs incorporate/transition agile SW procedures into the acquisition process**
    - **How to meet the intent of the of AFI 63-101**
    - **How to satisfy requirements of other processes (i.e., EVM)**
  - **Industry has pushed agile based SW development processes**
- **Goal**
  - **Establish agile aircraft systems SW development guidance & training focused on needs of the PO personnel**
  - **Establish best practices**
  - **Guidance on technical reviews**
  - **Understanding elements that impact cost, schedule, & performance**
  - **Etc.**

Agile Avionics SW Development

- Status
  - Commenced active participation in the Software Engineering Institute Agile Collaboration
  - Active membership in the NDIA Agile Working Group
  - Continuous involvement in the F-22 implementation of Scaled Agile Framework
  - Working with AFMC/ENS, SEI, and AFIT to establish training focused on the needs of the personnel in the imbedded avionics systems programs
    - Material based on best practices and lessons learned from participation in the above working groups and observations from F-22, B-2, F-15, and other programs
    - Including updated materiel in existing focus week training

Develop Training Tailored for DoD Aircraft Programs



A

- **Illustration of agile tents aligned with DoD System Engineering**
- **Sample metrics to track SW development progress**
- **Approach to satisfy earned value management requirements**
- **Subset of documents generated for government accountability**
- **Early sustainment posture**
- **Etc.**

B

—**Expected role, availability . . .**

—**Etc.**

C

—**Examples of impacts to flight testing**

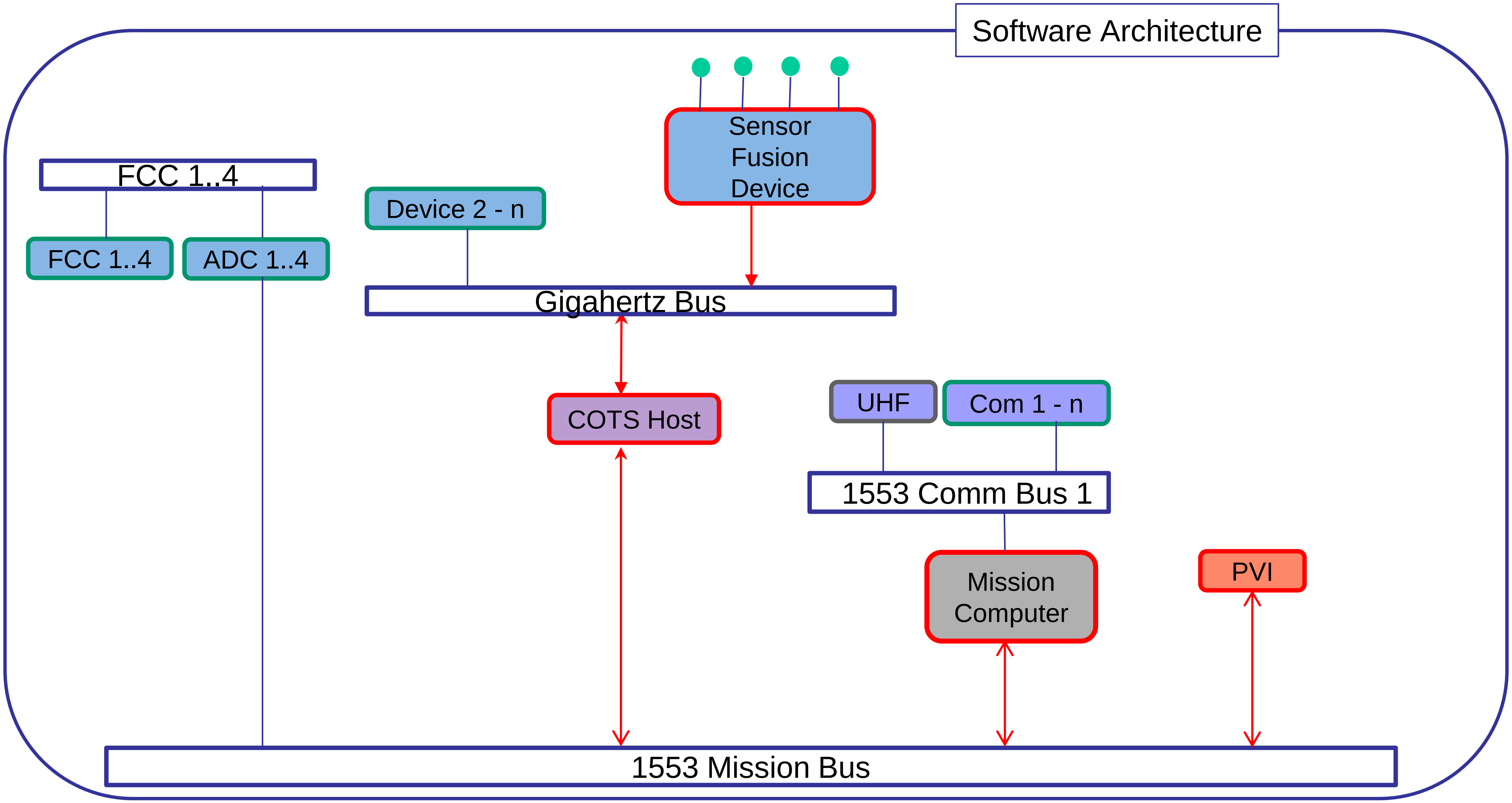
—**Etc.**

AFLCMC/EN-EZ SW Data Rights Strategy Process

Improve Acquisition of SW Data Rights

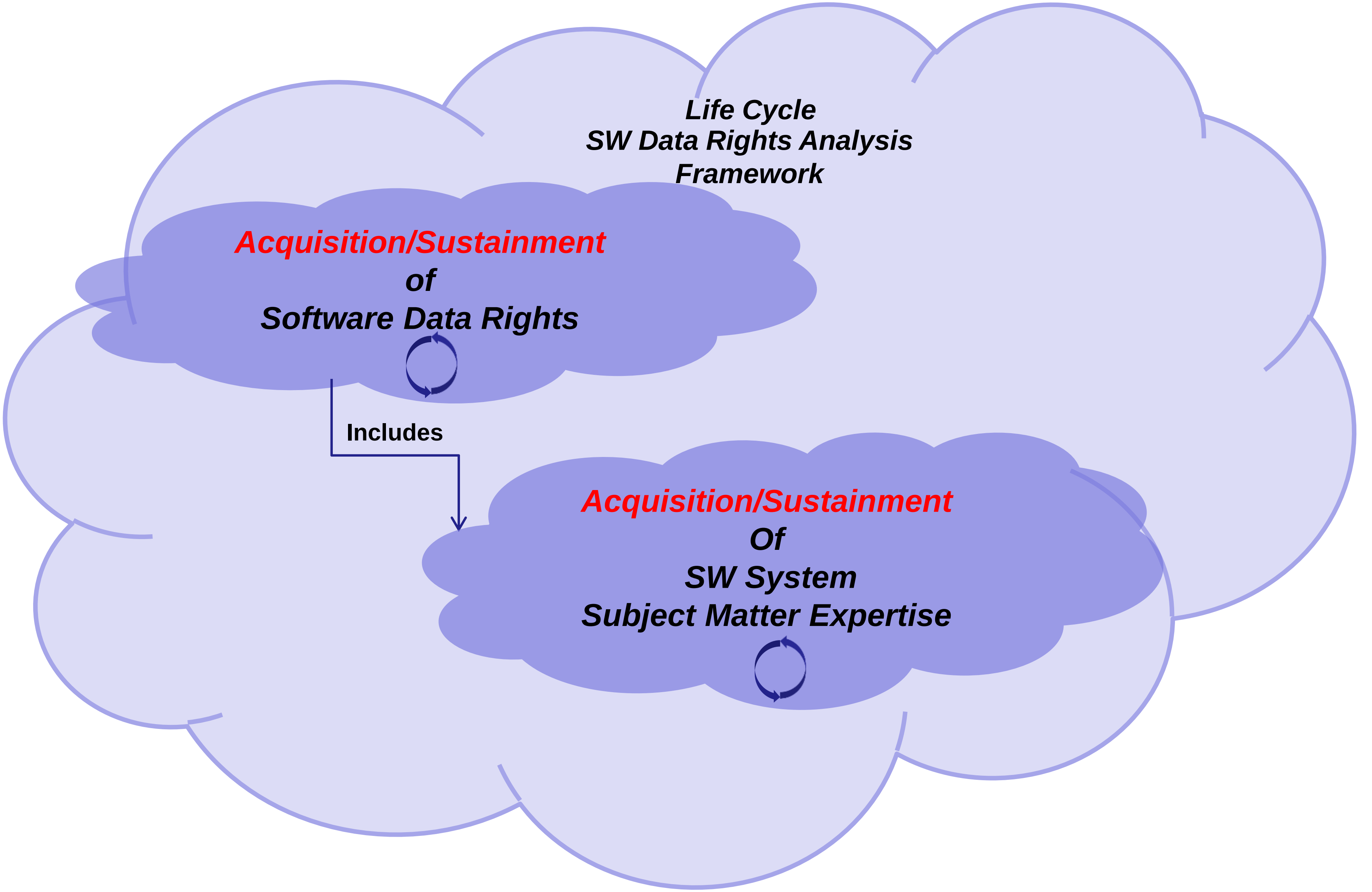
- Issue
  - Non-availability of program SW data rights for sustainment – assertion supported by:
    - 2011 AF Studies Board & Scientific Advisory Board reports
    - Table top discussions with 10 plus AFLCMC programs
      - No analysis executed to ID appropriate SW data rights
- Goal
  - Develop standard engineering analysis framework designed to ID, acquire, document, & retain appropriate SW data rights
    - Framework to include provisions for timely acquisition of government subject matter expertise congruent with utilization of acquired SW data rights
    - Cross organizational involvement (LCMC & AFSC) critical
    - Framework tenets included as part of core competency

SW Data Rights Analysis Example: Isolate Mission Thread



SW Data Rights Analysis Example: Analyze Thread Elements

LRU/ICD	Sensor → Sensor Fusion Device	ICD	COTS Host	ICD	Mission Computer	ICD	PVI
Expected Change Rate	Low	Low	Low	Low	High	Mod	High
Gov't **Development** Funded	0%	100%	0%	100%	100%	100%	100%
SW Type	Complex Algorithm	N/A	COTS SW	N/A	OFP	N/A	OFP
…							
Expected Rights	Restricted	Unlimited	COTS SW	Unlimited	Unlimited	Unlimited	Unlimited
Needed Rights	TBD	GPR	COTS SW	GPR	GPR	GPR	GPR
Current Rights	Restricted	GPR	COTS SW	GPR	GPR	GPR	GPR
Comments	Needed rights pending analysis of winning bid	See fusion device			Organic Support	Organic Support	Organic Support


Life Cycle
SW Data Rights Analysis
Framework
Acquisition/Sustainment
of
Software Data Rights
Includes
Acquisition/Sustainment
Of
SW System
Subject Matter Expertise

Training

- Focus Week course
- Course material developed via SEI
- AFIT course in works

Questions?

Dr. Marc Shaver
HQ AFMC/ENS
(937) 257-5621
marc.shaver.4@us.af.mil

Mr. Andrew Jeselson
HQ AFMC/ENS
(937) 257-6460
andrew.jeselson@us.af.mil

Mr. Curtis Jefferson
AFLCMC/EZAS
(937) 656-4879
curtis.jefferson@us.af.mil

Elicitation of Quality Agile User Stories Using QFD

NDIA 20th Annual Systems Engineering Conference

“Agile in Systems Engineering“

10:15 – 10:40 AM

October 25, 2017

Sabrina J. Ussery, Shahryar Sarkani, Thomas Holzer

Dissertation Topic

Department of Engineering Management and Systems Engineering
School of Engineering and Applied Science

The George Washington University
1176 G Street NW
Washington, DC 20052

Agile Requirements Engineering (RE)

The lack of standard Requirements Engineering (RE) practices in Agile negatively impacts system quality, contributing to 24% of the causes for challenged or failed projects.

- The 2015 CHAOS Standish Group report indicates Agile projects are 3x more likely to succeed than Waterfall projects due to increased customer collaboration and customer satisfaction. [2]

- The Agile community claims that they do not really tackle requirements in a structured way, which may bring problems to the software organization responsible for software built following an Agile method. [1]

- Though more successful in some respects, the lack of stand RE practices in Agile contributes to 24% of the reasons for challenged or failed projects due to poor requirements quality (i.e., unclear or volatile). [2]

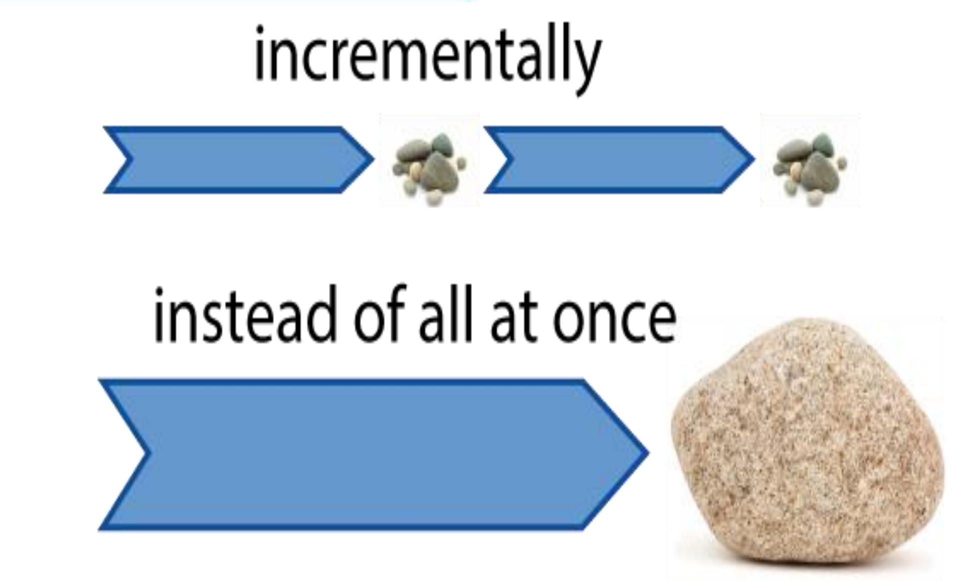
CHAOS RESOLUTION BY AGILE VERSUS WATERFALL

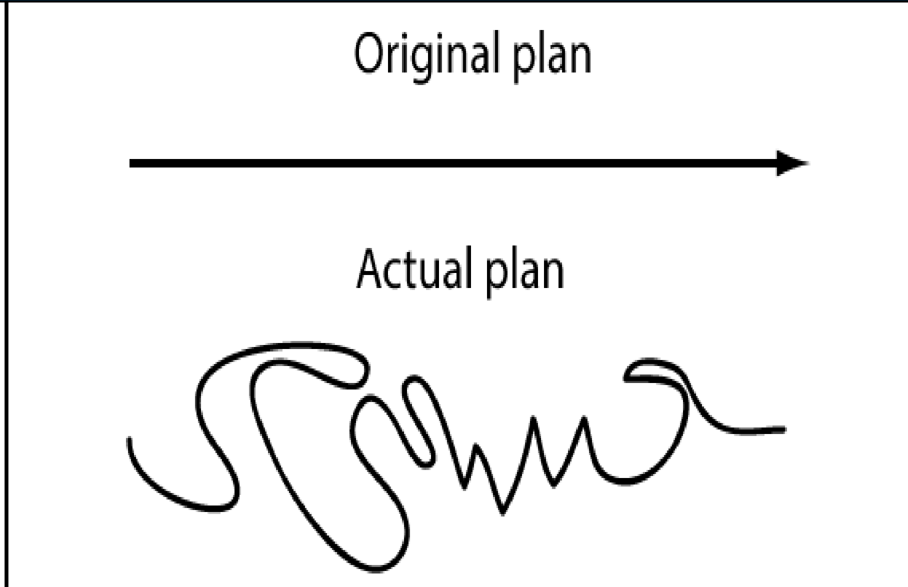
SIZE	METHOD	SUCCESSFUL	CHALLENGED	FAILED
All Size Projects	Agile	39%	52%	9%
	Waterfall	11%	60%	29%
Large Size Projects	Agile	18%	59%	23%
	Waterfall	3%	55%	42%
Medium Size Projects	Agile	27%	62%	11%
	Waterfall	7%	68%	25%
Small Size Projects	Agile	58%	38%	4%
	Waterfall	44%	45%	11%

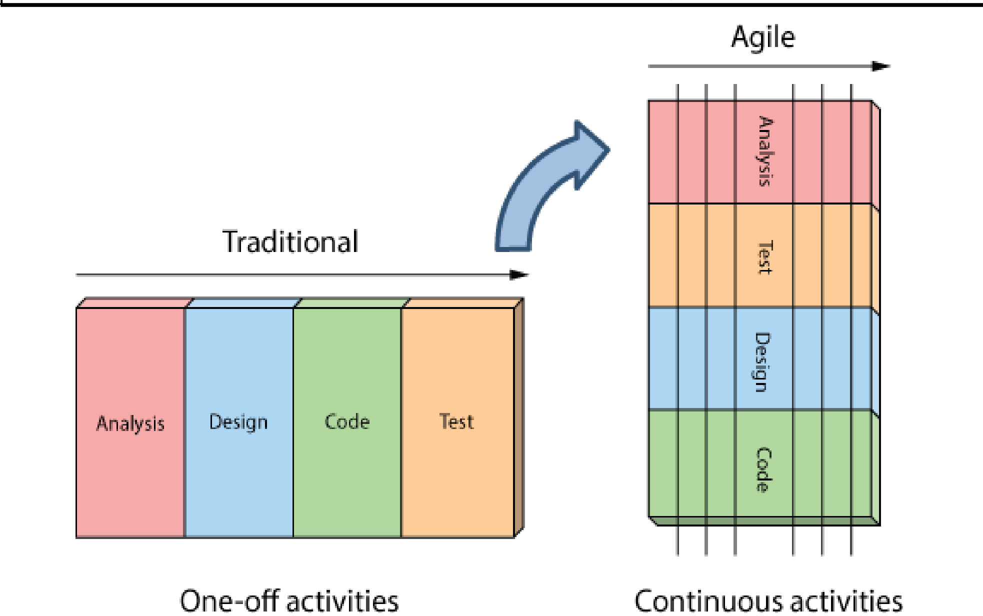
The resolution of all software projects from FY2011–2015 within the new CHAOS database, segmented by the agile process and waterfall method. The total number of software projects is over 10,000.

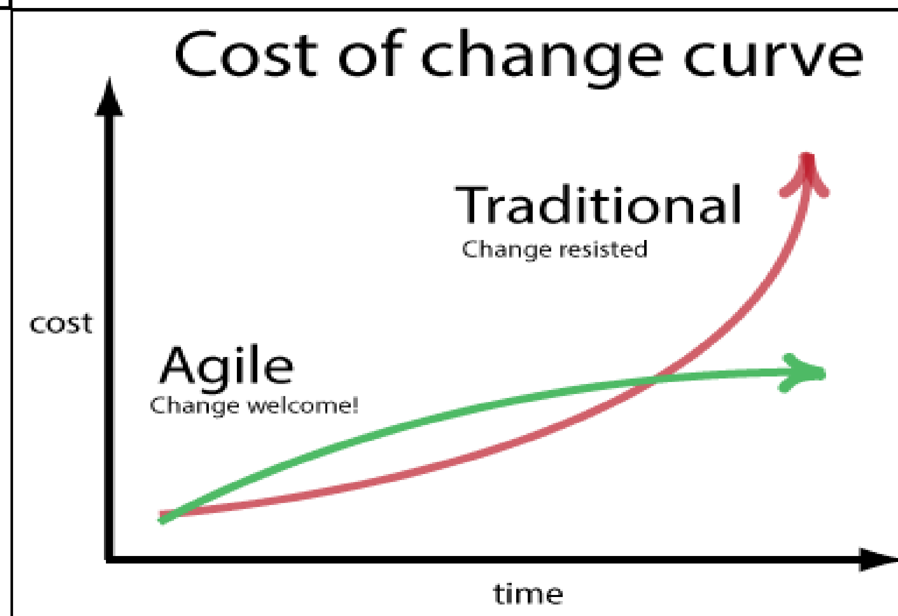
Image source: [2]

What is Agile?

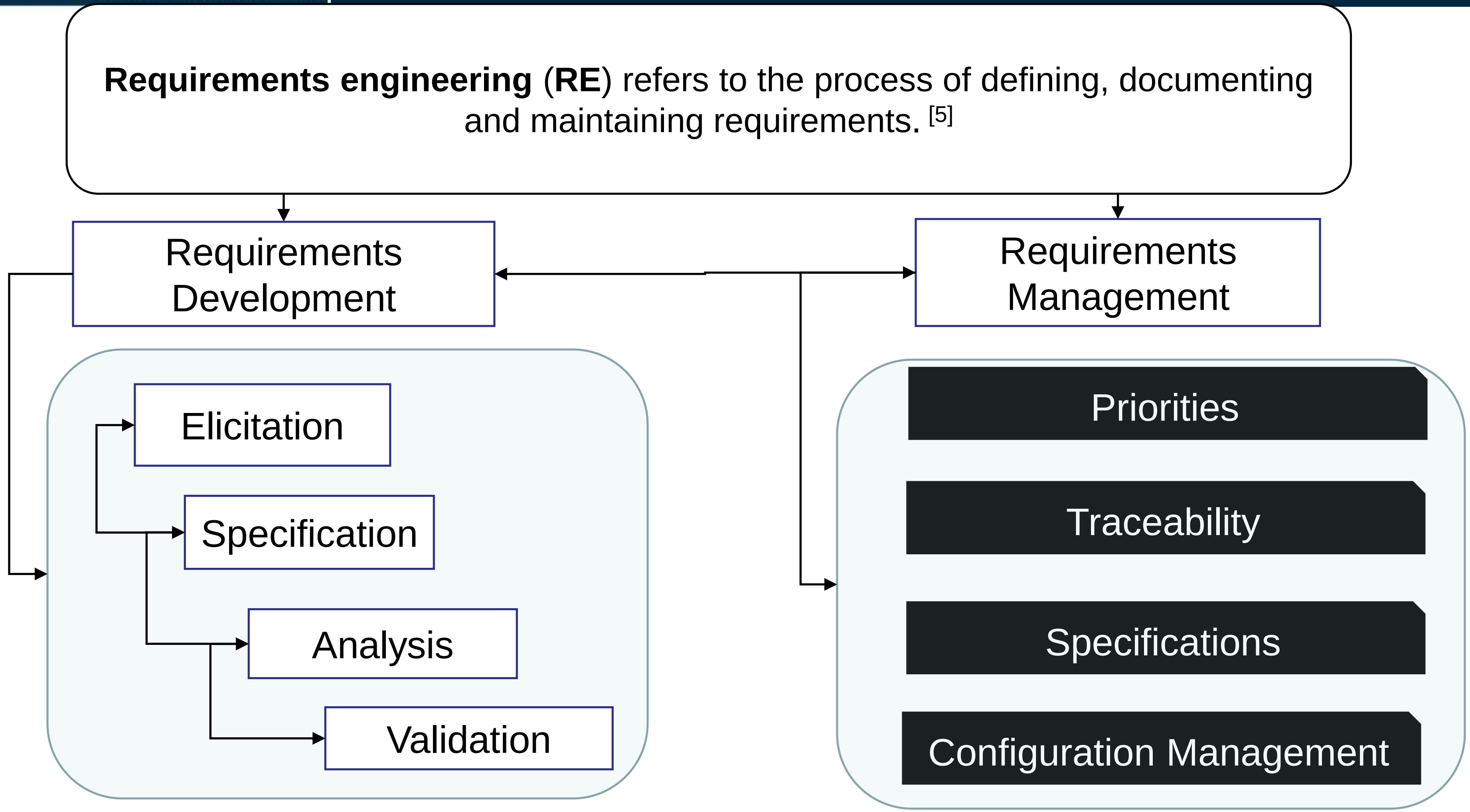






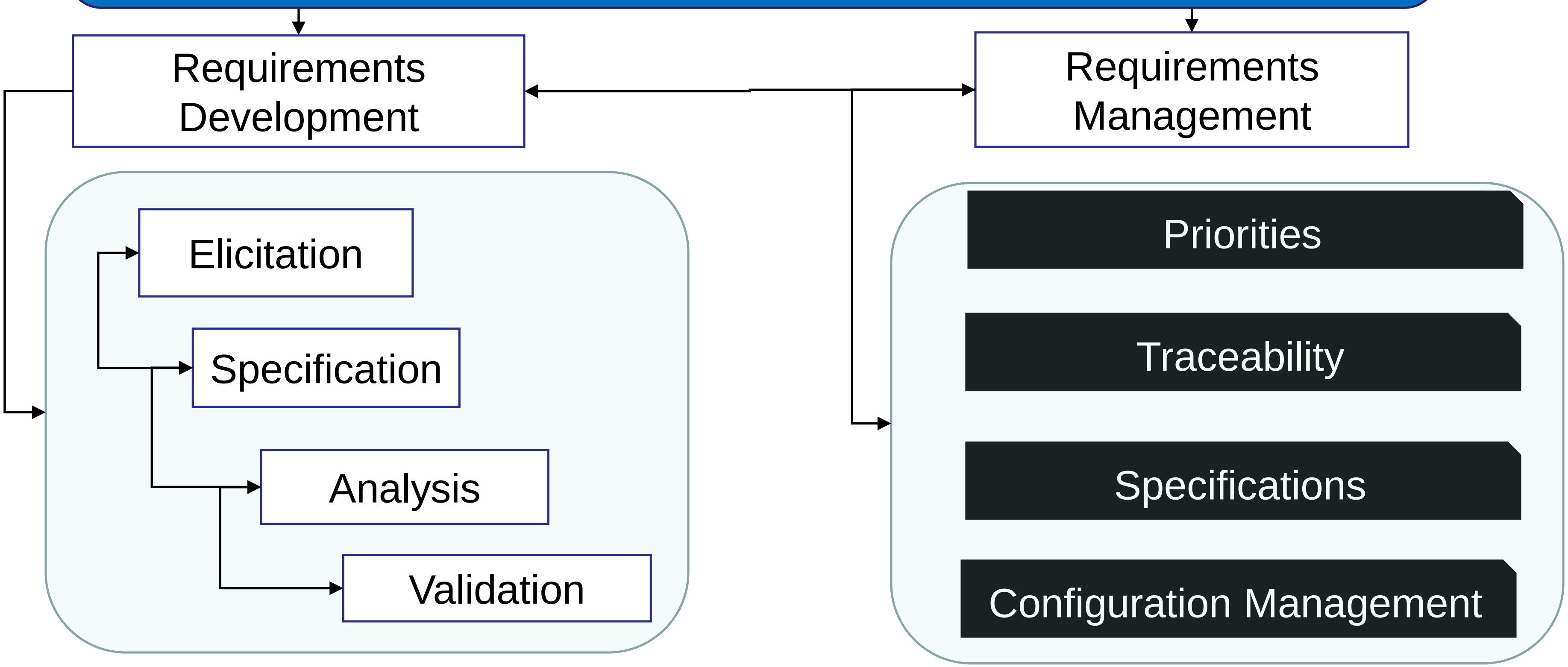


Agile RE: As Is



Agile RE: As Is

"Hall et al., reports that a large proportion (48%) of development problems stem from problems with the requirements. " [3]



Agile RE: As Is

"There are no documented RE activities which can be followed to obtain the user requirement in efficient manner …The Agile manifesto and all the methodologies should have standardized and documented set of RE activities." [3]

"The term 'requirements engineering' is avoided in the Agile community as it is often taken to imply heavy documentation with significant overhead." [4]

"A lengthy requirements analysis phase is considered to hinder the speed of development." [4]

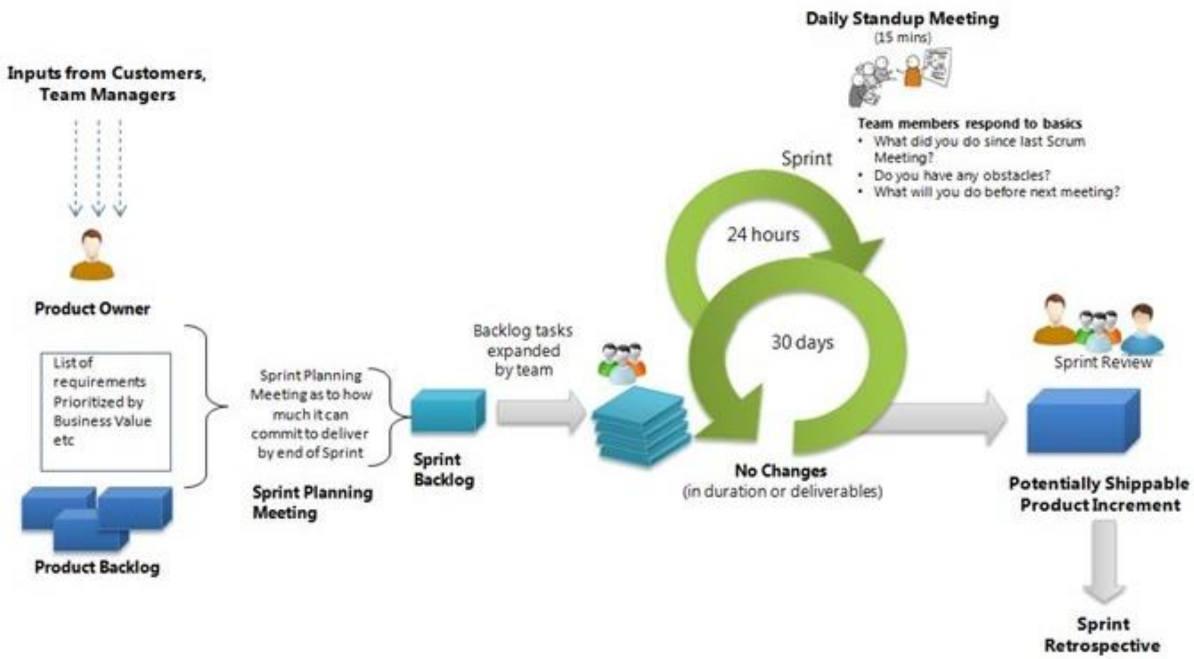


Image source: [28]

Agile RE: As Is

Academic research compares Agile approaches to traditional RE activities and suggests areas of opportunity for improvement.

Table 1. Traditional and agile approach for requirements engineering (RE) activities [4]

RE activities	Traditional RE approach	Agile RE approach	Agile practices used to support the RE activities
Requirements elicitation	Discovering all the requirements upfront	Iterative: requirements evolve over time and are discovered throughout the development process.	Iterative RE Face-to face communication
Requirements analysis and negotiation	Focus on resolving conflicts	Focus on refining, changing and prioritizing requirements iteratively	Iterative RE Face-to-face communication Constant planning Extreme prioritization
Requirements documentation	Formal documentation contains detailed requirements	No formal documentation	Face-to-face communication
Requirements validation	The consistency and completeness of requirements document	Focus on ascertaining whether the requirements reflect current user needs	Review meetings Face-to-face communication

Agile RE: As Is

Academic research surveys Agile approaches to traditional RE activities. Specifically, requirements documentation, stakeholder involvement, and requirements verification are called out as tractable opportunities for improvement.

[4]

Table 3. Characterizing tractability of risks in agile requirements engineering (RE)

RE risk	Agile practice or challenge	Impact of practice or issue	Degree of impact in agile practice	Character of problem
Lack of requirements existence and stability	Face-to-face Iterative RE Constant planning	Mitigates	Medium–High	Tractable
Issues with users' ability and concurrence	Iterative RE Customer access and participation	Mixed	High	Intractable
Inadequate user–developer interaction	Iterative RE Customer access and participation	Mixed	High	Tractable
Overlooking a crucial requirement	Requirement prioritization Review meetings and tests	Mitigates	Medium–High	Tractable
Modelling only functional requirements	Neglect of non-functional requirements	Exacerbates	Low	Intractable

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Agile RE: As Is

These sentiments are shared with other researchers, who also note issues with requirements management. [3] [6] No written documentation results in information loss when code is implemented and refactoring costs skyrocket.

[4]

Table 3. Characterizing tractability of risks in agile requirements engineering (RE)

RE risk	Agile practice or challenge	Impact of practice or issue	Degree of impact in agile practice	Character of problem
Lack of requirements existence and stability	Face-to-face Iterative RE Constant planning	Mitigates	Medium–High	Tractable
Issues with users' ability and concurrence	Iterative RE Customer access and participation	Mixed	High	Intractable
Inadequate user–developer interaction	Iterative RE Customer access and participation	Mixed	High	Tractable
Overlooking a crucial requirement	Requirement prioritization Review meetings and tests	Mitigates	Medium–High	Tractable
Modelling only functional requirements	Neglect of non-functional requirements	Exacerbates	Low	Intractable

Agile RE: As Is

"Stakeholder-appropriate **requirements** constitute critical determinants of **system quality**. Incorrect or missing requirements are supposed to lead to various problems in later phases such as effort and time overrun or an increased effort in acceptance testing. " [7]

[4]

Table 3. Characterizing tractability of risks in agile requirements engineering (RE)

RE risk	Agile practice or challenge	Impact of practice or issue	Degree of impact in agile practice	Character of problem
Lack of requirements existence and stability	Face-to-face Iterative RE Constant planning	Mitigates	Medium–High	Tractable
Issues with users' ability and concurrence	Iterative RE Customer access and participation	Mixed	High	Intractable
Inadequate user–developer interaction	Iterative RE Customer access and participation	Mixed	High	Tractable
Overlooking a crucial requirement	Requirement prioritization Review meetings and tests	Mitigates	Medium–High	Tractable
Modelling only functional requirements	Neglect of non-functional requirements	Exacerbates	Low	Intractable

User Story Issues

Image source: [9]

- Incompleteness (e.g., missing user story parts, business value, or acceptance criteria)
- Ambiguity
- Solution specific user stories
- Missing Non-functional requirements (NFRs)
- Inaccuracy
- Lack of bi-directional traceability leading to refactoring concerns
- Lack of integration with other RE techniques (use cases / user modeling)
- Lacking metadata for configuration management
- No automated support for user story generation [10 – 16]

Agile in Federal Acquisition

- Federal acquisition programs have begun to integrate aspects of Agile development into their strategy to leverage the benefits of Agile.
  - Shorter time to market for innovative solutions, earlier manifestation of system benefits, minimization of rework, and better requirements management.

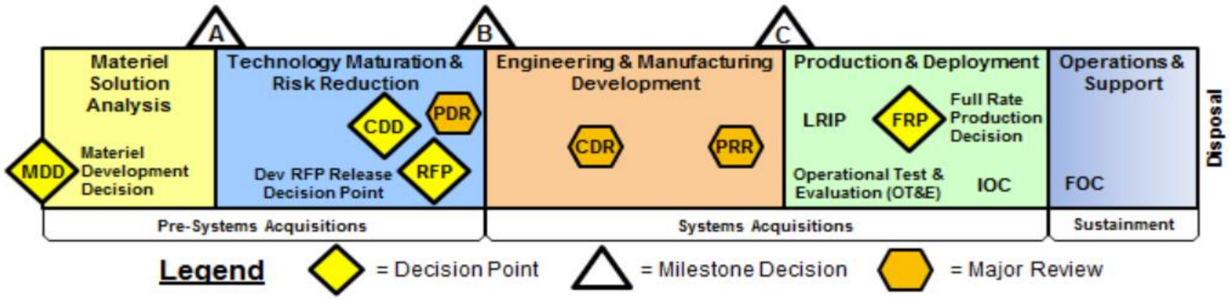


Image source: [26]

- With strong leadership, a well-informed program office, and a cohesive and committed teams, Agile could enable the DoD (and similar organizations) to deliver innovative IT operational solutions faster and more effectively than traditional incremental approaches. [24]

Agile and the DoD

- With an Agile acquisition framework, the DoD can keep deliver capabilities faster and respond more effectively to changes in operations, technology, and budgets.
- The MITRE Defense Acquisition Guide [24] aims to adapt proven principles of Agile development specifically for DoD use and echoes the justification of the research proposed herein by reiterating the need for DoD Agile processes to support the following:
  - Active user involvement in Agile Requirements Engineering activities
  - Accurate, concise, testable and clear user stories
  - Capturing of NFRs in users stories
  - Managing user story dependencies
  - Traceability of user stories to overarching mission threads
  - Development of flexible requirements documentation for approval throughout the acquisition process
  - Configuration Management of documentation as strategies or processes change.

"The US joint force will be smaller and leaner. But its great strength will be that it will be more agile, more flexible, ready to deploy quickly, innovative, and technologically advanced. That is the force for the future."

- Secretary Panetta, Defense Security Review, 5 Jan 12

Call for Research

- Call for complementing Agile RE processes with traditional methods, to strike a balance between project agility and stability [18] [22]
- Call for Agile RE processes and tools that [1] [19]:
    - Are easy to use and not time consuming
    - Supports customer and team collaboration
    - Supports Requirements Elicitation in the user's environment for distributed teams
    - Supports Requirements Management
    - Supports multi-dimensional prioritization
    - Supports automatic creation of user stories and related artifacts
    - Supports elicitation of NFRs
    - Support requirements storage and baselining for system reuse and refactoring
    - Automates verification of user stories to ensure quality before development
        - *Are they complete?*
        - *Are they accurate?*
        - *Are they ambiguous?*
        - *Are they consistent?*
        - *Do they contain data for Configuration Management?*

Abstract of Research Topic

Provide a framework to elicit and manage quality user stories using QFD

- This study evaluates the positive benefits of utilizing Quality Function Deployment (QFD) to elicit, analyze, and manage Agile requirements.
- Prior to this research, RE practices are seen as being incompatible with Agile as they can be heavily reliant on documentation. [25]
- Requirements Engineering is one of the most challenging and important parts of Systems Engineering. The quality of system requirements highly impacts system quality and project health.
- QFD serves as a structured approach to defining and translating customer needs to produce products.
  - Combines quality control with value engineering to fully meet the customer's expectations.
- This study will provide specific recommendations for use of QFD in Agile RE.

QFD

“A simple-but-powerful approach, coupled with a relatively inexpensive process, exists to bring the needed content, structure, organization, weighting and measurements to the decision-making process. Quality function deployment (QFD) is used in a growing number of product development organizations to provide assistance with the planning process. In the last 15 years, QFD has become a standard tool in requirements gathering, analysis and prioritization across all development organizations.” [23]

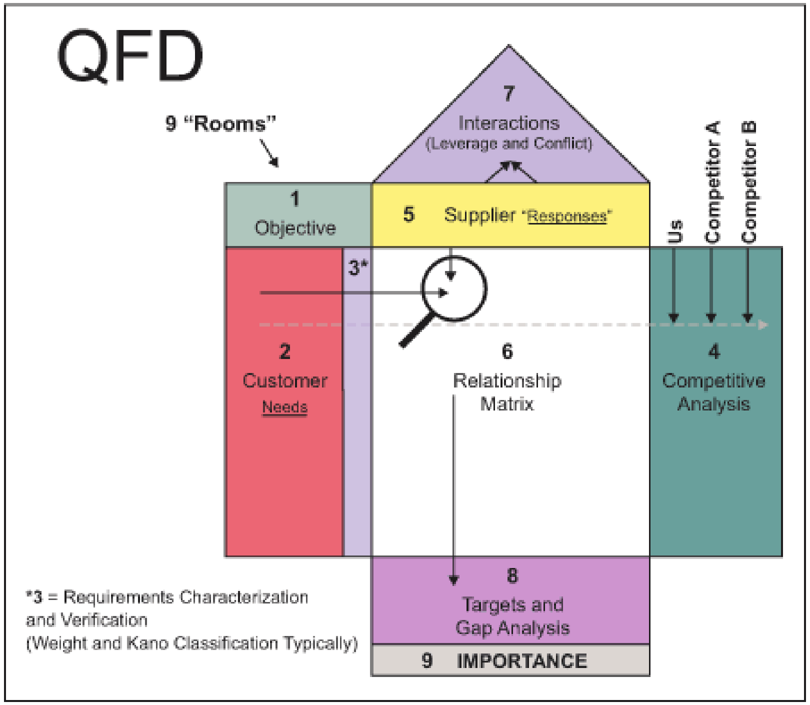
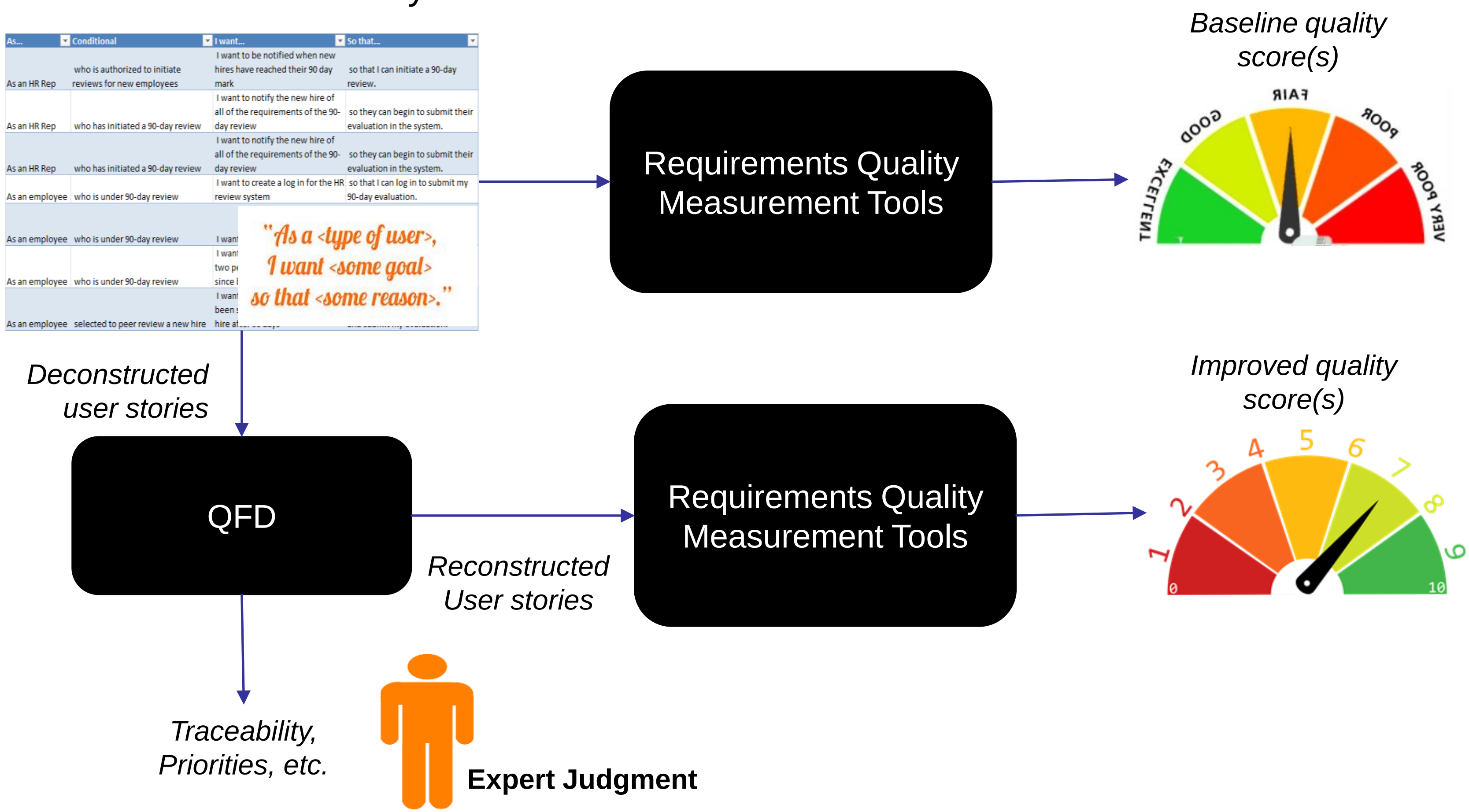


Image source: [23]

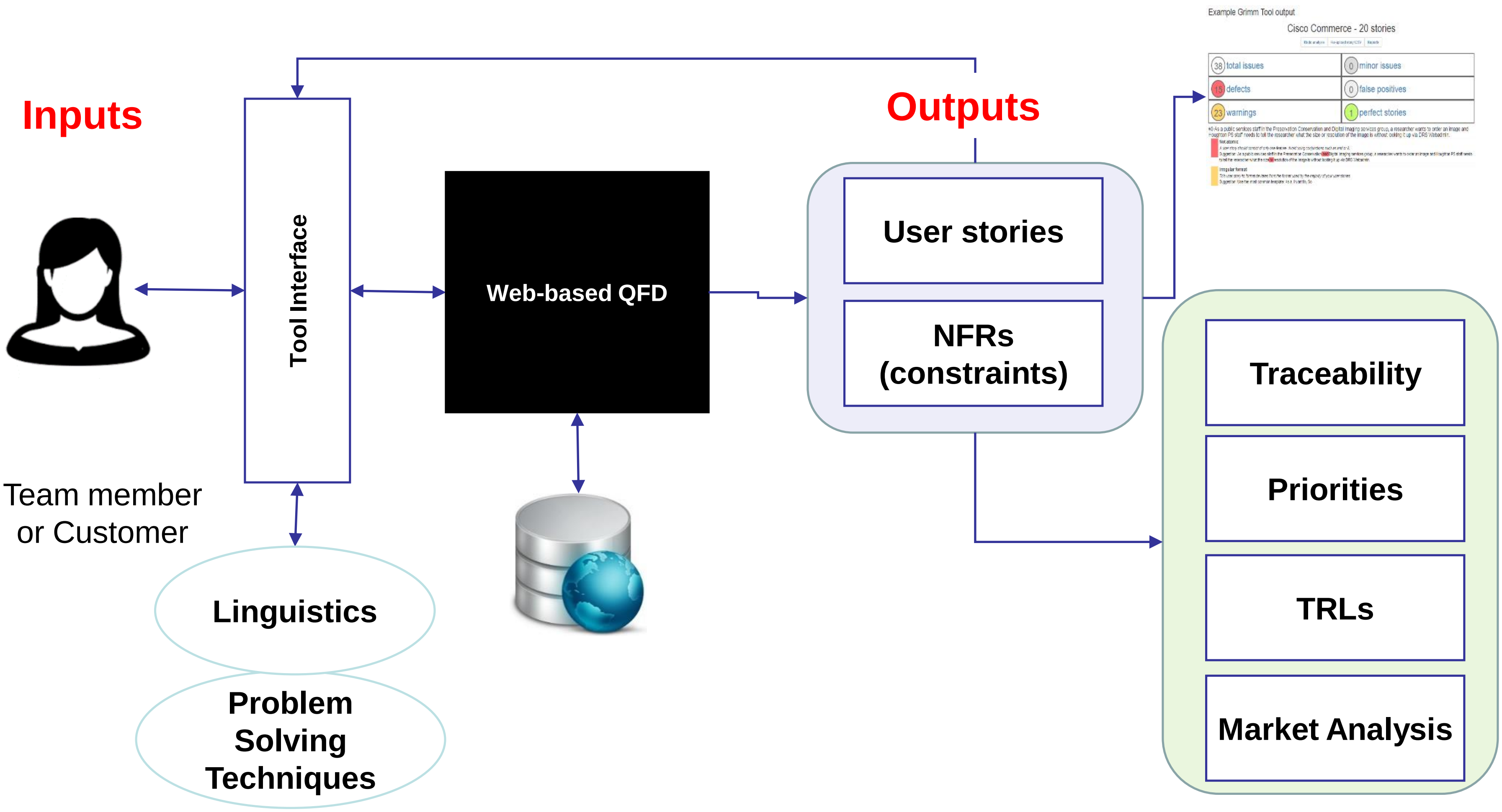
“Product [or system] planning begins with analyzing the performance of an existing product and improving or adding features. QFD can be instrumental in transforming products to meet continually changing customer needs and expectations.” [23]

Data Collection for QFD

For purposes of research, user story data sets (commercial and academic) to be deconstructed and recreated using QFD and quantitatively assessed for quality before and after model use. Inputs for quantitative metrics such as complexity assessments or prioritization will be uniformly randomized.

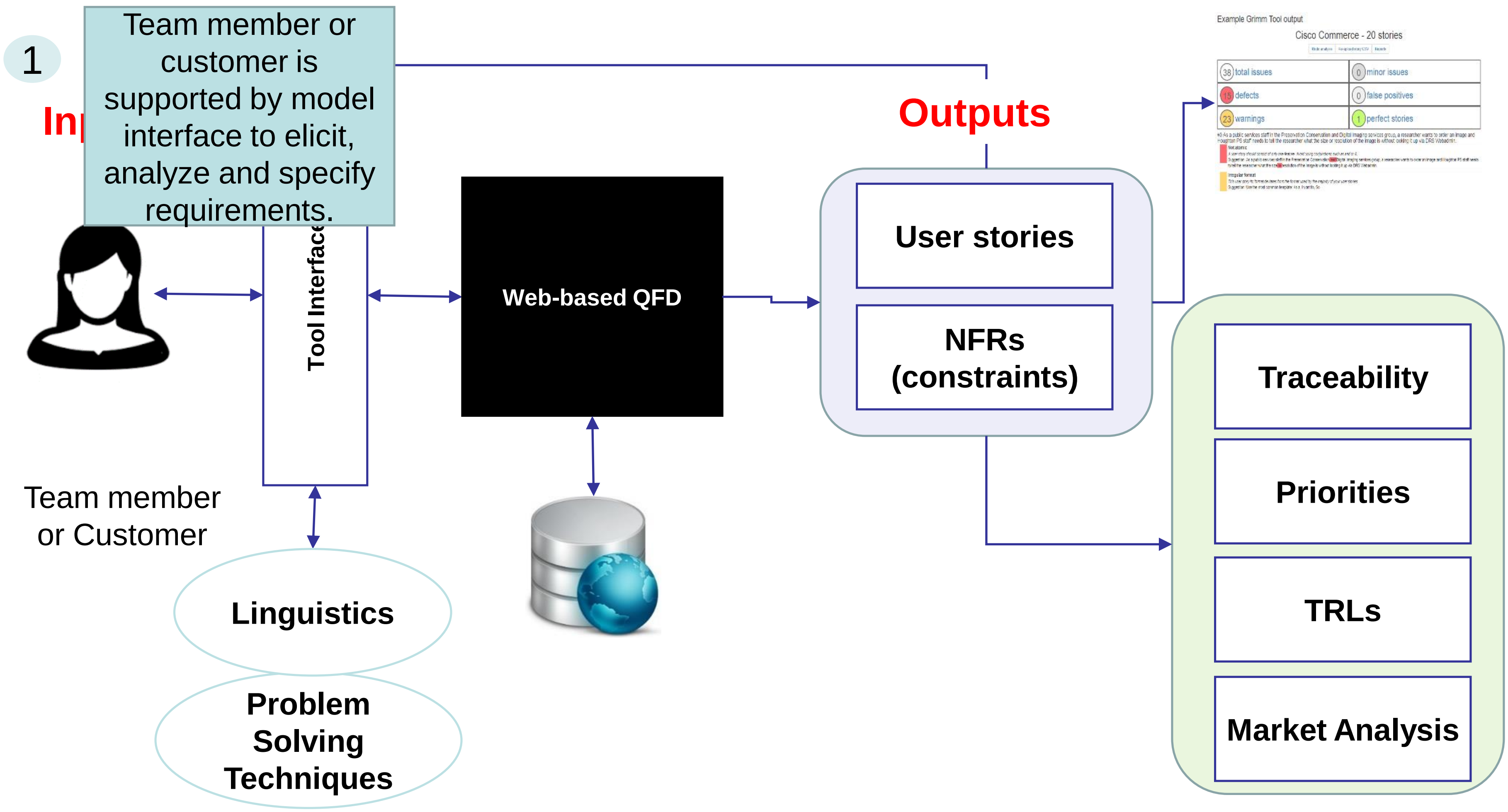


Proposed Model



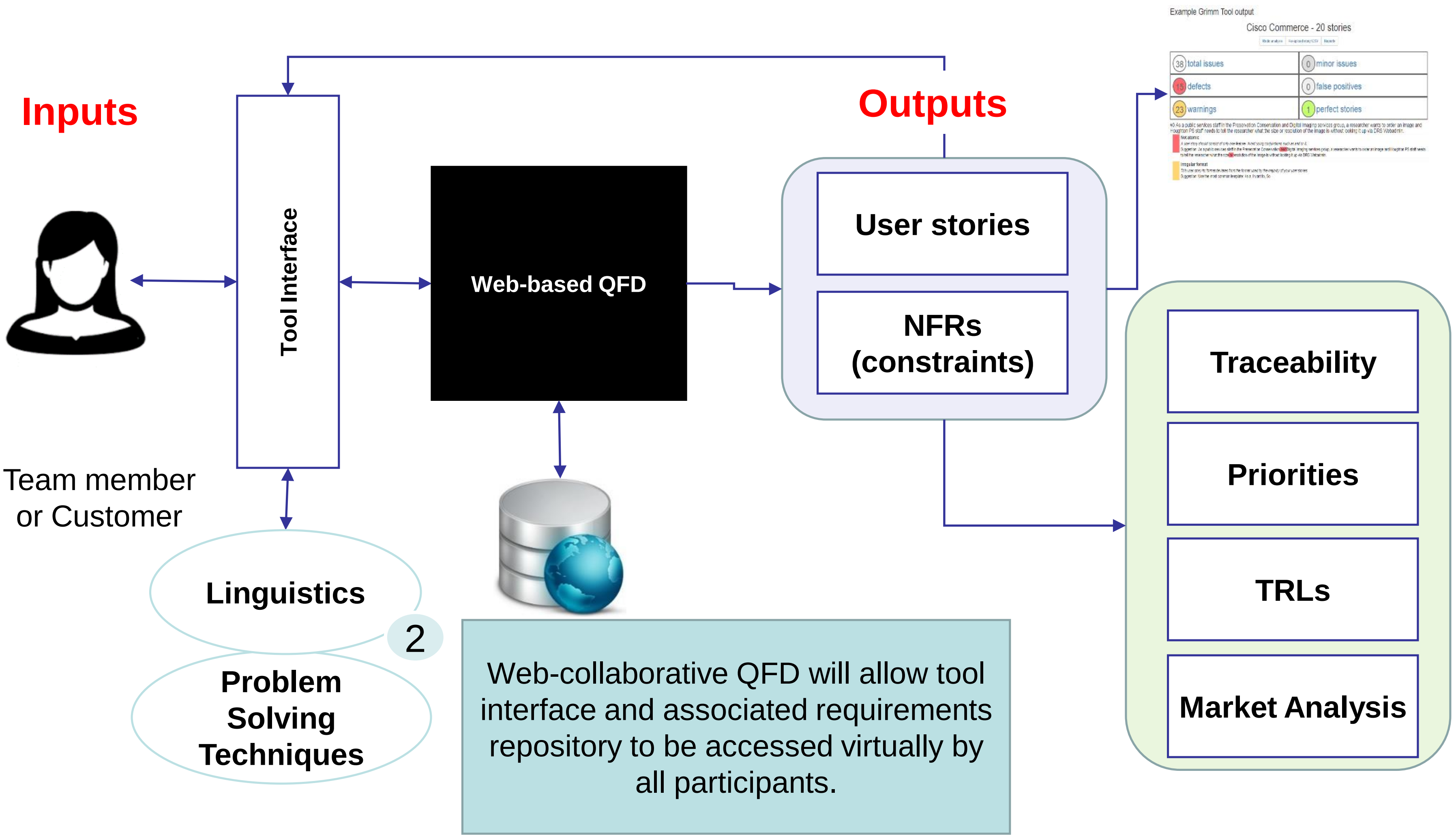
Provide a framework to elicit and manage quality user stories using QFD

Proposed Model



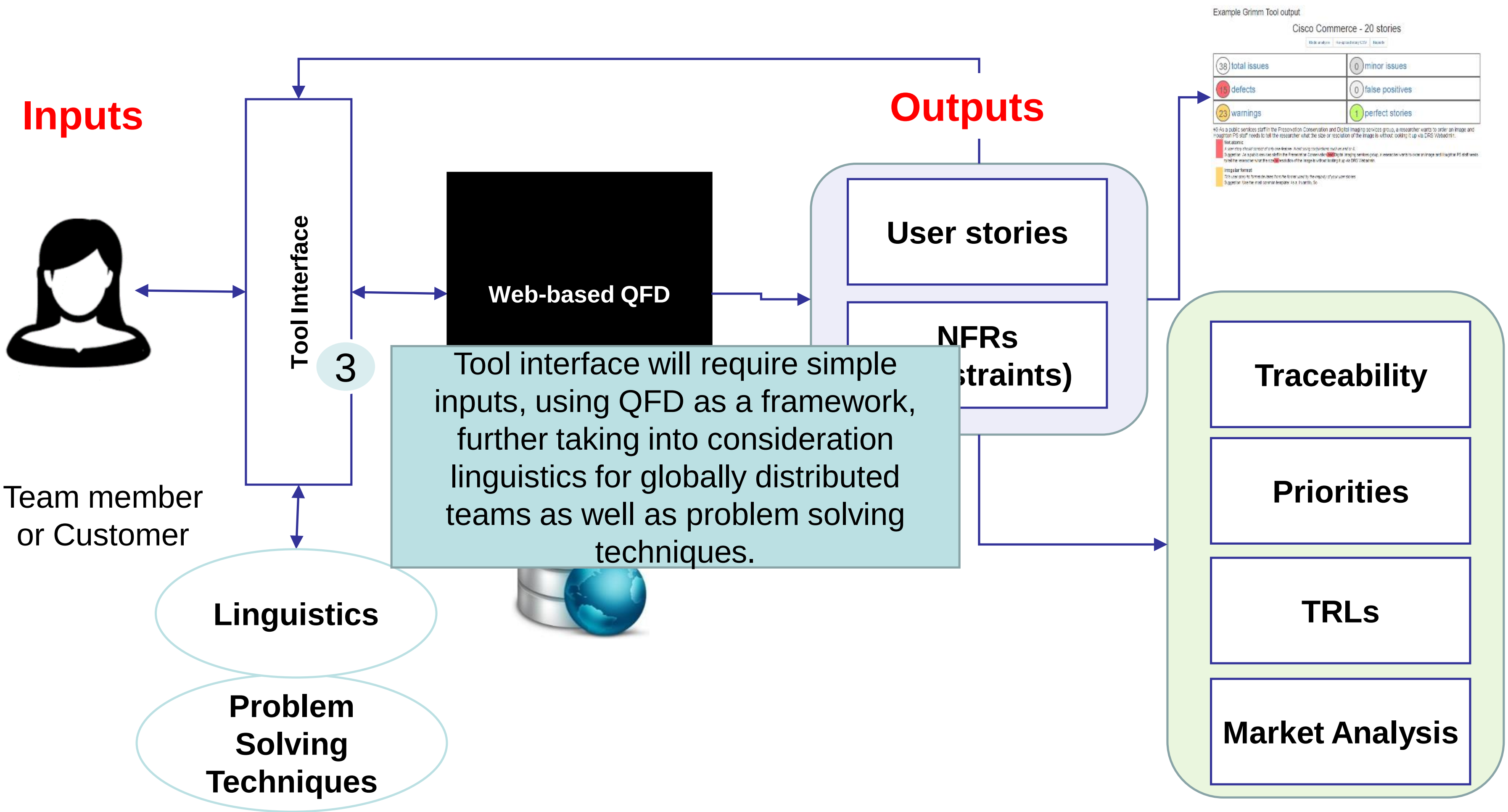
Provide a framework to elicit and manage quality user stories using QFD

Proposed Model



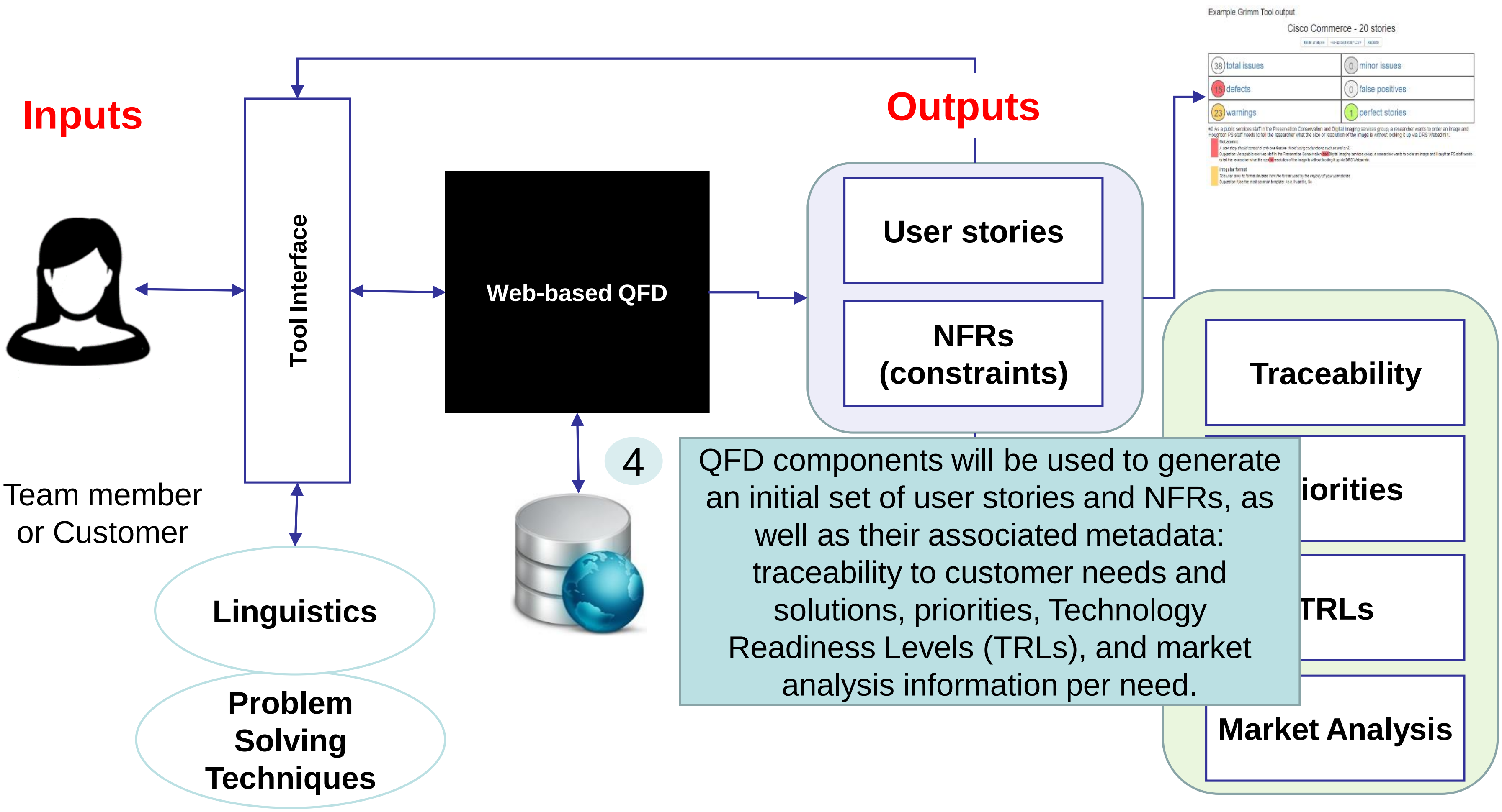
Provide a framework to elicit and manage quality user stories using QFD

Proposed Model



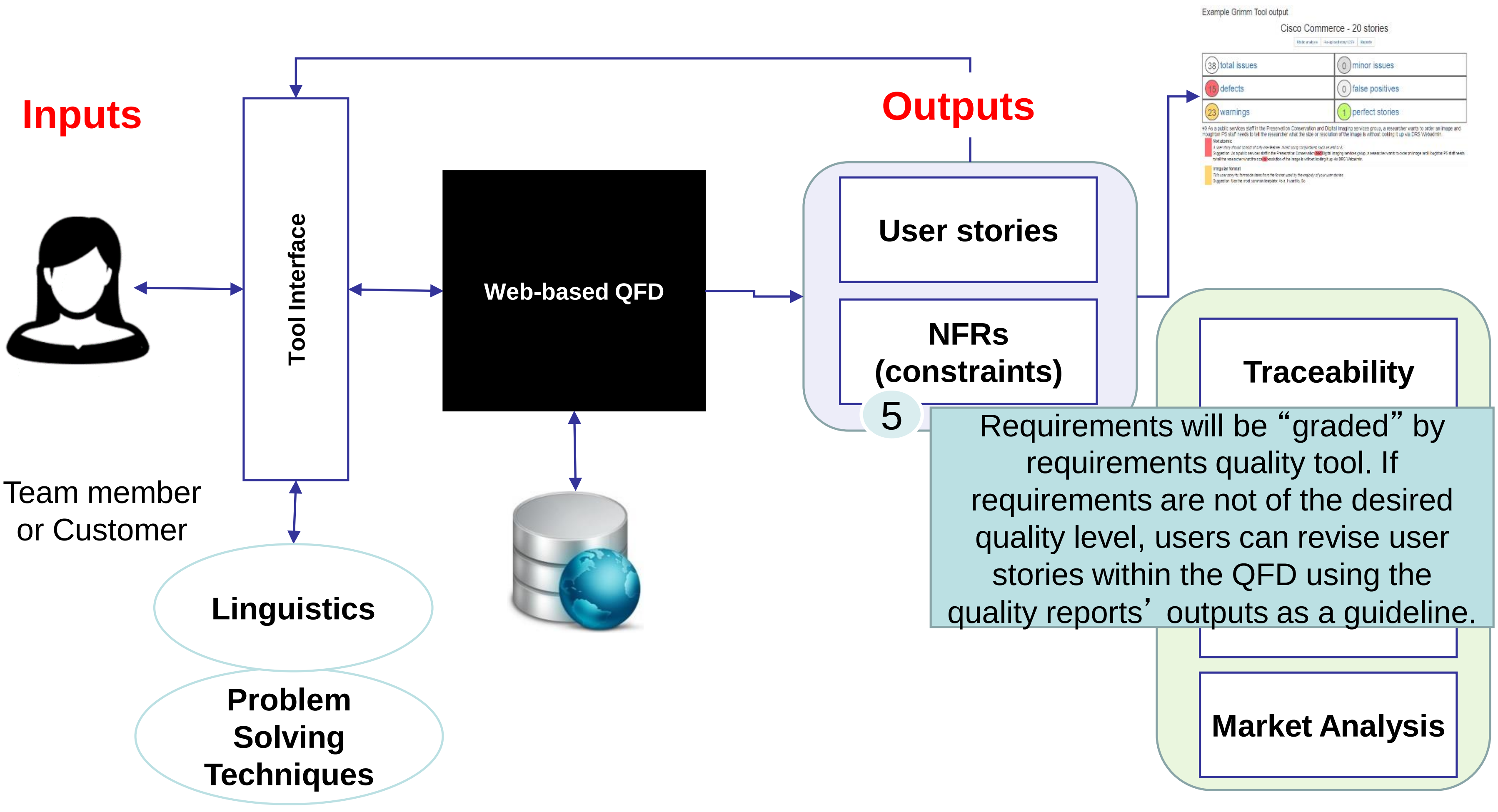
Provide a framework to elicit and manage quality user stories using QFD

Proposed Model



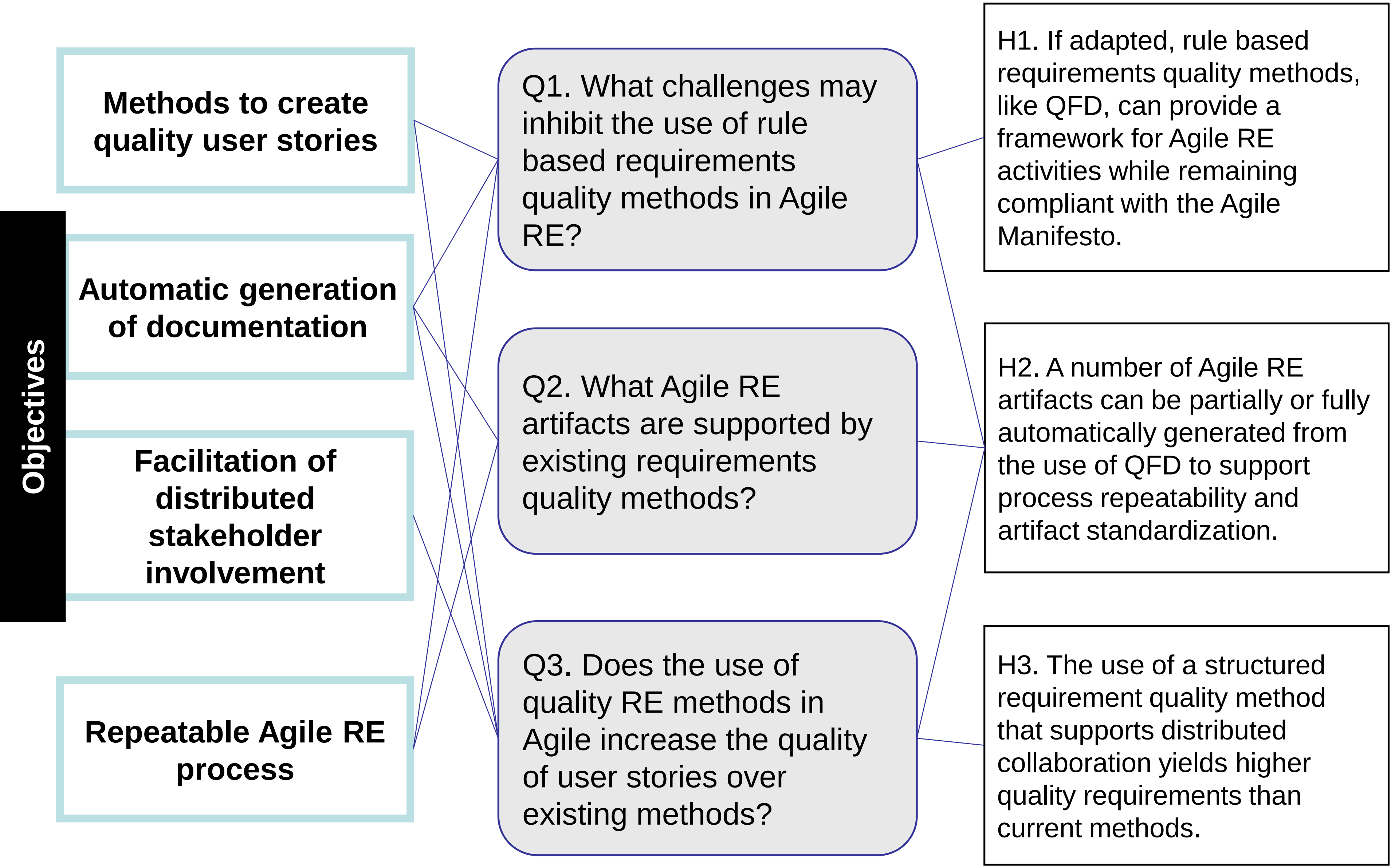
Provide a framework to elicit and manage quality user stories using QFD

Proposed Model



Provide a framework to elicit and manage quality user stories using QFD

Research Definition



Summary

- Results of research may recommend new Agile guidance for requirements elicitation and management including the use of modified QFD as:
  - a web-collaborative, user story elicitation support tool
  - a basis for configuration and requirements management
  - a platform to identify TRLs and competitor capabilities to drive prioritization and other portfolio decisions
  - a means to assess risk and complexity of key features
  - a requirements specification generator
- Use of Natural Language Processing (NLP) quality tools as a means to verify quality of requirements generated by QFD prior to implementation. Consideration will be given to use more than one NLP tool and results will be compared in paper.
- Future research could use the same data to evaluate the feasibility of adapting other RE techniques for use in Agile.

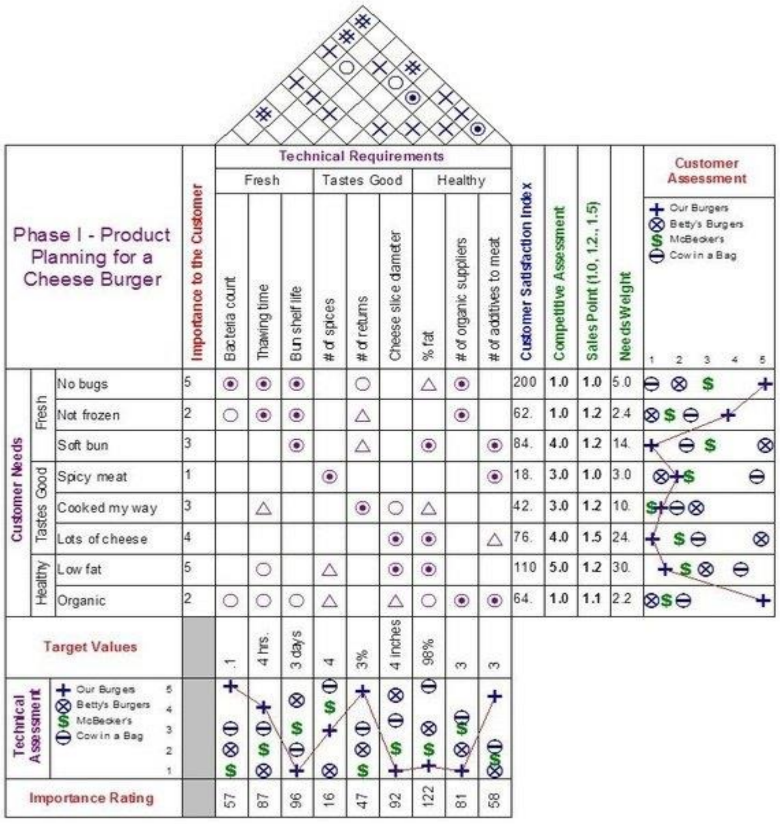


Image source: [27]

References

[1] Eberlein, A., & Leite, J. C. S. P. (2002, September). Agile requirements definition: A view from requirements engineering. In *Proceedings of the International Workshop on Time-Constrained Requirements Engineering (TCRE'02)* (pp. 4-8).

[2] Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch. (n.d.). Retrieved from https://www.infoq.com/articles/standish-chaos-2015

[3] Shah, T., & Patel, V. S. (2014). A review of requirement engineering issues and challenges in various software development methods. *International Journal of Computer Applications*, *99*(15), 36-45.

[4] Ramesh, B., Cao, L., & Baskerville, R. (2010). Agile requirements engineering practices and challenges: an empirical study. *Information Systems Journal*, *20*(5), 449-480.

[5] Agile Scrum Methodology for Mobile Apps. (2016, February 16). Retrieved September 29, 2017, from http://www.innovapptive.com/blog/Agile-scrum-methodology-for-mobile-apps/

[6] Asanka Dilruk, Senior Technology Lead Follow. (2015, April 24). Agile Requirements Engineering Practices: An Empirical Study. Retrieved September 29, 2017, from https://www.slideshare.net/AsankaDilruk/Agile-requirements-engineering-practices-an-empirical-study

[7] De Lucia, A., & Qusef, A. (2010). Requirements engineering in Agile software development. *Journal of Emerging Technologies in Web Intelligence*, *2*(3), 212-220.

[8] Mund, J., Fernandez, D. M., Femmer, H., & Eckhardt, J. (2015, October). Does Quality of Requirements Specifications matter? Combined Results of Two Empirical Studies. In *Empirical Software Engineering and Measurement (ESEM), 2015 ACM/IEEE International Symposium on* (pp. 1-10). IEEE.

[9] Lucassen, G., Dalpiaz, F., van der Werf, J. M. E., & Brinkkemper, S. (2016). Improving Agile requirements: the quality user story framework and tool. *Requirements Engineering*, *21*(3), 383-403.

[10] Challenges with User Stories. (2011, February 23). Retrieved from http://www.seilevel.com/requirements/challenges-with-user-stories

[11] 5 Common Mistakes We Make Writing User Stories. (n.d.). Retrieved from https://www.scrumalliance.org/community/articles/2011/august/5-common-mistakes-we-make-writing-user-stories

[12] 5 Common User Story Mistakes by Roman Pichler. (2017, January 31). Retrieved from http://www.romanpichler.com/blog/5-common-user-story-mistakes/

[13] Limitations of user stories. (n.d.). Retrieved from http://www.ferolen.com/blog/limitations-of-user-stories/

[14] Dahlgren, M. (2017, March 01). 7 reasons some user stories aren't useful stories – Magnus Dahlgren – Medium. Retrieved September 29, 2017, from https://medium.com/@MagnusDahlgren/7-reasons-some-user-stories-arent-useful-stories-d3d2dddbae60

[15] Identifying and Improving Bad User Stories. (n.d.). Retrieved from https://www.Agileconnection.com/article/identifying-and-improving-bad-user-stories?page=0%2C2

References

[16] Gaikwad, V., & Joeg, P. (2016). An Empirical Study of Writing Effective User Stories. *International Journal of Software Engineering and Its Applications*, *10*(11), 387-404.

[17] Paetsch, F., Eberlein, A., & Maurer, F. (2003, June). Requirements engineering and Agile software development. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on* (pp. 308-313). IEEE.

[18] Boehm, B. (2000) Requirements that handle IKIWISI, COTS, and rapid change. *IEEE Computer*, **33**, 99–102.

[19] Bjarnason, E., Wnuk, K., & Regnell, B. (2011, July). A case study on benefits and side-effects of Agile practices in large-scale requirements engineering. In *Proceedings of the 1st Workshop on Agile Requirements Engineering* (p. 3). ACM.

[20] Pfeiffer, S., & Eberlein, A. (2003). *Requirements engineering for dynamic markets*. University of Calgary, Department of Electrical and Computer Engineering.

[21] Paetsch, F., Eberlein, A., & Maurer, F. (2003, June). Requirements engineering and Agile software development. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on* (pp. 308-313). IEEE.

[22] Boehm, B. (2003) *Balancing Agility and Discipline: A Guide for the Perplexed.* Addison-Wesley, Boston, MA, USA.

[23] QFD a Good Tool to Use for Avoiding Product Failure. (n.d.). Retrieved from https://www.isixsigma.com/tools-templates/qfd-house-of-quality/qfd-good-tool-use-avoiding-product-failure/

[24] Modigliani, P., & Chang, S. (2014, March). *Defense Agile Acquisition Guide: Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities (Rep. No. 14-0391).* Retrieved from The MITRE Corporation website: https://www.mitre.org/sites/default/files/publications/MITRE-Defense-Agile-Acquisition-Guide.pdf

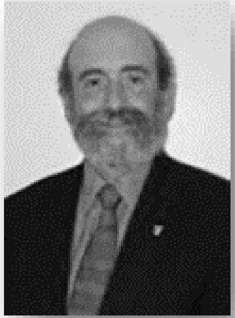
[25] US Department of Defense (DoD) is Going Agile. (n.d.). Retrieved from https://www.infoq.com/news/2014/05/DoD_Agile

[26] Acquisition Process Overview. (n.d.). Retrieved October 03, 2017, from http://acqnotes.com/acqnote/acquisitions/acquisition-process-overview

[27] What is the meaning of QFD "quality function deployment"? (n.d.). Retrieved from https://www.quora.com/What-is-the-meaning-of-QFD-quality-function-deployment

[28] Agile Scrum Methodology for Mobile Apps. (2016, February 16), Retrieved from http://www.innovapptive.com/blog/Agile-scrum-methodology-for-mobile-apps/

Sabrina Ussery has 10 years experience in industry working in systems engineering and program management. Sabrina has led many requirements engineering efforts for the FAA's NextGen Air Traffic Management (ATM) initiatives and spent 2 years as a Technical Product Owner in a Scaled Agile environment for a healthcare analytics organization. Sabrina is currently employed as a Senior Systems Engineer at Mosaic ATM Inc., leading systems engineering efforts for a number of FAA acquisition programs. Sabrina holds a B.S. in Applied Mathematics from Jacksonville State University and a M.S. in Aerospace Engineering from the Georgia Institute of Technology. She is currently a PhD candidate in Systems Engineering at The George Washington University.



Thomas Holzer, D.Sc., has been Adjunct Professor of Engineering Management and Systems Engineering at George Washington University, Washington, D.C., since 1999. He is the former Director, Engineering Management Office, Enterprise Operations Directorate, National Geospatial-Intelligence Agency. He has over 35 years of experience in lifecycle systems engineering, leading large-scale information technology programs, and process improvement initiatives. Dr. Holzer was responsible for the strategic evolution of the National System for Geospatial-Intelligence technical and operational infrastructure architectures; assuring the integrity of the systems engineering performed; and development of a proficient systems engineering workforce.
Dr. Holzer has D.Sc. and M.S. degrees in Engineering Management from George Washington University and a B.S. degree in Mechanical Engineering from the University of Cincinnati.

Shahryar Sarkani, D.Sc., is Adjunct Professor in the Department of Engineering Management and Systems Engineering at George Washington University, Washington, D.C. He has over 20 years of experience in the field of software engineering focusing on architecture and design. Dr. Sarkani earned the D.Sc. in Systems Engineering from George Washington University, an M.S. in Mathematics from the University of New Orleans, and a B.S. in Electrical Engineering from Louisiana State University.

Research Gone *Agile*

A Case Study on Using an Enterprise Transformation Process to Enable Agility in a Research Program

Rosa R. Heckle, PhD, rheckle@MITRE.org
Paul Matthews, pmatthews@MITRE.org

October, 2017

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author

MITRE

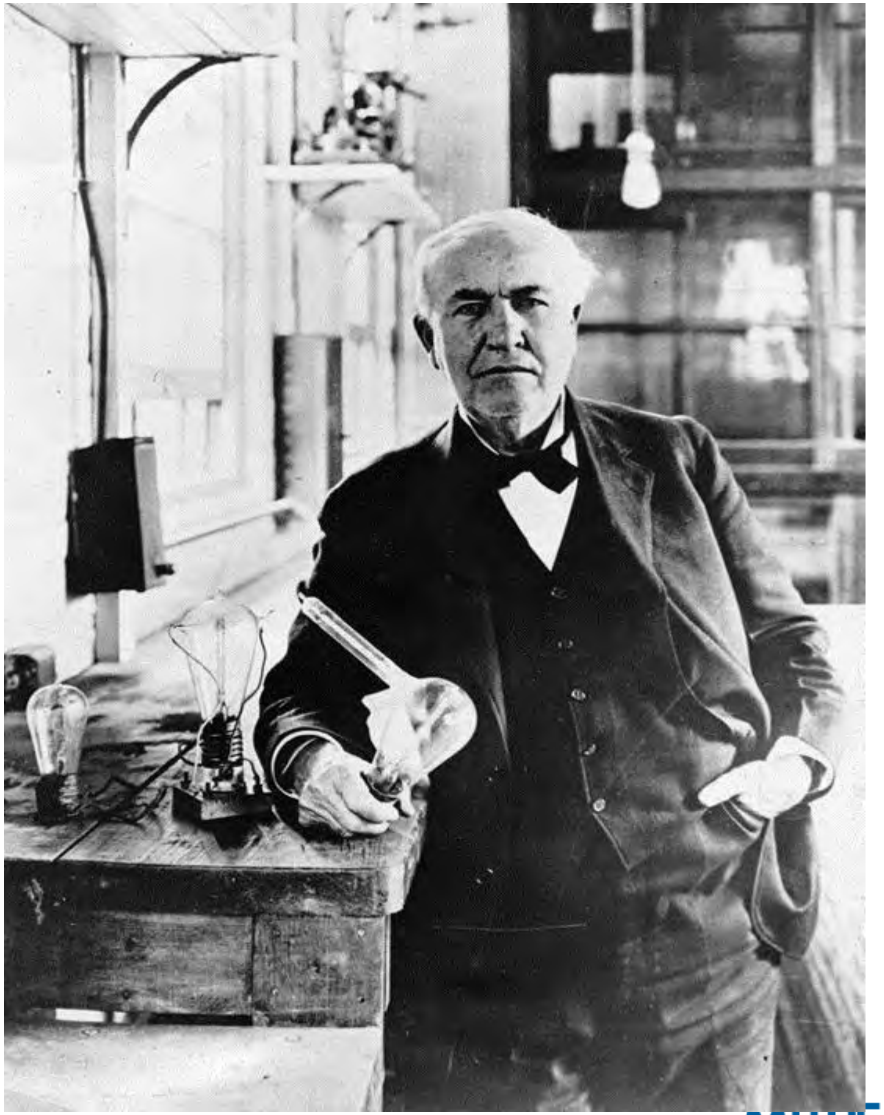
Retrieved 6/2017 from Youtube.com

But… This is Research!

"I have not failed you.

I've just found 10,000 ways that won't work."

Thomas Edison



Labeled for Reuse

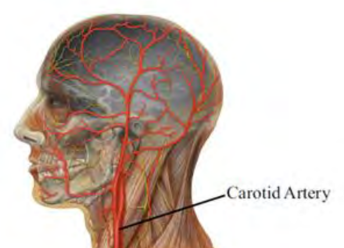
Case Study

Applied Research in Data Science

- Develop new analytic capabilities
- Evaluate COTS/GOTS analytic capabilities for domain use

Semantic Retrieval via Deep Learning

Find in-scene text



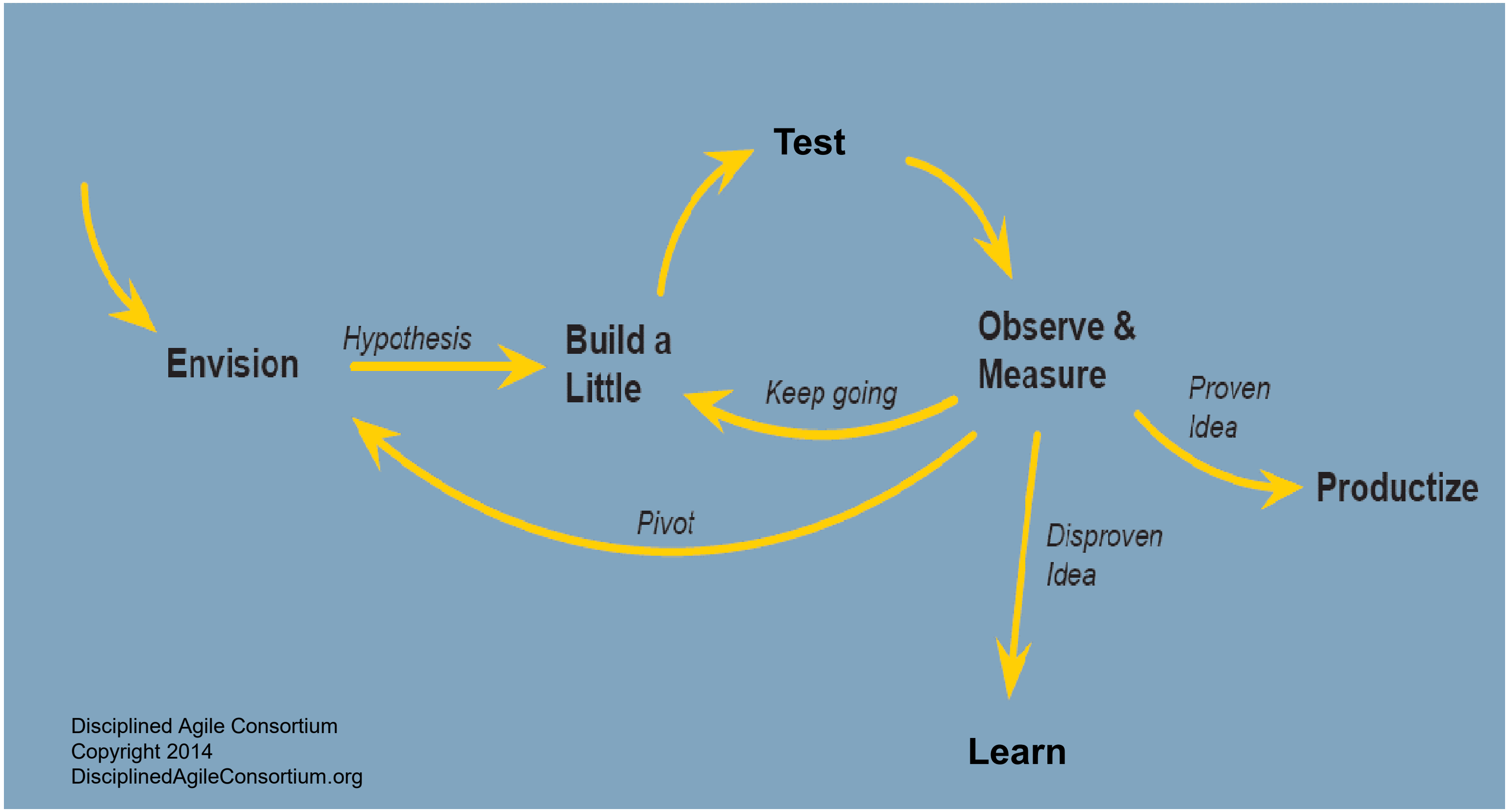
Labeled for Reuse

Forensic Analysis

Face Recognition

MITRE

Multimedia Processing Research (MPR) Project Lifecycle

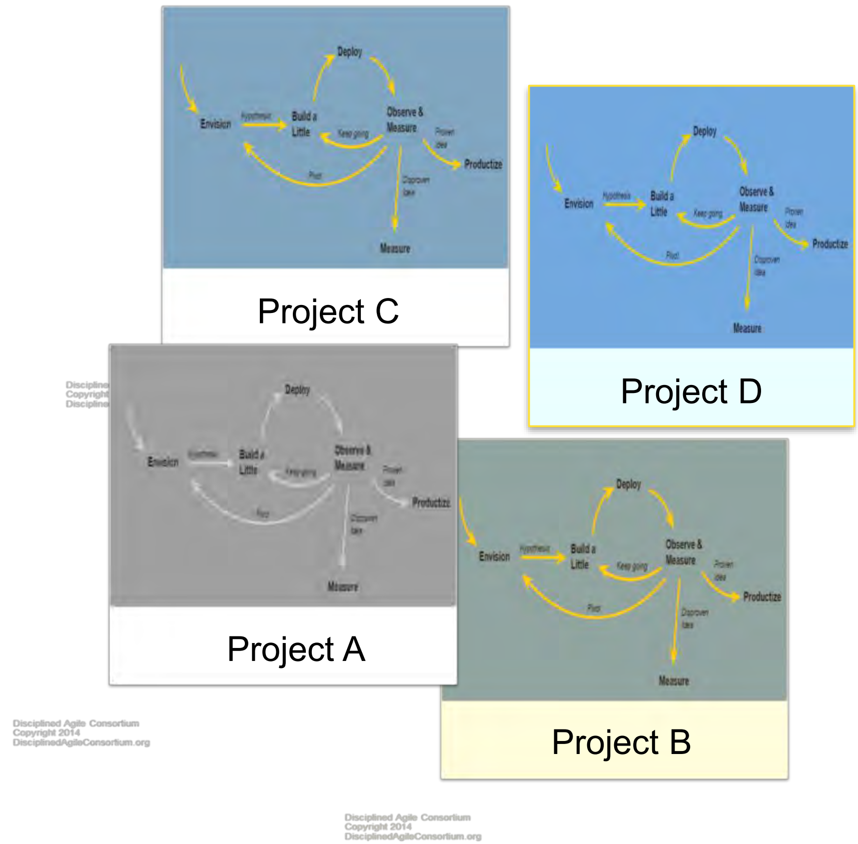


Exploratory Lifecycle

The Problem

Latency…

- Competing Projects
- Varied Research Interests
- Scarce Resources
- Redundancy
- Limited collaboration and synchronization among teams



MITRE

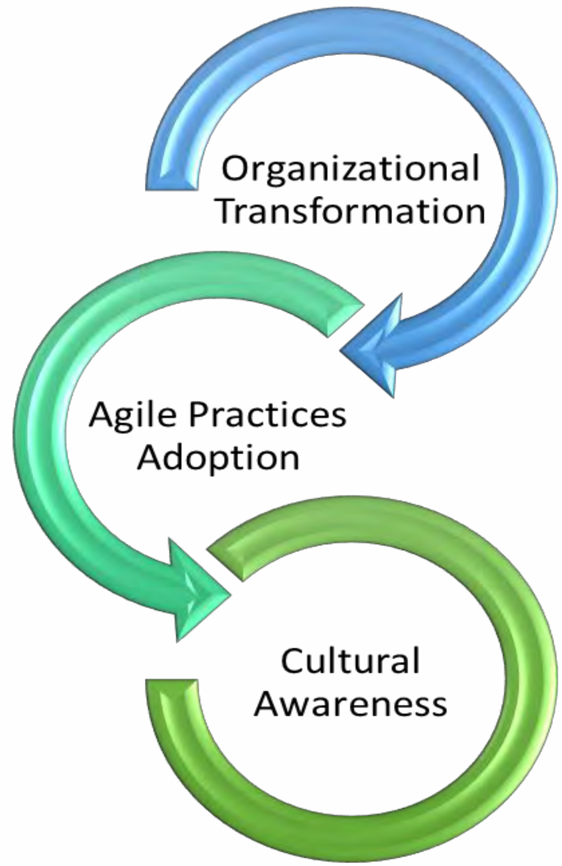
The Solution …

Improve Organizational Agility Through

Organizational Transformation

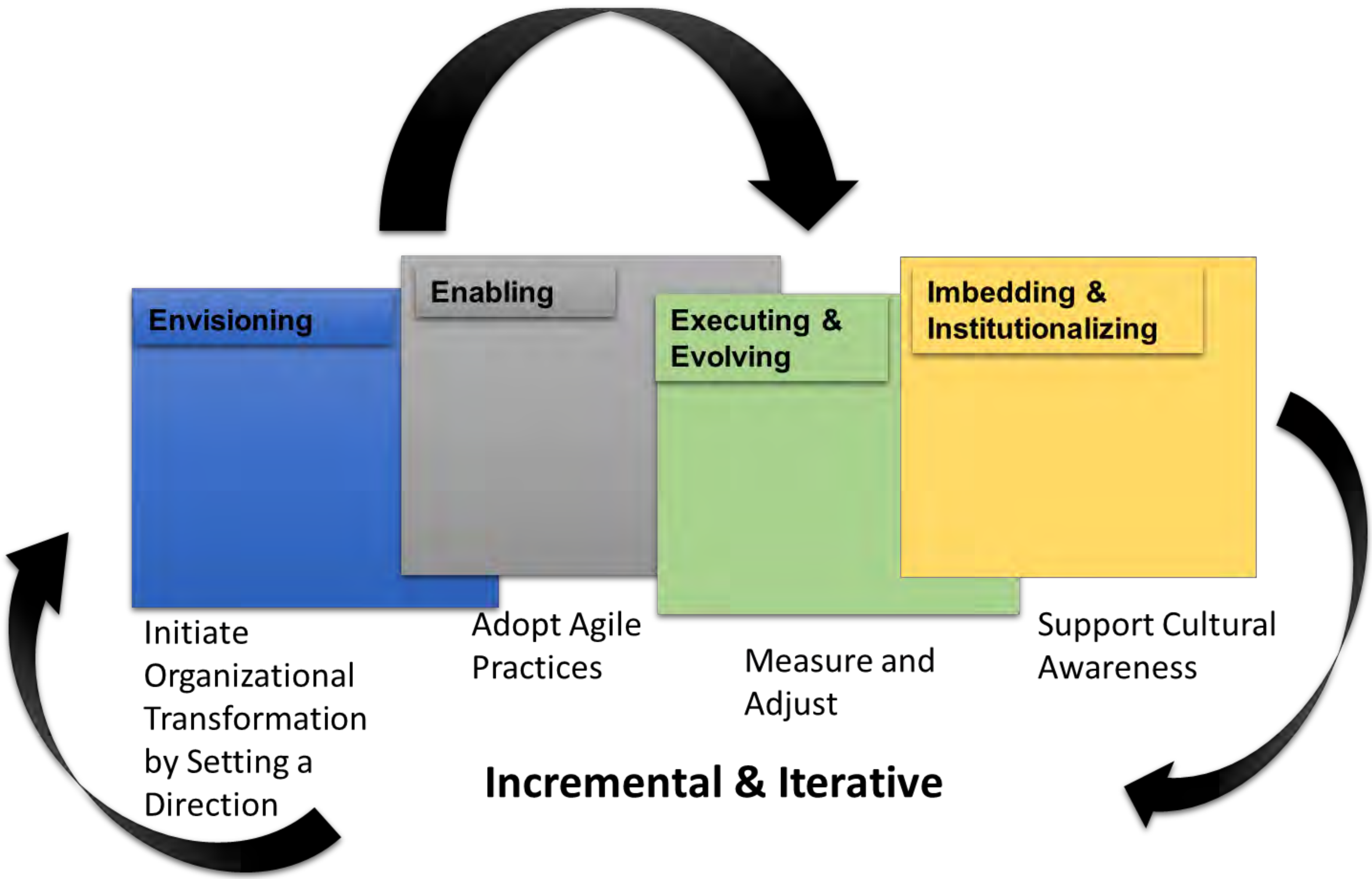
&

Adopting Agile Practices



3 Elements to
Attain & Sustain Agility

Organizational Transformation Process



MITRE

Develop a Program Strategy

- Environmental Scan
- Create Organizational Baseline
- Brainstorm Workshop
- Map R&D thrusts to Organizational Strategy
- Develop and Socialize

▪ What do we do?
▪ For whom and why do we do it?
▪ How do we make maximum impact?

Program Strategy

Vision:
Automated Multimedia Understanding

Mission:
The mission of the Multimedia Processing Research (MPR) Program is to conduct world-class scientific research to leverage and advance the state of the art in multimedia analysis technologies…

Identify Strategic Themes

Enterprise Goals

Program Vision

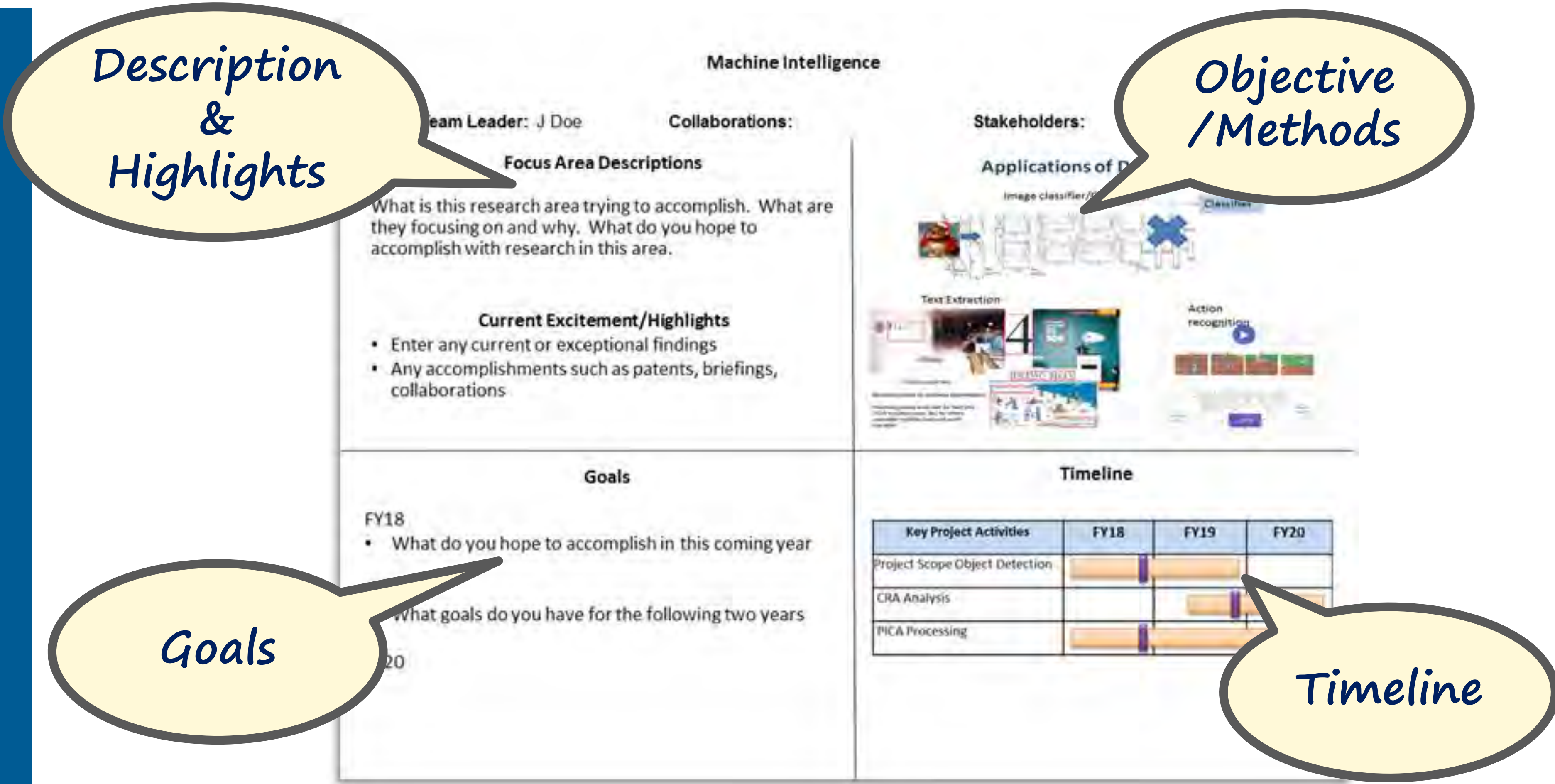
Strategic Themes

(Focus Areas)

- Visualization
- Forensics
- Identity Intelligence
- Machine Intelligence

www.bing.com/images

Set Goals for Each Focus Area

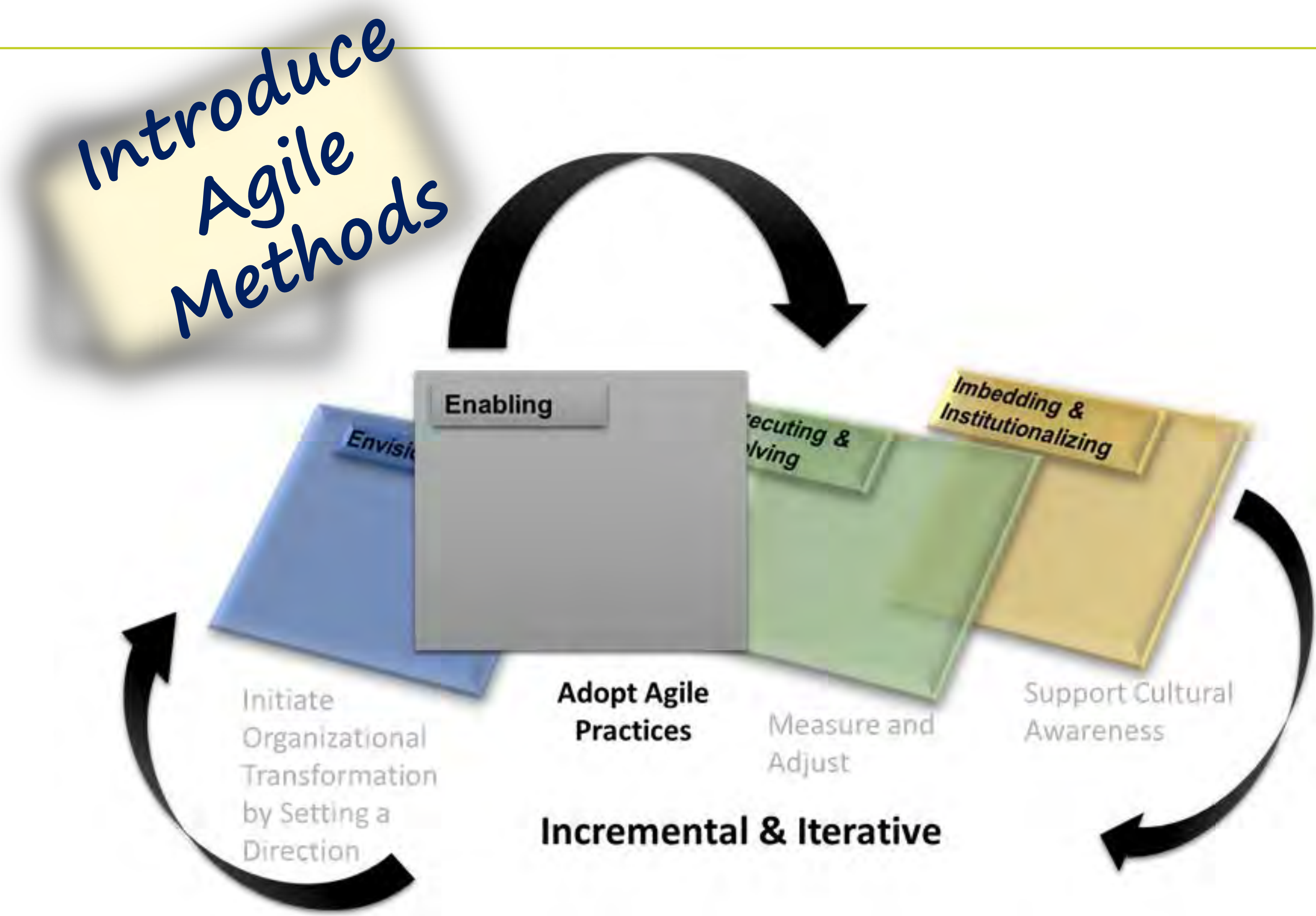


Quad Chart

Review & Synchronize Quarterly

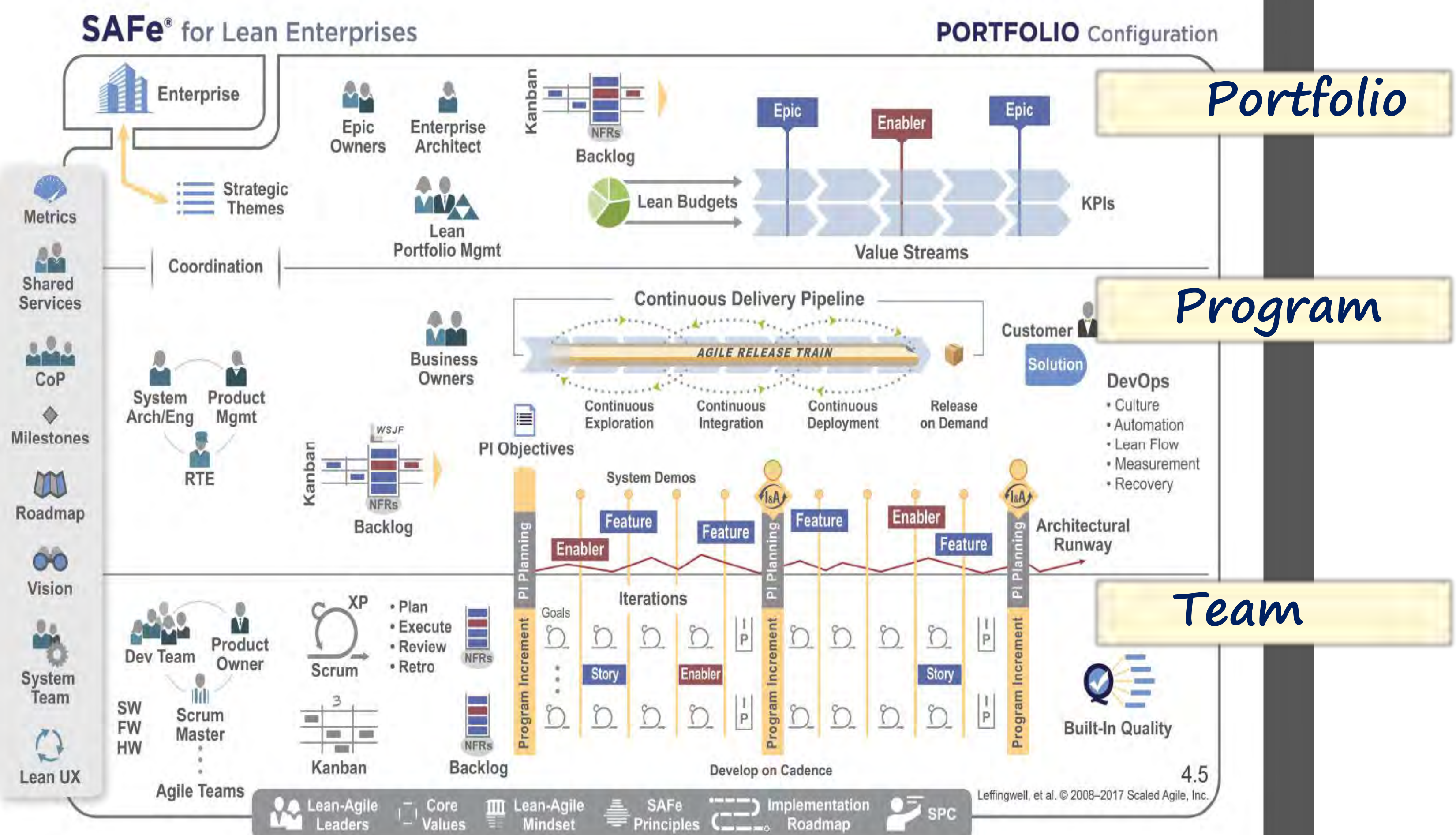
MITRE

Enabling

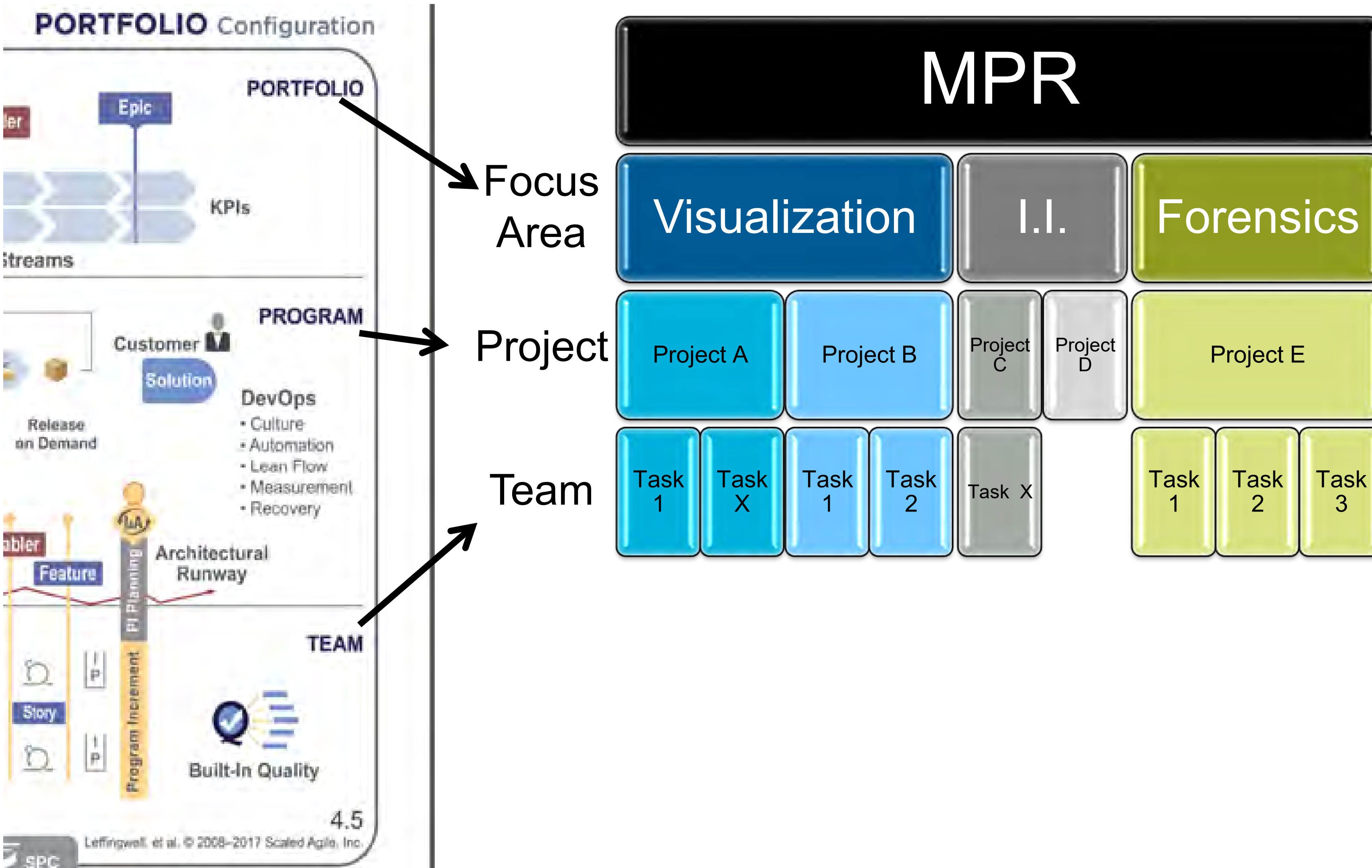


MITRE

SAFe Agile Framework

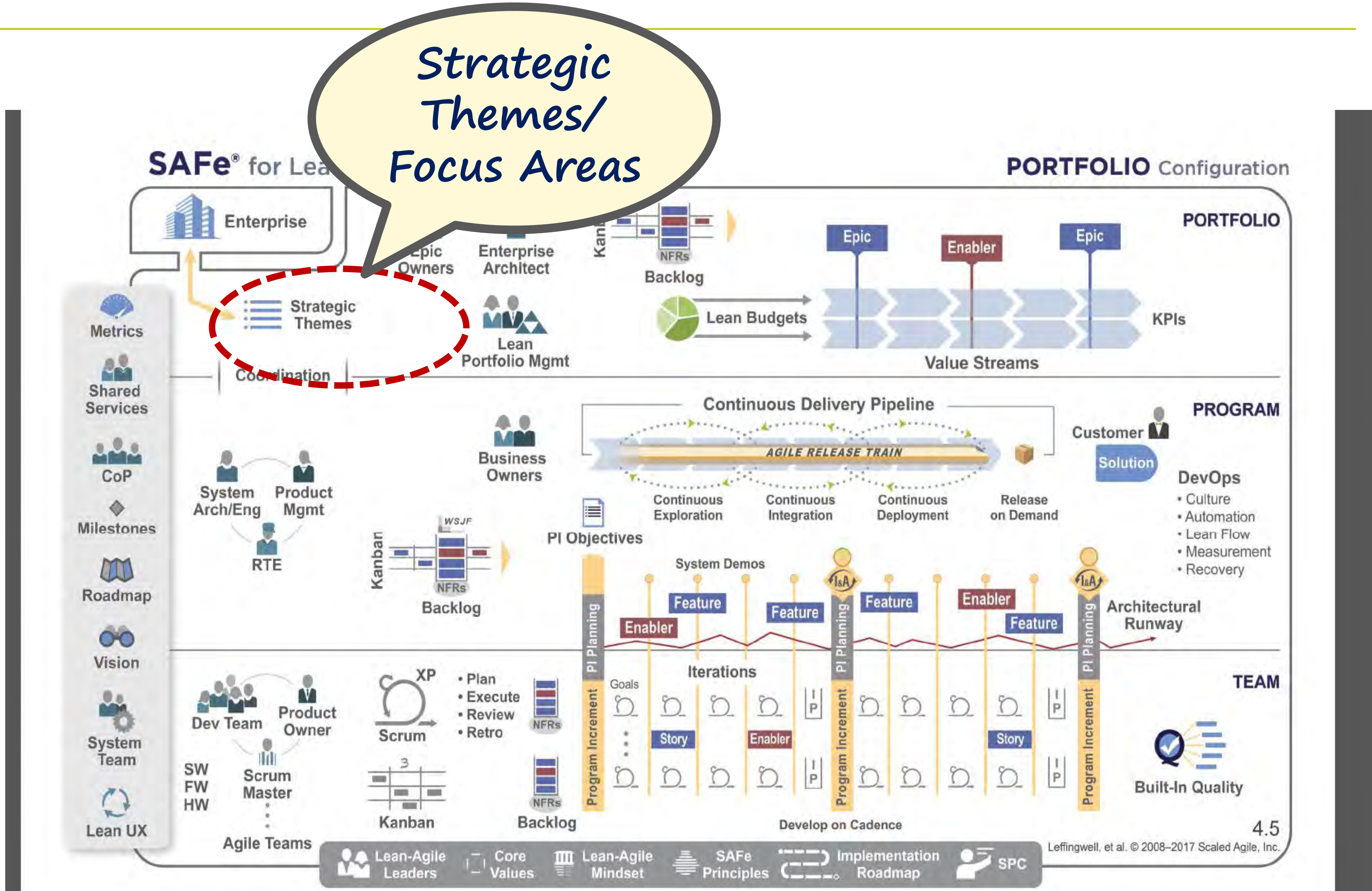


Align Organizational Structure



MITRE

Take What Fits from Scaled Agile Framework for the Enterprise (SAFe Agile)



MITRE

Identify Strategic Themes

Enterprise
Goals

Program Vision

Strategic
Themes

(Focus Areas)

Visualization

Forensics

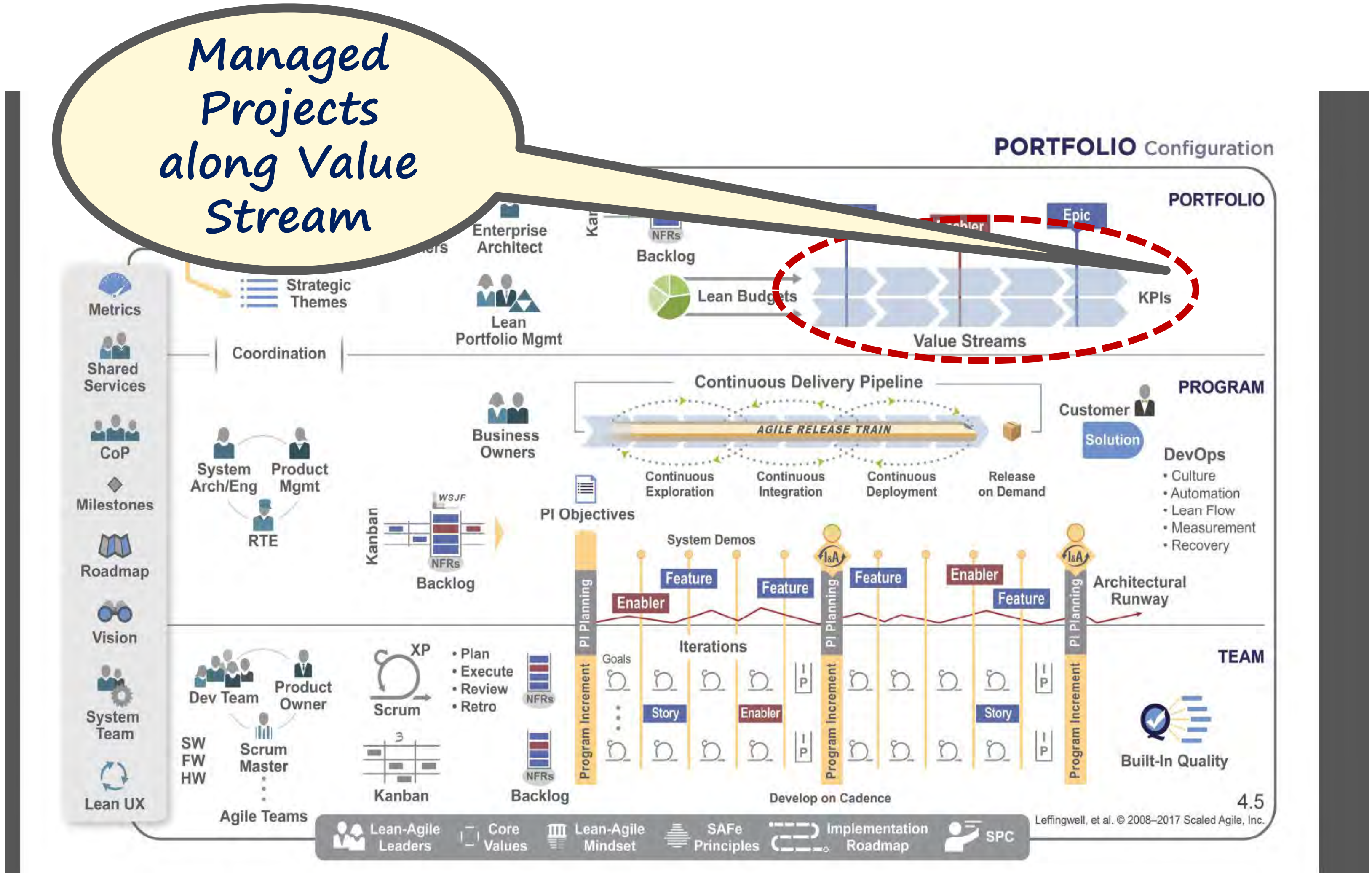
Identity
Intelligence

Machine
Intelligence

www.bing.com/images

MITRE

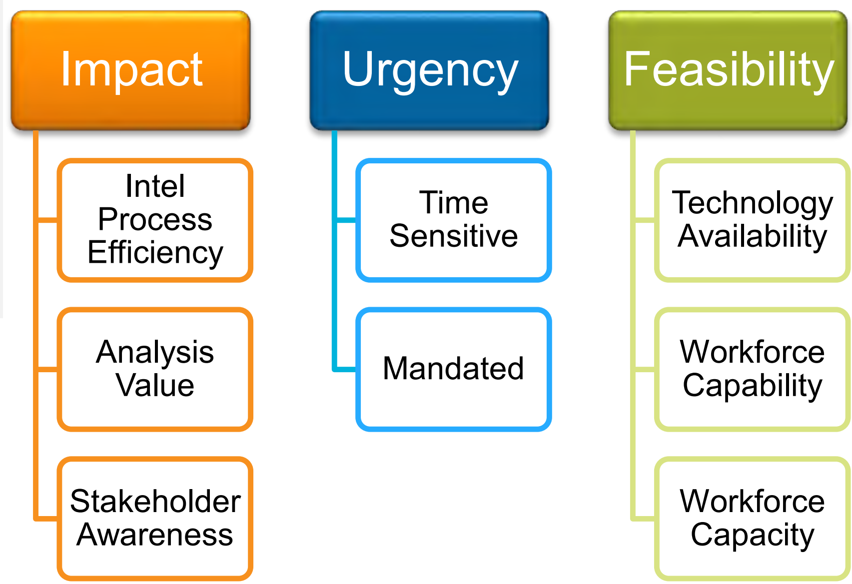
Take What Fits from SAFe Agile



Limit Work in Progress

- Terminate "Pet" Projects
- Limit development timeframe to months
- Dynamically reprioritize based upon changing demands and criteria
- Balance portfolio

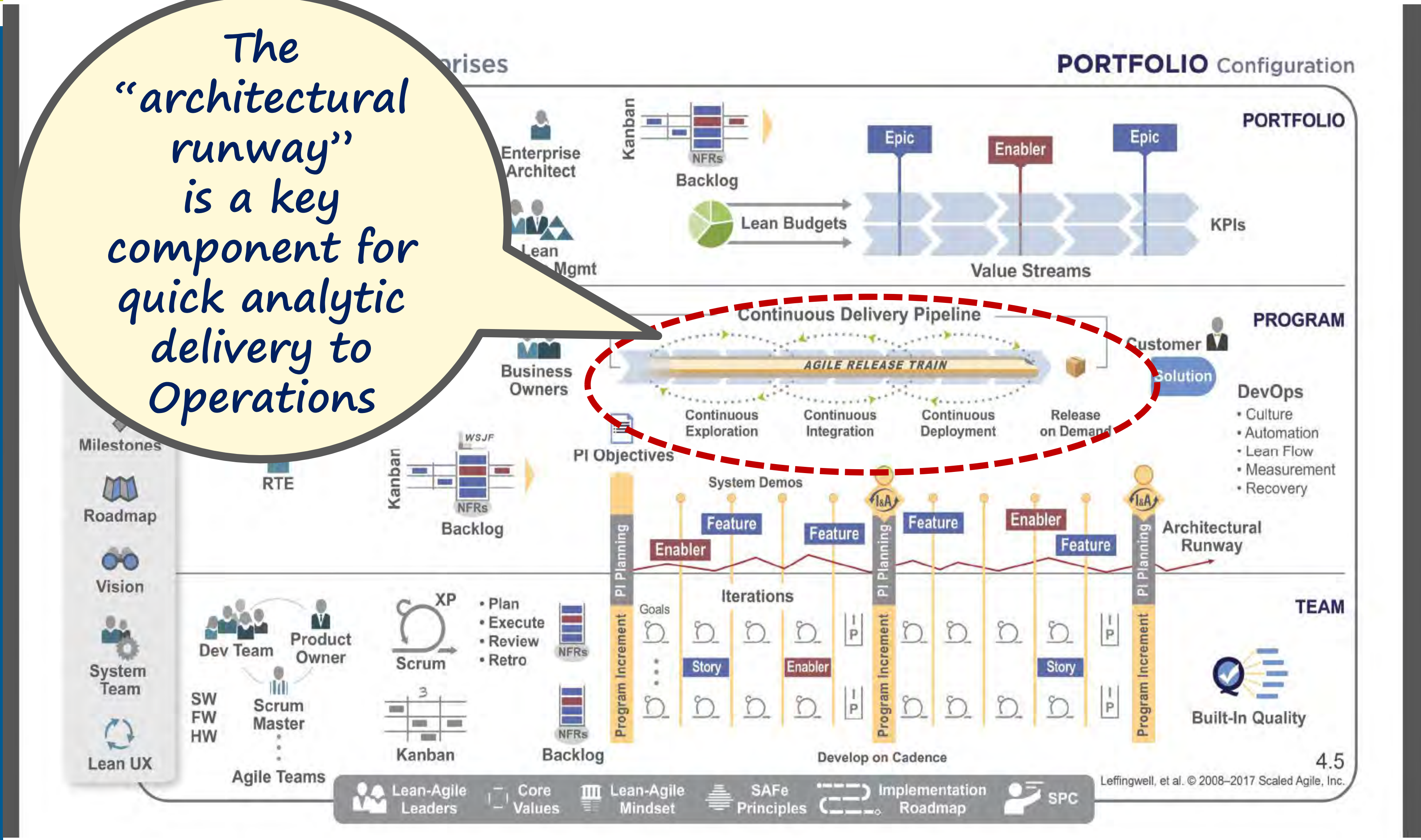
Set Program Priorities
Using Standard Criteria



MITRE

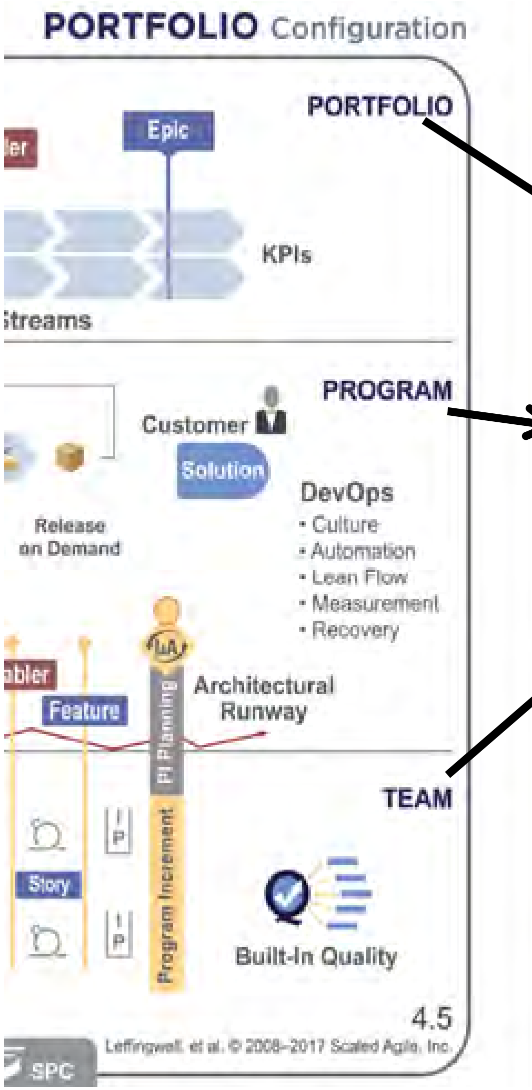
Stress Technology Planning

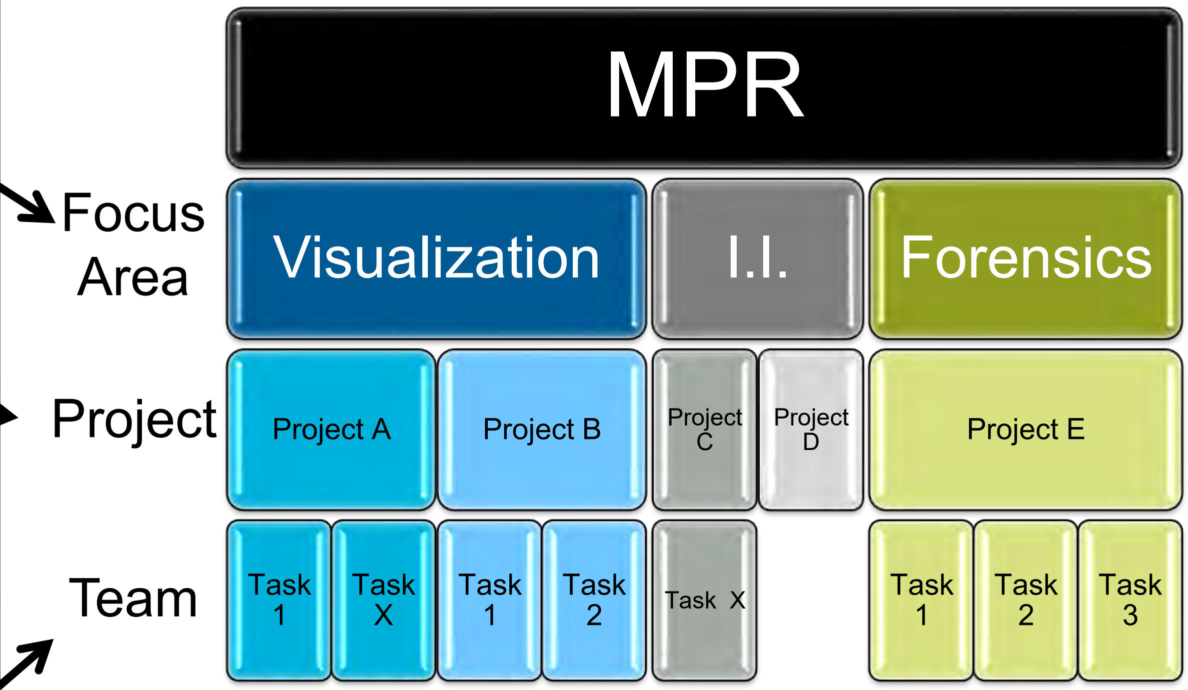
The "architectural runway" is a key component for quick analytic delivery to Operations



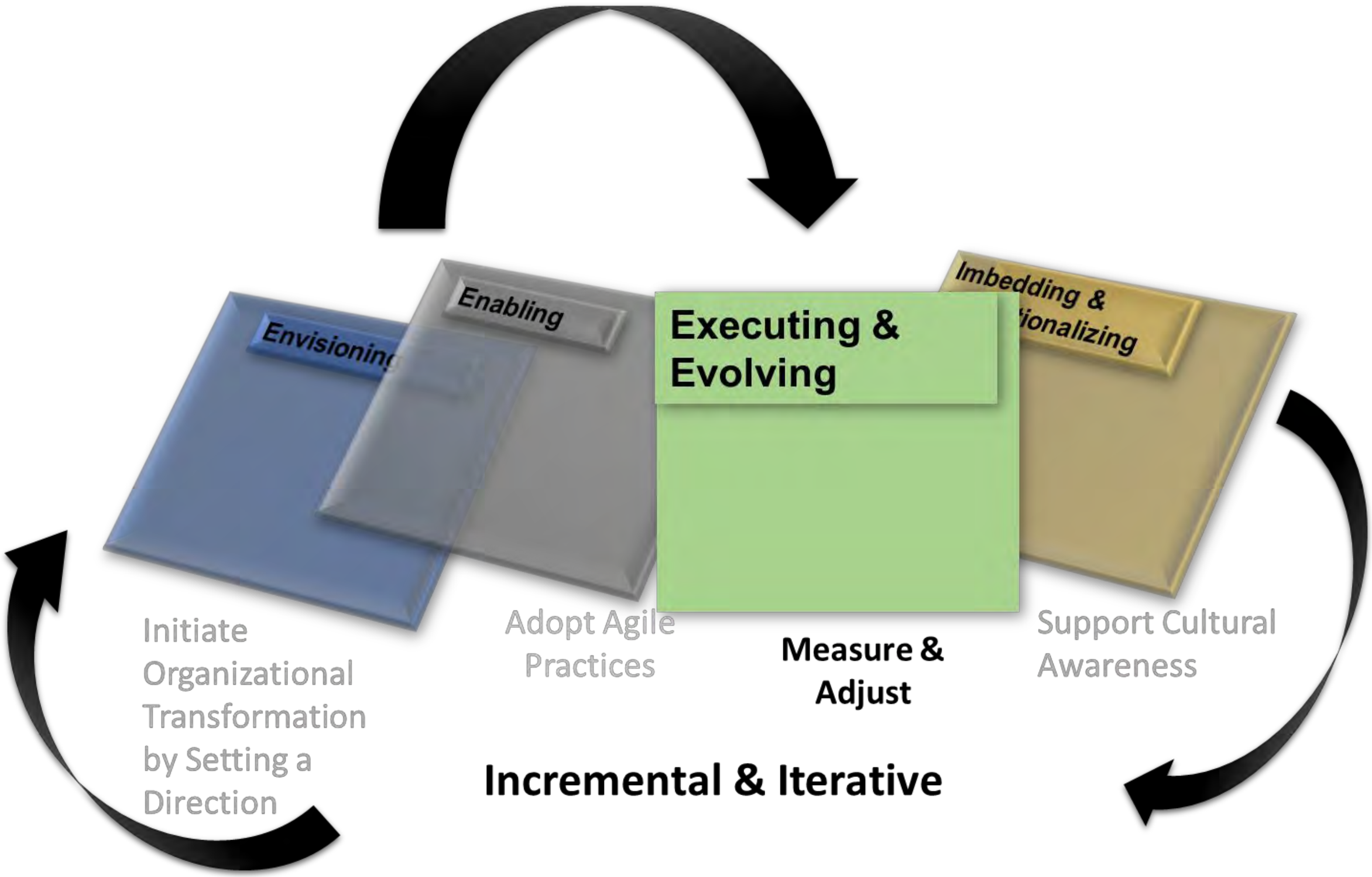
MITRE

Align Organizational Structure



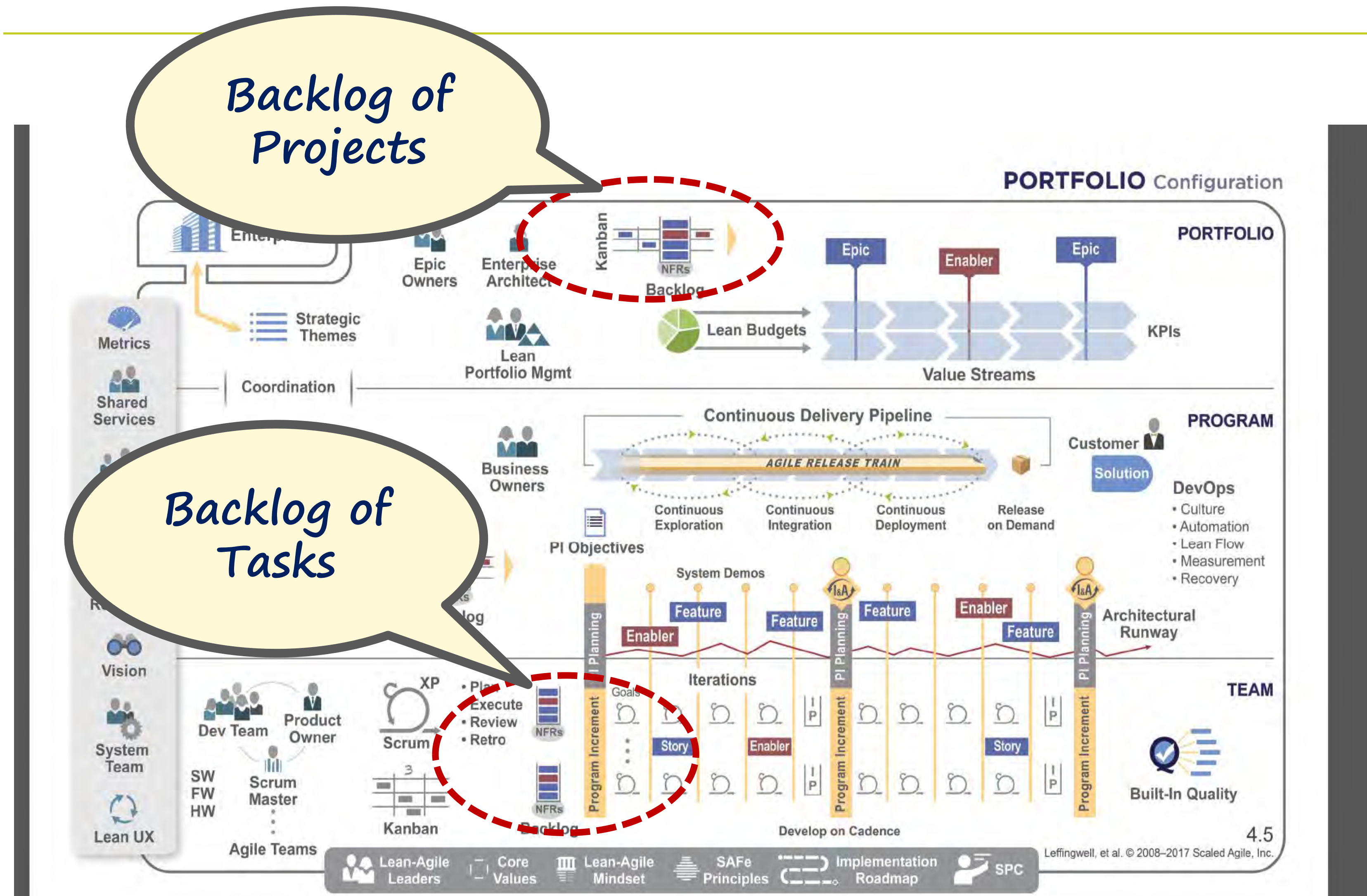


Executing and Evolving



MITRE

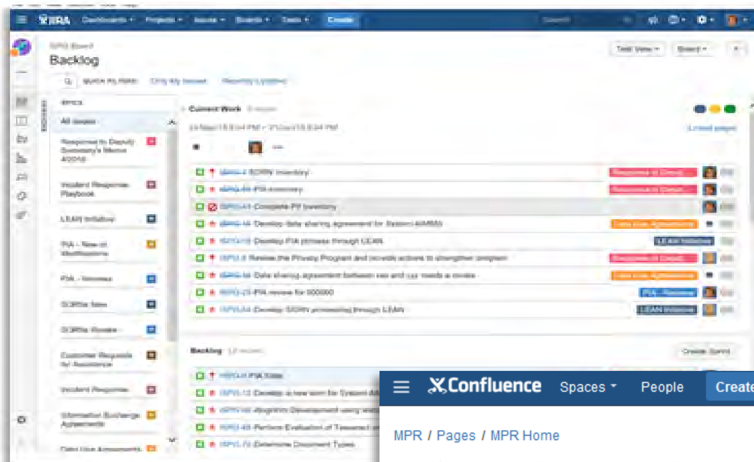
Take What Fits from SAFe Agile



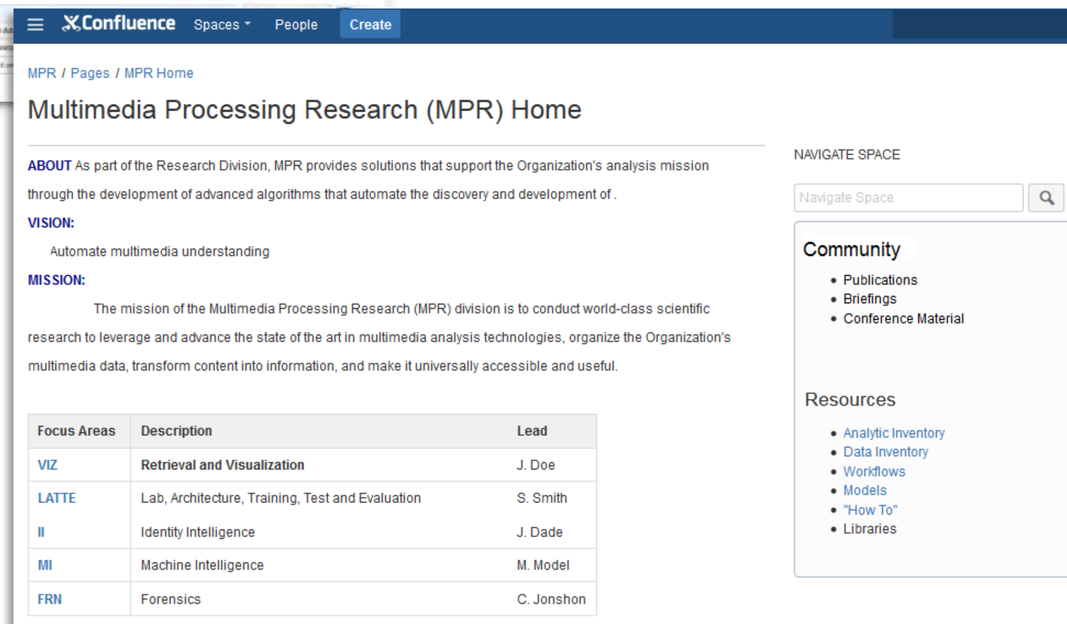
MITRE

Use Agile Full-Life-cycle Tools

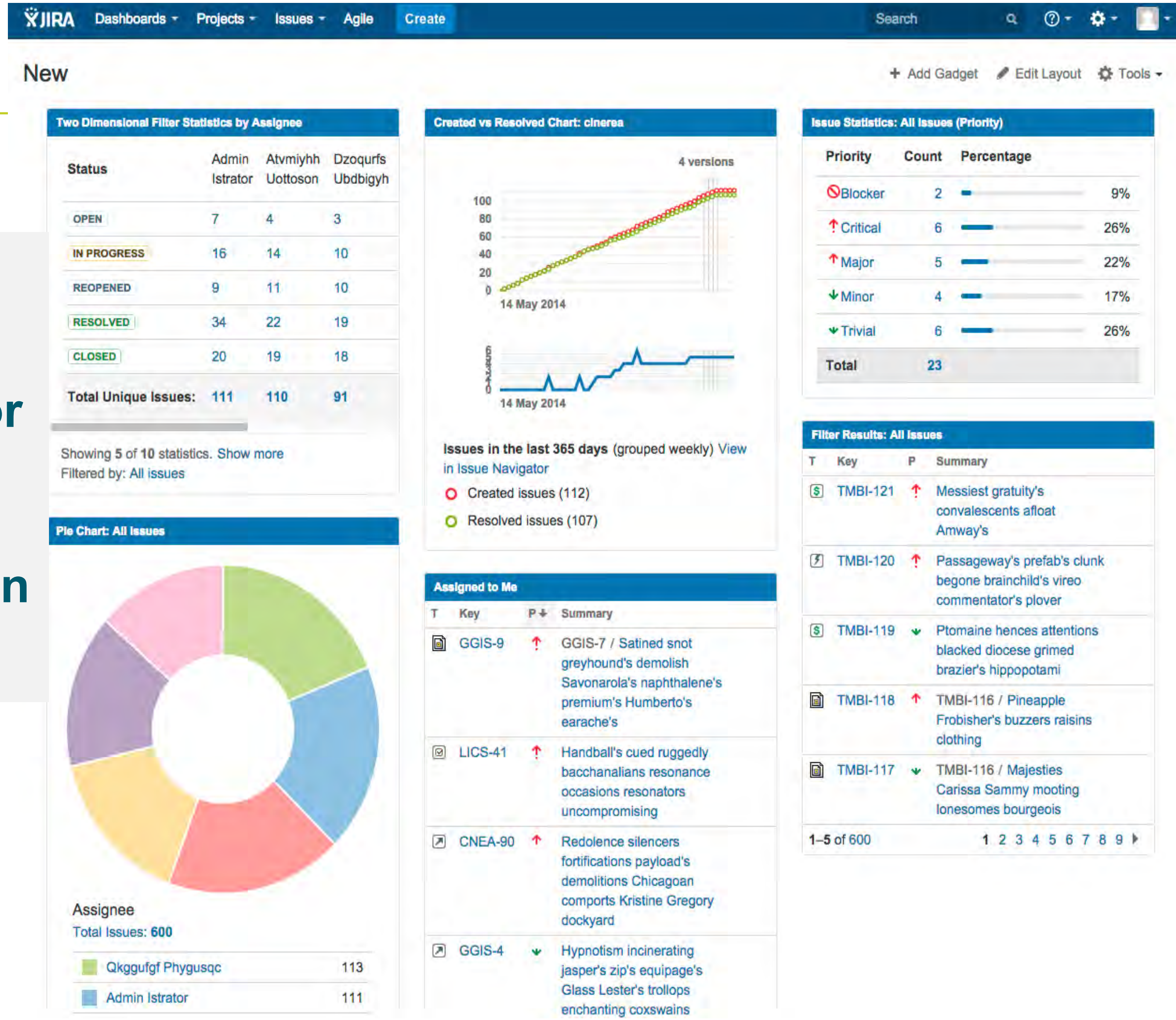
Backlog management



Wiki communication

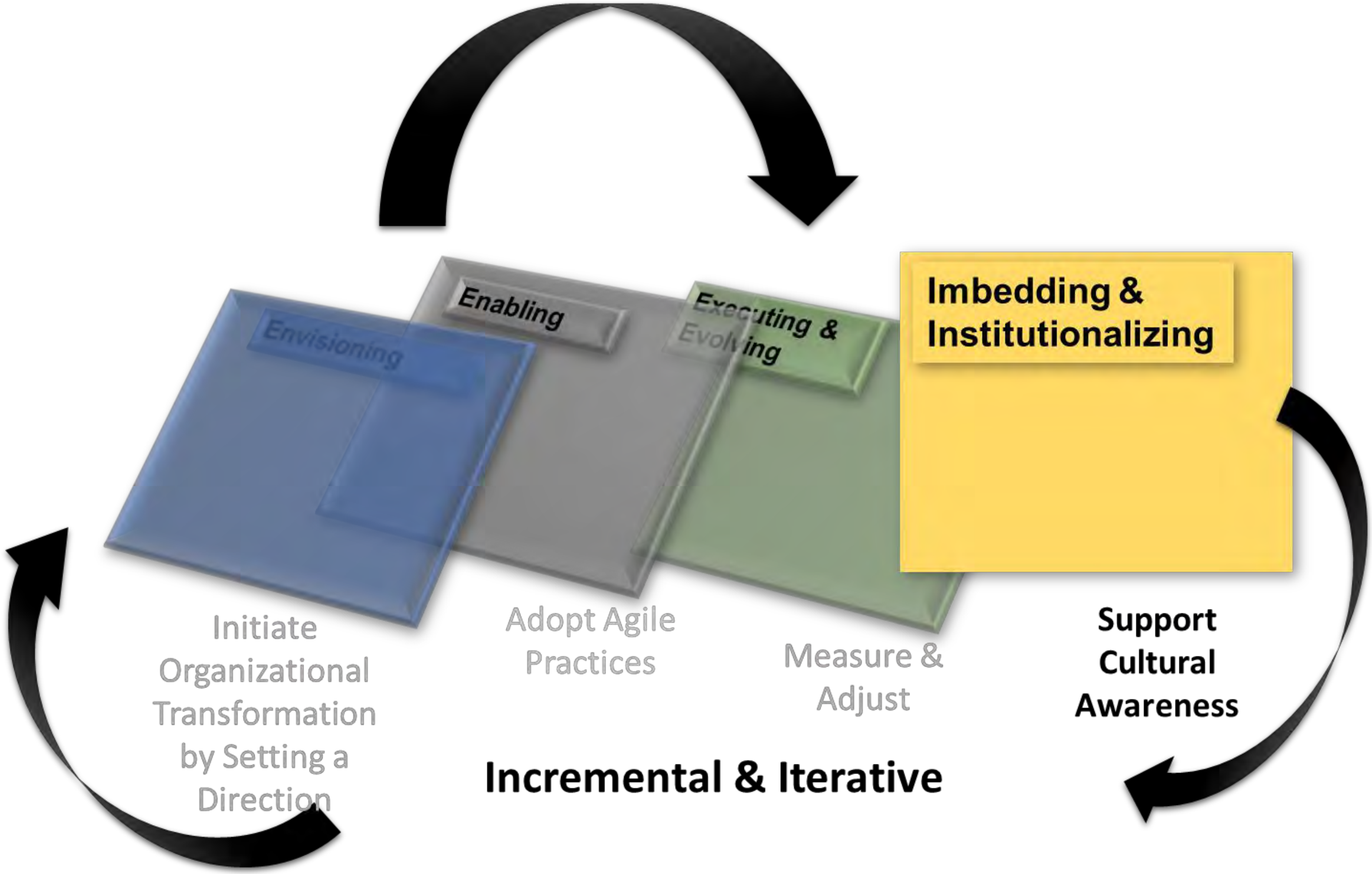


Using Dashboards for Decision Support and Communication



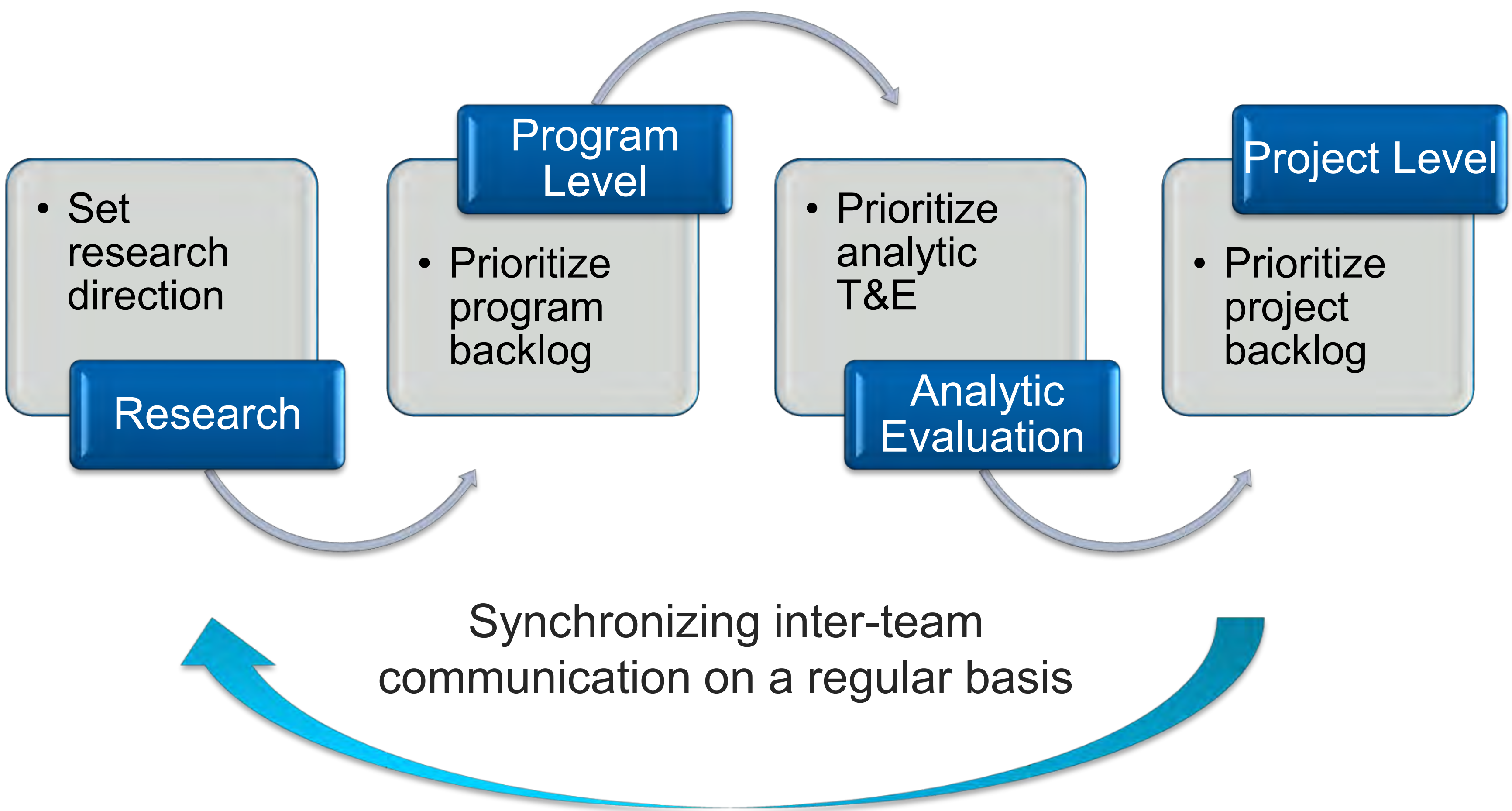
MITRE

Imbedding & Institutionalizing

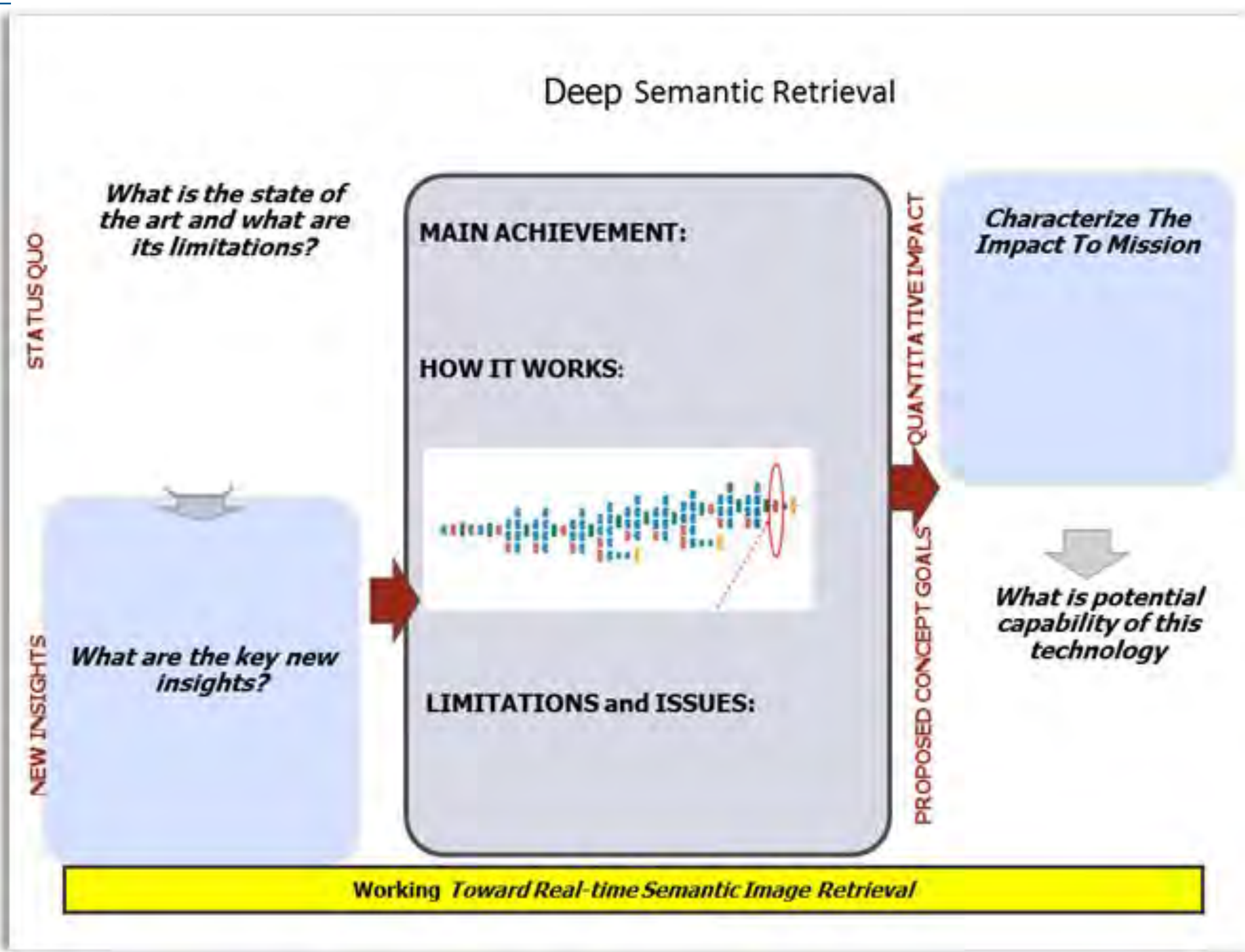


MITRE

Establish a Cadence



Develop Next Gen Agile Leaders

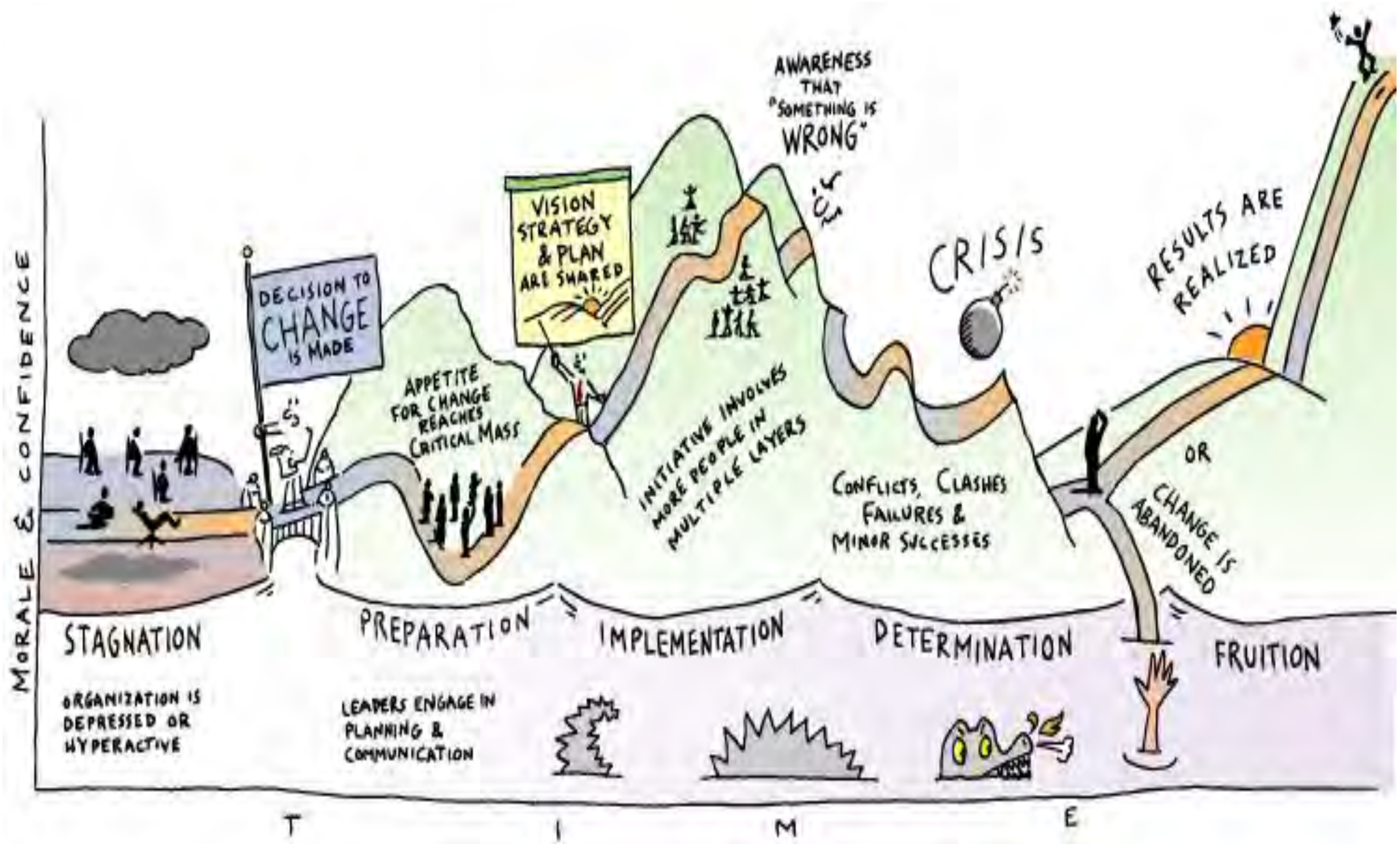


Requiring a Heilmeier Chart Supports Agile Readiness

Things to Remember

MITRE

Transitioning to a Steady State can be a Rocky Road!



Source: Duck, J.D. (2001). The change monster: The human forces that fuel or foil corporate transformation and change. New York: Crown Business., pgs. 16-17

In Summary

- Have a vision; organize the team structure and accountability
  - Apply change transformation process
- Determine the right fit of agile practices
- Use tools and metrics for program support
- Don’t be afraid to change
- Stay the course – it’s an evolution

MITRE

Labeled for Reuse

Agile research for maximum ***<u>IMPACT</u>***

Assessing the Impacts of TSCA Reform: A DoD Enterprise Wide Approach

Acquisition, Technology and Logistics

National Defense Industrial Association
20th Annual Systems Engineering Conference
Panel Discussion

October 25, 2017

TSCA Session Panelists

Dr. Patricia Underwood

Office of the Assistant Secretary of Defense,
Energy, Installations, and Environment

Mr. Jim Rudroff

Office of the Deputy Assistant Secretary of the Navy,
Environment

Mr. Sherman Forbes

Office of the Deputy Assistant Secretary of the Air Force,
Science, Technology and Engineering

Mr. Shane Esola

Defense Contract Management Agency,
Industrial Analysis Group

Platform Discussion Objectives

Provide overview of DoD - EPA engagement and the opportunities for providing useful information to EPA for consideration during risk evaluation and draft rule making.

Present the process for identifying DoD conditions of use and criticality of use for the initial 15 TSCA chemicals.

Present the outcome of a pilot industrial base assessment that considered suppliers, availability of potential chemical substitutes, and projects the associated industrial base impact of methylene chloride and *N*-methylpyrrolidone.

Discuss the market impacts should national security exemptions be incorporated into rule makings for specific chemicals and the conditions that may lead to the formation of DoD-specific niche markets.

Explore additional approaches and strategies to mitigate impacts to DoD.

Impacts of TSCA Reform: Some Key Questions

How can TSCA reform impact the DoD Mission?

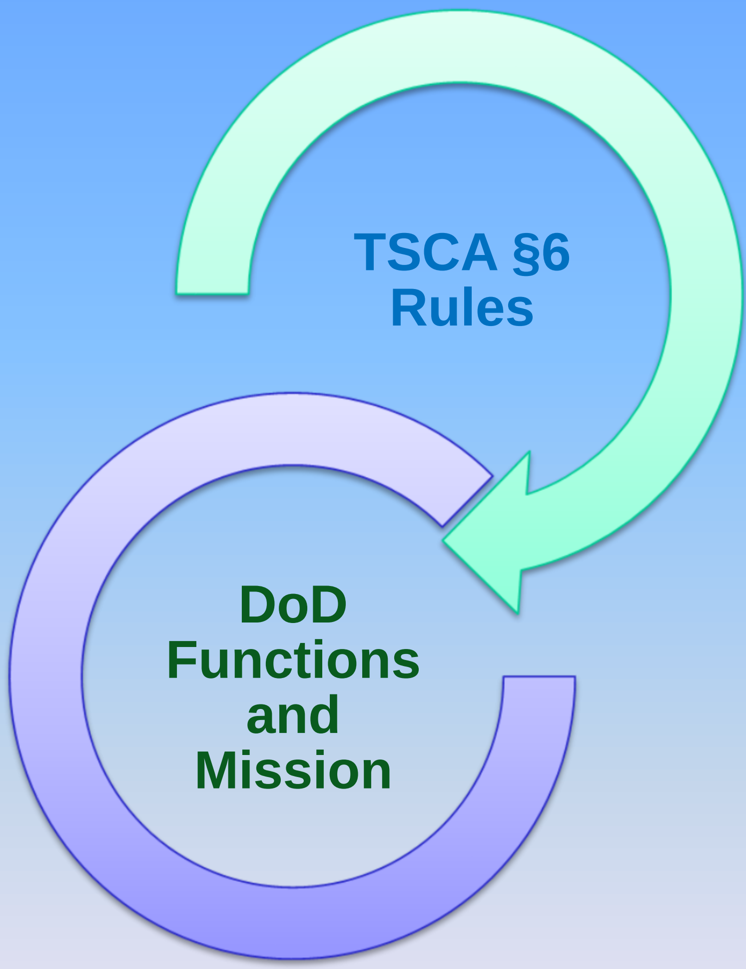
Does TSCA apply to Federal agencies?

Would a National Security Exemption help reduce supply chain and mission risks?

How will the Defense Industrial Base be impacted?

And how will that impact affect the DoD Mission?

Impacts to DoD from TSCA §6 Rulemaking



- EPA can apply one or more of the following risk management actions
  - Ban on manufacturing, processing, distribution and commercial uses of the chemical
  - Restriction of specific chemical uses
  - Regulation of disposal methods
  - Labeling requirements
  - Recordkeeping requirements
  - Notification requirements

- EPA risk management actions can impact a number of DoD functional areas
  - Adversely impact mission critical functions associated with acquisition & logistics
  - Increased workload
    - Reviewing safety/risk assessments
    - Determining DoD functions/systems affected
    - Assessing availability of substitute chemicals and whether they can meet DoD performance specifications

DoD Approach for Assessing and Mitigating Potential Mission Risks

- Engage with EPA OCSPP
  - Policy and legal
- Engage with EPA OPPT Chemical Mangers
  - Occupational uses
  - Occupation exposure data
- DoD Enterprise-wide Risk Evaluation
  - Identify mission critical uses and alternatives
  - Evaluate market impacts
  - Consider utility of National Security Exemption
- Comment on Chemical Specific Rule Making
  - Interagency
  - Public docket

Strategy depends on effective communication and information sharing with stakeholders across DoD, the Defense Industrial Base and the chemical manufacturers, formulators, and distributors.

Ongoing TSCA §6(a) Rulemaking

- Section 6(a) Work Plan Chemicals with Completed Risk Assessments
  - EPA Assessments for TCE, MC and NMP demonstrated significant risks to workers
    - Trichloroethylene (TCE)
      - Proposed rule to ban TCE use in commercial and consumer aerosol degreasing and as a spot cleaner in dry cleaning (December 2016)
      - Proposed rule to ban TCE use in commercial vapor degreasing (January 2017)
    - Methylene chloride (MC) and *N*-methylpyrrolidone (NMP)
      - Proposed rule to regulate MC and NMP in paint and coating removal (includes National Security Exemption) (January 2017)
  - OMB interagency review of draft rules – Sept-Nov 2016
  - OSD coordinated review and comment on TCE in aerosol degreasing/spot cleaning and on MC and NMP in paint removers

Methylene Chloride and NMP: Defense Industrial Base Assessment

DoD Uses

Aerospace products

Hexavalent chromium free aircraft conversion coatings

Aircraft parts requiring nondestructive inspection

Bonding, primers, sealants, and adhesives

Removal of coatings from corrosion sensitive components

National Security Exemptions

- Draft Rule on Methylene Chloride and NMP
  - Rulemaking proposes ban on all uses associated with paint and coating removal
  - Proposes National Security Exemption (NSE) for specific uses in Army, Navy and Air Force aviation and Navy ship maintenance applications
    - Use of currently available substitute chemicals or methods may lead to shortened service life for critical components (some of which are no longer manufactured), reduced availability and mission readiness of military aircraft and vessels, and an increased risk of catastrophic failure of safety critical parts
    - Time-limited exemption – 10 years with the potential for extension
  - DoD comments submitted to OMB and EPA
    - Selection of risk management options other than a ban
    - Separation of consumer versus industrial exposure risk including a recognition of existing industrial safety practices
    - Potential conflicts from multiple agencies implementing and enforcing occupational workplace exposure standards and controls

Defense Industrial Base Assessment

- DUSD ESOH CMRMP collaboration with Defense Contract Management Agency Industrial Analysis Center
- Identify industrial base suppliers including single, foreign and potential alternative suppliers
- Evaluate market impact of regulating MC and NMP for all conditions of use (supplier viability, price and chemical availability)
  - Fragility: A company's financial health and competitive environment within a sector
    - Financial outlook of company
    - Dependence on DoD sales
    - Number and type of firms in sector
    - Foreign dependency
  - Criticality: Importance of product to the DoD
    - Defense uniqueness
    - Skilled labor requirements for manufacturing product
    - Unique facility and equipment requirements
    - Available alternatives, including products and technologies
  - Leverage information and DCMA Financial Capability Group to assess potential effects of fluctuations in future demand and price on supplier viability
  - Evaluate potential for niche market to form due to national security exemption

Current TSCA §6(b) Rulemaking

- Section 6(b) – First 10 Chemicals for Risk Evaluation
  - Within 6 months, EPA must identify and publish a list of the first 10 chemicals for risk evaluation
  - List must be drawn from the 2014 update to the TSCA Work Plan
  - Publication triggers statutory deadlines
    - List of first ten chemicals published (November 29, 2016)
    - Scoping of risk evaluation within 6 months (June 2017)
    - Risk evaluation (3 to 3½ years)
    - Risk management rule identified “unreasonable risk” (2-4 years following risk evaluation)

Current TSCA §6(h) Rulemaking

- Section 6(h) Persistent, Bioaccumulative and Toxic Chemicals (PBTs)
  - Section 6(h) requires EPA to take expedited risk management action on certain PBT chemicals listed on the TSCA Work Plan
    - EPA must propose rules to reduce exposure to the extent practicable within 3 years (June 22, 2019) and finalized 18 months later
    - No risk evaluation required, only use and exposure assessment
  - Manufacturers could request full risk evaluation by September 19, 2016 in lieu of expedited action

TSCA High-Priority and Persistent, Bioaccumulative and Toxic (PBT) Chemicals

CASRN	Chemical	TSCA	DoD Use
123-91-1	1,4-Dioxane	High Priority: List of 10	Y
106-94-5	1-Bromopropane	High Priority: List of 10	Y
1332-21-4	Asbestos	High Priority: List of 10	
56-23-5	Carbon Tetrachloride	High Priority: List of 10	Y
3194-55-6 25637-99-4	Cyclic Aliphatic Bromide Cluster (HBCD)	High Priority: List of 10	
75-09-2	Methylene Chloride (MC)	High Priority: List of 10	Y
872-50-4	N-methylpyrrolidone (NMP)	High Priority: List of 10	Y
81-33-4	Pigment Violet 29	High Priority: List of 10	
79-01-6	Trichloroethylene (TCE)	High Priority: List of 10	Y
127-18-4	Tetrachloroethylene (PCE)	High Priority: List of 10	Y
1163-19-5	Decabromodiphenyl ethers (DecaBDE)	PBT: List of 5	
87-68-3	Hexachlorobutadiene (HCBD)	PBT: List of 5	Y
133-49-3	Pentachlorothio-phenol (PCTP)	PBT: List of 5	
68937-41-7	Tris (4-isopropylphenyl) phosphate	PBT: List of 5	Y
732-26-3	2,4,6-Tris(tert-butyl)phenol	PBT: List of 5	

EPA Next Steps:

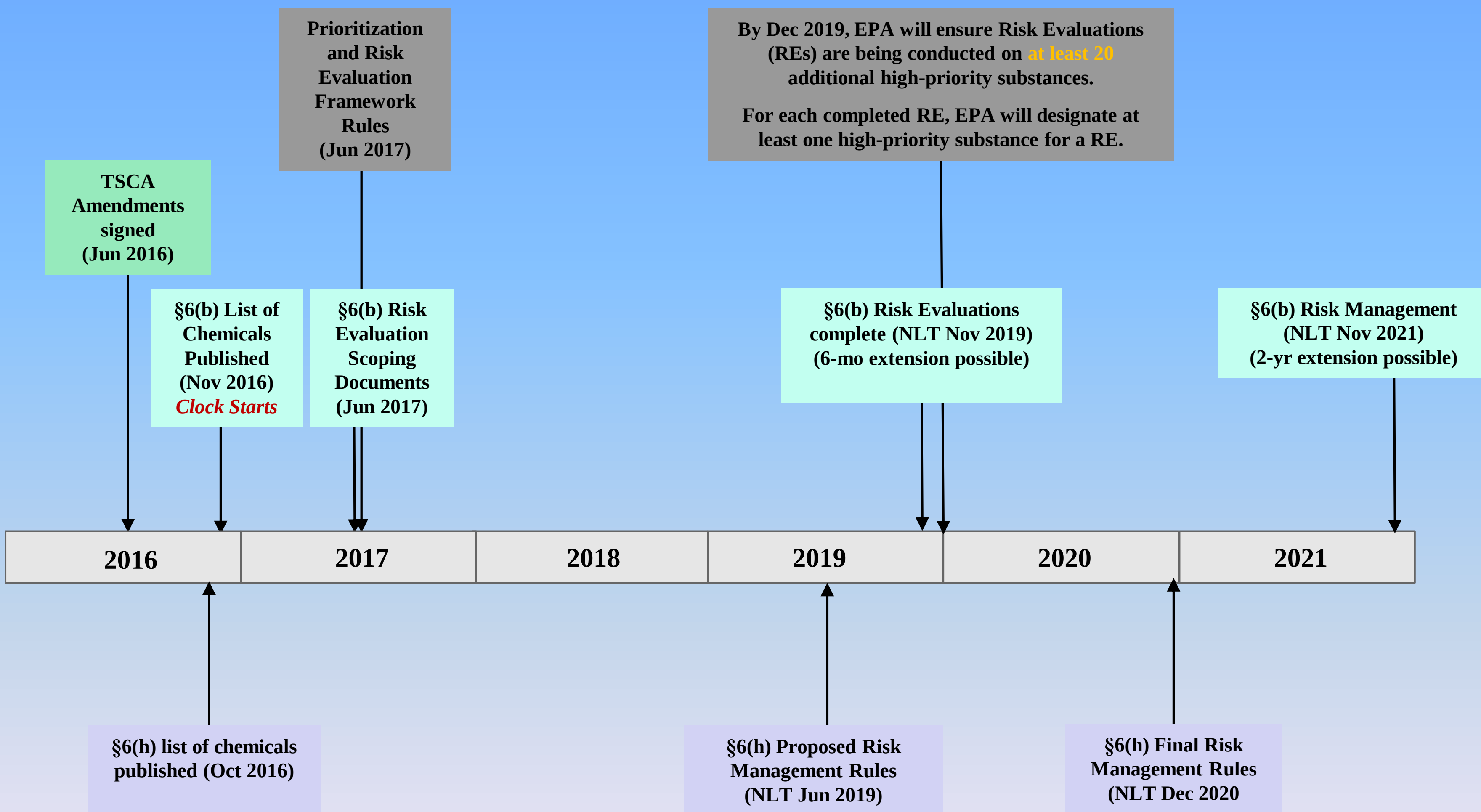
List of 10: EPA published risk evaluation scoping document in June 2017 to include the hazard(s), exposure(s), conditions of use, and the potentially exposed or susceptible subpopulation(s) the Agency plans to consider for the evaluation.

List of 5: EPA to propose expedited action not later than June 22, 2019.

▲ REACH regulated chemicals that are DoD mission critical

TSCA Reform Statutory Requirements Drive Aggressive and Unrelenting Timeline

Acquisition, Technology and Logistics



Questions regarding how TSCA will be implemented remain. However, the rapid advancement of rule making and the possibility for secondary and tertiary impacts to the DoD supply chain require DoD to support on-going engagement with EPA.

Panel Questions

How can TSCA reform impact the DoD Mission?

How will TSCA result in increased supply chain and mission risks?

How can DoD better engage with the Defense Industrial Base to understand market impacts?

Are chemical manufacturers aware of the potential impacts to the defense industrial base and the DoD mission?

Improving Effectiveness with respect to Time-To-Market and the Impacts of Late-stage Design Changes in Rapid Development Life Cycles

Abstract Reference number: 19738

Parth Devang Shah
Doctoral Candidate – Systems Engineering

Under the Guidance of Advisors:
Dr. Blake Roberts and Dr. Michael Grenn

Department of Engineering Management and Systems Engineering
School of Engineering and Applied Science

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Abstract

Data suggest that lifecycle developments are reducing by 40% within consumer goods, defense, retail, automotive, aerospace and service industries where rapid innovation is required. The author proposes a rapid systems engineering framework to address late design changes and allow for flexibility (i.e. to react to unexpected or late changes and its impacts) during the product development cycle using a Systems Engineering approach. A System Engineering approach is crucial in today's product development to deliver complex products into the marketplace. Past literature, research, and methods such as concurrent development, simultaneous engineering, knowledge management, component sharing, rapid product integration, tailored systems engineering processes, and studies on reducing product development cycles all suggest a research gap exist in specifically addressing late design changes due to the shortening of life cycle environments in increasingly competitive markets. The author's research suggests that:

1) product development cycles **time scales are now measured in months** instead of years,
2) more and more products have interdependent systems and environments that **are fast-paced and resource critical**,
3) **product obsolescence is higher** and more organizations are releasing products and services frequently,
4) increasingly **competitive markets** are leading to customization based on consumer feedback.

The author will quantify effectiveness with respect to success factors such as Time -To-Market, Return-Of-Investment, Life Cycle Time and flexibility in late design changes by complexity of product or service, number of late changes and ability to react and reduce late design changes.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Where does my research help?

A lot of work is being done with respect to reducing product development time, concurrent engineering, reducing, rapid product integration, lean and agile methodologies and system engineering advances.

However not much research is currently being focused on the consequences of these life cycle reductions. Due to the shortening of the lifecycles, a lot of design changes are pushed towards the end of the life cycle and changes are made to products and services even after the life cycle.

My research focuses on how to effectively deal with these design changes using a Systems Engineering approach and provide flexibility in the system life cycle process.

Measure of Effectiveness Factors – Time, Cost, Quality

- **Time –** Cycle Time, Product Development Time, Concept to Customer Time, Time to Market
- **Cost –** Return on Investment (ROI), Cost of Ownership, Cost of Development
- **Quality –** Customer Satisfaction, Number of Design Changes post Mass Production,

Research Questions

- Are we experiencing faster design/development lifecycles?
- Is the System Engineering process different for rapid timelines?
- Are late design change impacts different for short vs. long lifecycles?
- Are more and more organizations experiencing late design changes in their products and services?
- Are we moving towards a more tailored approach – i.e. based user feedback and performance in the marketplace?

Hypothesis & Definitions

Null Hypothesis (Ho) -
Incorporating a Rapid Systems Engineering approach will increase effectiveness in decision making and flexibility in design changes when used in fast paced and resource critical environments

***Alternate Hypothesis (Ha)* – Using a traditional approach will decrease effectiveness** in decision making and flexibility in design changes when used in fast paced and resource critical environments

Definitions:

Rapid Systems Engineering: Is as a set of System Engineering tools, methodologies and management techniques that results in a SE life cycle which help reduce the time to market from concept to implementation, without sacrificing the quality of products. [1]

Effectiveness: The capability to yield the desired result or outcome.

Flexibility: The ability of reacting to uncertainty and unexpected changes which would help with reducing the impact of output redesign.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Literature Summary

- **Reviewed over 1600 abstracts / titles on the following terms:**
  - Tailored System Engineering Processes
  - Rapid Systems Engineering
  - Concurrent / Simultaneous Engineering
  - Long vs. Short Development Cycles
  - Industry Cycle Processes – Time Studies
  - Speed – Success Relationship in NPD

- **Preliminary Results**
  - **Reduction in NPD Cycle times** is a reality [1,2,3,4]
  - More organizations are **undergoing design changes** not only just along the Life Cycle but also after the Go Live Stage [5,6,7]
  - **Quicker product obsolescence**, more product variations and customizations and increasing competition are all elements organization are experiencing [8,9]
  - **Everchanging customer demands** and **constant technological advances** have increased the innovation in products and services [10,11,12]
  - **Agile** system engineering practices have **matured for software** projects **while hardware** system engineering continues to embrace **classical development** techniques. [13,14]

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

NPD Cycle Time Study [22]

Product	Organization	Cycle Time (months)			
		Previous	Now	# Reduced	%
Automobile					
Construction equipment	Deere & Co.	84	50	34	**40%**
Car - Viper	Chrysler	72	36	36	**50%**
Car - Accord	Honda	60	36	24	**40%**
Trucks	Navistar	60	30	30	**50%**
Electric clutch brake	Warner	39	9	30	**77%**
Communication Gear	Codex	34	16	18	**53%**
Medical					
Medical Imaging machines	Polaroid	72	36	36	**50%**
Commercial & Defense					
Fiber Optic Gyroscope/Multiple projects	DARPA	60	36	24	**40%**
E-2D Advanced Hawkeye	Northrop Grumman	95	136	-41	**-43%**
Boeing 777	Boeing	60	60	0	**0%**
Boeing 778	Boeing	65	83	-18	**-28%**
Airbus A-380	Airbus	44	49	-5	**-11%**
Consumer Products					
Copier	Xerox	60	36	24	**40%**
Desk Jet Printers	HP	54	22	32	**59%**
Copier - FX 3500	Fuji-Xerox	38	29	9	**24%**
Work Computers	IBM	48	14	34	**71%**
Air powered grinders	Ingersol Rand	40	15	25	**63%**
Cordless phones	AT&T	24	12	12	**50%**
Wedding rings	Feature Ent.	4	0.25	4	**94%**
Coffee Brewers	Keurig Green Mountain	26	14	12	**46%**

A study on reduction in Cycle Times

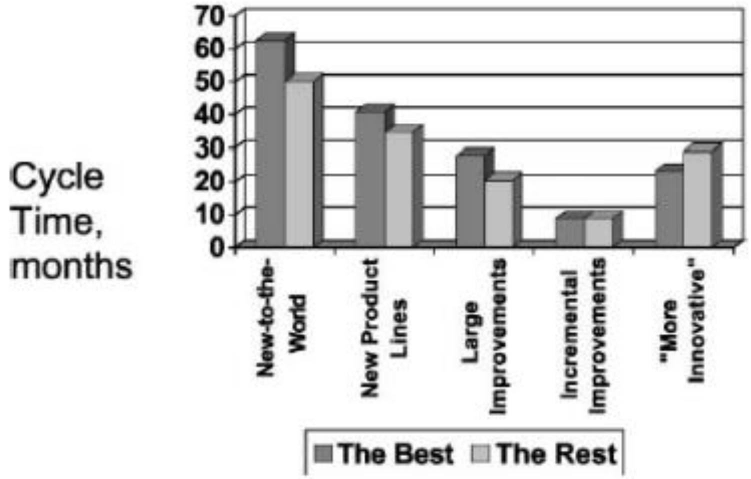


Fig. 4. Cycle time by project type.

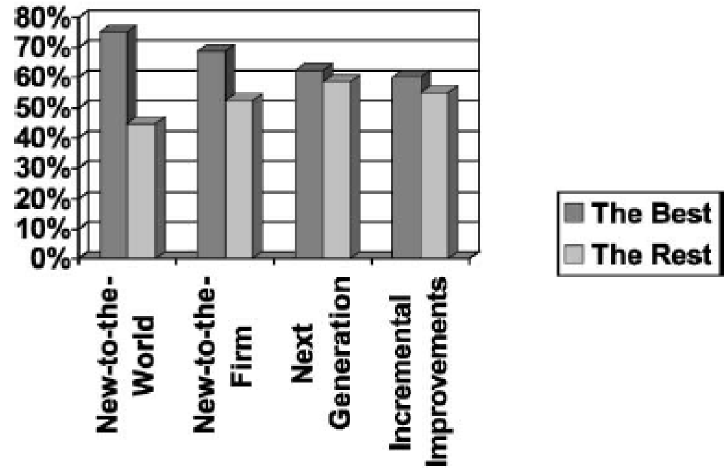


Fig. 5. Percentage of firms reducing cycle times in the last 5 years.

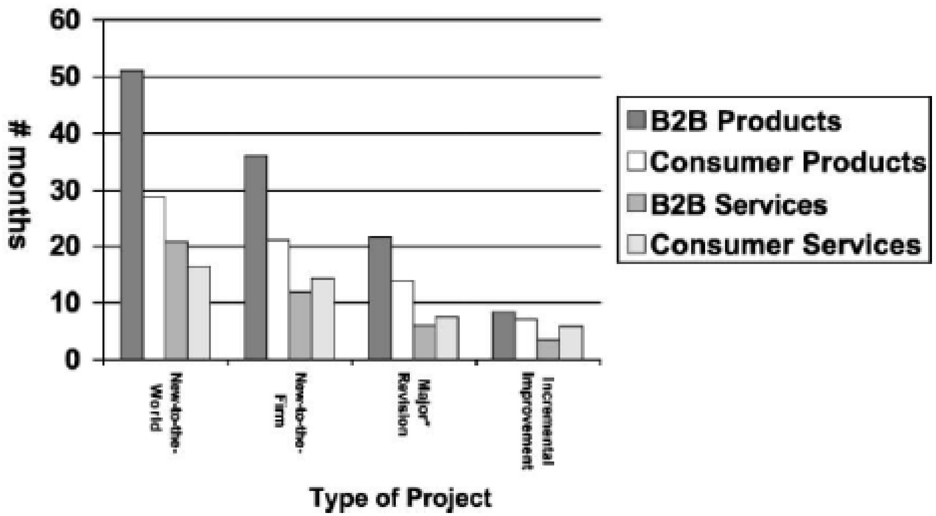


Fig. 7. NPD cycle time by market and product type.

Figure 1, 2 & 3: Source: Griffin, Abbie. (2002). Product Development Cycle Time for Business to Business Products. Industrial Marketing Management. 31. 291-304. 10.1016/S0019-8501(01)00162-6. [23,24]

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Development Phase Comparison & Consumer Products Adoption Rates

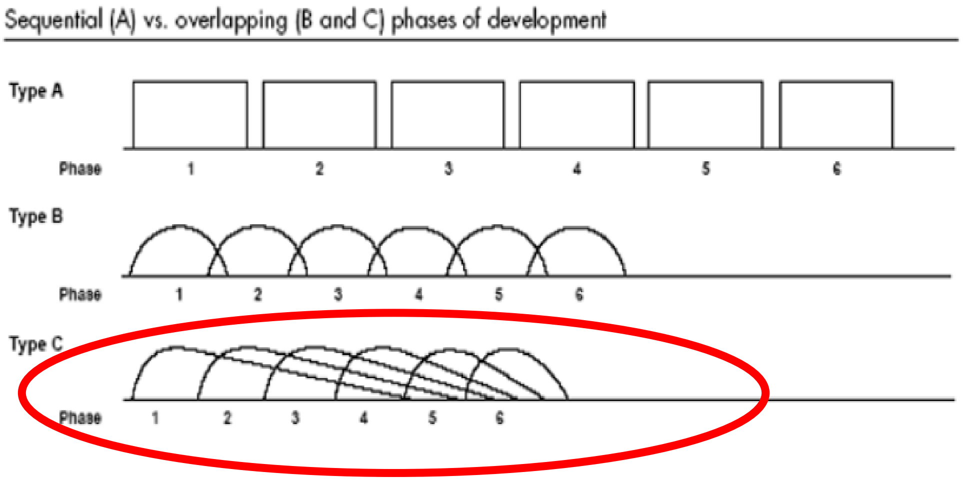


Figure 4: Source: Nonaka, Hirotaka TakeuchiIkujiro. “The New New Product Development Game.” Harvard Business Review, 1 Aug. 2014, hbr.org/1986/01/the-new-new-product-development-game. [21]

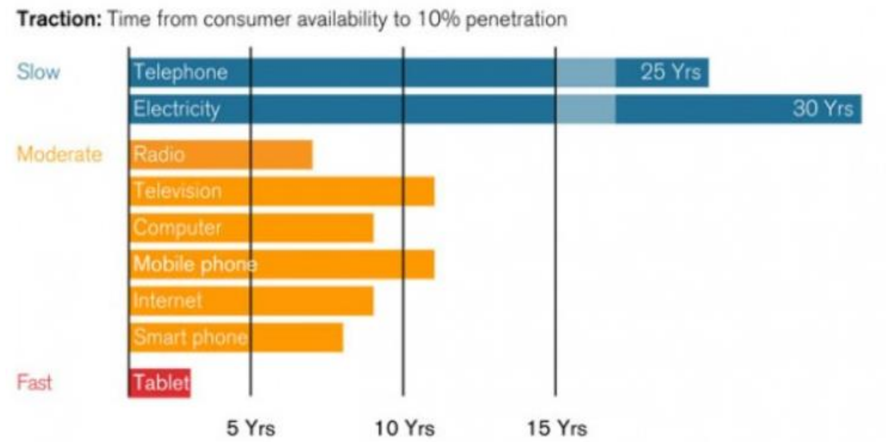


Figure 5: Source: DeGusta, Michael. “Are Smart Phones Spreading Faster than Any Technology in Human History?” MIT Technology Review, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history[22]

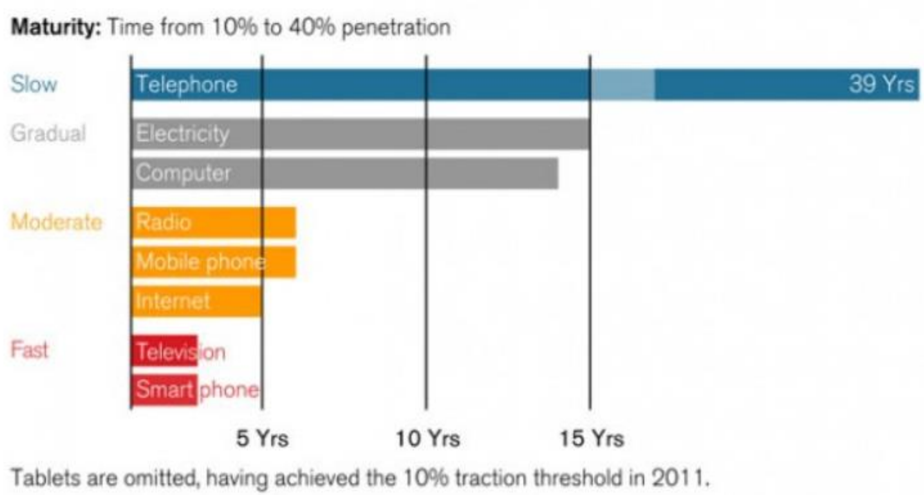


Figure 6: Source: DeGusta, Michael. “Are Smart Phones Spreading Faster than Any Technology in Human History?” MIT Technology Review, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/. [22]

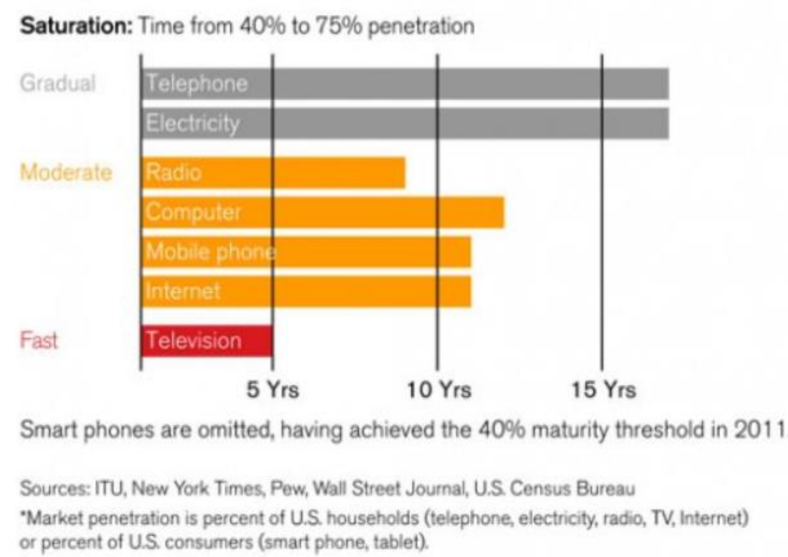


Figure 7: Source:DeGusta, Michael. “Are Smart Phones Spreading Faster than Any Technology in Human History?” MIT Technology Review, MIT Technology Review, 30 Dec. 2013, www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/. [22]

Examples for Discussion

The below examples share the good and bad side of focusing on time to market

Time & Flexibility – Next source of Competitive Advantage

Honda

- Honda manufactures **three variation** – Honda Pilot, Honda CRV & Acura MDX in **one flexible manufacturing line**. [18]
- Single Assembly line and switch lines for newly designed vehicles in hours
- Allows the company to reduce manufacturing time, faster time to market, make customizations easily based on consumer feedback and increase efficiency.
- Company is able to accomplish **Time, and Cost** targets.

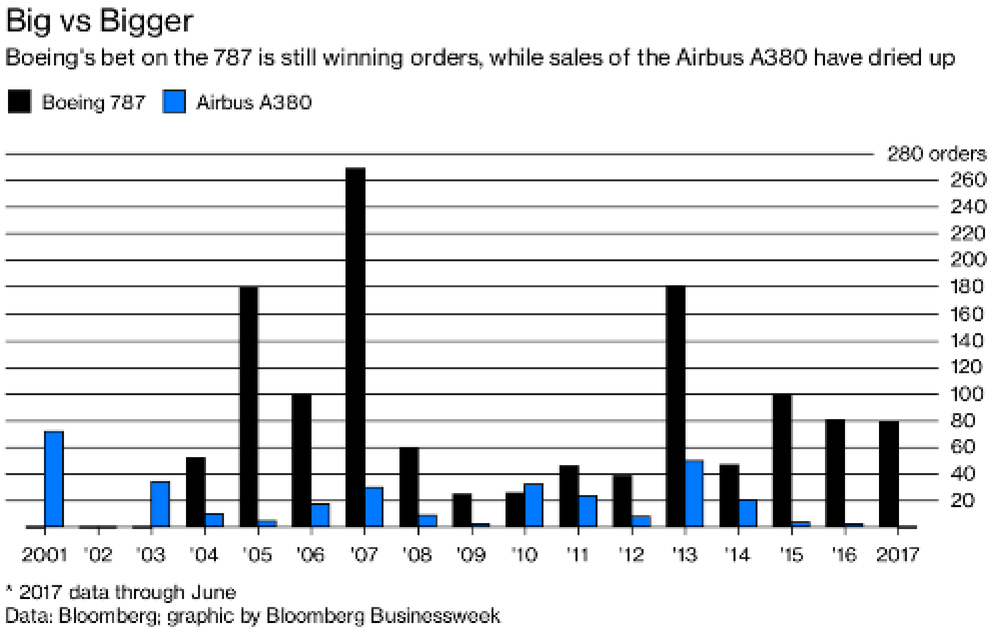
Figure 8, 9 & 10: Source: Eaton, Dan. "Honda starts production of Acura SUV in Ohio after $85M investment." Columbus Business First, Bizjournals.com, 1 June 2017, 16:14pm, www.bizjournals.com/columbus/news/2017/06/01/honda-starts-production-of-acura-suv-in-ohio-after.html.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Boeing's Gamble pays off after launch delays [16,17]

	Airbus A380	Boeing 787
Launch Date	August 2008	October 2011
Cost	$403.9 Million	$290.7 Million
Size	525	300 - 330
Deliveries	119	103
Order	259	1012

***Data as of Jan 2017



[Boeing 787 vs. Airbus A380 – A Time to Market Study]

Figure 11: Source:Topham, Gwyn. "Battle for the future of the skies: Boeing 787 Dreamliner v Airbus A380." The Guardian, Guardian News and Media, 29 Dec. 2013, www.theguardian.com/business/2013/dec/29/boeing-787-dreamliner-airbus-a380-battle-for-skies.

Figure 12: Katz, Benjamin D, and Julie Johnsson. "Boeing's Gamble on 787 Pays Off as Orders Outpace Airbus A380." Bloomberg.com, Bloomberg, 1 Aug. 2017, www.bloomberg.com/news/articles/2017-08-01/boeing-s-gamble-on-787-pays-off-as-orders-outpace-airbus-a380.

Volvo's Rapid Strategy

Volvo's 50% Attempt [15]

- Plans to reduce complete cycle time from **42 months to 20 months** on the XC90 Model by 2020
- Virtual testing & Simulation instead of prototype
- Common architectures and modules
    - **Volvo Engine Architecture (VEA)** – A Four cylinder engine which will be compatible in eight end-products, reducing complexity by **75% commonality.**
- Company is able to accomplish **Time, and Cost** targets.

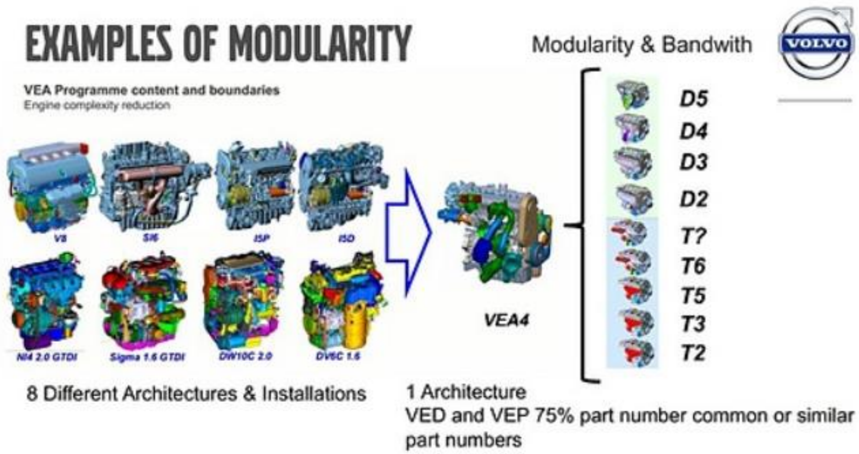


Figure 13 & Figure 14: Source: Morey, Bruce. "Volvo's Rapid Strategy aims at 20-month vehicle development;" SAE International. Oct 24, 2014. Web. March 4, 2017 <http://articles.sae.org/13621/>.

Samsung trips on Quality control measures in order to beat Apple

Samsung Galaxy Note 7 Recall

16.8% Share Price Drop & about $9.5 billion dent [19,20]

- Lab times and **testing periods were shrunk** to expedite approval and **focus on time-to-market**
- Increased complexity and faster timelines
- Battery Problem 1 – Battery size too small in one corner leading to short circuiting
- Battery Problem 2 – Incorrect welding by third party supplier

- Improved 8 point process for battery check and other quality related issues

Figure 16: Source: Wang, Jules. “Galaxy Note 7 explodes, and we're not talking demand.” Pocketnow, 24 Aug. 2016, pocketnow.com/2016/08/24/galaxy-note-7-explodes-in-china.

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Questions for the Audience

- Potential sources of data?
  - New Product Development Cycle Times from 2000 to 2017
  - Decrease or Increase in Manufacturing Cycle Times
  - Any time or cost comparison studies or data sources related to shortening of overall system life cycles

- Additional literature not included or missed during my review?

Biography

<u>Education:</u> Parth Devang Shah is currently a **Doctoral Candidate in Systems Engineering** at The George Washington University.

He also holds a **Bachelor's degree in Mechanical Engineering Technology** and a **Master's degree in manufacturing Leadership**, both earned at the Rochester Institute of Technology located in Rochester, NY.

<u>Professionally:</u> Parth is currently a **Director at Unique Instruments & Mfrs. Pvt. Ltd.** located in Bangalore, India. Unique Instruments is an Aerospace Company which specializes in manufacturing structural components for Commercial and Defense companies globally.
Prior to this, Parth Shah was a Senior Quality Engineer in the New Product Development Team at **Keurig Green Mountain** in Boston, MA.

<u>Contact Information:</u>
Parth Devang Shah
George Washington University
Email: pds4409@gwu.edu
Phone: +91 - 9845209059

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Questions, Concerns or Suggestions?

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Literature Summary - Papers

1. E. H. Kessler, and P. E. Bierly. "Is Faster really Better? an Empirical Test of the Implications of Innovation Speed." *IEEE Transactions on Engineering Management* 49.1 (2002): 2-12. Web.
2. Griffin, Abbie. *Product Development Cycle Time for Business-to-Business Products*. 31 Vol. , 2002. Web.
3. Jiyao Chen, R. R. Reilly, and G. S. Lynn. "The Impacts of Speed-to-Market on New Product Success: The Moderating Effects of Uncertainty." *IEEE Transactions on Engineering Management* 52.2 (2005): 199-212. Web.
4. R. J. Calantone, and C. A. Di Benedetto. "Performance and Time to Market: Accelerating Cycle Time with Overlapping Stages." *IEEE Transactions on Engineering Management* 47.2 (2000): 232-44. Web.
5. J. Lee, and P. Gupta. "Incremental Gate Sizing for Late Process Changes". 2010 IEEE International Conference on Computer Design. Web.
6. M. H. El-Jamal. "Requirements Change using Product Lifecycle Management for Manufacturing Processes in a Systems Engineering Context". 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications. Web.
7. P. M. Huang, A. G. Darrin, and A. A. Knuth. "Agile Hardware and Software System Engineering for Innovation". 2012 IEEE Aerospace Conference. Web.
8. R. Rai, and J. Terpenny. "Principles for Managing Technological Product Obsolescence." IEEE Transactions on Components and Packaging Technologies 31.4 (2008): 880-9. Web.
9. C. Jennings, D. Wu, and J. Terpenny. "Forecasting Obsolescence Risk and Product Life Cycle with Machine Learning." IEEE Transactions on Components, Packaging and Manufacturing Technology 6.9 (2016): 1428-39. Web.
10. A. Dibbo. "Measuring Marketing Performance." *Engineering Management Journal* 3.6 (1993): 255-8. Web.
11. D. Georgakopoulos, et al. "Internet of Things and Edge Cloud Computing Roadmap for Manufacturing." *IEEE Cloud Computing* 3.4 (2016): 66-73. Web.
12. S. Wang, L. Li, and J. D. Jones. "Systemic Thinking on Services Science, Management and Engineering: Applications and Challenges in Services Systems Research." *IEEE Systems Journal* 8.3 (2014): 803-20. Web.
13. E. Stelzmann. "Contextualizing Agile Systems Engineering." *IEEE Aerospace and Electronic Systems Magazine* 27.5 (2012): 17-22. Web.
14. S. B. Schapiro, and M. H. Henry. "Engineering Agile Systems through Architectural Modularity". *2012 IEEE International Systems Conference SysCon 2012*. Web.

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

References

15) Morey, Bruce. "Volvo’s Rapid Strategy aims at 20-month vehicle development;" SAE International. Oct 24, 2014. Web. March 4, 2017 <http://articles.sae.org/13621/>.

16) Topham, Gwyn. “Battle for the future of the skies: Boeing 787 Dreamliner v Airbus A380.” The Guardian, Guardian News and Media, 29 Dec. 2013, www.theguardian.com/business/2013/dec/29/boeing-787-dreamliner-airbus-a380-battle-for-skies.

17) Katz, Benjamin D, and Julie Johnsson. “Boeing's Gamble on 787 Pays Off as Orders Outpace Airbus A380.” Bloomberg.com, Bloomberg, 1 Aug. 2017, www.bloomberg.com/news/articles/2017-08-01/boeing-s-gamble-on-787-pays-off-as-orders-outpace-airbus-a380.

18) Eaton, Dan. “Honda starts production of Acura SUV in Ohio after $85M investment.” Columbus Business First, Bizjournals.com, 1 June 2017, 16:14pm, www.bizjournals.com/columbus/news/2017/06/01/honda-starts-production-of-acura-suv-in-ohio-after.html.

19) Reuters. “Samsung trips on quality control in rush to beat Apple iPhone 7.” The Indian Express, 6 Sept. 2016, indianexpress.com/article/technology/tech-news-technology/samsung-trips-on-quality-control-in-rush-to-beat-apple-iphone-7-3016094/.

20) Wang, Jules. “Galaxy Note 7 explodes, and we're not talking demand.” Pocketnow, 24 Aug. 2016, pocketnow.com/2016/08/24/galaxy-note-7-explodes-in-china.

21) Nonaka, Hirotaka TakeuchiIkujiro. “The New New Product Development Game.” Harvard Business Review, 1 Aug. 2014, hbr.org/1986/01/the-new-new-product-development-game.

22) Griffin, Abbie. (2002). Product Development Cycle Time for Business to Business Products. Industrial Marketing Management. 31. 291-304. 10.1016/S0019-8501(01)00162-6.

23) E. H. Kessler, and P. E. Bierly. "Is Faster really Better? an Empirical Test of the Implications of Innovation Speed." IEEE Transactions on Engineering Management 49.1 (2002): 2-12. Web.

24) Griffin, Abbie. Product Development Cycle Time for Business-to-Business Products. 31 Vol. , 2002. Web.

25) Jiyao Chen, R. R. Reilly, and G. S. Lynn. "The Impacts of Speed-to-Market on New Product Success: The Moderating Effects of Uncertainty." IEEE Transactions on Engineering Management 52.2 (2005): 199-212. Web.

26) R. J. Calantone, and C. A. Di Benedetto. "Performance and Time to Market: Accelerating Cycle Time with Overlapping Stages." IEEE Transactions on Engineering Management 47.2 (2000): 232-44. Web.

Additive Manufacturing – Challenges for the Systems Engineer and Program Manager

October 25, 2017

Bill Decker
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35806
724-612-0999
For further info: john.rice@dau.mil

www.DAU.mil

Ground rules

- This is a discussion, not a lecture
- Your opinions and viewpoints are welcomed
- There are no right/wrong answers

Agenda

- Introduction
- Additive Manufacturing (AM)
  - Defined
  - Advantages
  - Disadvantages
- What does this mean to PM?
- What does this mean to the Systems Engineer
- Discussion
  - How can we use AM? Now? Future?
- Conclusion

Introduction

- Additive Manufacturing is “hot topic”
  - Parts for production of airliners (Embraier and Airbus)

Allows airlines to customize interiors
Cost effective for LRP
Parts may be optimized for each application
To this point – no flight safety critical components

Additive Manufacturing

- What is it:
  - Objects are built up from a precursor material (powder)
  - Generally a uniform material
  - No molds, minimal machining
  - Great design freedom

AM Advantages

- Minimal tooling required
- Make many parts from “bucket of precursor dust”
- Cost effective – especially for small quantities
- Flexible – easier to make changes “on the fly”

AM Barriers/Risks

- Minimal standards for:
  - Materials
  - Processes
  - Qualification of machines
- Repeatability is likely only on one machine, in one location
- Qualification/certification of parts important
- Intellectual property issues – TBD
  - Being discussed by legal community

Systems Engineers' Concerns

- Contractor proposes to use AM part(s)
  - Is (are) the part(s) critical to operation?
    - Flight safety, safety of personnel, mission critical?
    - If no, then less to be concerned about
  - Is it proposed to make the part(s) in more than one location?
- Government proposes to use AM to make spares/perform repairs
  - Is (are) the part(s) critical to operation?
    - Flight safety, safety of personnel, mission critical?
  - Is it proposed to make the part(s) in more than one location?

SE Concerns (cont'd)

- Contractor proposes to use AM parts (cont'd)
  - Do the precursor materials meet a standard?
    - ASTM has only three metal powder standards as of Oct 17

      https://www.astm.org/Standards/additive-manufacturing-technology-standards.html
  - Have the AM machines been qualified?
    - No universal standards exist today
    - How have they demonstrated repeatability?

SE Concerns (cont’d)

- Potential problem areas (current state of AM)
  - Each part/component will require qualification
  - Are unique test procedures and equipment required for systems with AM components?
  - Future parts may require machines and processes that are no longer available (DMSMS)
  - Does the DoD plan to make parts using AM for repair?
    - Intellectual property licenses
    - Machine qualification at site of use
    - Are we sole source for material? Machines?

Discussion/Questions

- How can we use AM? Now? Future?

Conclusion

- AM for prototypes is often a great option
- AM for production is not yet ready for prime time
- AM is well suited for non-critical parts
- AM is flexible, and often cost savings

DoD Systems Engineering Policy, Guidance, and Standardization Update

Aileen Sedmak

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

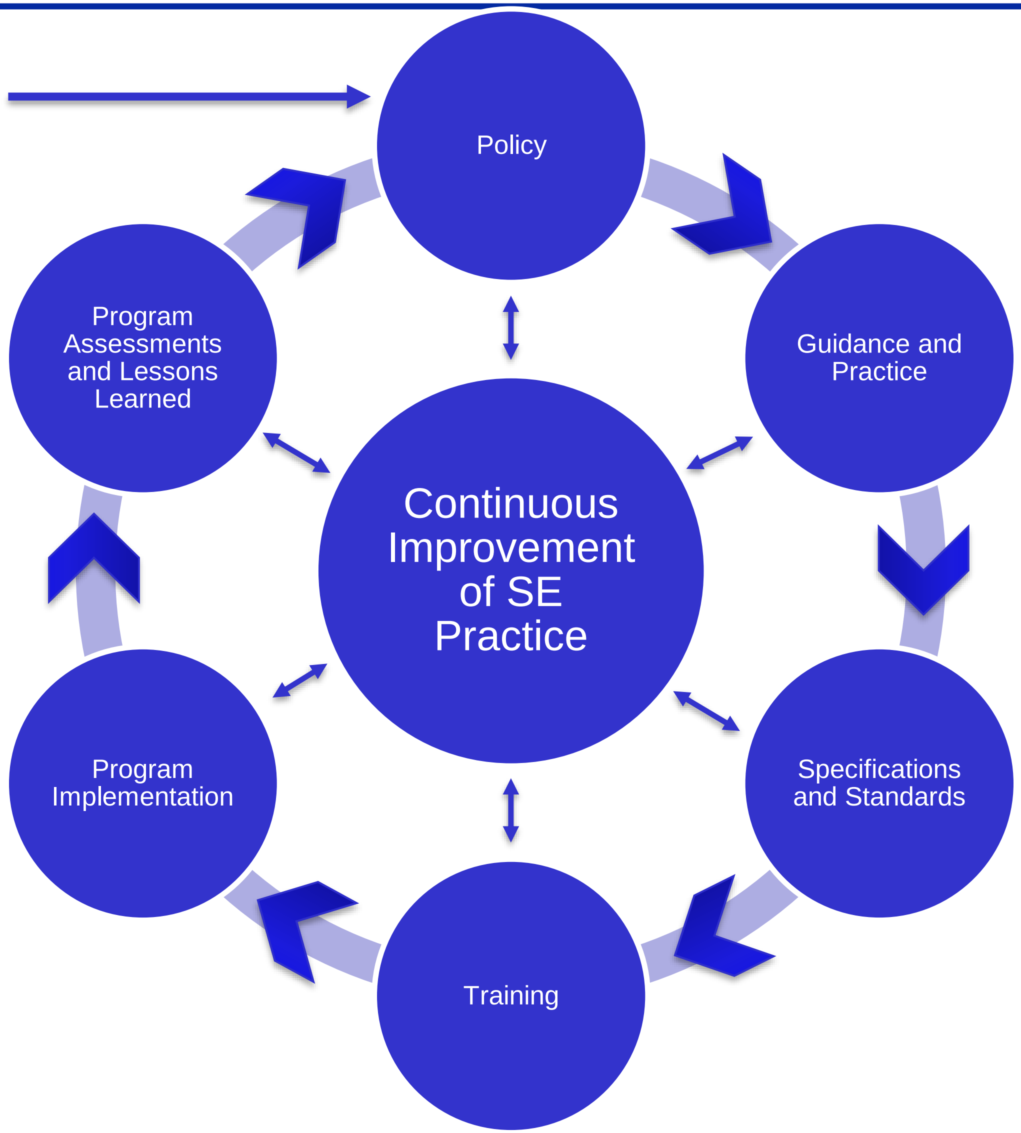
20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 25, 2017

Systems Engineering Policy and Guidance

Additional Drivers

- Legislation
- Leadership Initiatives
- Evidence-Based Best Practices



Recent / Emerging Changes to Systems Engineering Practice

- **Accomplishments**
  - DoDI 5000.02 Operation of the Defense Acquisition System, Change 3, August 10, 2017
  - Defense Acquisition Guidebook (DAG) Chapter 3, Systems Engineering
  - Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs
  - Additional SE Guidance efforts
- **Current Initiatives**
  - Prototyping and Rapid Fielding Policy (NDAA FY16 Section 804 and NDAA FY17 Section 806)
  - MIL-HDBK-61A, "Configuration Management Guidance"
  - Systems of Systems (SoS) ISO Non-government Standards (NGS)
- **Upcoming Drivers**
  - National Defense Authorization Act for Fiscal Year 2017 (NDAA FY17)
    - Sections 805 – 809 "Acquisition agility act"
    - Section 855 "Mission integration management"
    - Section 875 "Use of commercial or non-Government standards in lieu of military specifications and standards"

DoDI 5000.02
SE-Related Updates & Items of Note

- **Core Instruction - Operation of the Defense Acquisition System**

- **Enclosures**

1. Acquisition Program Categories and Compliance Requirements
2. Program Management
3. Systems Engineering
4. Developmental Test and Evaluation (DT&E)
5. Operational and Live Fire Test and Evaluation (OT&E and LFT&E)
6. Life-Cycle Sustainment
7. Human Systems Integration (HSI)
8. Affordability Analysis and Investment Constraints
9. Analysis of Alternatives (AoA)
10. Cost Estimating and Reporting
11. Requirements Applicable to All Programs Containing Information Technology (IT)
12. ~~Acquisition of Defense Business Systems (DBS)~~
13. Urgent Capabilities Acquisition ~~Rapid Fielding of Capabilities~~
14. Cybersecurity in the Defense Acquisition System

Change 1 to DoDI 5000.02 (January 26, 2017)
Approval authority for SEPs assigned to the Milestone Decision Authority (MDA)
Software assurance best practices for implementation of tools and risk-based remediation
"Modular Open Systems Approach" replaces "Open Systems Architecture"
DASD(SE) required to advise on incorporation of best practices for SE from across the Department
Specific risk mitigation techniques required to be considered
Removed congressional notification requirement for competitive prototyping waiver
Broaden MDA Waiver for any 2366b Certification requirements
Change 2 to DoDI 5000.02 (February 2, 2017)
Removed Enclosure 12 and referenced new DoDI 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017
Cancelled DTM 17-001, "Cybersecurity in the Defense Acquisition System," January 11, 2017 and incorporated into Enclosure 14
Change 3 to DoDI 5000.02 (August 10, 2017)
Administrative edits only

Universal Update to the DAG

February 2017 – Published and posted on the new DAU website

- **Improve guidance to fully reflect current policy and DoD initiatives**
- **Address recommendations from Better Buying Power 3.0 *Streamline documentation requirements and staff reviews***
- **Incorporate recognized Department-wide best practices**
- **Update formatting and structure of the document to align to new DAG standardization guidelines**

New DAG Website

The new DAG website enables:

- Access through multiple devices (computer, tablet, cell phone, etc.)
- Ease in publishing changes to chapter content

Systems Engineer is now Chapter 3 vice Chapter 4

https://www.dau.mil/tools/dag

DAG Chapter 3 Outline

CH 3 – 1.0 Purpose

CH 3 – 2.0 Background

- 2.1 Systems Engineering Policy and Guidance
- 2.2 Systems Engineering Plan
- 2.3 Systems Level Considerations
  - 2.3.1 Software
- 2.4 Tools, Techniques, and Lessons Learned
  - 2.4.1 Modular Open Systems Approach
  - 2.4.2 Modeling and Simulation
  - 2.4.3 Sustainability Analysis
  - 2.4.4 Value Engineering
  - 2.4.5 Lessons Learned, Best Practices, and Case Studies
- 2.5 Engineering Resources
- 2.6 Certifications
- 2.7 Systems Engineering Role in Contracting

CH 3 – 3.0 Business Practices: Systems Engineering Activities in the Life Cycle

- 3.1 Life-Cycle Expectations
  - 3.1.1 Systems Engineering in Defense Acquisition Program Models
  - 3.1.2 Systems of Systems
- 3.2 Systems Engineering Activities in Life-Cycle Phases (includes 6 subsections, one for each life-cycle phase)
- 3.3 Technical Reviews and Audits (includes 8 subsections, one for each technical review and audit)

CH 3 – 4.0 Additional Planning Considerations

- 4.1 Technical Management Processes (includes 8 subsections, one for each technical management process)
- 4.2 Technical Processes (includes 8 subsections, one for each technical process)
- 4.3 Design Considerations (includes 24 subsections, one for each design consideration)

New DAG Chapter 3 Major Content Changes

<u>Version 0 (February 2017)</u>

- **Emphasizes *<u>Modular Open Systems Approach</u>* in accordance with NDAA FY15 Section 801 (CH 3-2.4.1)**
- **Updates *<u>SEP approval authority</u>* based on NDAA FY16 Section 832 (CH 3-2.2)**
- **Addresses the key SE considerations for the *<u>defense acquisition models</u>* and life-cycle phases defined in the DoDI 5000.02, January 7, 2015 (CH 3-3.1, CH 3-3.2, and CH 3-3.3)**
- **Incorporates key tenets of the new *<u>DoD Risk, Issue, and Opportunity Management Guide</u>* developed in accordance with BBP 3.0 *Improve our leaders' ability to understand and mitigate technical risk* (CH 3-4.1.5)**
- **References recently *<u>DoD-adopted Non-Government Standards</u>* (IEEE/ISO/IEC15288, IEEE 15288.1, and IEEE 15288.2; EIA 649-1; AS 6500)**
- **Incorporates *<u>Department-wide best practices</u>* for software (CH 3-2.3.1), technical performance measures (CH 3-4.1.3 & CH 3-4.1.3.1), and technical planning process (CH 3-4.1.1)**
- **Enhanced Design Considerations in CH 3-4.3:**
  - Affordability -- SE Tradeoff Analyses; Anti-Counterfeiting; Corrosion Prevention and Control (CPC); Environment, Safety, and Occupational Health (ESOH); Intelligence (Life-cycle Mission Data Plan); Modular Design; and System Security Engineering
- **Removed obsolete information (e.g. In-Service Review (ISR))**

DAG Chapter 3 Recent Updates

Version 1 (May 2017)

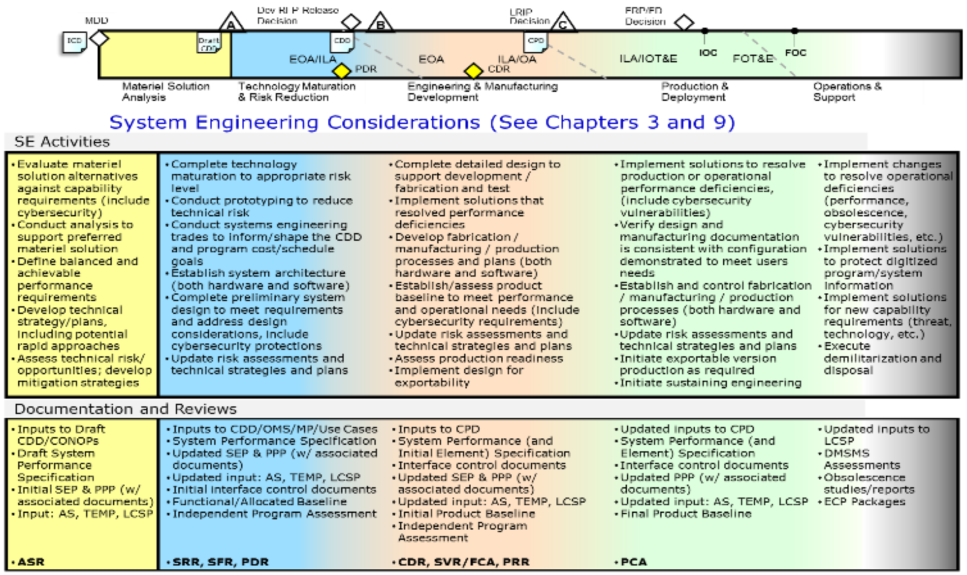
- **Incorporating Change 1 and Change 2 to DoDI 5000.02**
  - Sec 2.3.1 Software
    - Updated references for Model 3: Incrementally Deployed Software Intensive Program to the new DoDI 5000.75
  - Sec 3.1.1 SE in the Defense Acquisition Program Models
    - Updated references for Model 3: Incrementally Deployed Software Intensive Program to the new DoDI 5000.75
    - Updated terminology for Model 4: Accelerated Acquisition Program «Rapid Fielding of Capabilities» to «Urgent Capability Acquisition»
  - Sec 3.2 SE in the Activities in Life-Cycle Phases (Multiple Sub-sections)
    - Addressed updates to prototyping policy (e.g., congressional waiver requirement for not conducting competitive prototyping removed)
  - Sec 4.1.5 Risk Management
    - Minor edits to address risk management techniques consistent with 10 U.S.C. 2431b
- **Addressed User Feedback**
  - Clarifying the Systems Engineer's responsibility in the Program Office
  - Replacing the System Threat Assessment Report (STAR) with the Validated On-line Life-cycle Threat (VOLT) report
  - Other administrative changes

Constantly maintaining the currency of the DAG

DAG CH 1 – Functional Integrated Master Plan (IMP) / Integrated Master Schedule (IMS) Inputs

- **DAG CH 1-3.4 provides guidance on integrated acquisition planning and execution**
  - Describes the IMP/IMS for planning, scheduling, and execution expectations
  - Emphasizes that the program-level IMP/IMS depends upon the development and integration of inputs from all functional areas.
- **Includes typical functional inputs for:**
  - Systems Engineering
  - Product Support
  - Contracting
  - Test & Evaluation
  - Budget
  - Production
  - International Acquisition & Exportability

DAG CH 1 – Figure 12: SE Considerations



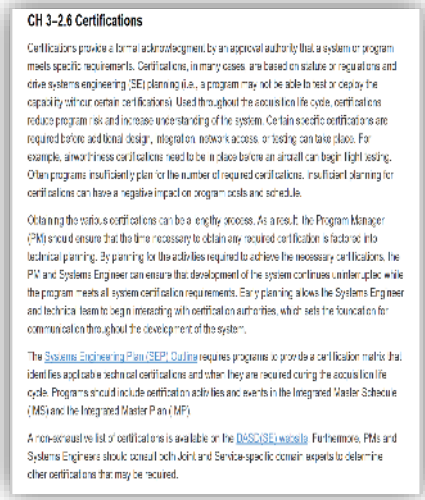
shortcut.dau.mil/DAG/CH01.03.04.03.01

SE influence in DAG Chapter 1 – Program Management

DAG CH3 - Supplemental Guidance
Acquisition Program Technical Certifications

- **UPDATED Acquisition Program Technical Certifications Summary**
  - Lists a non-exhaustive set of program and system-level certifications
  - Supplements DAG CH 3-2.6 Certifications
  - Provides a starting point to program managers and systems engineers for identifying applicable certification requirements
  - Posted on the DASD(SE) Guidance webpage:

http://www.acq.osd.mil/se/pg/guidance.html



CH 3–2.6 Certifications

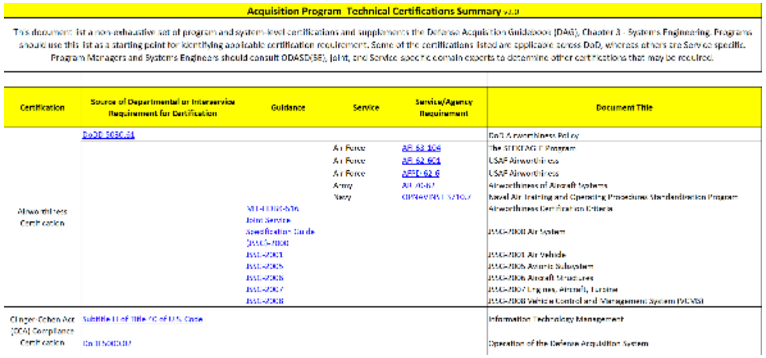
Certifications provide a formal acknowledgment by an approval authority that a system or program meets specific requirements. Certifications, in many cases, are based on statute or regulations and drive systems engineering (SE) planning (i.e., a program may not be able to test or deploy the capability without certain certifications). Used throughout the acquisition life cycle, certifications reduce program risk and increase understanding of the system. Certain specific certifications are required before additional design, integration, network access, or testing can take place. For example, airworthiness certifications need to be in place before an aircraft can begin flight testing. Often programs insufficiently plan for the number of required certifications. Insufficient planning for certifications can have a negative impact on program costs and schedule.

Obtaining the various certifications can be a lengthy process. As a result, the Program Manager (PM) should ensure that the time necessary to obtain any required certification is factored into technical planning. By planning for the activities required to achieve the necessary certifications, the PM and Systems Engineer can ensure that development of the system continues uninterrupted while the program meets all system certification requirements. Early planning allows the Systems Engineer and technical team to begin interacting with certification authorities, which sets the foundation for communication throughout the development of the system.

The Systems Engineering Plan (SEP) Outline requires programs to provide a certification matrix that identifies applicable technical certifications and when they are required during the acquisition life cycle. Programs should include certification activities and events in the Integrated Master Schedule (IMS) and the Integrated Master Plan (IMP).

A non-exhaustive list of certifications is available on the DASD(SE) website. Furthermore, PMs and Systems Engineers should consult both Joint and Service-specific domain experts to determine other certifications that may be required.

DAG CH 3-2.6 Certifications



Acquisition Program Technical Certifications Summary

This document list a non-exhaustive set of program and system-level certifications and supplements the Defense Acquisition Guidebook (DAG), Chapter 3 - Systems Engineering. Programs should use this list as a starting point for identifying applicable certification requirement. Some of the certifications listed are applicable across DoD, whereas others are Service specific. Program Managers and Systems Engineers should consult ODASD(SE), Joint, and Service specific domain experts to determine other certifications that may be required.

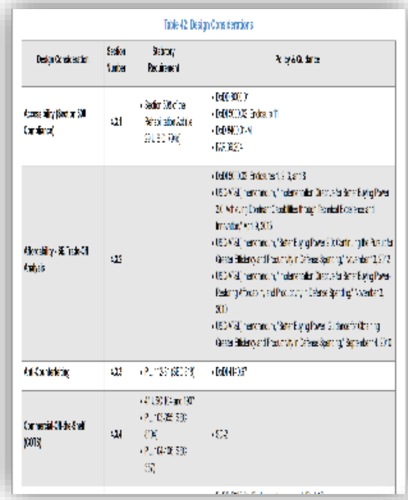
Certification	Source of Departmental or Interservice Requirement for Certification	Guidance	Service	Service/Agency Requirement	Document Title
Airworthiness Certification	DoDD 5030.61				DoD Airworthiness Policy
			Air Force	AR 63 104	The SEEKEAGLE Program
			Air Force	AR 62 601	USAF Airworthiness
			Air Force	AFPD 62 6	USAF Airworthiness
			Army	AR 70-62	Airworthiness of Aircraft Systems
			Navy	OPNAVINST 3710.7	Naval Air Training and Operating Procedures Standardization Program
		MIL-HDBK-516			Airworthiness Certification Criteria
		Joint Service Specification Guide (JSSG-2000)			JSSG-2000 Air System
		JSSG-2001			JSSG-2001 Air Vehicle
		JSSG-2005			JSSG-2005 Avionic Subsystem
		JSSG-2006			JSSG-2006 Aircraft Structures
		JSSG-2007			JSSG-2007 Engines, Aircraft, Turbine
		JSSG-2008			JSSG-2008 Vehicle Control and Management System (VCMS)
Clinger-Cohen Act (CCA) Compliance Certification	Subtitle III of Title 40 of U.S. Code				Information Technology Management
	DoDI 5000.02				Operation of the Defense Acquisition System

Acquisition Program Technical Certification Summary

DAG CH3 - Supplemental Guidance
Design Considerations Standards Summary

- **NEW DAG Chapter 3 Design Considerations Standards Summary**
  - Identifies standards relevant to the design considerations discussed in the DAG CH 3-4.3 Design Considerations
  - Supplements Table 42, which lists the relevant statutes, policy, and guidance for each design consideration
  - Provides program managers and systems engineers appropriate standards they may incorporate into acquisition contracts
  - Posted on the DASD(SE) Guidance webpage:

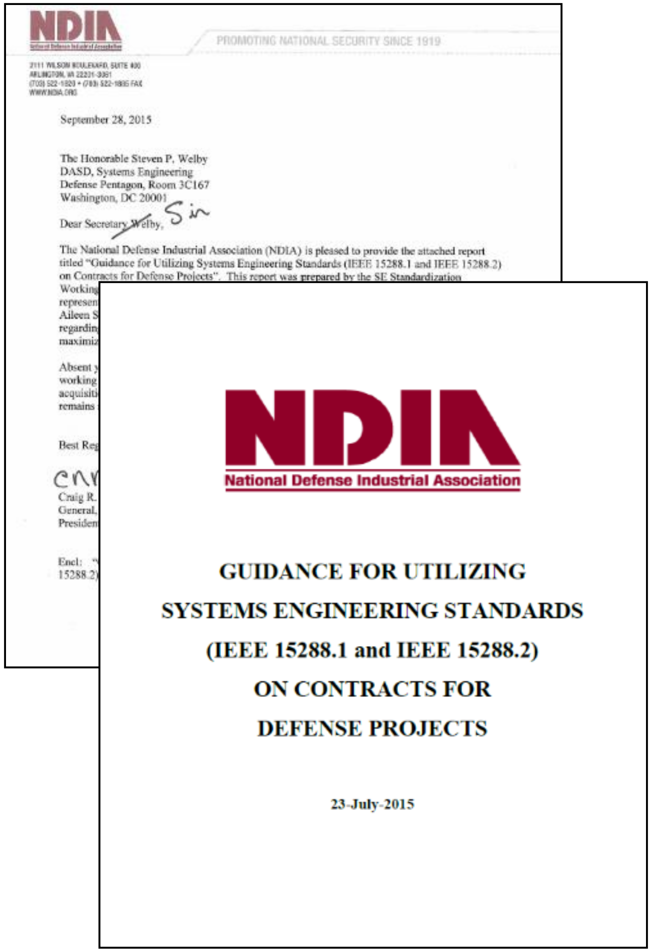
    https://www.acq.osd.mil/se/docs/2017-DAG3-Std.pdf



DAG CH 3-4.3 Design Considerations, Table 42

Design Considerations Standards Summary

IEEE 15288.1 & 15288.2 NDIA Utilization Guidance



NDIA

PROMOTING NATIONAL SECURITY SINCE 1919

September 28, 2015

The Honorable Steven P. Welby
DASD, Systems Engineering
Defense Pentagon, Room 3C167
Washington, DC 20001

Dear ~~Secretary Welby~~, Sir

The National Defense Industrial Association (NDIA) is pleased to provide the attached report titled "Guidance for Utilizing Systems Engineering Standards (IEEE 15288.1 and IEEE 15288.2) on Contracts for Defense Projects". This report was prepared by the SE Standardization

NDIA

National Defense Industrial Association

GUIDANCE FOR UTILIZING SYSTEMS ENGINEERING STANDARDS (IEEE 15288.1 and IEEE 15288.2) ON CONTRACTS FOR DEFENSE PROJECTS

23-July-2015

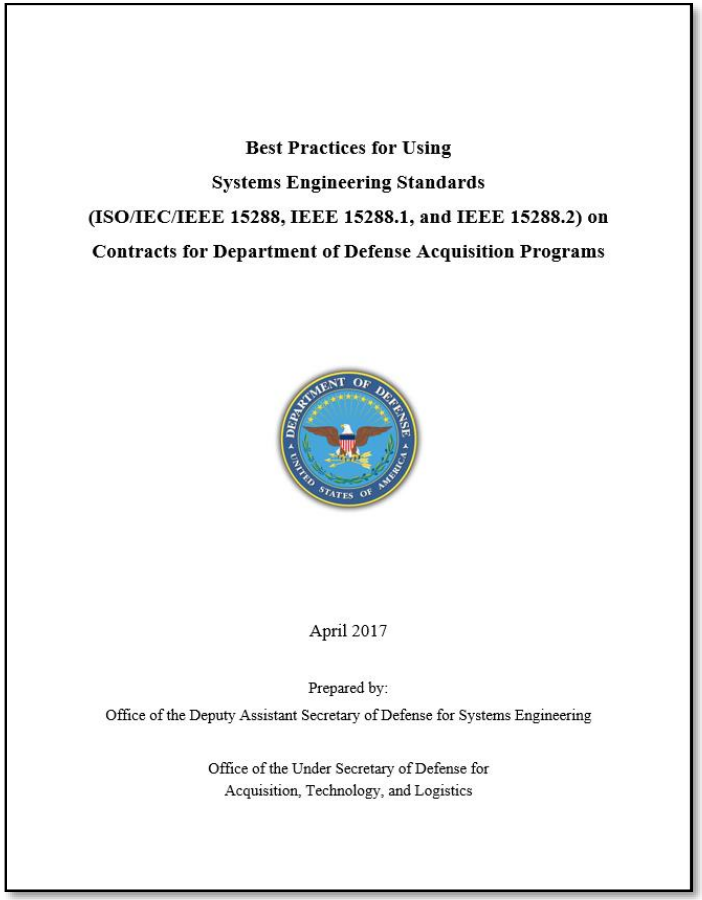
- **At an NDIA SE Division meeting, industry partners expressed concern over the number of normative requirements in the new standards**
  - 750+ normative requirements in 15288.1
  - 1600+ normative requirements in 15288.2
- **NDIA initiated SE Standardization Working Group to develop recommended guidance for effectively and efficiently using the new SE standards on contract**
- **NDIA, in collaboration with DoD representatives, drafted guidance for using 15288.1 and 15288.2 on contract**
- **NDIA provided the guidance as recommendations to DoD, which represented industry's perspective and is aimed at maximizing value to both Government and industry**

Without appropriate tailoring of the SE Standards, assessing compliance could add significant burden and cost on both the Government and industry

DoD Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs Implementation Guidance

- **Collaborated with key DoD stakeholders:**
  - Army, Navy, Air Force, DCMA, DPAP, DAU, and Defense Standardization Program Office (DSPO)
- **The DoD Implementation Guide:**
  - Incorporates relevant DoD statute, policies, and procedures
  - Addresses ISO/IEC/IEEE 15288 as it establishes the common SE framework that is the basis for the two companion standards (IEEE 15288.1 and 15288.2)
  - Provides tailoring template that the Government can use to efficiently convey the specific set of requirements to industry

http://www.acq.osd.mil/se/docs/15288-Guide-2017.pdf



Best Practices for Using
Systems Engineering Standards
(ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on
Contracts for Department of Defense Acquisition Programs

April 2017

Prepared by:
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Office of the Under Secretary of Defense for
Acquisition, Technology, and Logistics

DoD leveraged the NDIA recommended guidance

Other New SE Guidance, White Papers and Publications

- ***Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*** **(Jan 2017)**
- ***Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report Outline Guidance*** **(Feb 2017)**
- **"Model-Based Systems Engineering: Enabling the Digital Engineering Practice in the Department of Defense," Kristen Baldwin, Getting It Right 7(3), February 27, 2017: 1, 3.**
- ***Digital Model-based Engineering: Expectations, Prerequisites, and Challenges of Infusion*** **(Mar 2017), developed by the Model-Based Systems Engineering (MBSE) Infusion Task Team**
- ***Guidebook for Acquiring Engineering Technical Services (ETS) Best Practices & Lessons Learned Version 2.0*** **(Apr 2017)**

These documents can be found at

http://www.acq.osd.mil/se/pg/guidance.html &
http://www.acq.osd.mil/se/pubs/index.html

Recent / Emerging Changes to Systems Engineering Practice

- ✓ **Accomplishments**
  - DoDI 5000.02 Operation of the Defense Acquisition System, Change 3, August 10, 2017
  - Defense Acquisition Guidebook (DAG) Chapter 3, Systems Engineering
  - Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs
  - Additional SE Guidance efforts
- ➢ **Current Initiatives**
  - Prototyping and Rapid Fielding Policy (NDAA FY16 Section 804 and NDAA FY17 Section 806)
  - MIL-HDBK-61A, “Configuration Management Guidance”
  - Systems of Systems (SoS) ISO Non-government Standards (NGS)
- **Upcoming Drivers**
  - National Defense Authorization Act for Fiscal Year 2017 (NDAA FY17)
    - Sections 805 – 809 “Acquisition agility act”
    - Section 855 “Mission integration management”
    - Section 875 “Use of commercial or non-Government standards in lieu of military specifications and standards”

Prototyping and Rapid Fielding Policy

NDAA FY16 Sec 804 and NDAA FY17 Sec 806 established new authorities for Prototyping and Rapid Fielding

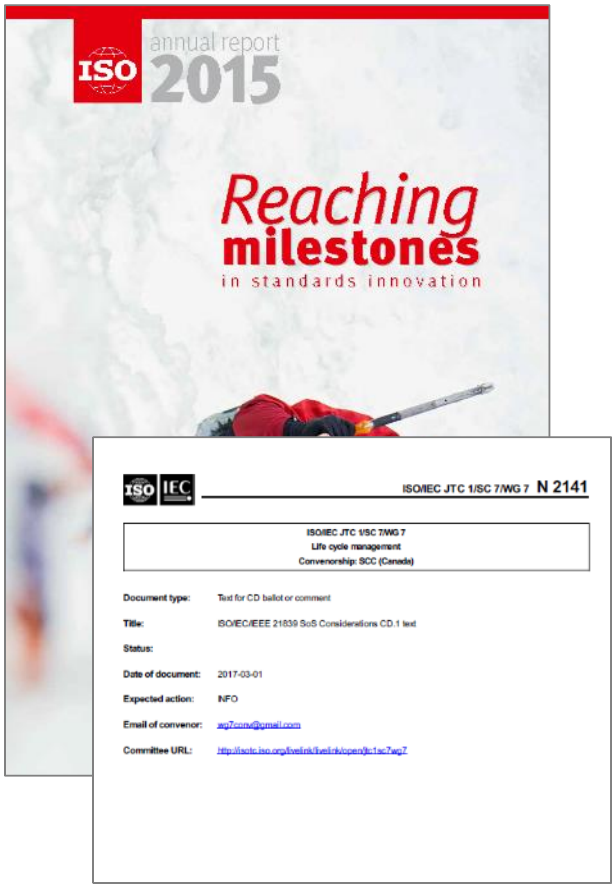
- **NDAA FY16 Section 804:**
  - **Objective:** Accelerate our speed of innovation, maintain DoD's lethality, and rapidly deliver warfighting capabilities within a two to five year period
  - **Rapid Prototyping:** Use innovative technologies to rapidly develop fieldable prototypes that can be successfully demonstrated in an operational environment and provide for a residual operational capability
  - **Rapid Fielding:** Use proven technologies or off-the-shelf capability to field production quantities of new or upgraded systems with minimal development required
- **NDAA FY17 Section 806:**
  - **Objective:** To mature and demonstrate high risk components/technologies separate from a program of record
- **DoD Policy will:**
  - Address broad, overarching DoD prototyping practices
  - Include rapid prototyping and rapid fielding as two potential methods
  - Allow the Services to develop and implement Service unique prototyping policy aligned with statute

MIL-HDBK-61A Revision

- **Update MIL-HDBK-61A, "Configuration Management Guidance" to provide overarching guidance for Configuration Management (CM) on DoD programs**
  - Retain guidance but remove implementation-level information, focusing on the "inherently government" functions for CM
  - Incorporating tailoring guidance and providing relationship to SAE/EIA-649, SAE/EIA 649-1, and GEIA HB-649A
- **Additional areas to be addressed:**
  - CM of electronic data models
    - State of the art for systems design and development has evolved over time
    - Use of non-digital documentation has migrated to use of digital artifacts
  - CM of software elements versus hardware elements
    - Prevalence of ever greater reliance on software/firmware in DoD systems
- **MIL-HDBK-61A revision ongoing**
  - Initiated in October 2015
  - Air Force leading a tri-Service Working Group
  - Draft update estimated to be complete in early 2018

Systems of Systems Engineering (SoSE) Standardization

ISO/IEC JTC 1/SC1
SoSE Study Group Report



ISO/IEC/IEEE 21839 Committee Draft

- **Three new Systems of Systems standards in development based on recommendation of 2016 ISO Study Group on SoS Standards**
- **ISO/IEC/IEEE 21839**

  Systems and software engineering -- System of systems considerations in life cycle stages of a system
  - Based on TTCP Best Practices Guide
  - CD released in May 2017; 270 comments received and resolved; next version slated for October 2017
- **ISO/IEC 21841**

  Taxonomies of SoS Types
  - Elaboration of ISO/IEC 15288 Annex G
  - Initial CD now complete and will be released for comment this fall
- **ISO/IEC 21840**

  Application of SE Processes for SoSE across the life cycle
  - Elaboration of ISO/IEC 15288 Annex G
  - Draft in work

Recent / Emerging Changes to Systems Engineering Practice

✓ Accomplishments

- DoDI 5000.02Operation of the Defense Acquisition System, Change 3, August 10, 2017
- Defense Acquisition Guidebook (DAG) Chapter 3, Systems Engineering
- Best Practices for Using SE Standards on Contracts for DoD Acquisition Programs
- Additional SE Guidance efforts

✓ Current Initiatives

- Prototyping and Rapid Fielding Policy (NDAA FY16 Section 804 and NDAA FY17 Section 806)
- MIL-HDBK-61A, "Configuration Management Guidance"
- Systems of Systems (SoS) ISO Non-government Standards (NGS)

➢ Upcoming Drivers

- National Defense Authorization Act for Fiscal Year 2017 (NDAA FY17)
  - Sections 805 – 809 "Acquisition agility act"
  - Section 855 "Mission integration management"
  - Section 875 "Use of commercial or non-Government standards in lieu of military specifications and standards"

Sections 805 – 809
“Acquisition Agility Act”

- **Requires major defense acquisition programs (MDAPs) to be more flexible**
  - Provides warfighter capabilities more quickly but with flexible, open-system architectures that allow components to evolve with technologies and threats.
  - Requires use of modular open system approaches (MOSA), to maximum extent practicable, in MDAP design and development i.e. more flexibility to incorporate weapon system components
  - SECDEF establishes MDAP cost and fielding targets
  - Requires Independent Technical Risk Assessments (ITRA) to assess technology and manufacturing risks to inform milestone decision points
  - Amends technical data rights for major system interfaces
- **Calls for weapon system components and their underlying technologies be matured through a separate, dedicated development path**
  - Matured in parallel with the large acquisition program of record
  - Identified prototyping as one method to separately mature technology

Goal: Improve the DoD’s ability to field and evolve weapon systems

Section 855
"Mission Integration Management"

Goal: Improve critical Joint military capabilities that need close technical and operational coupling and integration across many systems

Key Points from Legislation on Mission Integration Management (MIM)

SEC. 855. MISSION INTEGRATION MANAGEMENT.

(a) IN GENERAL.—The Secretary of Defense shall establish mission integration management activities for each mission area specified in subsection (b).

(b) COVERED MISSION AREAS.—The mission areas specified in this subsection are mission areas that involve multiple Armed Forces and multiple programs and, at a minimum, include the following:

(1) Close air support.
(2) Air defense and offensive and defensive counter-air.
(3) Interdiction.
(4) Intelligence, surveillance, and reconnaissance.
(5) Any other overlapping mission area of significance, as jointly designated by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff for purposes of this subsection.

(c) QUALIFICATIONS.—Mission integration management activities shall be performed by qualified personnel from the acquisition and operational communities.

Four recommended mission areas with options for additional areas

(d) RESPONSIBILITIES.—The mission integration management activities for a mission area under this section shall include—

(1) development of technical infrastructure for engineering, analysis, and test, including data, modeling, analytic tools, and simulations;
(2) the conduct of tests, demonstrations, exercises, and focused experiments for compelling challenges and opportunities;
(3) overseeing the implementation of section 2446c of title 10, United States Code;
(4) sponsoring and overseeing research on and development of (including tests and demonstrations) automated tools for composing systems of systems on demand;
(5) developing mission-based inputs for the requirements process, assessment of concepts, prototypes, design options, budgeting and resource allocation, and program and portfolio management; and
(6) coordinating with commanders of the combatant commands on the development of concepts of operation and operational plans

Six 'responsibility' areas

Section 875

"Use of commercial or non-Government standards in lieu of military specifications and standards."

The majority of the requirements have been accomplished in response to Acquisition Reform

- **Changes to DFARS to encourage contractors to propose commercial or non-Government standards and industry-wide practices was approved by the DAR Council and is awaiting publication in the Federal Register for public comment**
- **Seeking relief on the waiver requirement for the use of military specifications; the current process of controlling development, revision, etc. of military specifications and standards is more effective**
- **Working with the DoD Components to develop plans for negotiating licenses for standards to be used across the Department of Defense**

Conclusion

- SE is a continually evolving practice.
- Policy, guidance, and standards are constantly being revised to reflect the current state of SE.
- We will continue to keep the SE practitioner and acquisition community informed of new and emerging updates.

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Aileen Sedmak

ODASD, Systems Engineering

703-695-6364 |

aileen.g.sedmak.civ@mail.mil

Implementation of the Reliability & Maintainability (R&M) Engineering Body of Knowledge (BoK)

Andrew Monje

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 25, 2017

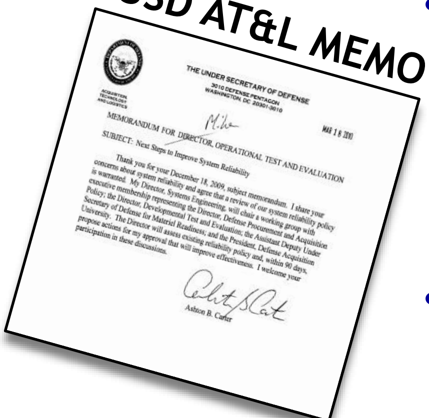
Agenda

- **Policy**
- **Guidance/Body of Knowledge**
- **Workforce Development**
- **Instantiating the Body of Knowledge**

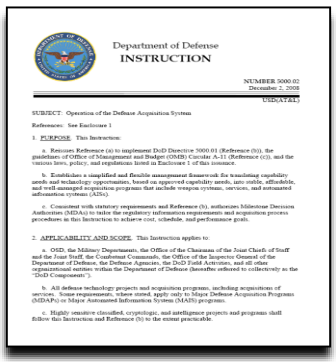
Policy

Reliability Analysis, Planning, Tracking and Reporting

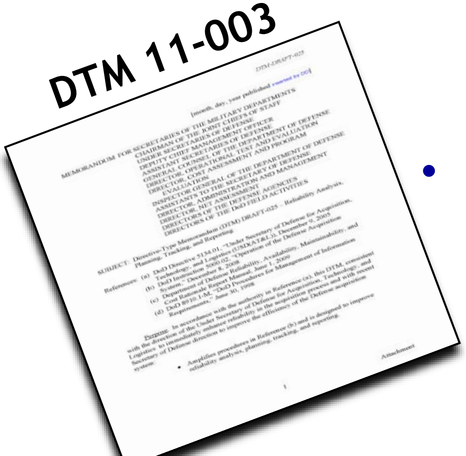
USD AT&L MEMO



DoDI 5000.02



DTM 11-003



- **Impetus for Reliability Policy (Mar 2010)**
  - Directed by Dr. Carter in response to memo from DOT&E (Dec 2009)
  - DASD(SE) to assess existing reliability policy and propose actions to improve effectiveness
- **DoD Acquisition Policy (DoDI 5000.02)**
  - Does not adequately or uniformly consider R&M engineering activities throughout the acquisition process
  - Fails to capture R&M planning in new or existing acquisition artifacts to inform acquisition decision making
- **DTM 11-003 (Approved 21 Mar 2011)**
  - Amplifies current DoDI 5000.02 by requiring PMs to perform reliability activities
  - Institutionalizes planning and reporting timed to key acquisition activities

DTM 11-003 was instantiated into DoDI 5000.02 in January 2015

Establishing an Effective R&M Engineering Program

Capability Description Document

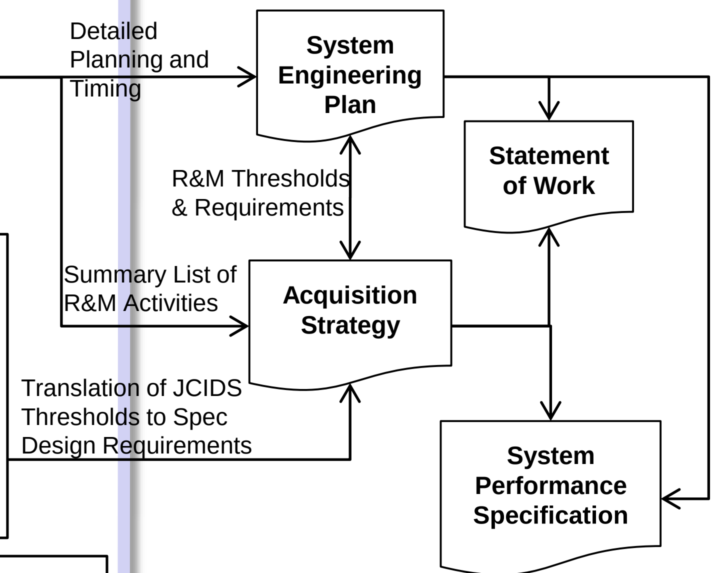
5000.02 Enclosure 3 SE R&M Requirements

Engineering Activities
- R&M allocations, block diagrams and predictions
- Failure definitions and scoring criteria
- Failure Mode, Effects and Criticality Analysis (FMECA)
- Built-in Test (BIT) and maintainability demonstrations
- Reliability Growth testing at system/subsystem level
- Failure Reporting, Analysis and Corrective Action System

Preliminary RAM-C Report in support of Milestone (MS) A and updated for RFP Release Decision Point, MS B, & MS C
- Provides an audit trail that documents and supports JCIDS thresholds
- Ensures correct balance between the sustainment metrics (Availability-KPP, Materiel Reliability-KSA, and O&S Cost-KSA)
- Provides early risk reduction by ensuring sustainment thresholds are realistic (feasible) and correct (valid)

Reliability Growth Strategy
- Documents system-level reliability growth curves in the SEP beginning at MS A and updated in the Test & Evaluation Master Plan (TEMP) beginning at MS B
- Establishes intermediate goals for reliability growth curves that will be tracked through fully integrated system-level T&E events until the threshold is achieved
- Requires MS C PMs and Operational Test Agencies to assess reliability growth required to achieve the reliability threshold during IOT&E

Tracking and Monitoring
- Requires PMs to report status of reliability objectives and/or thresholds as part of the formal system engineering review process
- Incorporates Reliability Growth Curves into the DAES review process



Program Execution and R&M Engineering BoK

Table 1. R&M Engineering Activities by Functional Area

Functional Area	R&M Engineering Activities	MSA	TMRR	EMD	P&D	O&S
Project Management	Formulate a comprehensive R&M program using appropriate reliability growth strategy	•	•	•	•	•
Project Management	Integrate R&M Engineering Program in SEP including a system reliability growth curve	•	•	•		
Project Management	Prepare/Update RAM-C Report and attach to the SEP	•	•	•		
Project Management	Report R&M status during formal design review process and technical reviews (SRR, PDR, CDR, etc.)	•	•	•		
Project Management	Prepare reliability growth assessment of the likelihood of meeting the CDD threshold by IOT&E			•		
Project Management	Evaluate reliability growth and report status in DAES reviews until the threshold is achieved		•	•	•	

R&M Service Leadership Coordination

- **Meetings with R&M Service leadership**
  - Provide update on what is happening within DoD regarding R&M engineering
  - Discuss R&M workforce development
  - Review strategies to better connect policy and guidance with program execution
  - Discussions on various R&M topics such as R&M standardization, predictions and derating, RAM-C update, and software
- **Participation in annual Reliability and Maintainability Symposium (RAMS®)**
  - DoD/Industry Roundtable: R&M Service leadership and their industry counterparts share challenges and solutions
- **Provide status and feedback of program execution to R&M service leads.**
  - Identify systemic areas that require improvement or guidance
  - Provide feedback to workforce development i.e., DAU

R&M Engineering Body of Knowledge (BoK)

- **The BoK is organized in the following three areas:**
  - First, by the defense acquisition life cycle phases
  - Second, by functional area (Project Management, Systems Engineering, Test and Evaluation, Procurement)
  - Third, each functional area lists R&M engineering activities that trace back to the required R&M engineering activities established in DTM 11-003

Table 1. R&M Engineering Activities by Functional Area

Functional Area	R&M Engineering Activities	MSA	TMRR	EMD	P&D	O&S
Project Management	Formulate a comprehensive R&M program using appropriate reliability growth strategy	•	•	•	•	•
Project Management	Integrate R&M Engineering Program in SEP including a system reliability growth curve	•	•	•		
Project Management	Prepare/Update RAM-C Report and attach to the SEP	•	•	•		
Project Management	Report R&M status during formal design review process and technical reviews (SRR, PDR, CDR, etc.)	•	•	•		
Project Management	Prepare reliability growth assessment of the likelihood of meeting the CDD threshold by IOT&E			•		
Project Management	Evaluate reliability growth and report status in DAES reviews until the threshold is achieved		•	•	•	

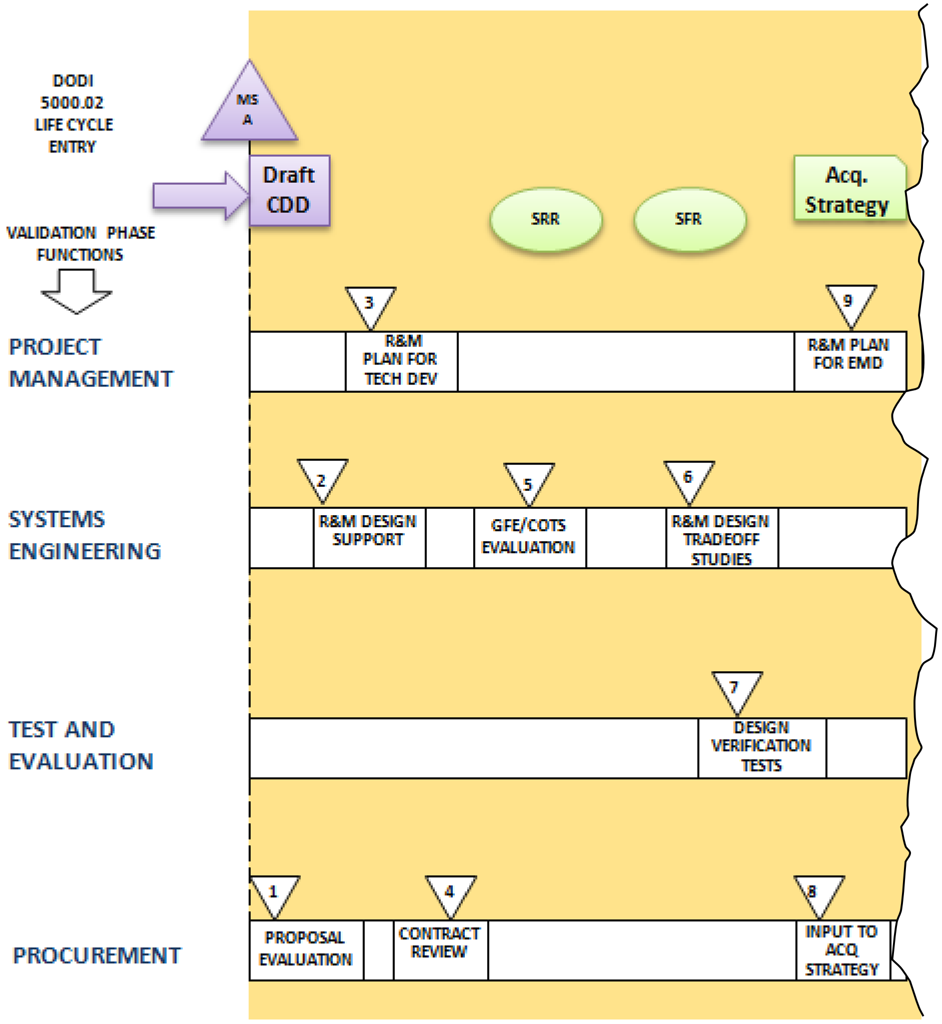
Some activities occur in more than one phase

R&M Engineering BoK Functional Areas

- **The BoK defines and allocates R&M activities to the functional areas into which a materiel acquisition program can normally be divided:**
  - Project Management
    - Planning, definition, and implementation of R&M control criteria, assurance procedures, in-process review for compliance, and R&M decision-making criteria
  - Systems Engineering
    - R&M design analyses, trade-off study, failure mode effects and criticality analysis, R&M problem and correction, and R&M design support
  - Test and Evaluation
    - Planning and conducting tests for evaluation and demonstration of R&M
  - Procurement
    - Definition, documentation, and review of R&M requirements and provisions in procurement requests, requests for proposals, contracts and exhibits
- **R&M engineering activities should be properly integrated across all functional areas of the program in order to implement an effective R&M engineering program**

R&M Engineering BoK Activity Overview

- **The BoK identifies specific activities needed to support each DTM-required R&M engineering activity**
  - MSA phase – 13
  - TMRR phase – 14
  - EMD phase – 14
  - P&D phase – 13
  - O&S phase – 5
- **Each acquisition phase has a figure showing timelines for the activities for each functional area**



BoK Application Example

- **Program has progressed to TMRR phase**
- **Determine that a required engineering activity is to "Formulate a comprehensive R&M program using appropriate reliability growth strategy"**

Table 1. R&M Engineering Activities by Functional Area

Functional Area	R&M Engineering Activities	MSA	TMRR	EMD	P&D	O&S
Project Management	Formulate a comprehensive R&M program using appropriate reliability growth strategy	•	•	•	•	•

- **Activity associated with the TMRR phase is part of the Project Management functional area**

Table 2-3. Project Management R&M Tasks – TMRR Phase

R&M Task	Description
3 Develop/review R&M planning for TMRR phase	Review the R&M plans to ensure conformance to requirements defined in the RFP and contract and to verify consistency with requirements and provisions.

BoK Application Example

- **Each activity in each phase has an activity overview, control procedure, data requirements, and review criteria**
  - **Overview of activity**
    - Brief description of the activity and its importance
  - **Control Procedure**
    - Procedure that should be followed in accomplishing the activity
  - **Data Requirements**
    - Data required to complete the activity
  - **Review Criteria**
    - Criteria to be used in determining if the activity has been completed successfully

TMRR Phase Activity 3

2.1.1 Develop/Review R&M Planning for TMRR Phase

TASK 3

The R&M engineer and project management team review the R&M program planning for the TMRR phase that the Government developed before initiating the TMRR phase and contract. The team updates the planning as appropriate to reflect specification changes approved during negotiations.

……

R&M PLANNING for TMRR: CONTROL PROCEDURE

The Government R&M planning for the TMRR phase should be updated from the MSA phase. (MIL-HDBK-338B Section 12, MIL-HDBK-470A Section 4.2 and Appendix A, MIL-HDBK-2165 Task 100 and Appendix A) The planning as a minimum should address the following in the appropriate program planning documents:

- *Management* – Identify the organizational elements and personnel and clearly define their responsibilities and functions.
- *Management Tasks* – Prepare a detailed listing and description of each R&M task and the procedures to evaluate the status of and to control each task.
- *Resources* – Estimate the Government R&M funding and man-hours for each R&M task (or task that the R&M team is involved in) required in the TMRR phase.
- *Objectives* – Determine provisions for updating the quantitative and qualitative R&M objectives to reflect the current approved configuration and the related analyses and trade-off studies.
- *Problem and Risk Areas* – Establish procedures for identifying critical R&M problems and risks and the plans for resolving and mitigating these problems in the TMRR phase.
- *Acquisition Program Documents* – Provide steps for updating the R&M inputs to the Systems Engineering Plan (SEP), Acquisition Strategy (AS), the RAM-C Report, the Test and Evaluation Master Plan (TEMP), and other program documents as required……..

R&M PLANNING FOR TMRR: DATA REQUIREMENTS

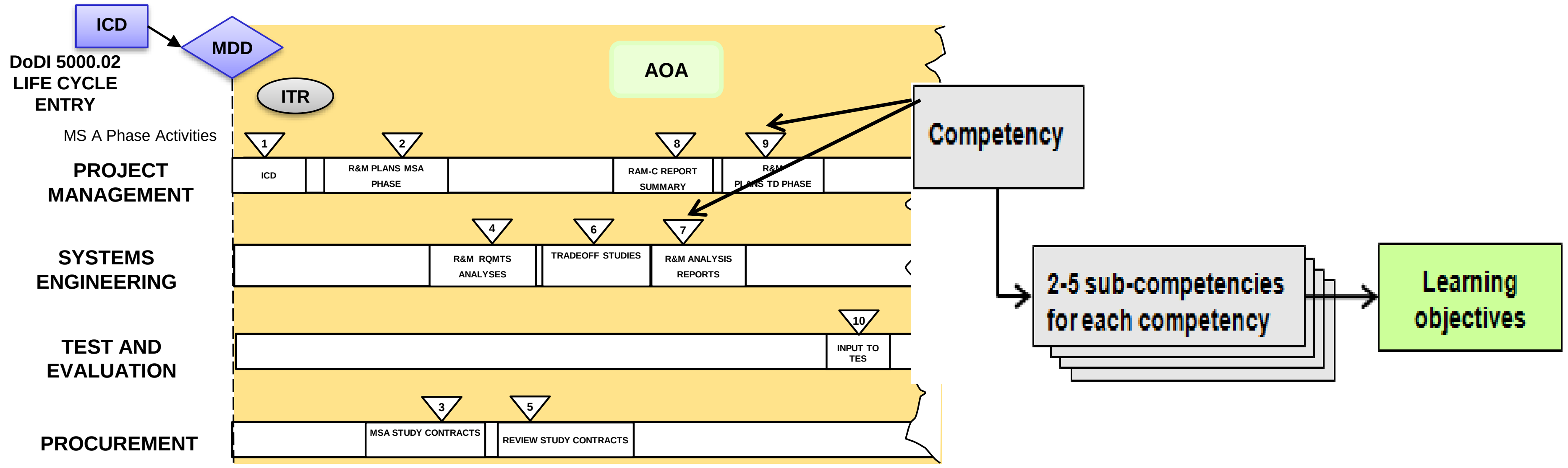
The contractor's R&M program plans should include the data requirements outlined above and as required by the RFP. The Government should review these plans in preparation for the System Requirements Review (SRR). The plans should allow for updating as plans or procedures change by mutual agreement to conform to the needs of the program. Essential features of the contractor's approved R&M plans should be integrated into appropriate sections of the SEP and internal program documents including technical review entrance criteria.

R&M PLANNING FOR TMRR: REVIEW CRITERIA

- The contractor's R&M program plans satisfy the requirements outlined in the control procedure and data requirements above.

Workforce Development

R&M Competencies

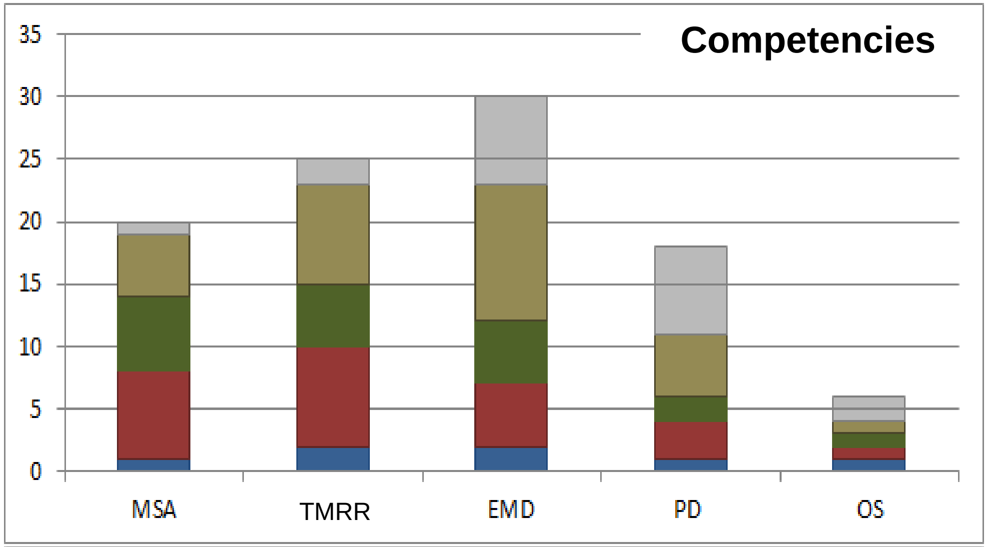


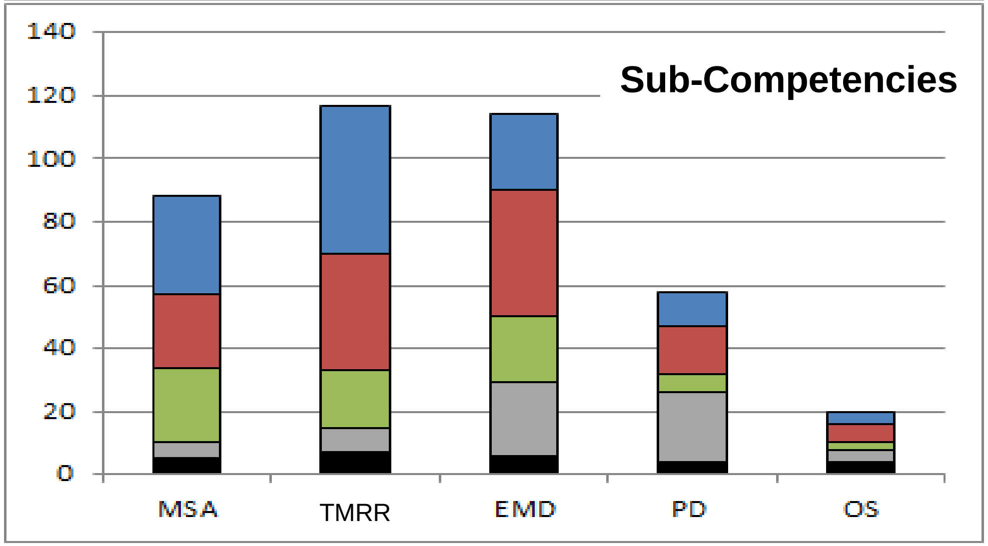
- Competencies are focused by program functional areas
- Developed competencies, sub-competencies, and supporting standard skills for basic, intermediate, and advanced career levels to support learning architecture development
- Mapped sub-competencies to DAU courseware learning objectives

The R&M competency structure spans the acquisition life cycle, and addresses all levels of proficiency

R&M Competencies
by Acquisition Phase and Functional Area

- **DoD R&M Competencies and Sub-competencies show population distribution across acquisition phases**
- **Technical project management (includes planning activities) and systems engineering contain greatest number of competencies**
- **All functional areas are present in each acquisition phase, although the relative weightings may change**



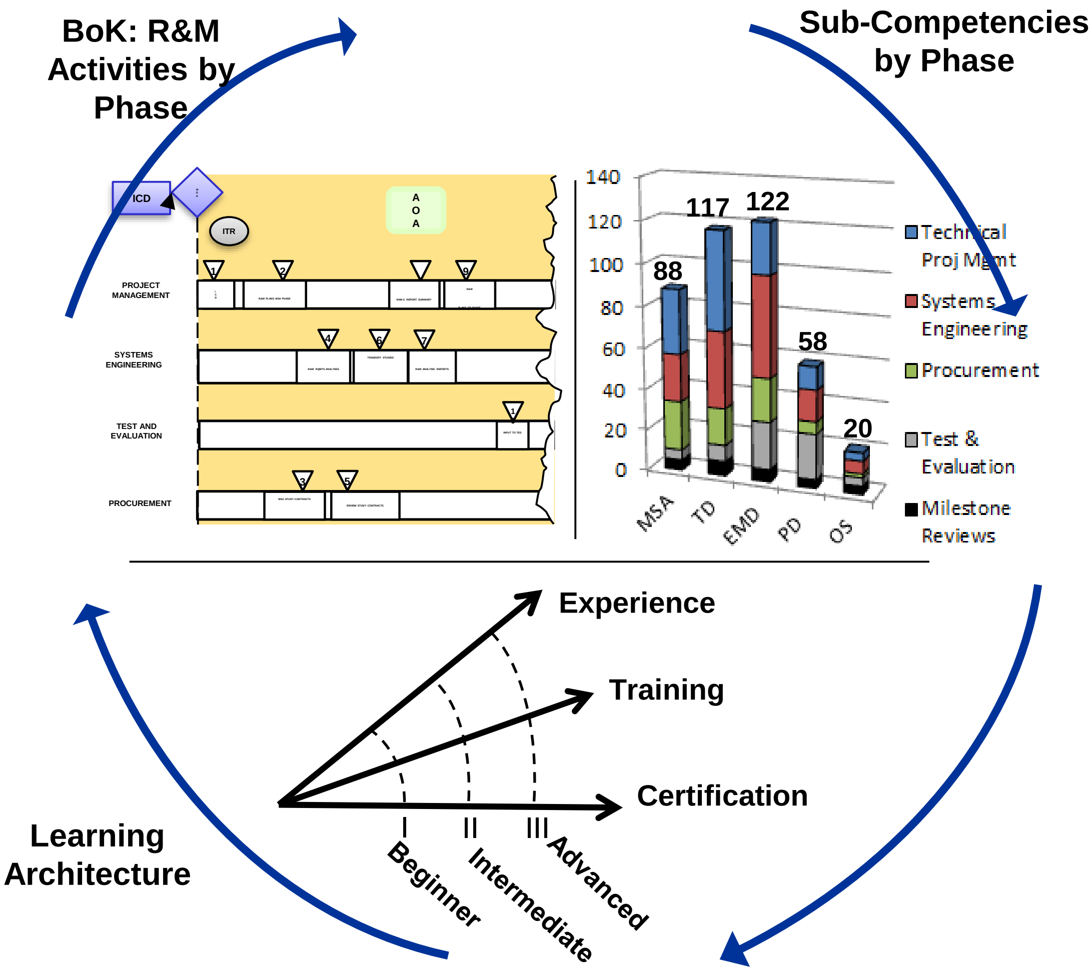


R&M Engineering Learning Architecture

- **Purpose: career development guidance for the R&M Engineer**
- **R&M Learning Architecture – consolidation of desired:**
  - **Education**
  - **Experiences**
  - **Training Available to the DoD community**
- **Defined body of knowledge for each DAWIA Level**
- **Organizes R&M experiences and training within each DAWIA level**
  - **R&M Engineering / Acquisition**
  - **R&M Design Analysis**
  - **R&M Product Support Planning**
  - **R&M Test**
  - **R&M Procurement**

Workforce Development

R&M Engineering Learning Architecture



- **DoD R&M Engineering Competency Structure Requires a Comprehensive Learning Architecture**
- **R&M Competencies = 99**
- **R&M Sub-competencies = 405**
- **OSD with support from DAU and Services is defining the approach**
- **Sources for R&M training:**
  - **DAU**
  - **Services**
  - **Academia**

Learning architecture supports capability and career growth for the DoD R&M Engineering Workforce

Rev July 24, 2013

Instantiating the R&M Engineering BoK R&M Engineering CoP Overview

- **Objective of the R&M Engineering Community of Practice (CoP) - to provide the DoD R&M Engineer a user-friendly integrated reference source for**
  – R&M Engineering Technical Information on specific topics
  – R&M Engineering Career Development
  – R&M Engineering General Knowledge

- **Emphasis on R&M Engineering relevant information, but more global topics such as Cost Estimating, Contracting, etc. can be addressed by inserting links to relevant DoD sites**

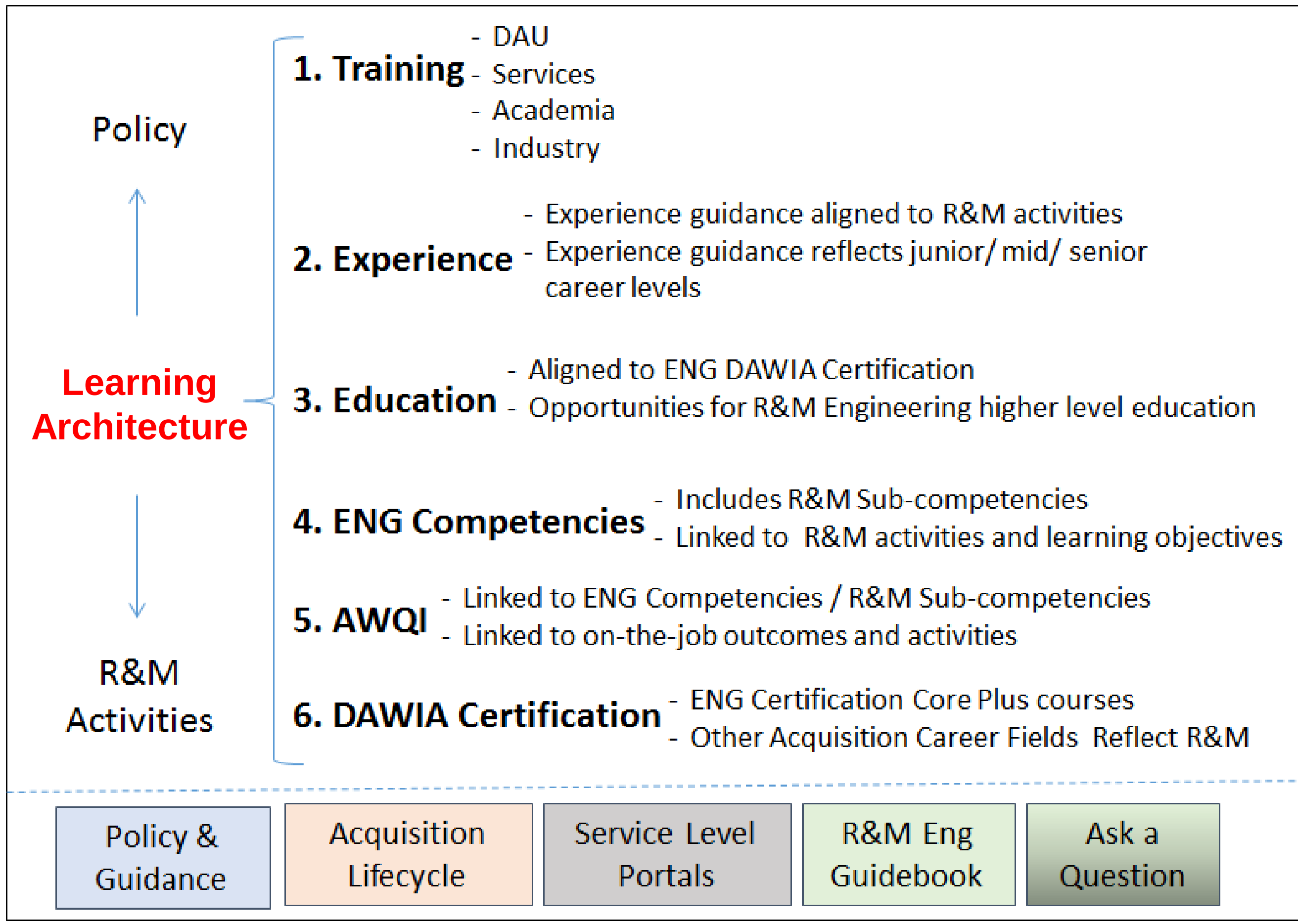
- **R&M CoP to be hosted from DAU's new Sharepoint interactive platform**

- **Membership / access levels to content planned to be controlled by DAU via CAC credentials**
  – Government (Phase 1)
  – Government Support Contractor
  – DoD Contractors
  – Industry / Open

Learning Architecture Integration Within the R&M CoP

- ***Example: the R&M Engineer has clicked on the "Learning Architecture" term to bring up more detailed information ….***

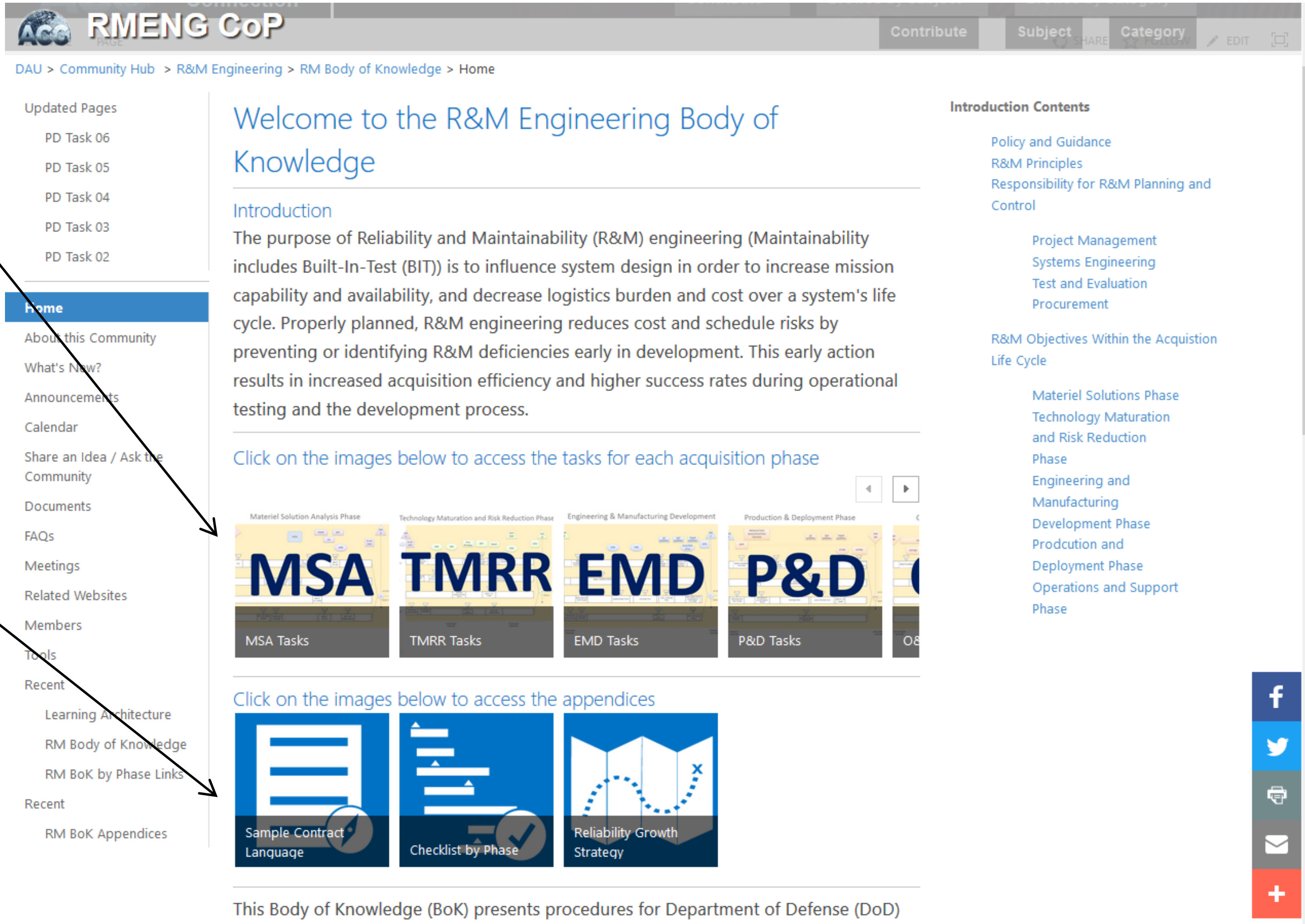
- The Learning Architecture forms a "hub" of information for R&M career development
- Each of the six categories decomposes to lower levels of information detail
- Horizontal integration occurs to Policy and R&M Activities
- A variety of products, body of knowledge and tools are linked to each category within the learning architecture infrastructure
- DoD Program Management also can use the Learning Architecture to augment personnel management practices
- Interactive tiles allow for navigation to specific topics. More tiles can be added to represent additional topics



Home Page – R&M Content Example

- *… the R&M CoP Home Page starts with an interactive DoD Acquisition Lifecycle diagram*

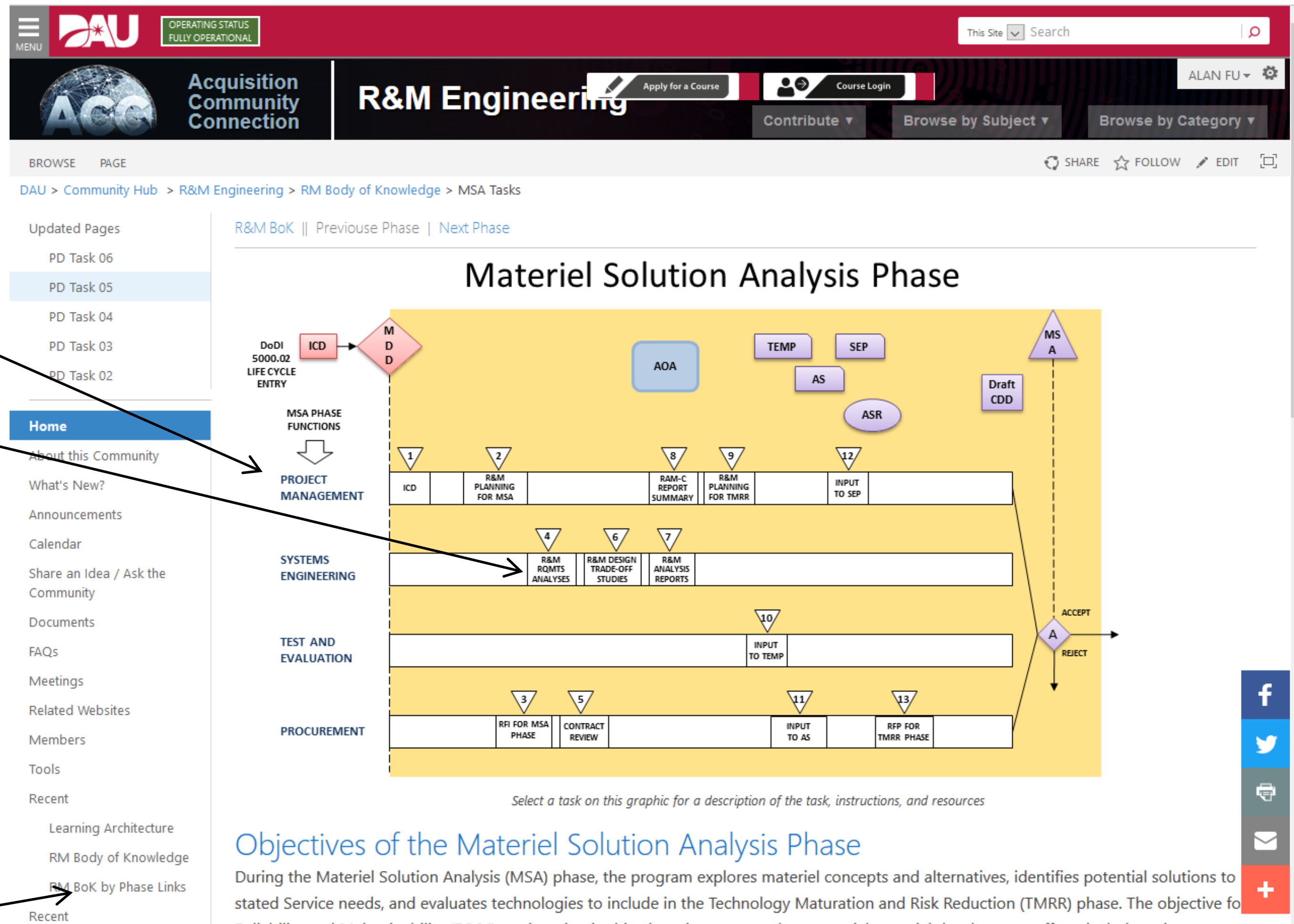
- Each DoD acquisition phase graphic may be decomposed, showing lower level R&M information for that selected acquisition phase
- Navigation "buttons" can be added to allow the R&M Engineer to easily navigate between webpages
- Other terms in the graphic may be hyperlinked to provide additional R&M related information when selected
- … this Home Page may also include interactive tiles for the R&M Engineer to directly access specific information



"Phase Level" Page Example – MSA Phase

- ***Example: the R&M Engineer has clicked on "MSA phase" and now views R&M MSA functional areas and individual activities ….***

- This graphic, from the R&M Engineering Guidebook, identifies the R&M activities for the MSA phase by functional area listed on left
- Each functional area name and individual activity names/numbers may be hyperlinked to provide further information for the R&M Engineer …
- Other terms present in the graphic may also be hyperlinked for more information
- The interactive tiles from the home page continue to be visible for the R&M Engineer to directly access specific information



Summary

- Service-level leadership engagement essential to work across centers, commands, etc.
- Define required engineering activities across the acquisition timeline for each functional area.
- Outreach is key to ensure successful implementation
- Continued refinement and assessment of execution with the Services and industry (e.g., RAMS)
- Maintain currency of the Body of Knowledge with DoD and Industry engagement

Body of Knowledge must be reactive in response to program execution to be effective

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Mr. Andrew Monje

ODASD, Systems Engineering

703-692-0841

andrew.n.monje.civ@mail.mil

Are We Doing Enough in Requirements Management?

STEVEN H. DAM, PH.D., ESEP
CHRIS RITTER
SPEC INNOVATIONS
STEVEN.DAM@SPECINNOVATIONS.COM

Outline

- Why Do I Need More Than a Spreadsheet?
- What Kinds of Requirements Are We Trying to Capture?
- How Can I Improve My Requirements Management and Analysis Capabilities?

Why Do I Need More Than a Spreadsheet?

What Do Spreadsheets Do?

- Pro
  - Spreadsheets are a wonderful tool for dealing with numbers
    - Excel can perform significant math functions
    - Excel can also plot the numbers very well
- Con
  - Spreadsheets require a schema for collecting information
  - Most Requirements are not pure numbers
    - Functional requirements require context
    - Non-functional requirements are often non-numerical
  - Spreadsheets are not databases (CM, Baselining and other capabilities are difficult)
  - Spreadsheets cannot provide the functional analysis and simulation capabilities needed

So why are we using spreadsheets for requirements management?

Why Are Spreadsheets Used?

- It's what I have
- I know how to use it
- It's cheap
- Everyone has MS Office
- My management won't buy anything else
- The requirements tools are complicated and expensive
- I don't want to learn a new tool

The end result is poor quality requirements are developed and the cost of fixing them later in the lifecycle grows by orders of magnitude

To High Quality Requirements We Need to:

- Support requirements analysis
  - Quality attributes
  - Quality checkers
- Support requirements management
  - Importing capability
  - Configuration Management (i.e. change history, baselining)
- Support functional analysis
  - Includes simulation for verification of models
- Track to Test Results
  - Traceability between test results and requirements
- Be collaborative
  - Commenting capability
- Be scalable
  - Need to store and visualize large number of objects in a database

What Kinds of Requirements Are We Trying to Capture?

What Level Am I Trying to Capture?

Different kinds of analyses are needed to develop high quality requirements

The Requirements Hierarchy

Number of Requirements,
Level of Detail Increases

User Needs

A capability or feature identified by a User as being needed to perform his mission

Conceptual Requirements

A high-level requirement generated during the concept development phase. Contained in ORD, CONOPS

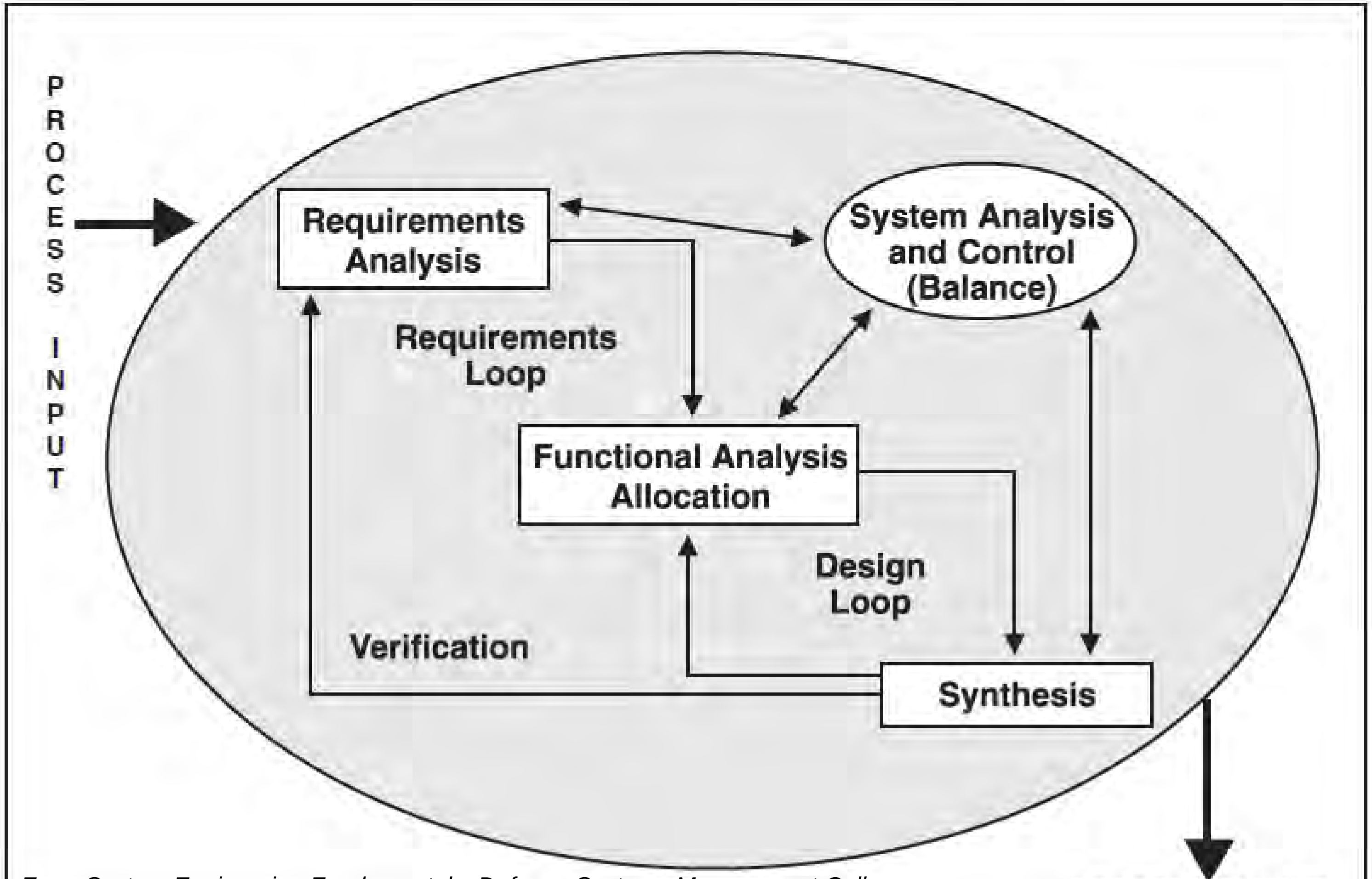
System Requirements

A requirement that describes in technical language the desired capabilities of a system.

Application/Component Specifications

Requirement that is at the level of detail needed for actually designing a new capability. Contained in System Requirements Specification (SRD)

The SE Process Develops Requirements

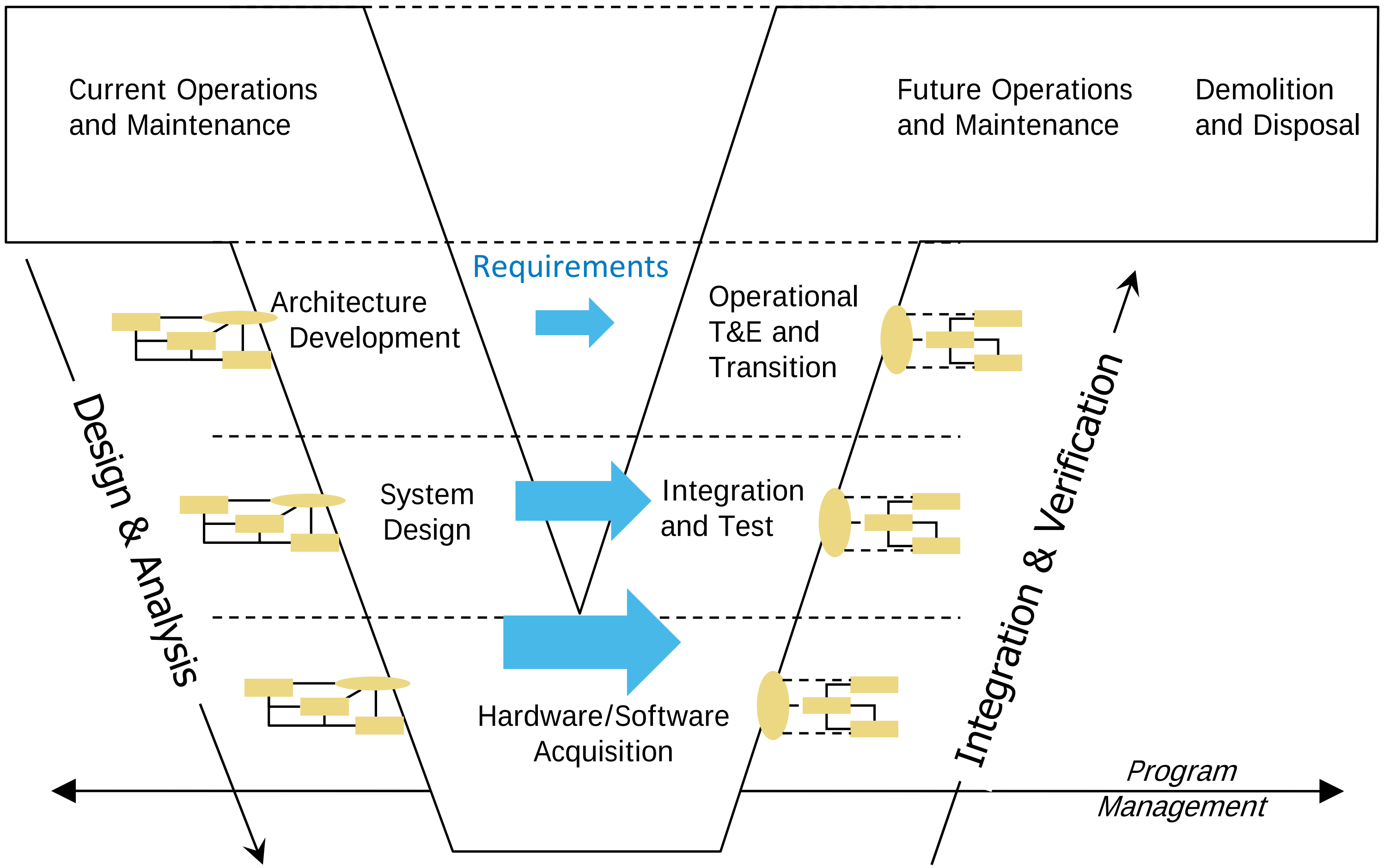


From System Engineering Fundamentals, Defense Systems Management College, October 1999

Figure 1-3. The Systems Engineering Process

- Process input starts with user needs
- Process output results in specifications for the next level of decomposition
- The steps in the process can be executed in any order and simultaneously
- Result is *functional* and *non-functional* requirements for each level

Role of Requirements in the Lifecycle

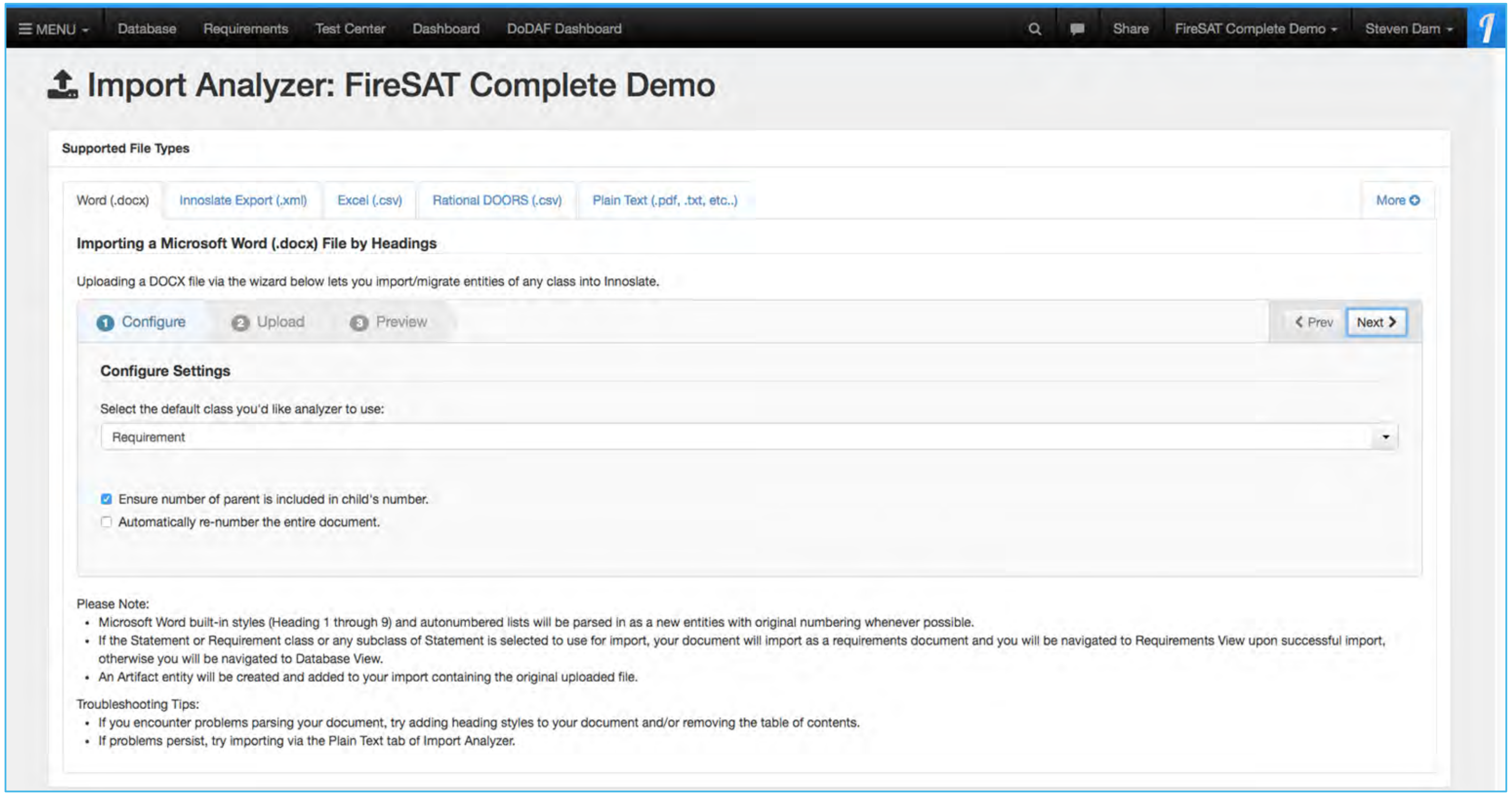


- Requirements are developed at the beginning of the lifecycle
- Resulting components, systems, and complete architectures are validated later in the lifecycle using these requirements
- The number of requirements increases as we decompose the architecture

How Can Improve My Requirements Management and Analysis Capabilities?

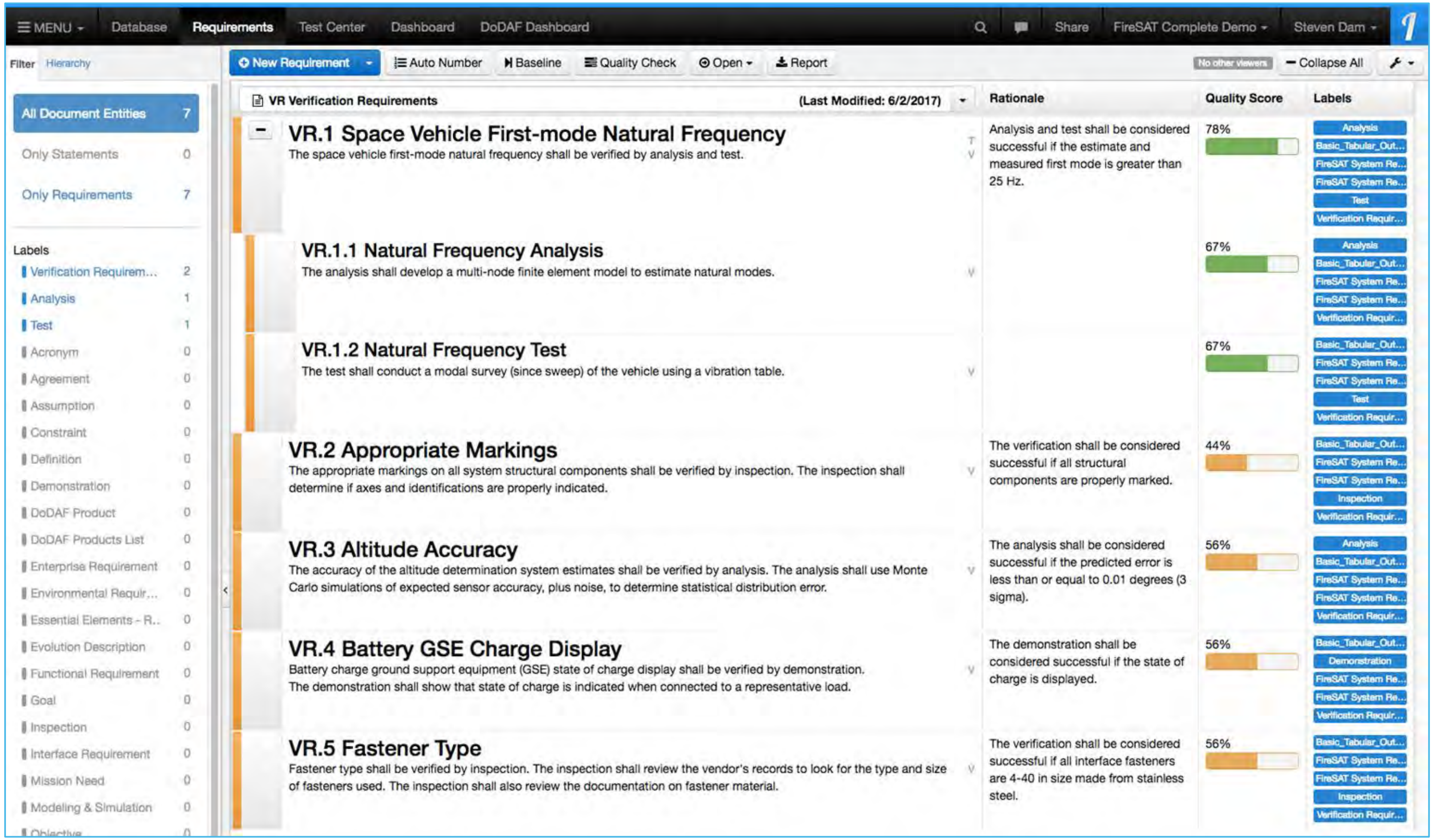
Step 1: Capture Originating Artifacts

- Import directly
  - MS Word files
  - CSV
  - DOORS CVS
  - Plain Text (PDF)
  - XML
- Analyze numbering scheme to create parent-child relationships automatically
- Preview before saving



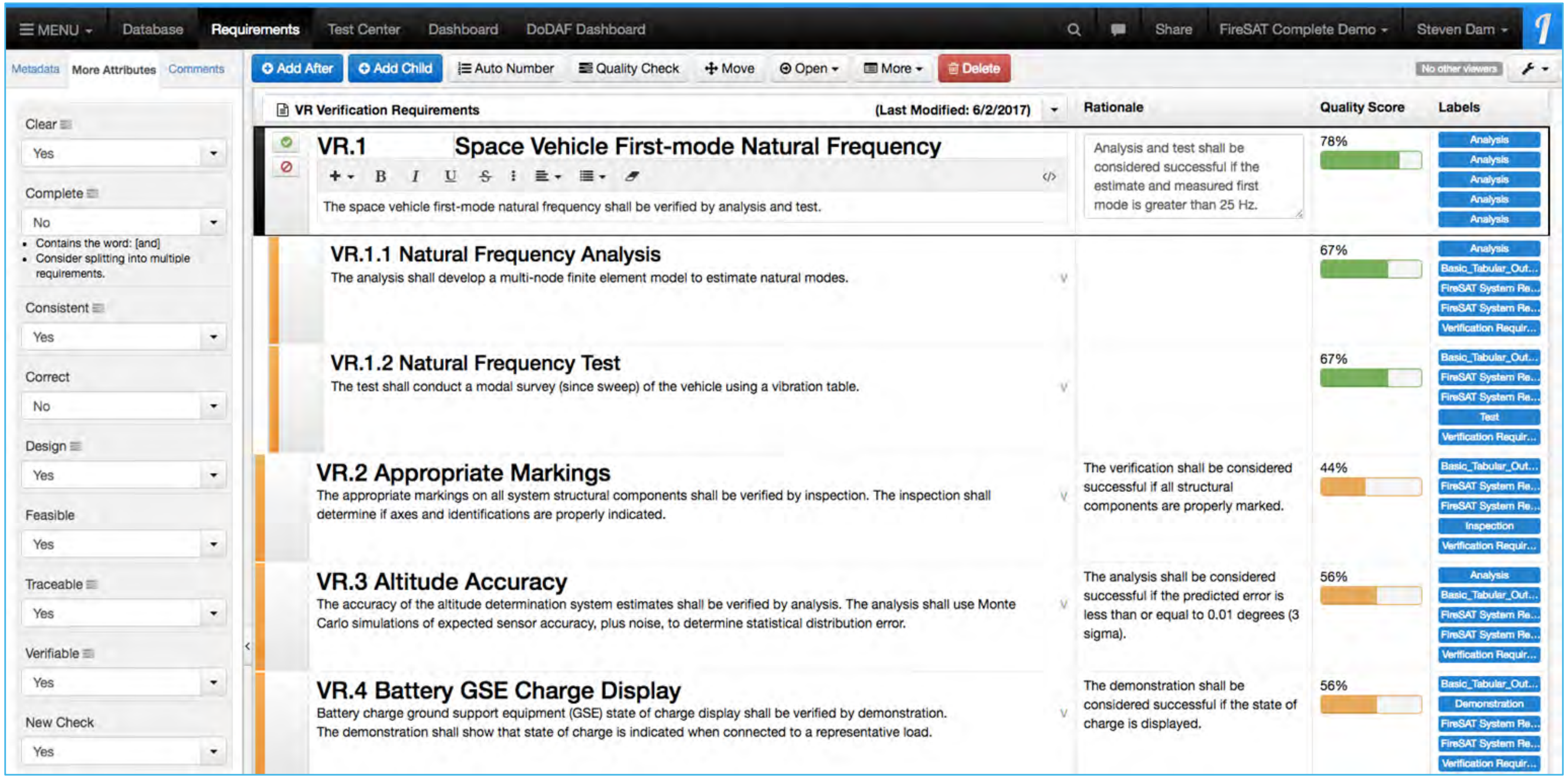
Step 2: Analyze Requirements

- Quality Check each requirement
- Add a Rationale
- Create Reports
- Visualize requirements

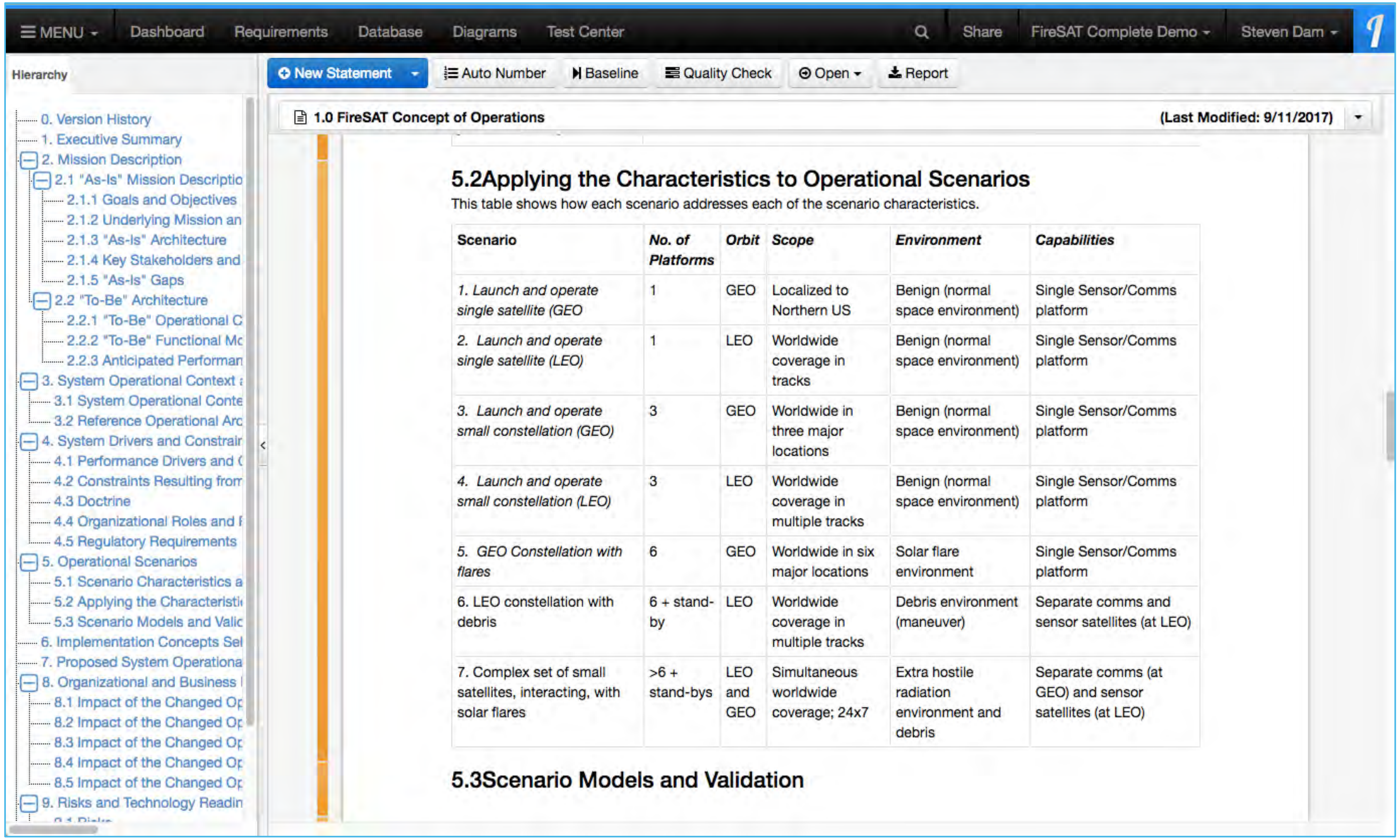


Step 3: Review and Approve Requirements

- Have reviewers provide comments on requirements, but don't let them change the requirement
- If you want reviewers to change requirements create a branch for them to edit
- Baseline requirements when completed



Step 4: Develop Scenarios



5.2Applying the Characteristics to Operational Scenarios

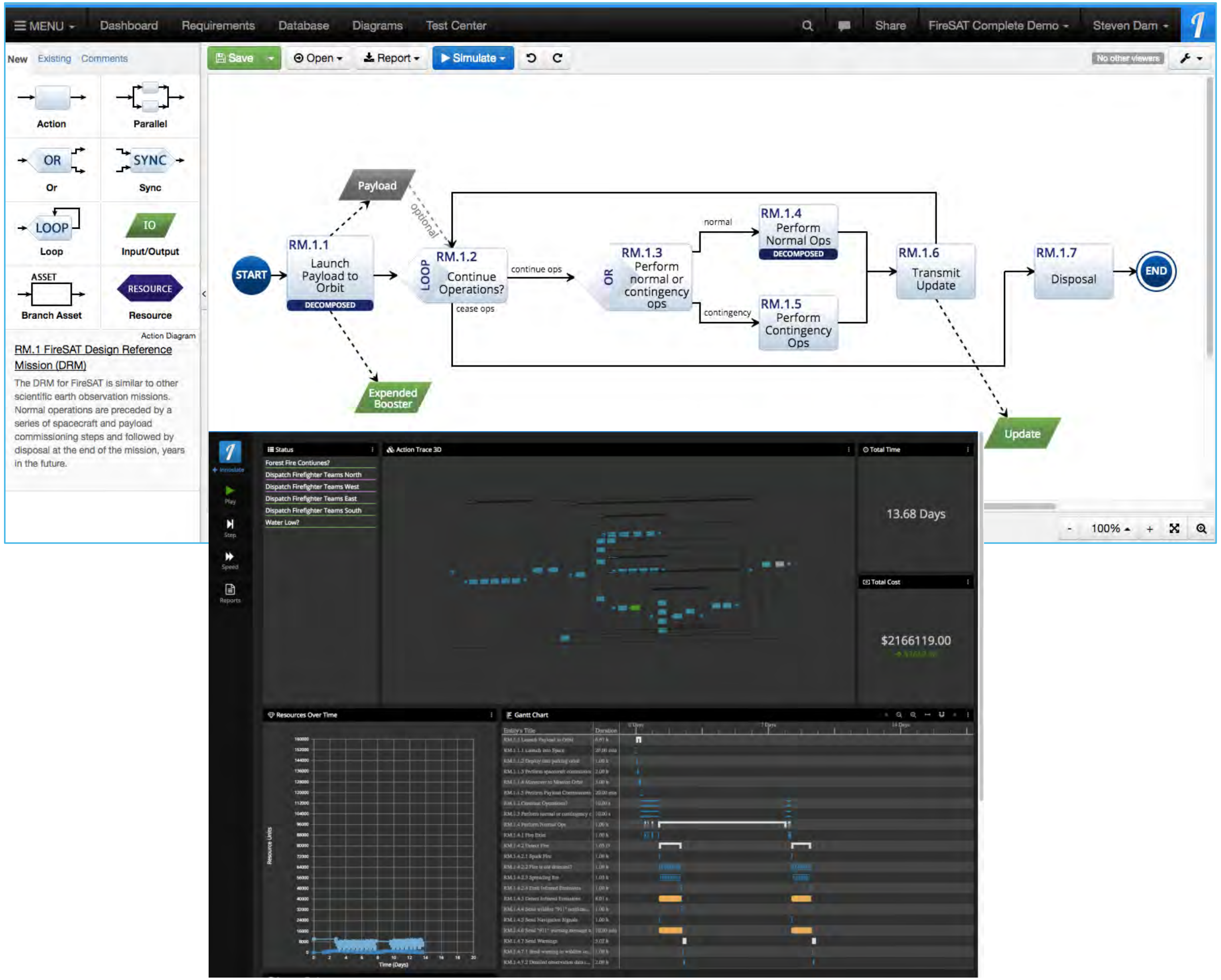
This table shows how each scenario addresses each of the scenario characteristics.

Scenario	No. of Platforms	Orbit	Scope	Environment	Capabilities
1. Launch and operate single satellite (GEO	1	GEO	Localized to Northern US	Benign (normal space environment)	Single Sensor/Comms platform
2. Launch and operate single satellite (LEO)	1	LEO	Worldwide coverage in tracks	Benign (normal space environment)	Single Sensor/Comms platform
3. Launch and operate small constellation (GEO)	3	GEO	Worldwide in three major locations	Benign (normal space environment)	Single Sensor/Comms platform
4. Launch and operate small constellation (LEO)	3	LEO	Worldwide coverage in multiple tracks	Benign (normal space environment)	Single Sensor/Comms platform
5. GEO Constellation with flares	6	GEO	Worldwide in six major locations	Solar flare environment	Single Sensor/Comms platform
6. LEO constellation with debris	6 + stand-by	LEO	Worldwide coverage in multiple tracks	Debris environment (maneuver)	Separate comms and sensor satellites (at LEO)
7. Complex set of small satellites, interacting, with solar flares	>6 + stand-bys	LEO and GEO	Simultaneous worldwide coverage; 24x7	Extra hostile radiation environment and debris	Separate comms (at GEO) and sensor satellites (at LEO)

5.3Scenario Models and Validation

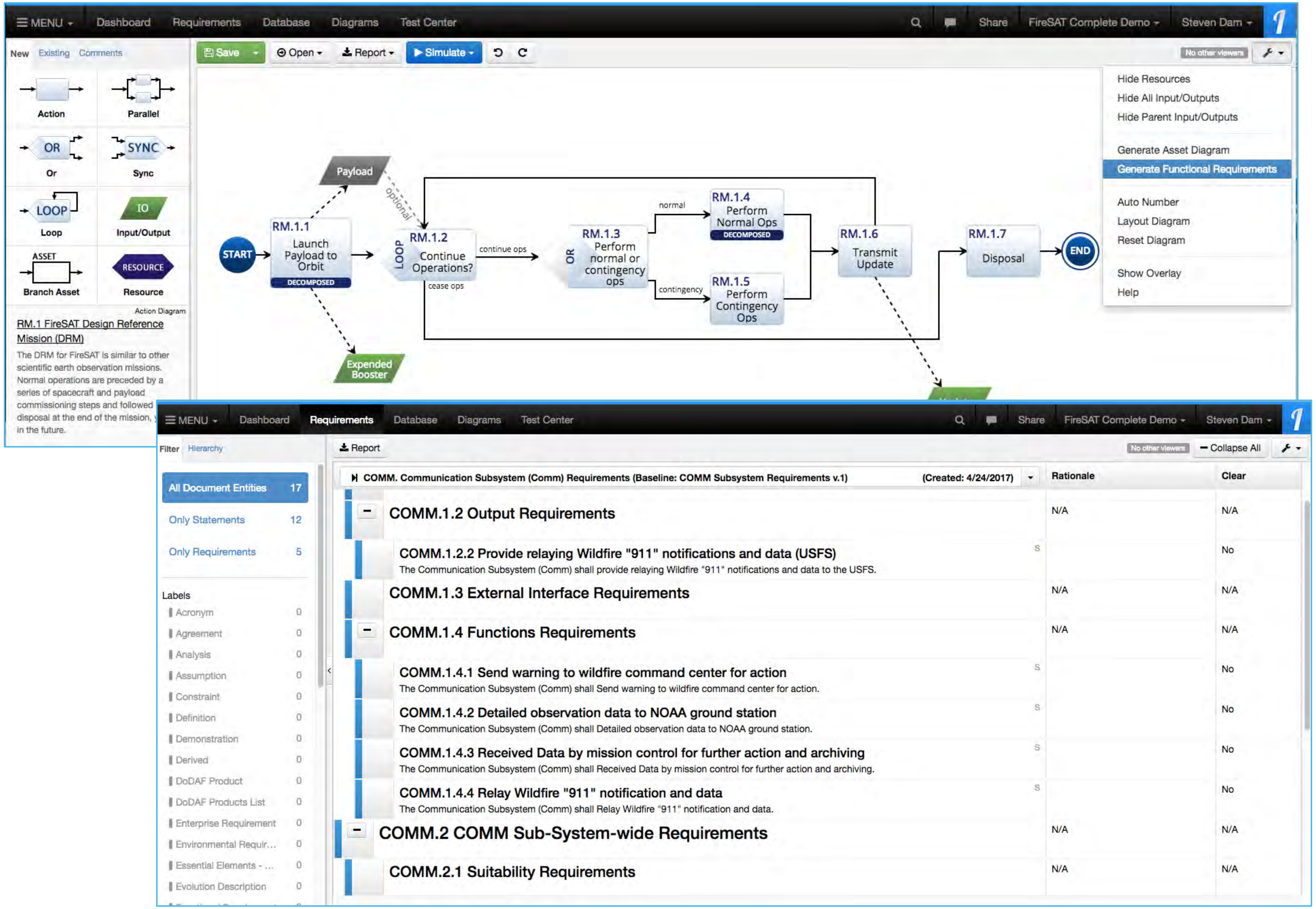
- Scenarios are used to validate user needs and identify functional requirements
- Use CONOPS to create a good set of scenarios

Step 5: Model and Verify Scenarios



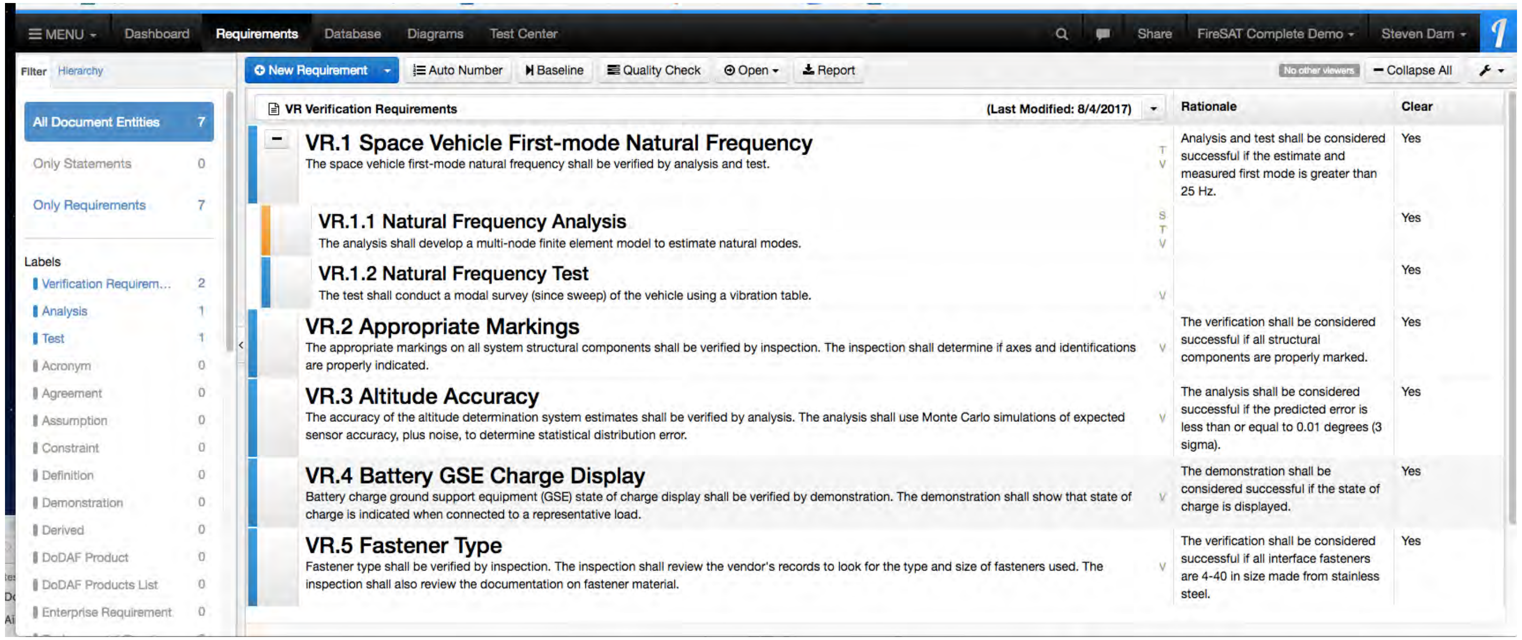
- Decompose to get more detailed functional requirements
- Include physical constraints and resources to obtain non-functional (performance) requirements
- Verify models/ requirements via simulation

Step 6: Generate Lower Level Requirements



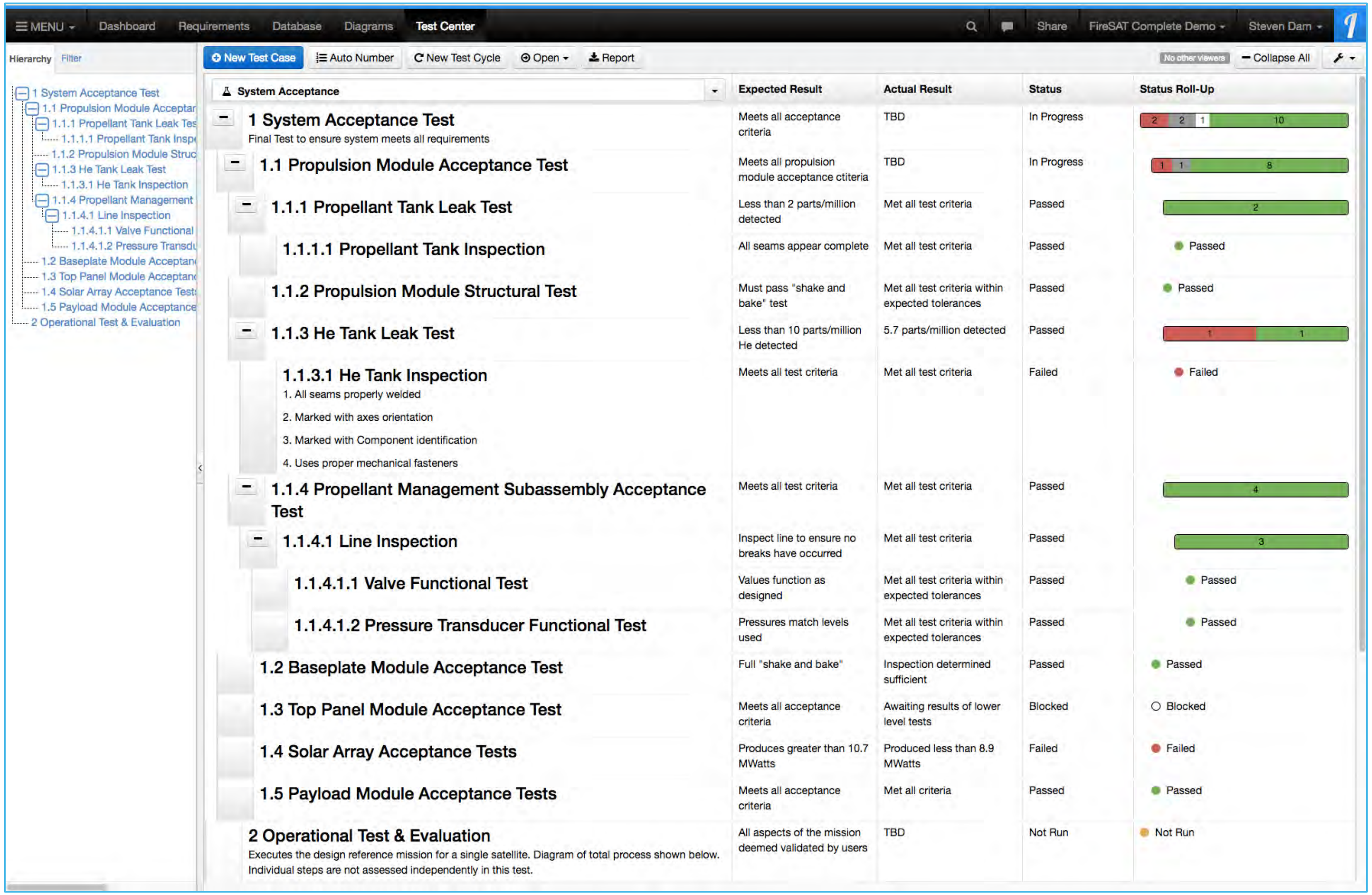
- Generate requirements" from models
- Edit lower level requirements
- Publish (baseline) requirements

Step 7: Develop Verification Requirements



- In parallel with steps 3-6, you can derive the verification requirements
- These requirements specify the verification methods as well

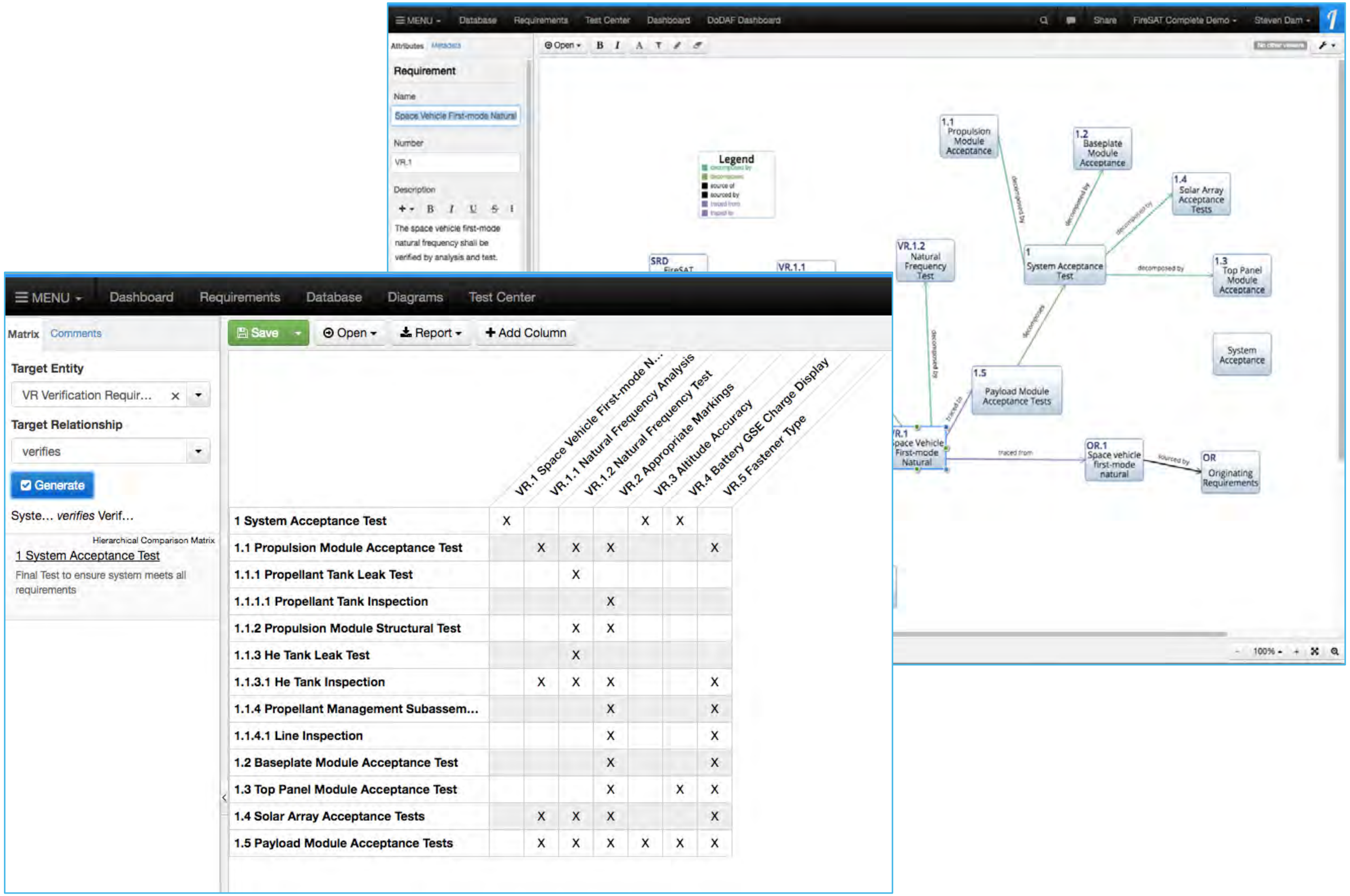
Step 8: Develop Test Cases



- Capture test cases and results (when it's time)
- Roll-up more detailed test cases to higher levels
- Link to test plan and requirements (next slide)

Step 9: Trace Verification Requirements to Test Cases

- Use tools to show all relationships or comparison matrix for a specific relationship
- Modify attributes and relationships as needed
- Produce RVTM and other reports to show requirements are met



	VR.1 Space Vehicle First-mode N...	VR.1.1 Natural Frequency Analysis	VR.1.2 Natural Frequency Test	VR.2 Appropriate Markings	VR.3 Altitude Accuracy	VR.4 Battery GSE Charge Display	VR.5 Fastener Type
1 System Acceptance Test	X				X	X	
1.1 Propulsion Module Acceptance Test		X	X	X			X
1.1.1 Propellant Tank Leak Test			X				
1.1.1.1 Propellant Tank Inspection				X			
1.1.2 Propulsion Module Structural Test			X	X			
1.1.3 He Tank Leak Test			X				
1.1.3.1 He Tank Inspection		X	X	X			X
1.1.4 Propellant Management Subassem...				X			X
1.1.4.1 Line Inspection				X			X
1.2 Baseplate Module Acceptance Test				X			X
1.3 Top Panel Module Acceptance Test				X		X	X
1.4 Solar Array Acceptance Tests		X	X	X			X
1.5 Payload Module Acceptance Tests		X	X	X	X	X	X

Next Steps

- Repeat steps 1-9 as needed for lower levels of decomposition
- Stop when you have the selection criteria to decide what to buy or build
- Then go through the integration and verification process (right side of “V”) and document results as you go
- Make sure that the overall model meets good modeling practices
- Perform risk analysis and other analyses as needed

Summary

- Requirements analysis is a critical part of requirements management
- Modeling and simulation are critical to ensuring you have the requirements you need and are developing systems that work
- To be successful in moving from spreadsheets to model-based systems engineering you need help from your process and tool
- You will know you are successful when you system gets fielded ahead of schedule and under budget

Engineering Autonomy

Mr. Robert Gold

Director, Engineering Enterprise
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

Outline

- Defense Research & Engineering (R&E) Strategy
- Key Research and Development Areas
- Background
- Engineering Challenges
- Summary

Defense Research & Engineering Strategy

Mitigate current and anticipated threat capabilities

Enable new or extended capabilities affordably in existing military systems

Create technology surprise through science and engineering

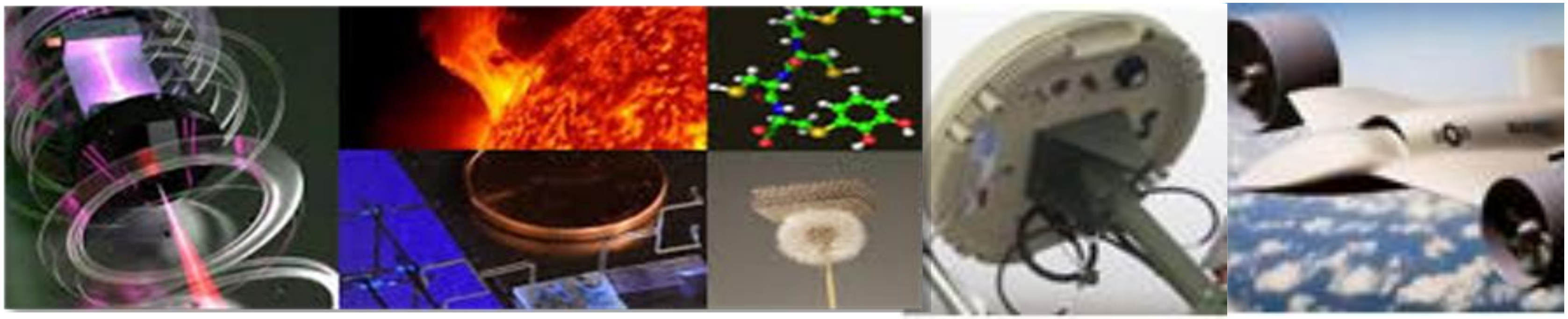
Focus on Technical Excellence

Deliver Technologically Superior Capabilities

Grow and Sustain our S&T and Engineering Capability

Key Research & Development Investment Areas

- Autonomy & Robotics
- Electronic Warfare / Cyber
- Microelectronics
- Hypersonics
- Directed Energy
- Manufacturing
- Artificial Intelligence / Man-Machine Interface
- Future of Computing
- Novel Engineered Materials
- Precision Sensing: Time, Space, Gravity, Electromagnetism
- Emerging Biosciences
- Understanding Human and Social Behavior



Background

- DoD emphasis on the increased use of autonomous systems
- DASD(SE), in collaboration with Services, assessed current autonomy efforts and associated engineering challenges
- The purpose was to ascertain the ramifications of autonomous systems on DoD engineering practice

Engineering Challenges

- **Increase Level of Experimentation**
  - Understand autonomy trade-space for architecture/conceptual designs
  - Engage Warfighter in experimentation to set expectations
  - Engage Industry Partners to conduct mission-specific experiments
- **Standardize Taxonomy**
  - Develop autonomy-consistent terms, definitions, and phraseology (e.g., authorized/control entities, flexible/supervised autonomy, human on/outside the loop)
- **Refine Requirements Development**
  - Apply tools to translate natural language into logical and mathematical statements usable for logic definitions
  - Advance methods to encode interactions between operators and the system for requirements traceability

Engineering Challenges

- **Understand/Manage Human-Machine Interaction**
  - Allocation of functions between human and machine
  - Explore techniques for ensuring operators trust autonomous systems
- **Facilitate Trust and Social Interactions**
  - Develop software assurance tools to enhance ‘trust’
  - Define techniques for monitoring and bounding autonomous system behaviors
  - Understand social dynamics of autonomous systems to effectively communicate and collaborate with humans

Engineering Challenges

- **Enhance Analysis, Evaluation, and Certification**
  - Explore use of formal methods to analyze autonomous systems
  - Enable rapid evolution of autonomous capabilities thru:
    - Rapid deployment of software upgrades
    - Perform system certifications concurrently with design
    - Use of modular open systems architecture
- **Synchronize Technology Development with Life Cycle Planning**
  - Rapid autonomous system development and technology transition will mandate effective coordination between engineering and product support activities.

Engineering Challenges

- **Understand Consequences of Self-Learning Systems**
  - Evaluate consequences of autonomous system behavior being dictated by hardware, software, and system data.
    - Artificial intelligence will allow new levels of autonomy
- **Understand Impact to the Work Force**
  - Develop the Body of Knowledge for autonomous systems to support competency development
  - Mission-specific work force education and experience
  - Establish Science, Technology, Engineering, and Mathematics relationships with academic institutions

Summary

- **Fielding Autonomy-Enabled Warfighting Capability will require close collaboration with:**
  - Research, Engineering, and Test & Evaluation
  - Acquisition and Operational Communities
  - Our Industry Partners
- **Collaboration needs to occur through planned demonstrations and prototyping, especially at Engineering Commands where these systems are currently designed.**
- **Autonomy technologies will impact the collective workforce, inclusive of the challenges unique to the engineering community.**

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Mr. Robert Gold

ODASD, Systems Engineering

703-695-3155

robert.a.gold4.civ@mail.mil

The Drive for Innovation in Systems Engineering

D. Scott Lucero

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 25, 2017

Defense Research & Engineering Strategy

Mitigate current and anticipated threat capabilities

Enable new or extended capabilities affordably in existing military systems

Create technology surprise through science and engineering

Focus on Technical Excellence

Deliver Technologically Superior Capabilities

Grow and Sustain our S&T and Engineering Capability

Evolving Capability

- **Up until World War II, almost all munitions missed the mark**
  – Massing of forces needed to achieve effects
- **Strategic government investments created an "offset" providing technological advantage**
  – Atomic weapons, precision guided munitions allow reliable targeting
  – Massing of forces no longer absolute necessity
- **Current innovations are driven by industry**
  – Broadly available technology creates a need for velocity

Systems Are Changing

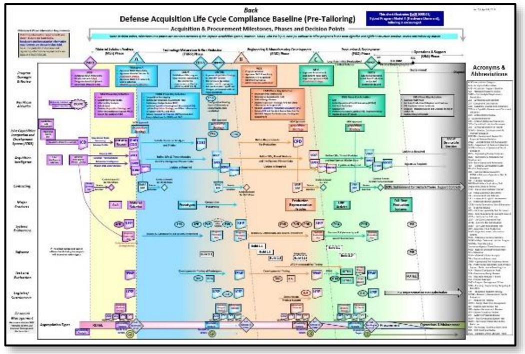
From:	To:
Systems built to last	Systems built to evolve
Heuristic-based decisions	Data-driven decisions
Deeply integrated architectures	Layered, modular architectures
Hierarchical development organizations	Ecosystems of partners, agile teams of teams
Satisfying requirements	Constant experimentation and innovation
Automated systems	Learning systems
Static certification	Dynamic, continuous certification
Standalone systems	Composable sets of mission focused systems

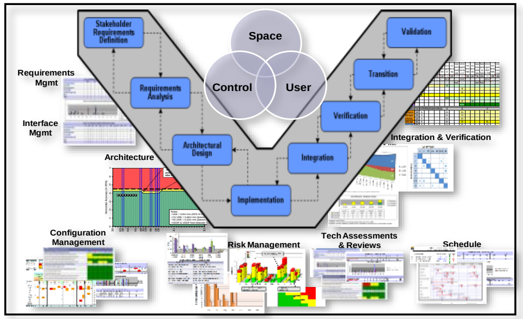
Systems Engineering Needs to Change

Credit: Derived from David Long, Former INCOSE President

Industrial Age Acquisition and Engineering Processes

- **Taylor's scientific management**
  - Empirical methods to synthesize workflows to improve economic efficiency
  - Inspires industrial and systems engineering, business process management, lean six sigma, operations research
- **Optimizing engineering & production drives need for stable requirements, well-defined processes**
- **Optimizing methods to *change* engineering & production requires increasing the cycles of learning:**
  - To identify necessary changes
  - To incorporate those changes into systems

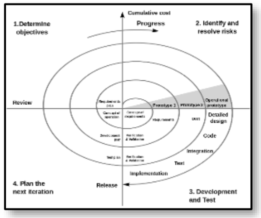




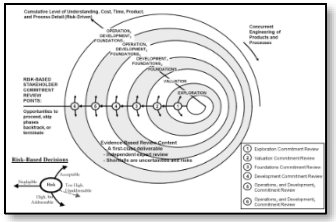
Initiatives to Accelerate Change

- **National Defense Authorization Act (NDAA) for Fiscal Year 2017 Acquisition Agility Act**
  - Modular Open Systems Approaches
  - New authorities for prototyping, experimentation & rapid fielding
  - Defining requirements likely to evolve due to evolving technology, threat or interoperability needs
- **Reorganization of USD(AT&L) – NDAA FY2017**
  - Creates separate organizations for acquisition and for innovative technologies
- **Middle Tier Acquisition Policy – NDAA FY2016**
  - Creates alternate acquisition path for rapid prototyping and fielding
- **Engineered Resilient Systems – 2011**
  - Research and development of deep tradespace analysis methods to address the nature of evolving missions and threats
- **Joint Urgent Operational Needs processes – 2004**

Methods for Managing Software-Intensive Acquisitions

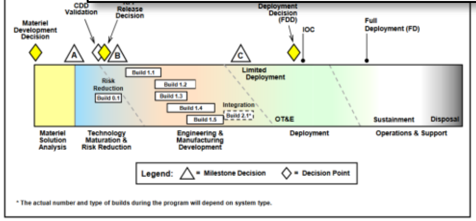


Spiral Development Model (Boehm 1986)

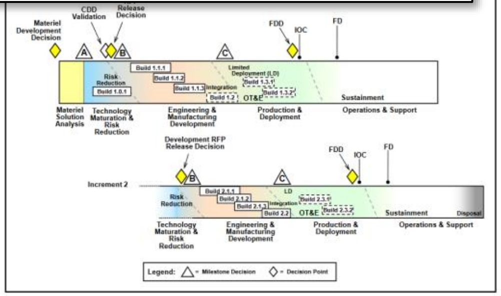


Incremental Commitment Model (Boehm 2007)

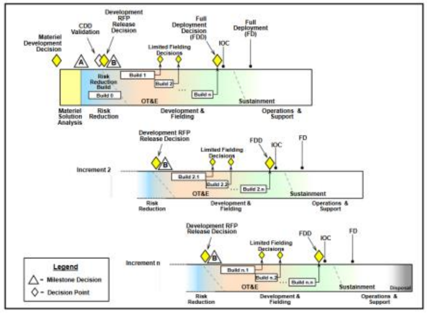
DoD Instruction 5000.02 – Operation of the Defense Acquisition System (Jan 2015)



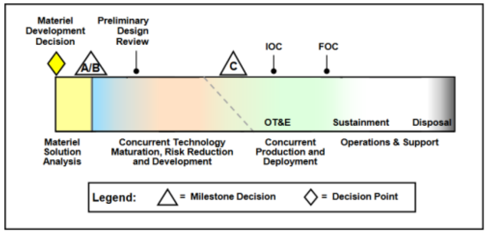
Software Intensive



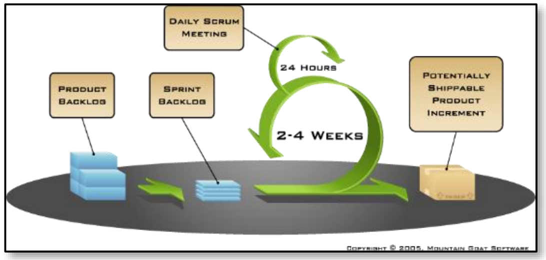
Hybrid – Software Dominant



Incrementally Deployed Software Intensive



Accelerated



Agile Development – 2001

Other Systems Engineering Perspectives

- **MIL-STD-499 Engineering Management**
  - Issued by Air Force in 1969 and 1974
    - Draft MIL-STD-499B never published in 1990’s acquisition reform era
  - Not time-sequenced, like the V-model
  - Process seems to encourage trades in the “need-space” and the “solution-space”
  - Less focused on production
  - Less prescriptive – less useful in organizing activities

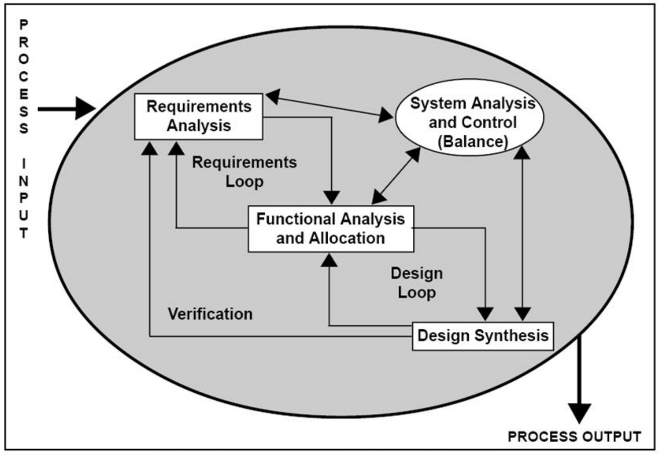
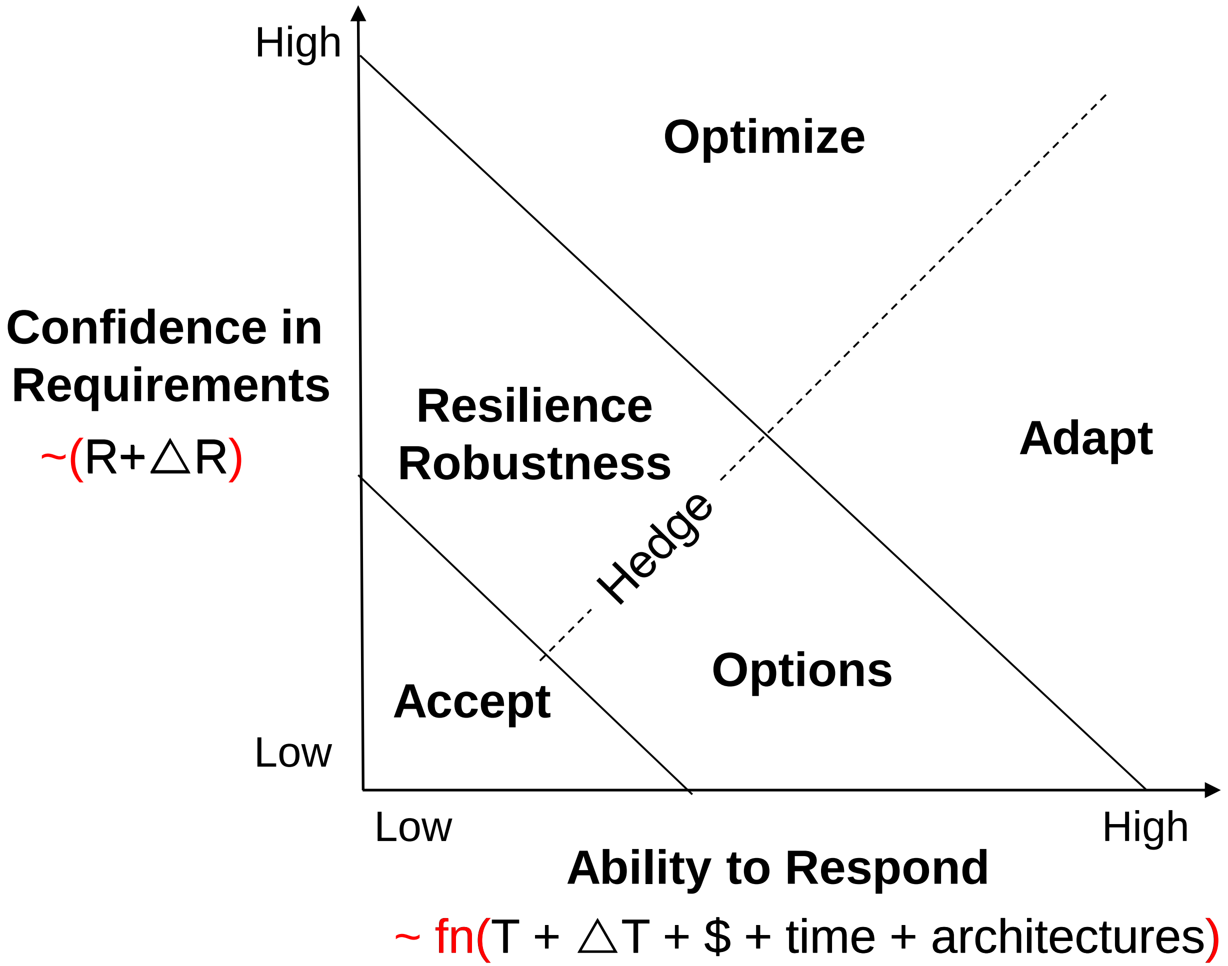


Figure 1-3. The Systems Engineering Process

Methods for Selecting Acquisition Approaches



Notes:

- Framework helps overcome tendency to develop optimal solutions to static requirements
- Each axis belongs to a separate community
- Uncertainty around Requirements and Technology can be informed by intelligence community

Credit: Derived from Michael Pennock, Stevens Institute

Interesting Research Questions

- Gauging confidence in requirements, ability to respond
- Analysis of trades across the mission space and the solution space
- Gauging risk, rework
- Hedging methods
- Actual increases in velocity of capability delivered
- Methods to increase ability to respond
  - e.g., MBSE, advanced manufacturing
- Dynamic and continuous learning and certification
- Multiple systems interrelationships
  - Portfolio management, mission engineering
- Others?

For Additional Information

D. Scott Lucero

Deputy Director, Strategic Initiatives

Office of the DASD

Systems Engineering

571-372-6452 | don.s.lucero.civ@mail.mil

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace

http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering

http://www.acq.osd.mil/se

Technical Performance Risk Management for Large Scale Programs

Brian Davenport
Ji Li

October 2017

Technical Performance Risk Management

- **The Challenge**
  - Development of large scale systems and system of systems often face considerable cost and schedule challenges. Technical performance risk is one of the most common drivers behind those challenges due to the potential of perturbation to the upfront architecture and design as well as the backend verification and validation efforts.
- **The Context**
  - Technical performance issues can often be ambiguous, under-defined, or unknown until later stages of the system development life cycle where the functional product has a greater degree of maturity.
  - This dynamic has a higher degree of risk in large scale multi-iteration or Agile development based programs due to end-to-end product maturity occurring late in the development and integration life cycle.
    - New mission needs, such as greater cybersecurity and autonomy, serve to further complicate these technical performance issues

The Approach

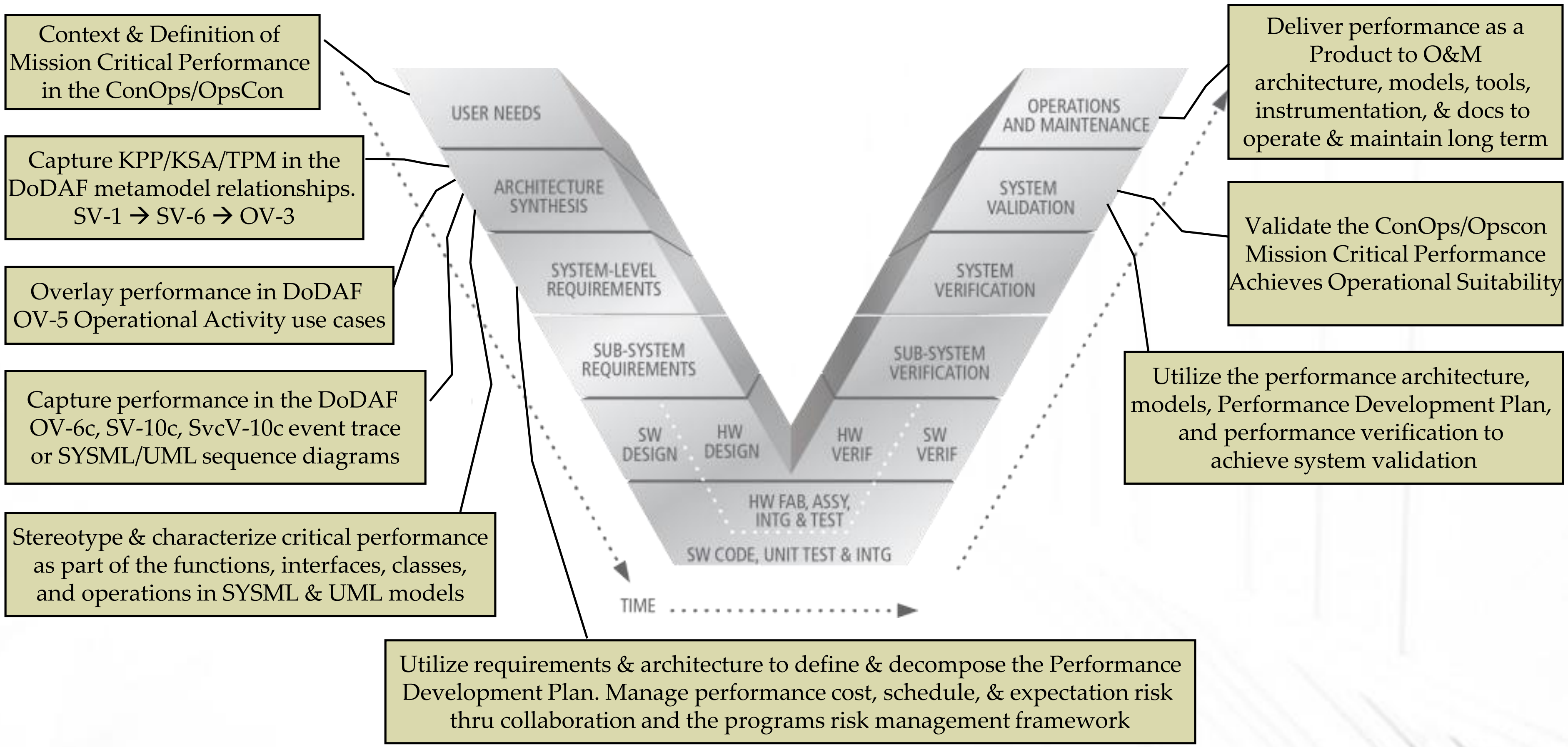
- Not all technical performance is created equal
  - Up Front
    - Negotiate TPMs and Performance Verification Criteria: Must Have, Want to Have, Nice to Have
    - Manage customer, stakeholder, and leadership expectations
  - In Phase
    - Apply rigorous performance management at critical phases
- Establish technical performance as part of the culture
  - 'Bake it in' to your Systems Engineering technical baseline
    - Integrate Performance throughout all levels of the Systems Engineering 'V'
  - Manage the risk at all levels and maximize your flexibility
  - Model it, Measure it, and Analyze it

UNRESTRICTED CONTENT – NON-EXPORT CONTROLLED

Not all technical performance is created equal

- Performance, defined in absolutes, drives cost and schedule risk into a program
  - "Work Smarter Not Harder" – Work with your customers to categorize performance needs: Must Have, Want to Have, Nice to Have
    - Drive 'Must Have' performance into all levels of the technical baseline thru the SE 'V'
    - Mitigate risk of 'Want to Have' and 'Nice to Have' by negotiating sell off of lower category performance - Worst case sell off, 95% sell off, confidence intervals, sample sizes, acceptable or alternate verification methods
- "Tell me, I will forget. Show me, I will remember. Involve me, I will understand"
  - Drive customer & stakeholder engagement, involve them in your performance plans, risks, and mitigations, manage their expectations though the collaboration, communication, integrity, and trust built by your actions
- Apply rigorous performance management methodology at critical phases
  - Performance Requirements & Implementation
  - Performance Design
  - Performance Integration, Test, and Verification

Establish technical performance as part of the culture



Drive 'Must Have' Performance into the Technical Baseline & the Program Culture

Performance Requirements and Implementation

- Performance Boundaries need to be crisp, clear and verifiable:

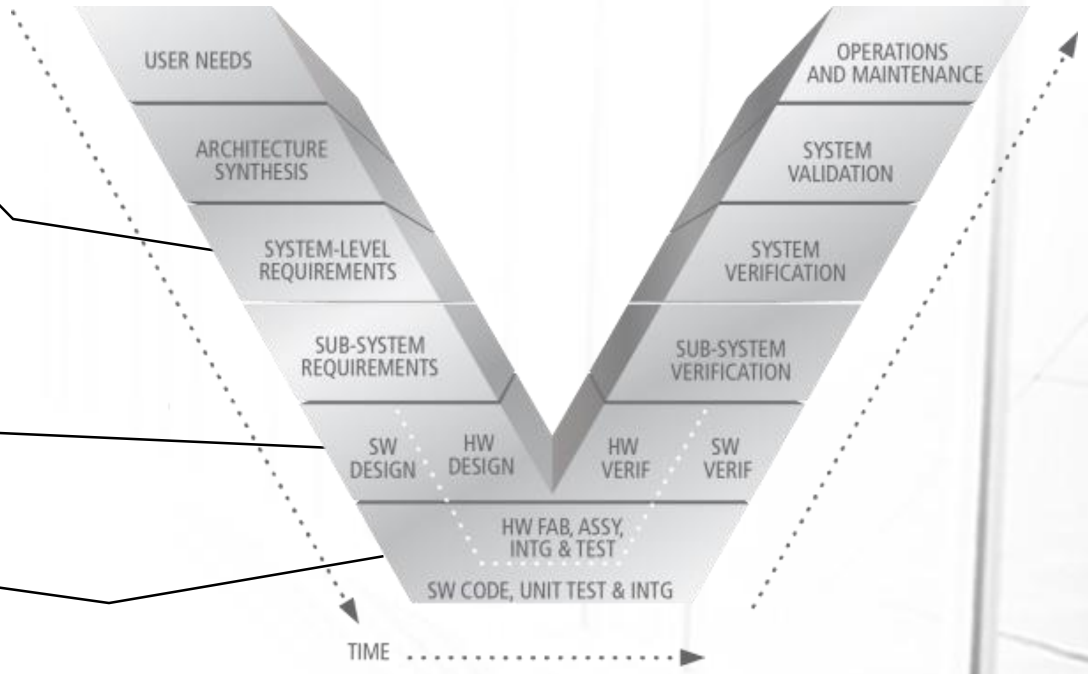
  - Latency: last bit in last bit out vs. first bit in first bit out, etc
  - Infrastructure: CPU/MEM, LAN/WAN, Storage -> Loading Condition, Virtual Environment, Nominal vs. Worst Case, etc
  - Accuracy and Error: Truth source, Filter criteria, statistical sell off points

- Agreed upon assumptions need to be clearly documented and periodically reviewed

- See Next Slide

- Performance issues are hard to fix. Use DevOps, Agile, Scrum methodology to shorten the Observe, Orient, Decide, Act (OODA) loop

- As the system matures, periodic performance regression tests will be desirable to continuous monitor the system performance -> Automation is necessary to achieve performance monitoring.



Not well defined or managed perf requirements = significant cost/schedule impact

Performance Design

Performance Design

Design to Meet Performance Requirements

- Performance is not an after thought
- Do it early: preliminary design and detailed design
- Evaluate COTs for performance sustainability and testability
- Evaluate for obsolescence and software patches

Design for Performance Evaluation and Data Collection

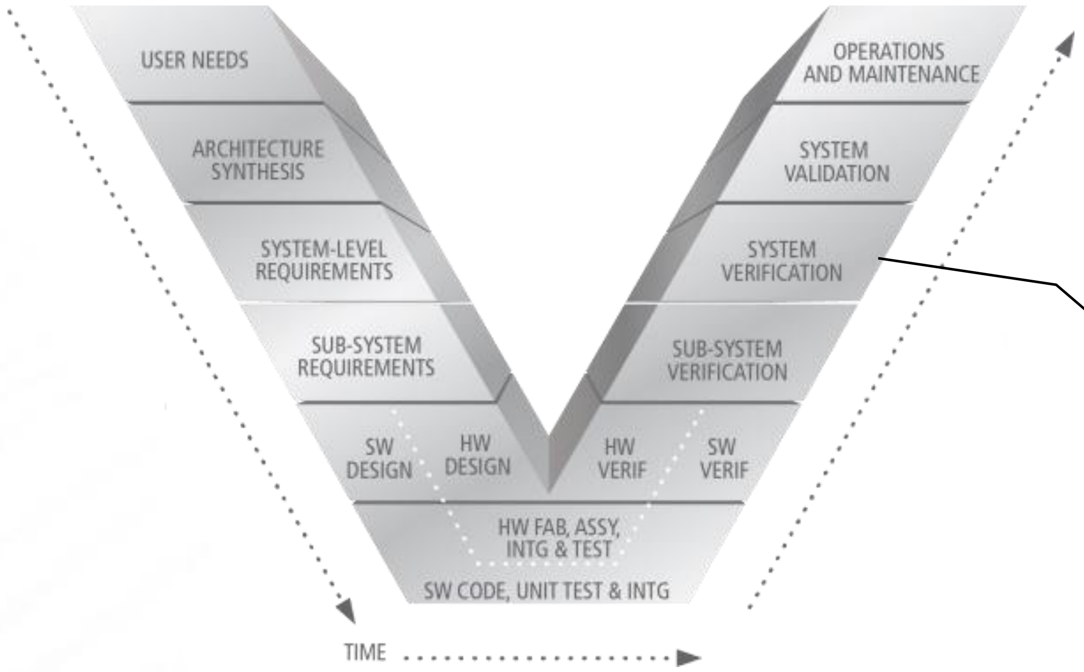
- **Instrumentation**
  - Seed data to drive the software
  - Test scripts for sample size
  - Test loading/configuration
  - Logging Mechanism
- **Post Processing and Analysis:**
  - Correlation scheme
  - Post processing scripts to parse and correlate the data
  - Analysis Work Instruction

Design for Risk Mitigation and Continuous Risk Management

- Perf Maturity Road Map: MBSE -> Prototype -> Unit Test -> Integrated Environment -> Ops Like Environment
- Define road map transition plans and ensure the plans are incorporated in the program/SE master plan

Design for Off-Nominal Conditions

Performance Integration, Test and Verification



- Sum of the lower level performance estimations is not always smaller or equal to the high level performance. Sometimes 1 + 1 = 11. Manage both low level performance and high level performance.
- Be aware of the interdependencies and assumptions.
- Performance verification test should be a check box. System/subsystem/CI performance issues need to be detected, investigated and resolved early to reduce cost/schedule risks.
- Tooling/instrumentations need to be qualified and managed with change configuration management for formal performance qualification test
- IA and Cyber security will have performance impact

UNRESTRICTED CONTENT – NON-EXPORT CONTROLLED

Thank you!

Q & A

UNRESTRICTED CONTENT – NON-EXPORT CONTROLLED

Contact Information

- Brian Davenport
  Raytheon
  (303) 344-6715
  bmdavenport@Raytheon.com
- Ji Li
  Raytheon
  (720) 858-5279
  ji.li@Raytheon.com

UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH

Free and Open Source Tools to Assess Software Reliability and Security

NAVAIR

Vidhyashree Nagaraju, Venkateswaran Shekar, Thierry Wandji[2] and Lance Fiondella[1]

[1]*University of Massachusetts*, North Dartmouth, MA 02747

[2]*Naval Air Systems Command*, Patuxent River, MD 20670

Questions?

Outline

- Year I deliverables summary
- Guidance
- Software Failure and Reliability Assessment Tool (SFRAT)
  - Architecture
  - Review of Year I functionality
  - Year II functionality
- Software Defect Estimation Tool (SweET)
- Goals

State of software reliability

- Software reliability studied for 50+ years
  - Methods have not gained widespread use
    - Disconnect between research and practice
- Diverse set of stakeholders
  - Reliability engineers
    - May lack software development experience
  - Software engineers
    - May be unfamiliar with methods to predict software reliability

YEAR I (3/15-2/16) DELIVERABLE SUMMARY

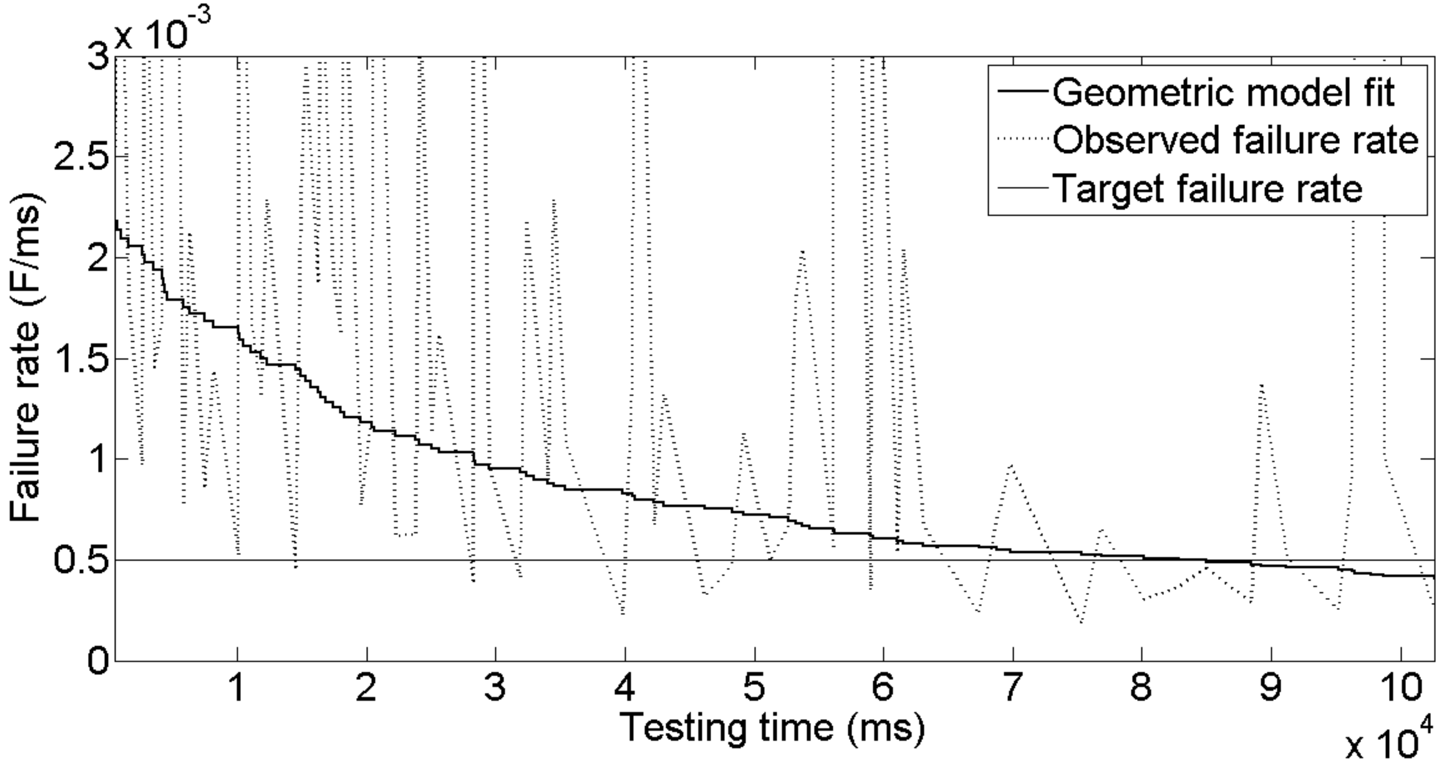
Summary of Year I deliverables

- Implemented open source software reliability tool
  - Data conversion routines
  - Trend tests for reliability growth
  - Two failure rate models
    - Assume failure rate decreases as faults detected and removed
  - Three failure count models
    - Count faults detected as function of time
  - Tested on dozens of data sets
  - Two goodness of fit measures

Estimates enabled by software reliability models

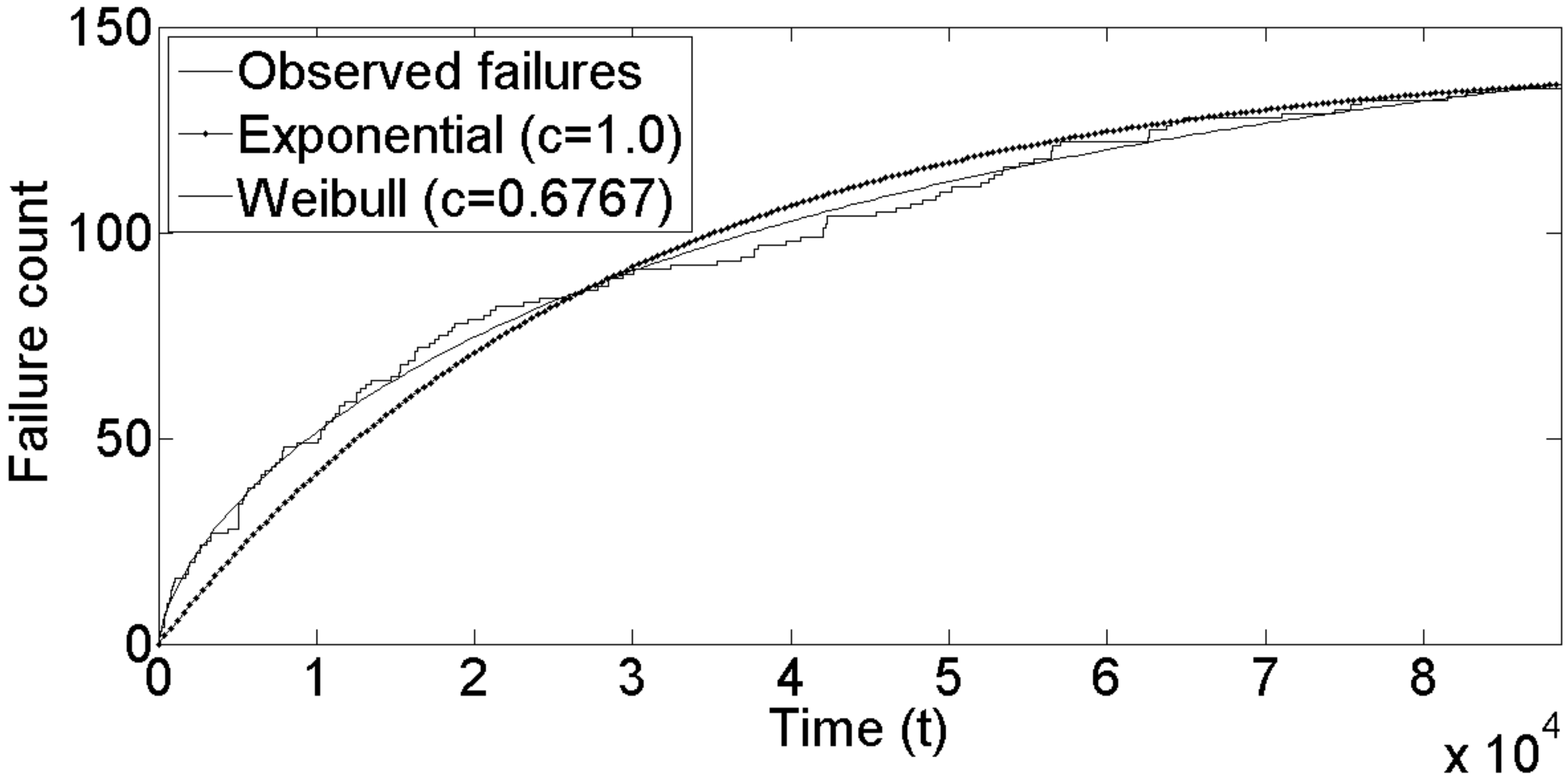
- Number of
  - Faults detected with additional testing
  - Remaining faults
- Mean time to failure (MTTF) of next fault
  - Testing time needed to remove next k faults
- Probability software does not fail before completion of fixed duration mission

Failure rate model



Model characterizes decreasing trend in failure rate

Failure time/count models



Model characterizes fault discovery process

UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH

sasdlc.org/lab/projects/srt.html

Software Failure and Reliability Assessment Tool (SFRAT)

Description

The key to the success of all software is its reliability. The Software Failure and Reliability Assessment Tool (SFRAT) is an open source application to estimate and predict the reliability of a software system during test and operation. It allows users to answer the following questions about a software system during test:

1. Is the software ready to release (has it achieved a specified reliability goal)?
2. How much more time and test effort will be required to achieve a specified goal?
3. What will be the consequences to the system's operational reliability if not enough testing resources are available?

SFRAT runs under the R statistical programming framework and can be used on computers running Windows, Mac OS X, or Linux

Resources

WARNING: Web instance is for demonstration only. Please do not upload sensitive data to the site

Web instance
Example failure data sets
SFRAT Github repository
User's Guide
Contributor's Guide

Publications

Search:

Year	Type	Publication

GUIDANCE

Software Reliability Growth Modeling

- No single model characterizes all data sets best
- Models supplementary mathematical guidepost
  - Used in conjunction with SDLC activities to identify, implement, and test functional requirements
- Do not prescribe a single model
- Learn to track before planning in SEPs & TEMPs
- Emphasize
  - Effective communication between system, reliability, and software engineers
  - Frequent use of quantitative SRGM throughout DT and OT to assess progress toward software and system reliability goals

Software Reliability Growth Tracking

- For reliability growth tracking to be effective
  - Failures and their severity must be clearly defined
  - Impact on mission and end-to-end capability in order to produce data suitable for reliability growth tracking
  - Will be impacted by updates to interacting subsystems including hardware, mechanical, sensing, and operator usage

Data formats

- Based on data formats
  - Failure Rate models
    - Inter-failure times - time between $(i-1)^{st}$ and i^{th} failure, defined as $t_i = (\mathbf{T}_i - \mathbf{T}_{i-1})$
    - Failure times – vector of failure times,
      $$\mathbf{T} =< t_1, t_2, \dots, t_n >$$
  - Failure Counting models
    - Failure count data - length of the interval and number failures observed within it,
      $$< \mathbf{T}, \mathbf{K} >=< (t_1, k_1), (t_2, k_2), \dots, (t_n, k_n) >$$
  - Possible to use change requests during DT

Data quality

- Accuracy
  - Critically depends on availability of failure data
  - Inaccurate records of time make model fitting and prediction difficult
- Even when data available
  - Practitioner must know how to filter and organize data for use in models
    - Filter to exclude: non-software issues, duplicate failures, etc…

SOFTWARE FAILURE AND RELIABILITY ASSESSMENT TOOL (SFRAT)

ARCHITECTURE

SFRAT user modes

- Graphical user interface
  - Web and intranet
- Developer mode
  - Incorporate additional models
- Power user
  - Incorporate into internal software testing processes
- Benefits
  - Can help contractors, FFRDCs, and government quantitatively assess software as part of data collection, reporting, and oversight

SFRAT – File structure

install_script.R

server.R

ui.R

utility

- Data
  - a.Data_Tools.R
- Metrics
  - a.GOF.R
- Plots
  - a.PlotModelResults.R
  - b.Plot_Raw_Data.R
  - c.Plot_Trend_Tests.R
- Prediction
  - a.Detailed_prediction.R
- tables
  - a.DataAndTrendTables.R
  - b.ModelResultTable.R
- RunModels.R

trend_tests

1. Laplace_trend_test.R
2. RAA.R

models

- GO
- DSS
- Wei
- JM
- GM

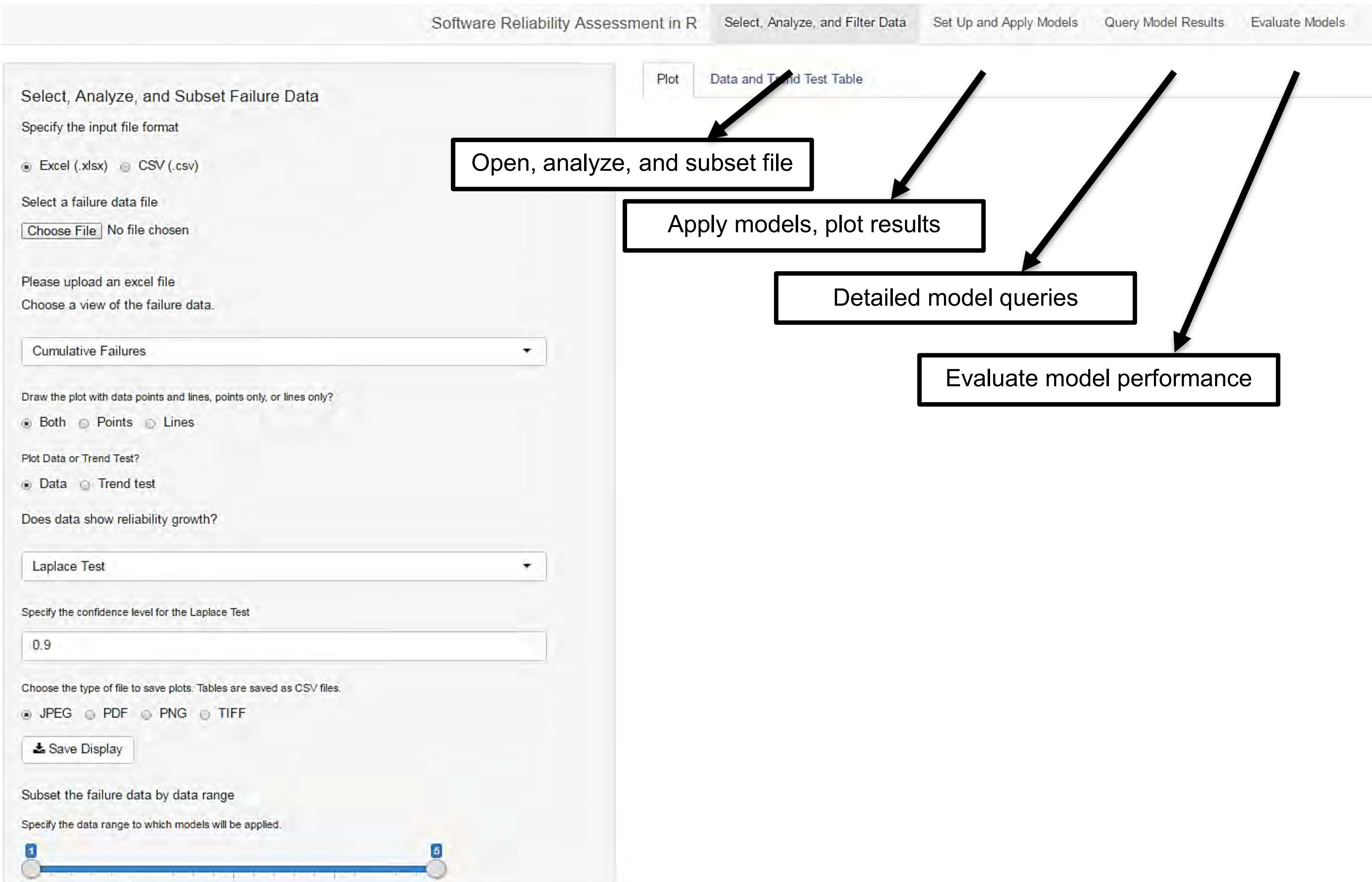
New models added in the "models" folder

Power user mode

- Code can be tailored for internal use
  - Build into existing automated software testing procedures to provide near real-time feedback of reliability trends
  - Many industry standard programming languages can call R functions
    - Visual Basic, Java, C/C#/C++, and Fortran
    - Ensures tool will integrate smoothly

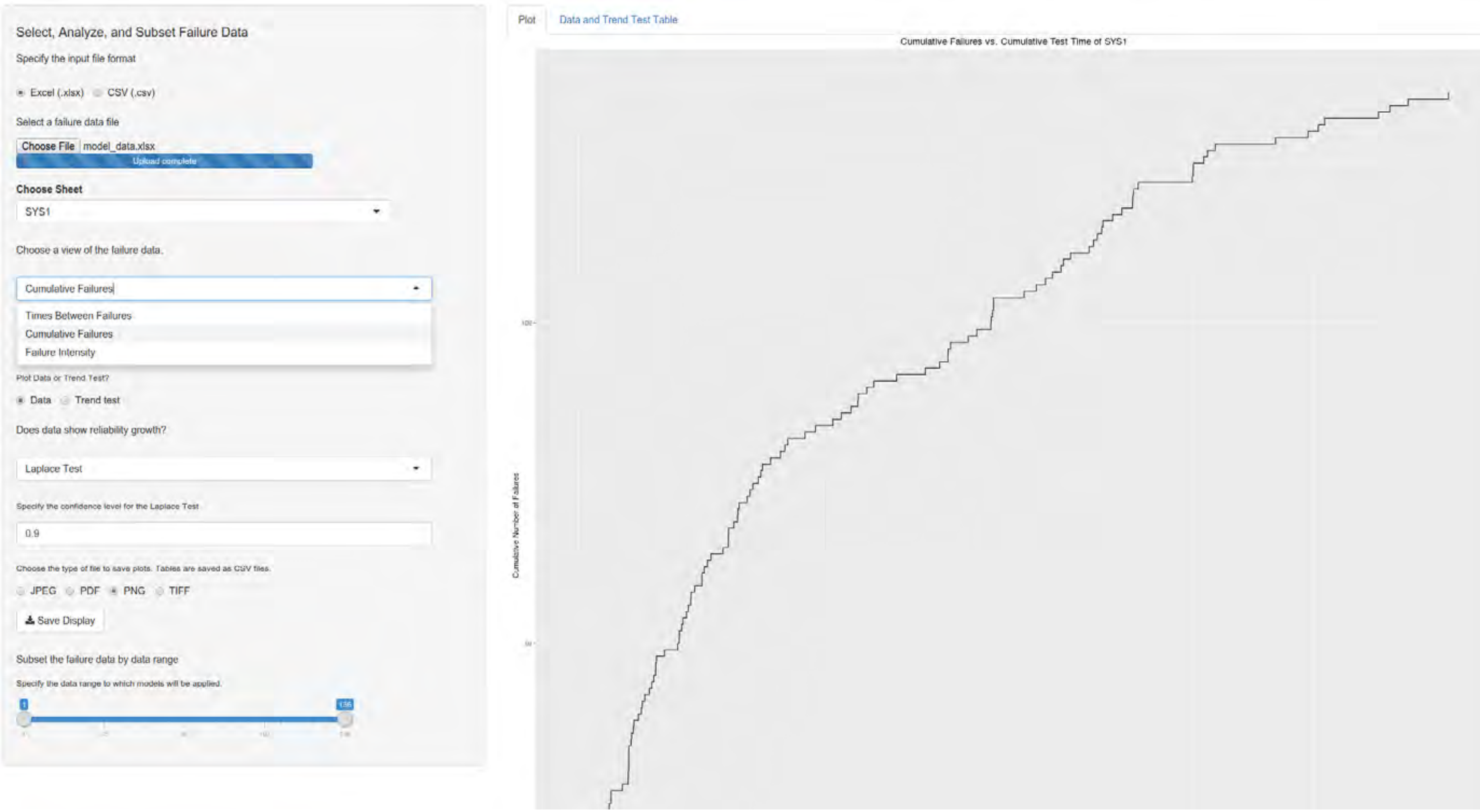
REVIEW OF YEAR I FUNCTIONALITY

SFRAT - Tab view



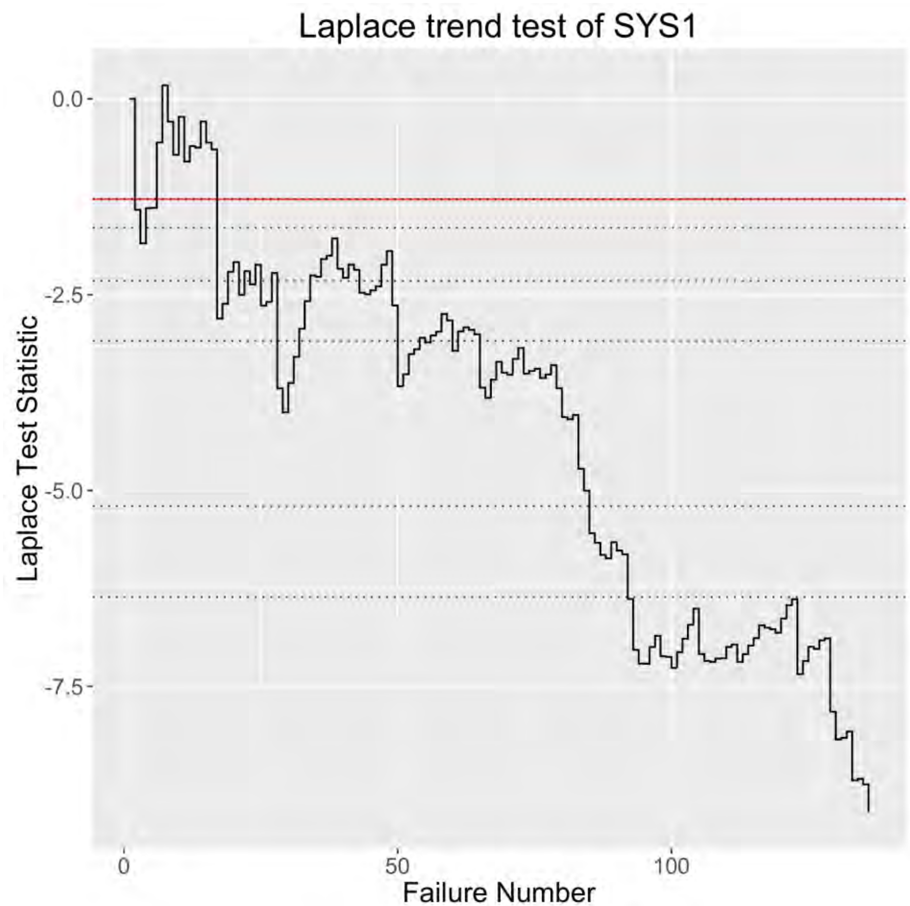
Tab 1
Select, Analyze, and Filter data

Tab 1 – After data upload



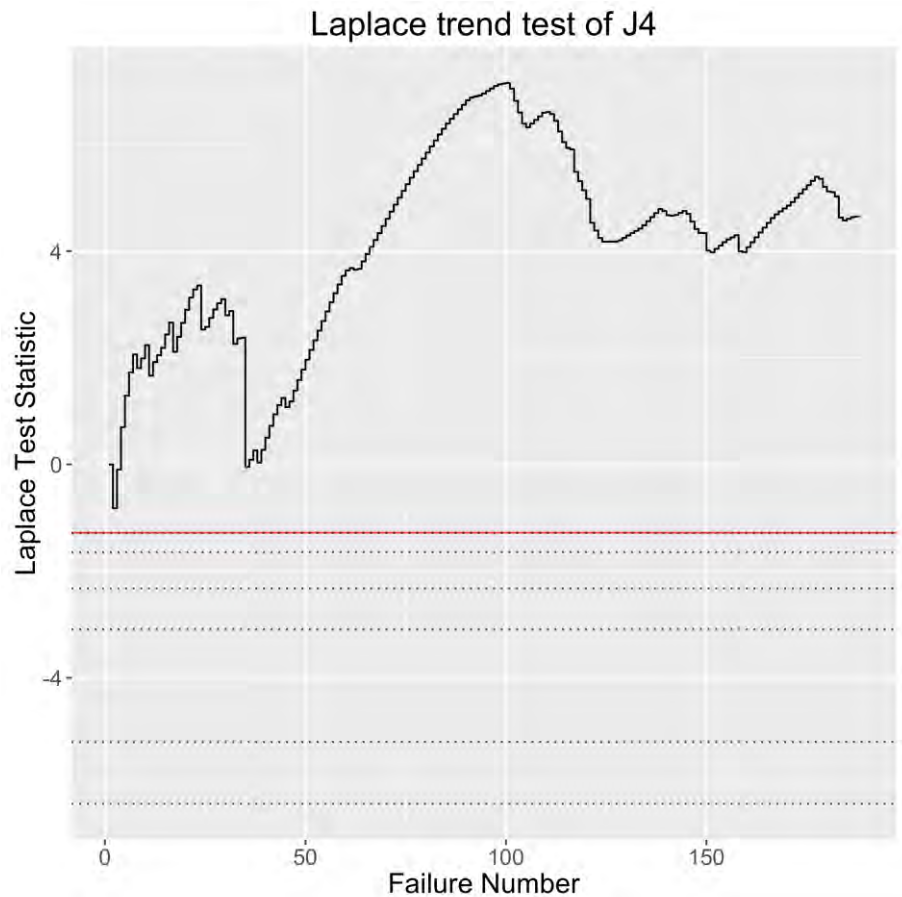
Cumulative failure data view

Laplace trend test – SYS1 data



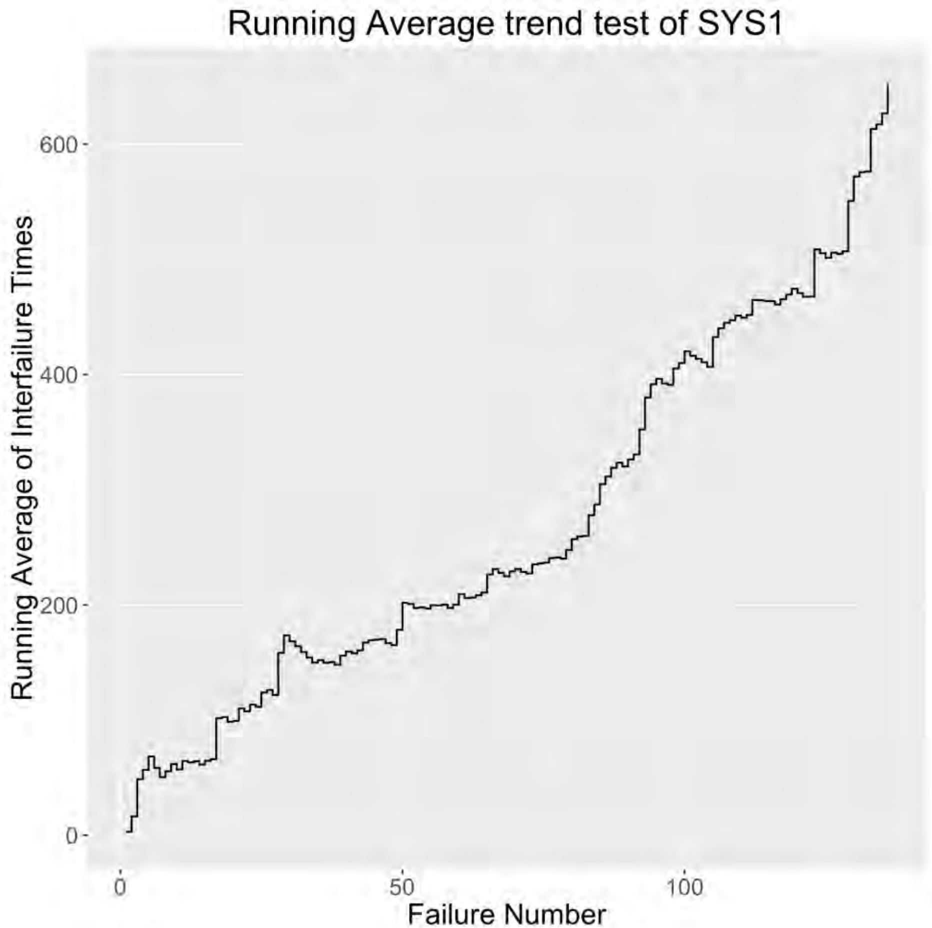
Decreasing trend indicates reliability growth
(Indicates application of SRGM appropriate)

Laplace trend test – J4 data



Does not exhibit reliability growth
(Indicates additional testing required)

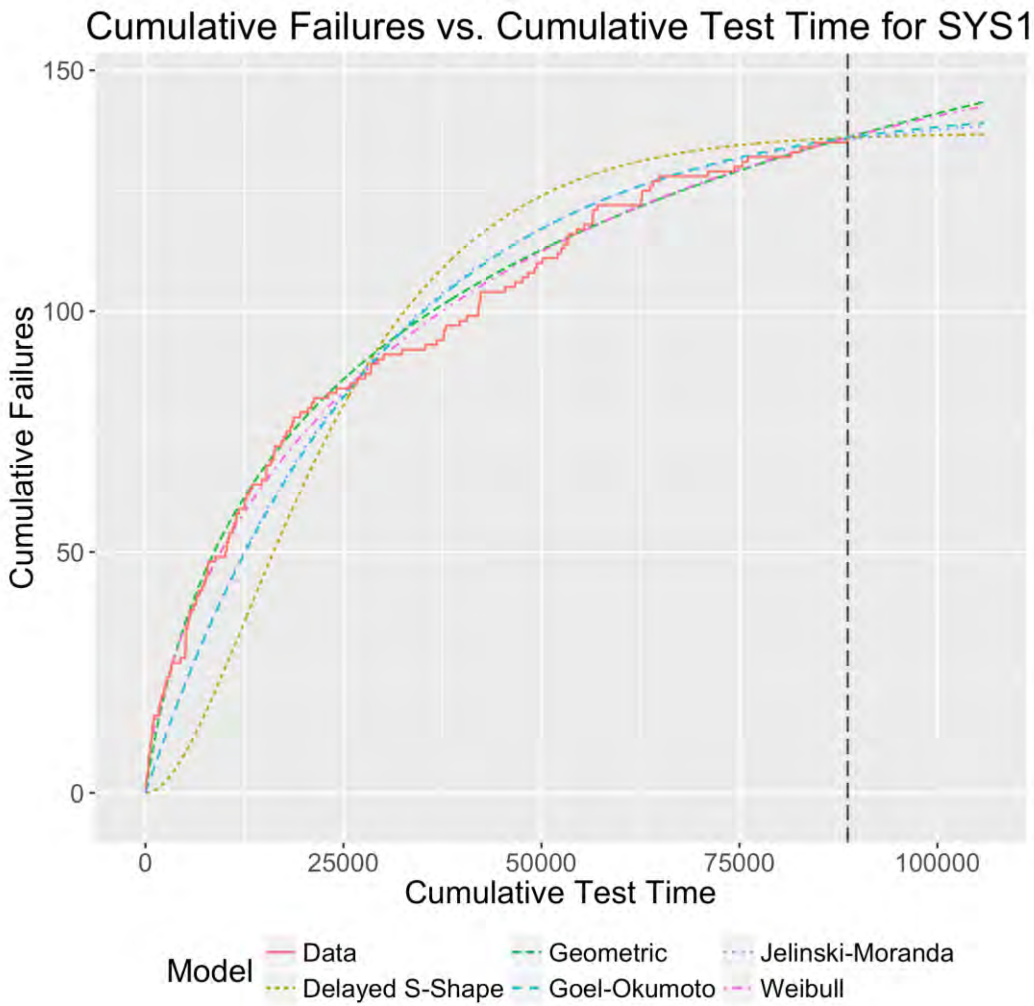
Running Arithmetic Average – SYS1 data



Increasing trend indicates reliability growth

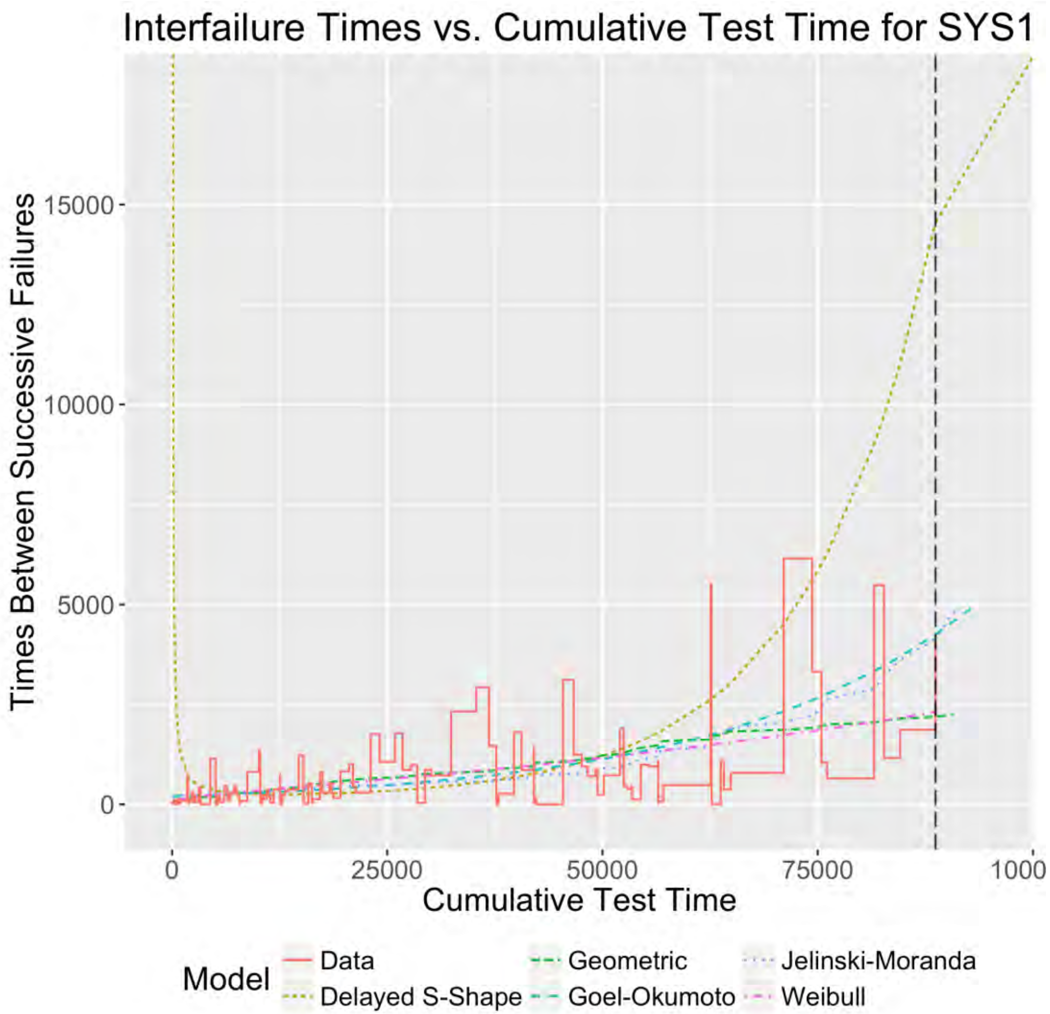
Tab 2
Set Up and Apply Models

Cumulative failures



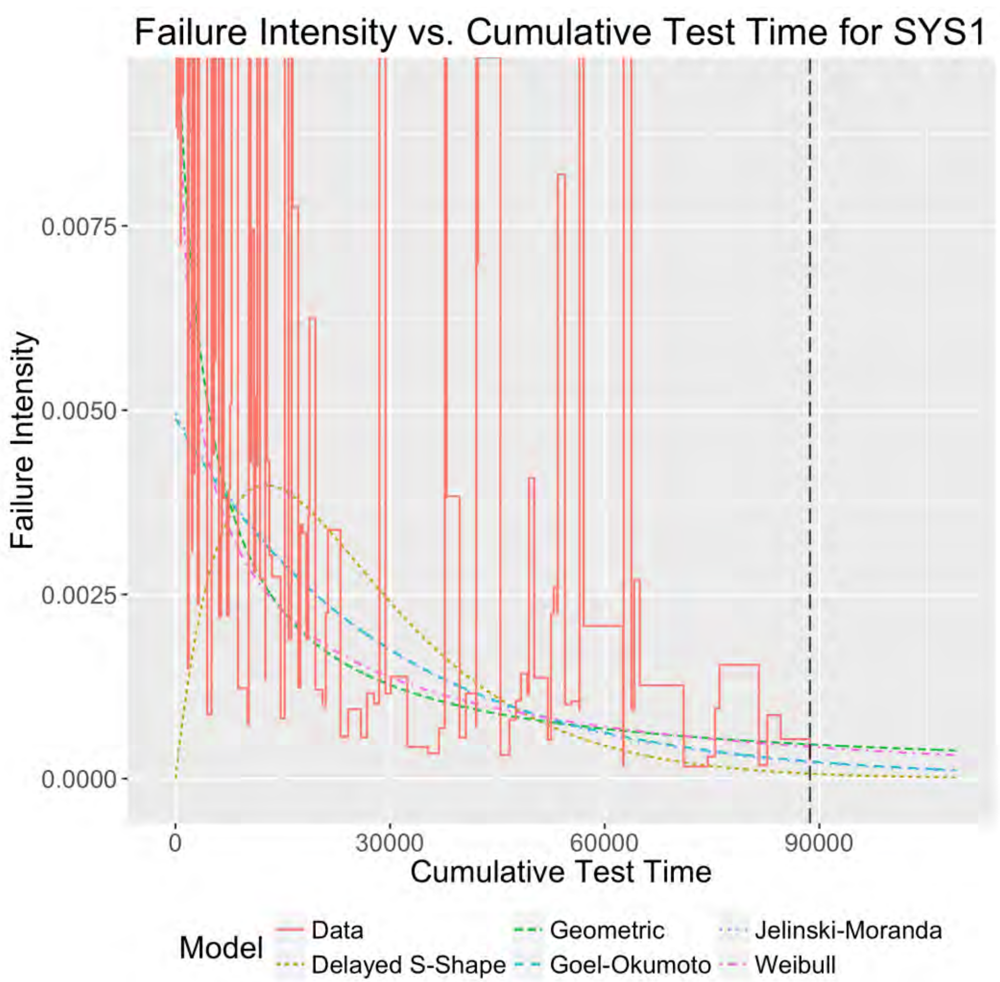
Plot enables comparison of data and model fits

Time between failures



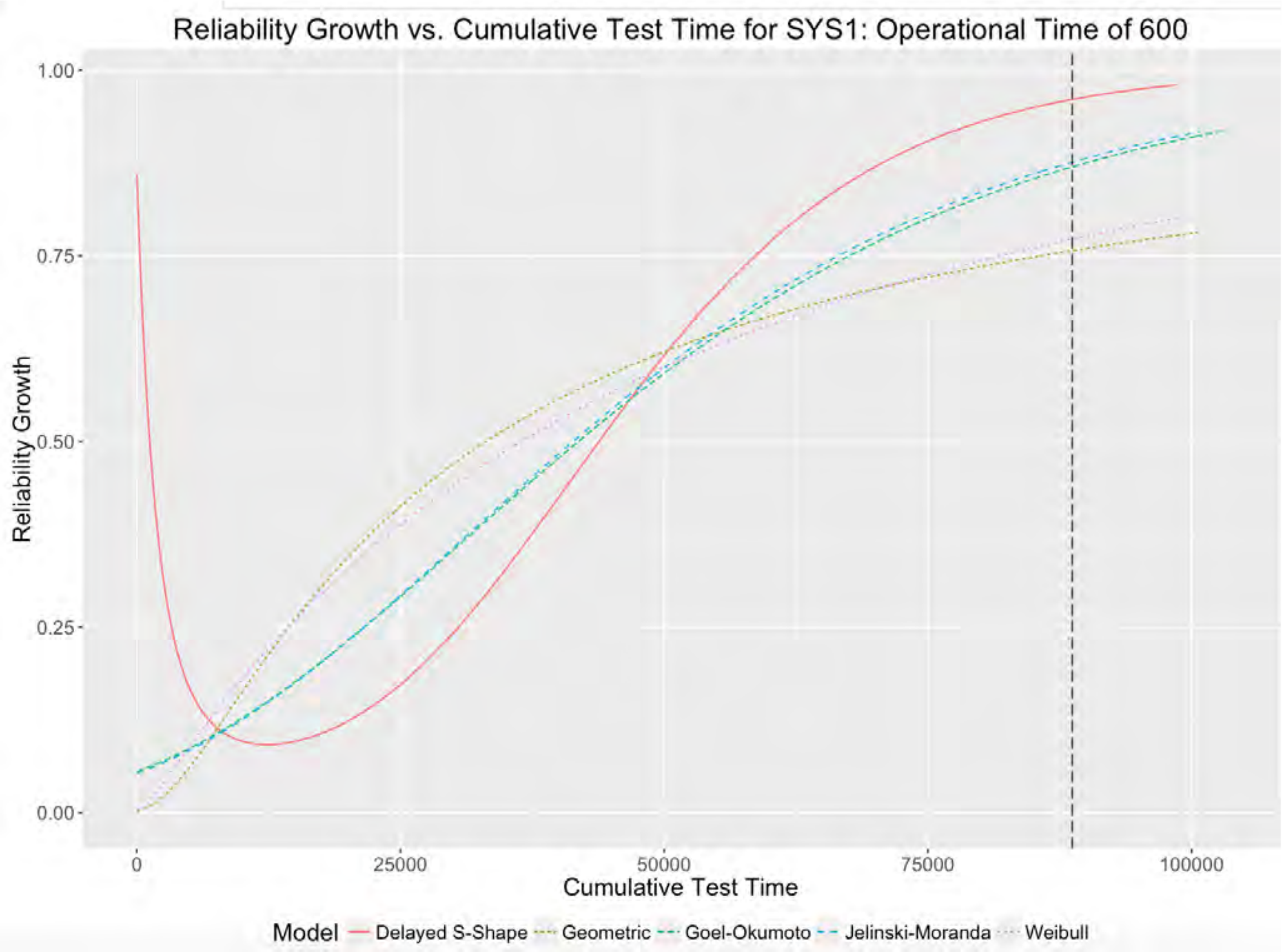
Times between failures should increase (indicates reliability growth)

Failure intensity



Failure intensity should decrease (indicates reliability growth)

Reliability growth curve



Can determine time to achieve target reliability

Tab 3
Query Model Results

Failure Predictions

	Model	Time to achieve R = 0.9 for mission of length 4116	Expected # of failures for next 4116 time units	Nth failure	Expected times to next 1 failures
	All	All	All	All	All
1	Delayed S-Shape	12401.1541529981	0.2468563	1	NA
2	Geometric	1592716.45936287	1.8774731	1	2170.03088926781
3	Goel-Okumoto	62829.7672027733	0.9036154	1	4591.28466949961
4	Jelinski-Moranda	59915.2917457156	0.8561255	1	4869.80650205625
5	Weibull	259865.770847692	1.7259537	1	2353.05254648438

Showing 1 to 5 of 5 entries

Previous 1 Next

Can identify potential schedule overruns

Tab 4
Evaluate Models

AIC and PSSE

	Model	AIC	PSSE
	All	All	All
1	Delayed S-Shape	2075.146	296.34925
2	Geometric	1937.034	84.32708
3	Goel-Okumoto	1953.613	23.07129
4	Jelinski-Moranda	1950.534	19.60037
5	Weibull	1938.161	74.94496

Showing 1 to 5 of 5 entries

Previous 1 Next

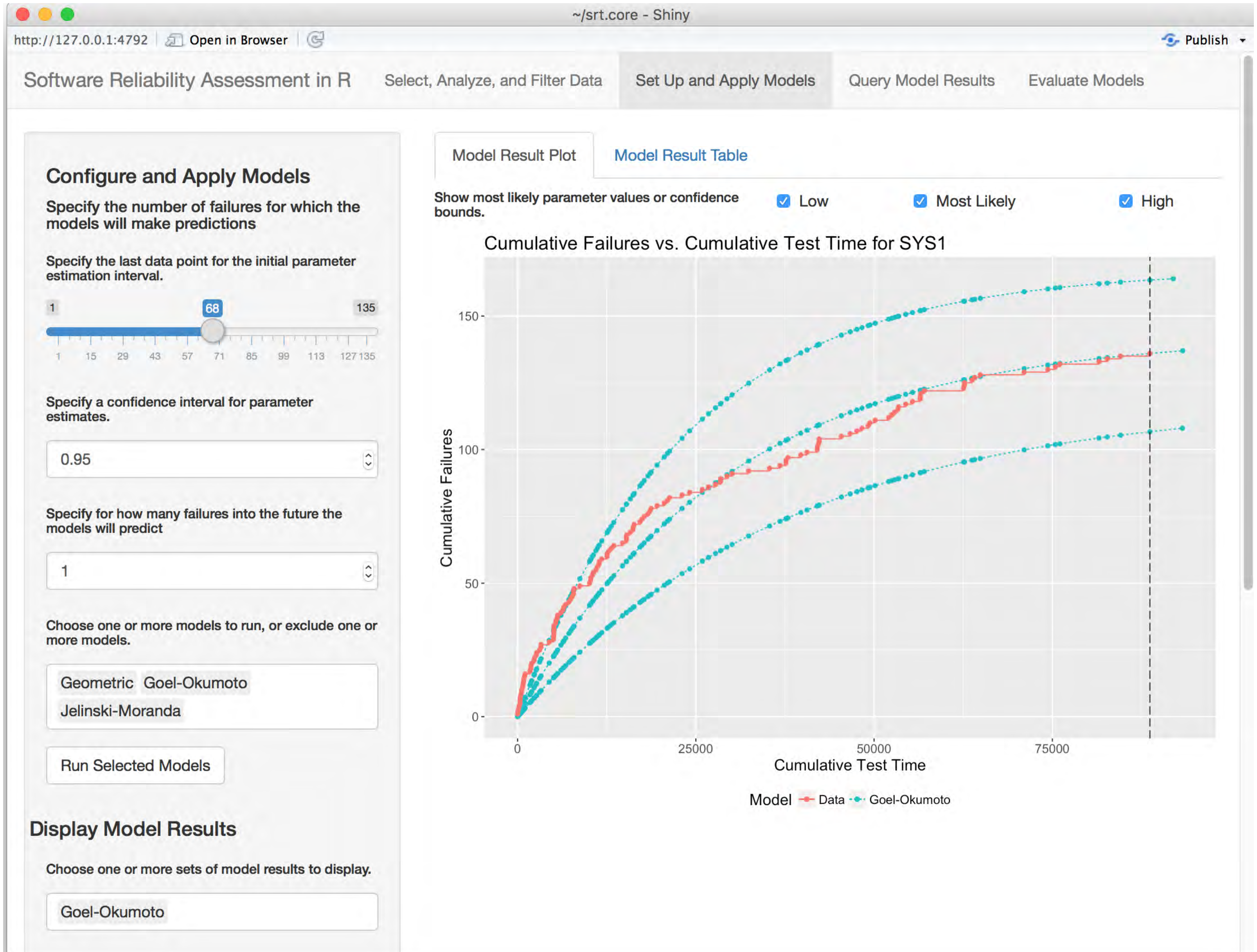
Lower values preferred

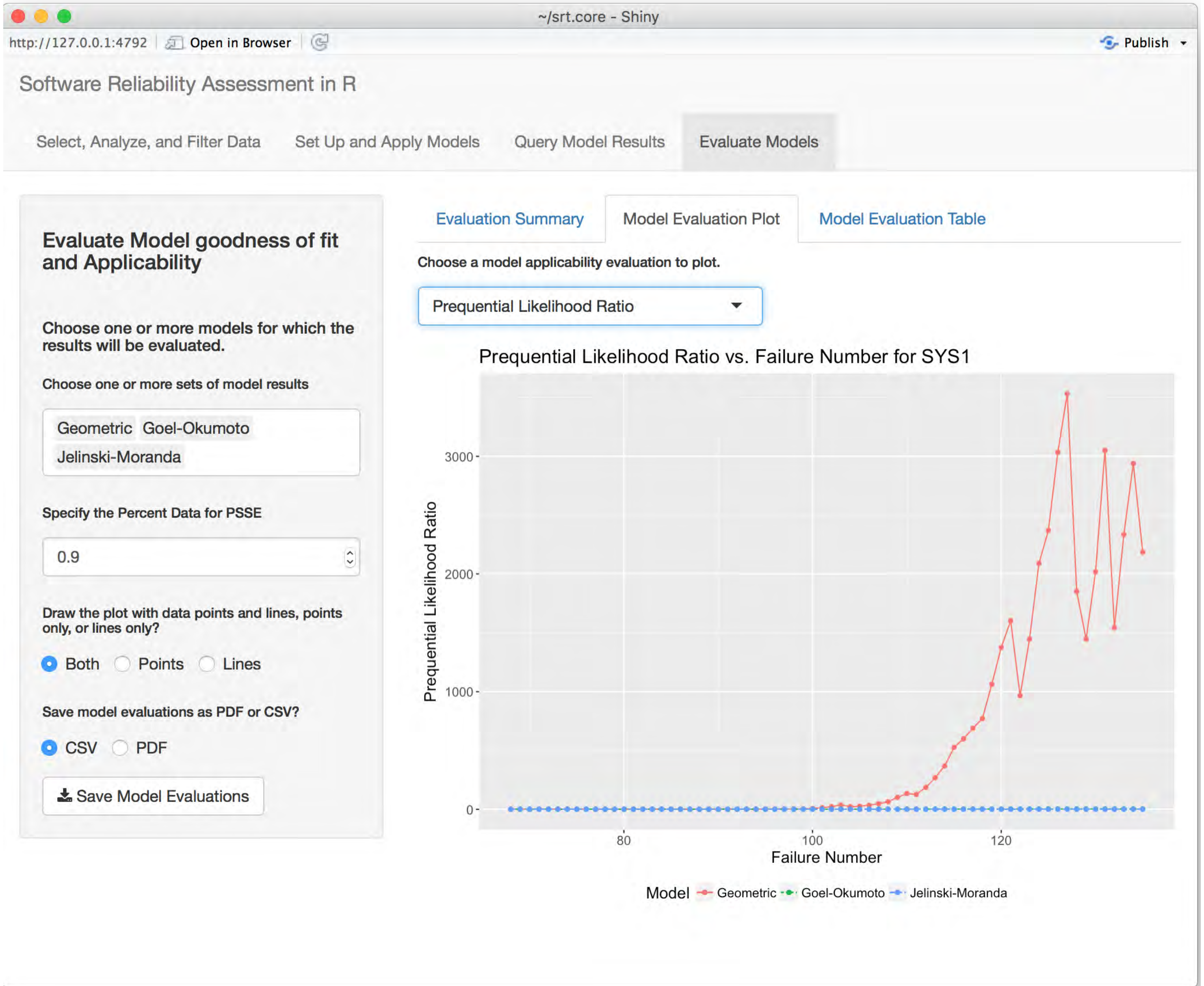
UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH

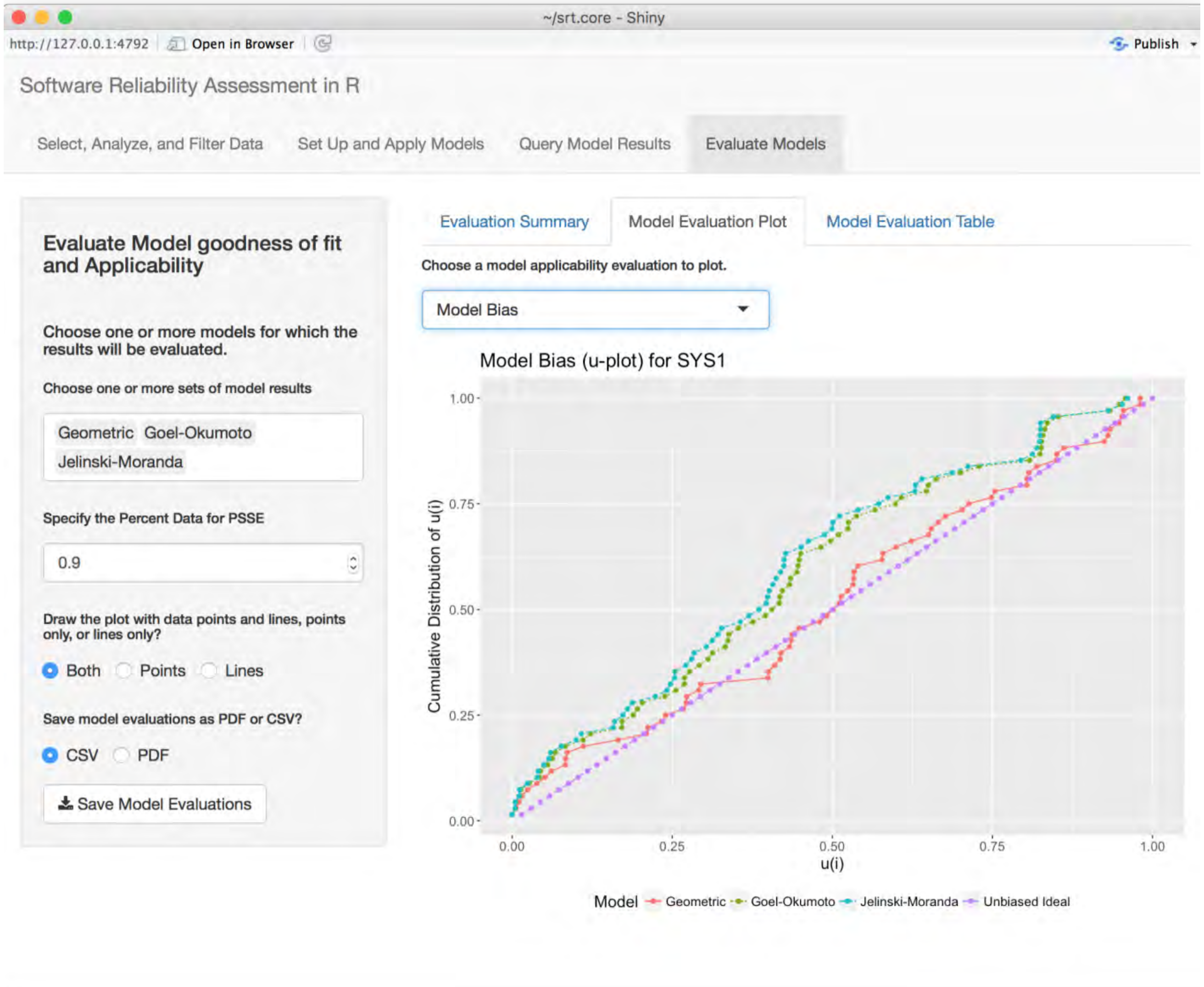
YEAR II (7/16-7/17) SFRAT FUNCTIONALITY

- Upper and lower confidence limits
  - Graphical and tabular values
- Model Evaluation Criteria
  - Prequential likelihood (PL) ratio
    - Identify model more likely to produce accurate estimates
      - Higher preferred
  - Model bias (MB) and MB trend
    - Indicate whether model over/underestimates times between failures
- Optimal release

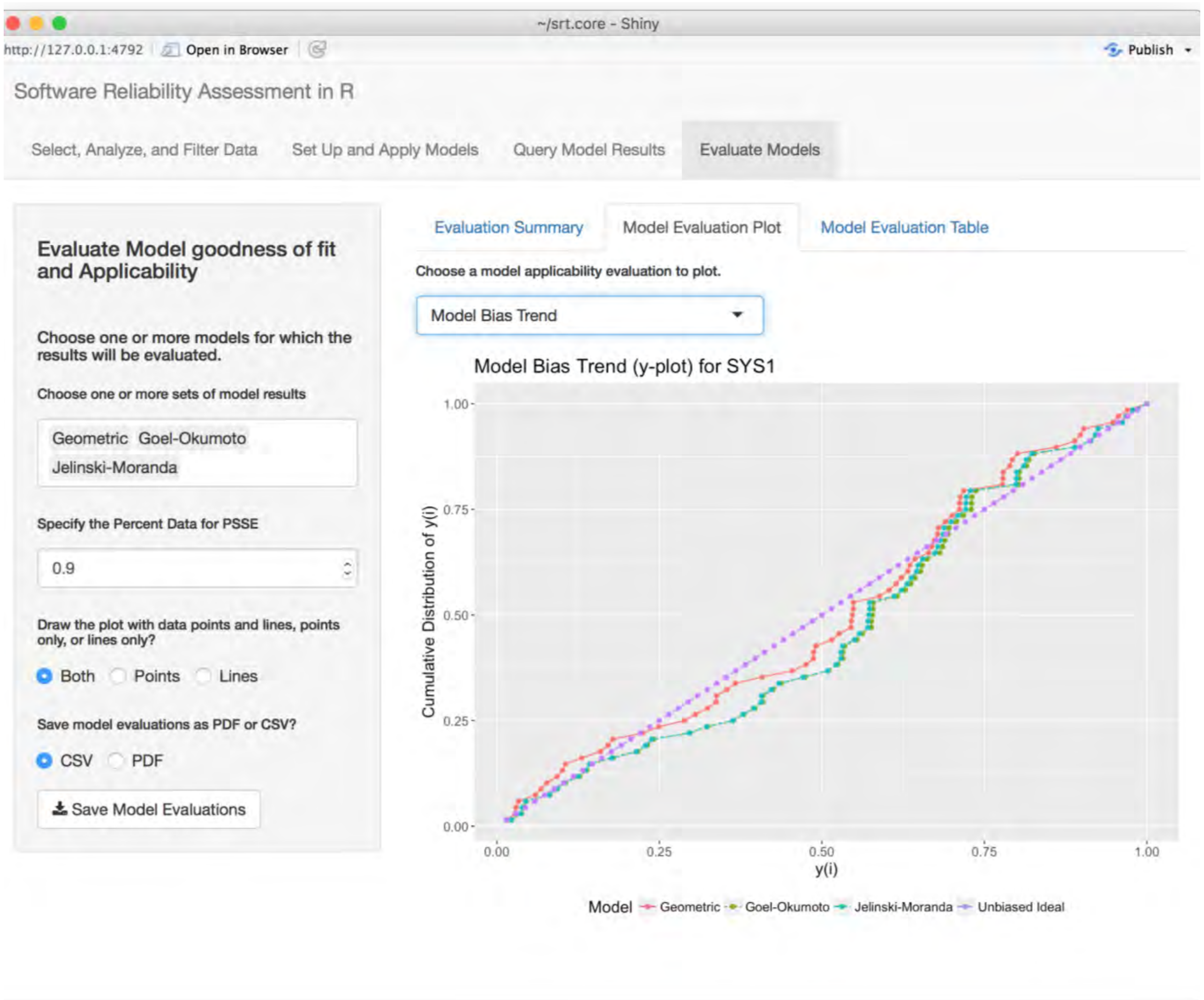
UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH



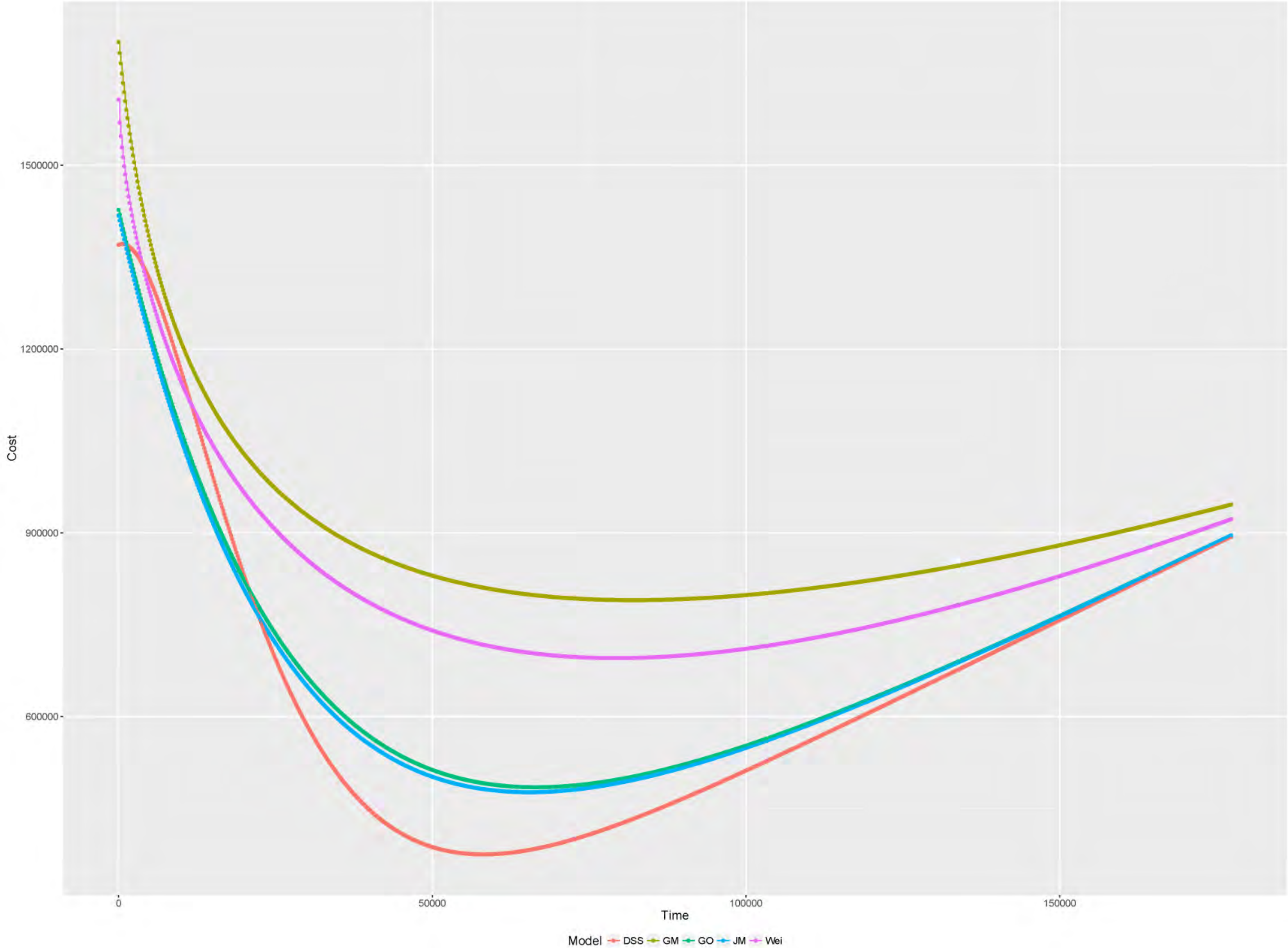

~/srt.core - Shiny
http://127.0.0.1:4792
Open in Browser
Publish
Software Reliability Assessment in R
Select, Analyze, and Filter Data
Set Up and Apply Models
Query Model Results
Evaluate Models
Evaluate Model goodness of fit and Applicability
Choose one or more models for which the results will be evaluated.
Choose one or more sets of model results
Geometric
Goel-Okumoto
Jelinski-Moranda
Specify the Percent Data for PSSE
0.9
Draw the plot with data points and lines, points only, or lines only?
Both
Points
Lines
Save model evaluations as PDF or CSV?
CSV
PDF
Save Model Evaluations
Evaluation Summary
Model Evaluation Plot
Model Evaluation Table
Choose a model applicability evaluation to plot.
Prequential Likelihood Ratio
Prequential Likelihood Ratio vs. Failure Number for SYS1
Prequential Likelihood Ratio
3000
2000
1000
0
80
100
120
Failure Number
Model
Geometric
Goel-Okumoto
Jelinski-Moranda



Models above line estimate more frequent times between failures than those observed



Models below line estimate more frequent times between failures than those observed


1500000
1200000
900000
600000
Cost
0
50000
100000
150000
Time
Model DSS GM GO JM Wei

SOFTWARE DEFECT ESTIMATION TOOL (SWEET)

SWEEP (Software Error Estimation Program)

- Implemented four modes
  1. Time-based model
     - Estimates and tracks errors during system test and integration cycle
  2. Phase-based model
     - Provides defect information before running any code
  3. Planning aid
     - Generates an error discovery profile based on historical data
  4. Defect injection model
     - Allows user to understand probable defect injection profile

Software Defect Estimation Tool (SweET)

Description

The Software Defect Estimation Tool (SweET) is an open source application to track error identification and removal efforts during the software development lifecycle. SwEET is a free and open source version of the SoftWare Error Estimation Program (SWEEP) and SweET uses Weibull software reliability growth model utilizing Expectation Conditional Maximization algorithm to ensure stability and performance of the model fitting process. SweET simplifies four models of SWEEP into three modes:

1. **Mode A**: Time-based model: Estimates and tracks errors during system test and integration cycles.
2. **Mode B**: Phase-based and planning aid model: Predict and track defects for multiple phases and can provide defect information before running any code, whereas the planning aid model generates an error discovery profile based on the phase based historical data to help a software prohect achieve its objectives.
3. **Mode C**: Defect injection model: Allows the user to understand the probable defect injection profile and resulting efficiency and effectiveness of the verification process.

SweET runs under the Python 3.x programming framework and can be used on computers running Windows, Mac OS X, or Linux

Resources

Example data sets
SweET Github repository
User's Guide (In preparation)

GOALS

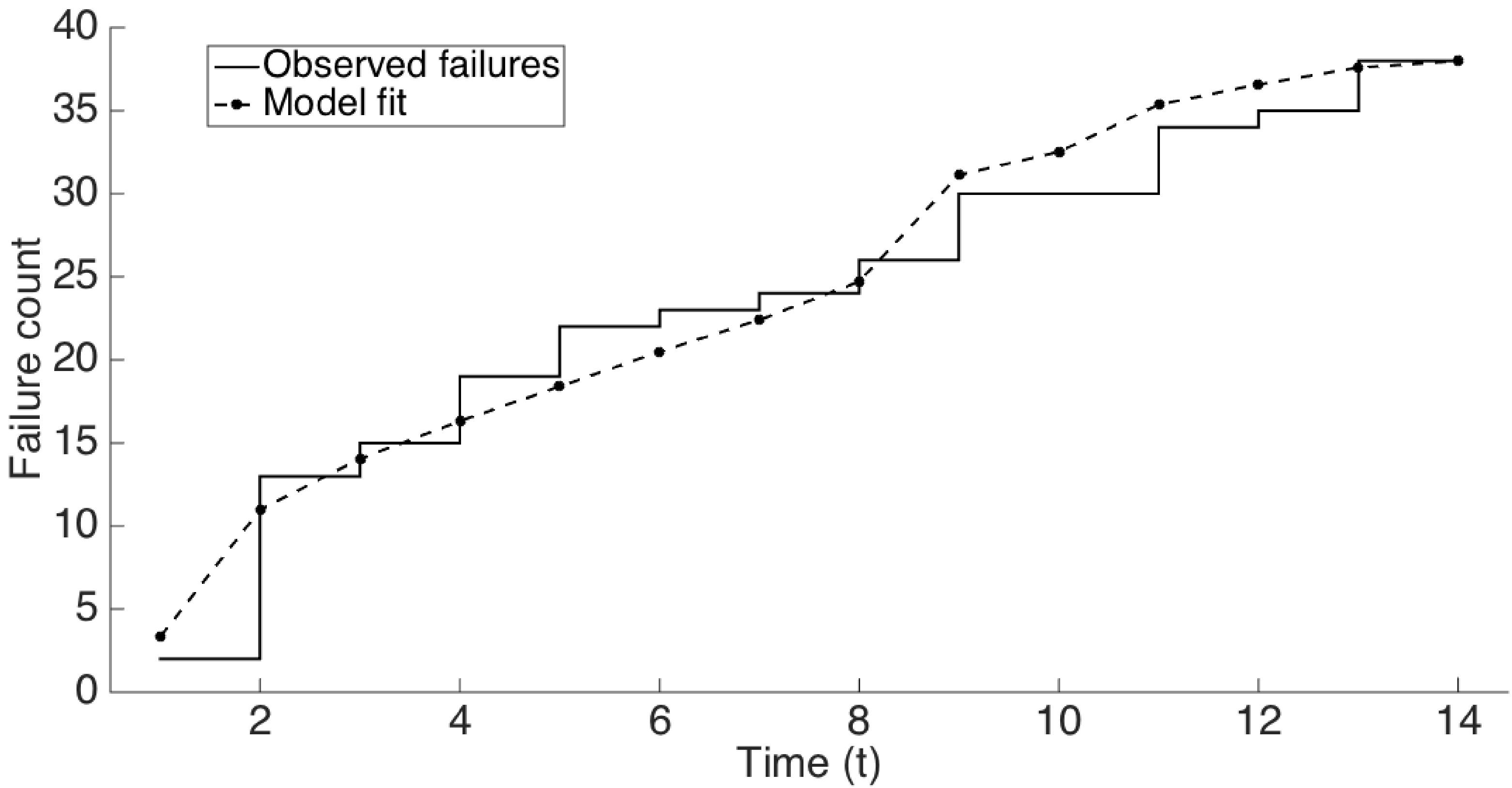
Activities

- Update documentation
- Outreach, education, and training
  - Visit DoD labs and listen to practical concerns underlying modeling requirements
  - Work with existing users
- Coordinate contributions from developers
  - Failure severity decomposition
  - Software readiness metrics
  - Additional models, Bayesian, covariate
  - Expand architecture to additional stages of lifecycle

Covariate data example

week	Execution Time (hr)	Failure Identification Work (person hr)	Computer Time-Failure Ident. (hr)	Failure Identified
1	.0531	4	1.0	1
2	.0619	20	0	1
3	.1580	1	0.5	2
4	.0810	1	0.5	1
5	1.0460	32	2.0	8
6	1.7500	32	5.0	9
7	2.9600	24	4.5	6
8	4.9700	24	2.5	7
9	0.4200	24	4.0	4
10	4.7000	30	2.0	3
11	0.9000	0	0	0
12	1.5000	8	4.0	4
13	2.0000	8	6.0	1
14	1.2000	12	4.0	0
15	1.2000	20	6.0	2
16	2.2000	32	10.0	2
17	7.6000	24	8.0	3
total	32.8000	296	60.0	54

Covariate model data fit



Stakeholder outreach

Acknowledgements

- This work was supported by (i) the Naval Air Warfare Center (NAVAIR) under contract N00421-16-T-0373 and (ii) the National Science Foundation (NSF) (#1526128).

Air Force Materiel Command

Software Development Challenges in AFMC (Agile Software Development and Data Rights)

Abstract # 19902

25 Oct 2017

Dr. Marc Shaver, HQ AFMC/ENS
Mr. Andrew Jeselson, HQ AFMC/ENS
Mr. Curtis Jefferson, AFLCMC/EZAS

Breaking Barriers … Since 1947

Outline

- Introduction (Dr. Marc Shaver)
- HQ AFMC/EN ASD Questionnaire Results (Mr. Andrew Jeselson)
- AFLCMC/EN-EZ Agile Software Development (ASD) Workshop (Mr. Curtis Jefferson)
- AFLCMC/EN-EZ SW Data Rights Strategy Process (Mr. Curtis Jefferson)

Introduction

- The Air Force Engineering Enterprise led efforts identifying knowledge, skills, and process gaps within the workforce
- Two software related topics were:
  - Awareness of Agile, Flexible SW Development & Sustainment Methodology to include Agile SW Development (ASD)
  - Software Data Rights Strategy process
- AF Life Cycle Management Center (AFLCMC), with AF Materiel Command (AFMC) support, leading efforts to address these topics
- A key initial outcome of these efforts is the requirement to develop education and training for the engineering workforce
  - Education will capitalize on existing DAU and other courses providing basic understanding of ASD and Data Rights
  - Focus on AF unique practices, processes, and tools
  - Initial concepts under development

Background

- **ASD**
  - **Well understood and widely used commercially and, in DoD Information Technology (IT) and Business System applications**
  - **DoD weapon system acquisition now moving to apply ASD**
    - **No standard DoD weapon system specific ASD methodology or training**
  - **AFMC Engineering Council tasked AFMC/EN to study ASD to define scope and types of ASD employed and associated training**
  - **AFLCMC also interviewed programs to gather ASD lessons learned and best practices**
  - **AF pursuing weapon system specific ASD education addressing:**
    - **Implementation approaches, barriers and enablers, weapon system specific ASD challenges/problems/successes, and other management considerations**

Background (con't)

- Software Data Rights Strategy
  - Data rights vital for life cycle management
  - Programs need to carefully consider appropriate Software Data Rights, especially related to sustainment, early in program's lifecycle
  - AFLCMC/EN-EZ developed a standard process for producing an Intellectual Property (IP) Strategy for Weapon System Software
  - Repeatable process that produces SW Data Rights strategy
    - Provides consistent approach for identification, justification, and documentation of the program's SW data rights; and assures persistence of the software data rights procured over program life cycle through early and continuous participation of government organic SW support agencies
  - AFLCMC has codified the SW Data Rights Strategy as a standard process

Agile Software Development (ASD) Questionnaire

Background	**Issues**

▪ ASD has existed for decades for commercial and some DoD IT and Business System applications -- commercial training is available
▪ DoD weapon system acquisition and sustainment efforts are now applying ASD, however, there is no weapon system specific ASD training available to address unique DoD ASD applications
	• ASD Training Action Item was assigned at 25 Feb 16 AFMC Engineering Council (EC) to:
	  • ID programs/efforts that are using ASD Methodologies
	  • ID ASD Training Needs & Gaps
	• Stood-up cross-Center ASD SME team: EC members assigned SMEs for their Center
	• ASD Questionnaire sent to cross-Center ASD SME team

Bottom Line

- **17 Nov 16 EC**: Received ASD Training Questionnaire responses from cross-Center ASD SME team members. HQ AFMC/ENS and AFIT/LS personnel reviewed, consolidated, and analyzed the responses. The results indicate there is a pervasive need for ASD, and especially SCRUM training. The responses helped determine ASD Training Needs/Gaps and support development of Air Force ASD Training Plan.

- Upon your request, the ASD Questionnaire can be delivered to you
  - Contact Mr. Andrew Jeselson, HQ AFMC/ENS, andrew.jeselson@us.af.mil

HQ AFMC/EN ASD Questionnaire
Samples of Data Collected

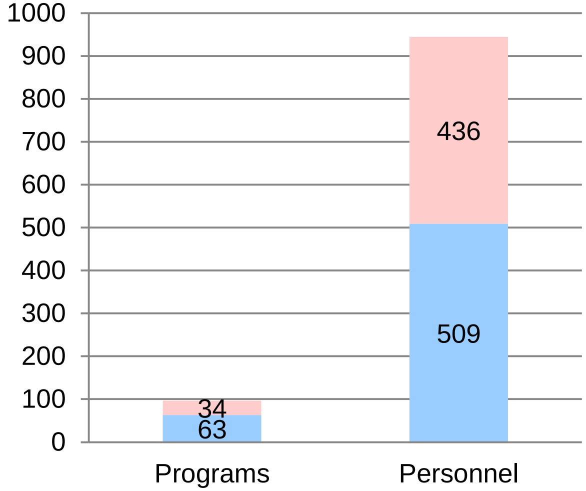
Data Collected

- Program identification data
- Type of ASD employed
- Current training expenditures
- Future training requirements

Center	Program Name	Kind of Program	Program Phase using ASD: MSA	TD	EMD	PD	OS	Type of ASD	Total # Personnel	Training Offered	Training Needed	Current Expenditures
[illegible]	JWS	Business/IT					X	Scrum	0	N	Y	
	F-22	ACWS					X	Safe	20			
	[illegible]	[illegible]					X	Scrum	?			
	B-2	ACWS					X	Cont Integration	?	Y	Y	
	CRH	Weapon System			X			Scrum	?			
	[illegible]	ACWS					[illegible]	[illegible]	[illegible]			
AFSC 76 SMXG Tinker AFB	[illegible] Mission Planning	[illegible]					[illegible]	[illegible]	[illegible]			
	B-1 Mission Planning	Development/Maintenance					X	Scrum	12	Y	N	$ 5,000
	76 SMXG Tools	Development/Maintenance					X	Scrum	21			
AFTC/[illegible]	TBA-FAAB	Business/IT application program					X	SCRUM	4			
	[illegible]	[illegible]					[illegible]	[illegible]	4			
	TBA-FMR	Business/IT application program					X	SCRUM	4	[illegible]	N	$ 13,000
	[illegible]	[illegible]					[illegible]	[illegible]	[illegible]			
	COOL	Operations [illegible] program					X	SCRUM	3			
	TBA-MRTFB	Business/IT application program					X	SCRUM	4			
AFRL/ RX	ICE – Integrated Collaborative Environment	Laboratory Program – for internal use	X					Scrum, RUP, Kanban, Extreme Programming	3	N	Y	

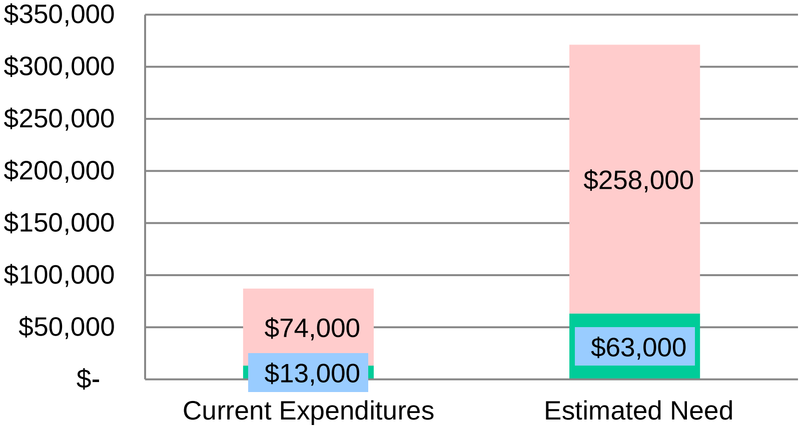
HQ AFMC/EN ASD Questionnaire Results

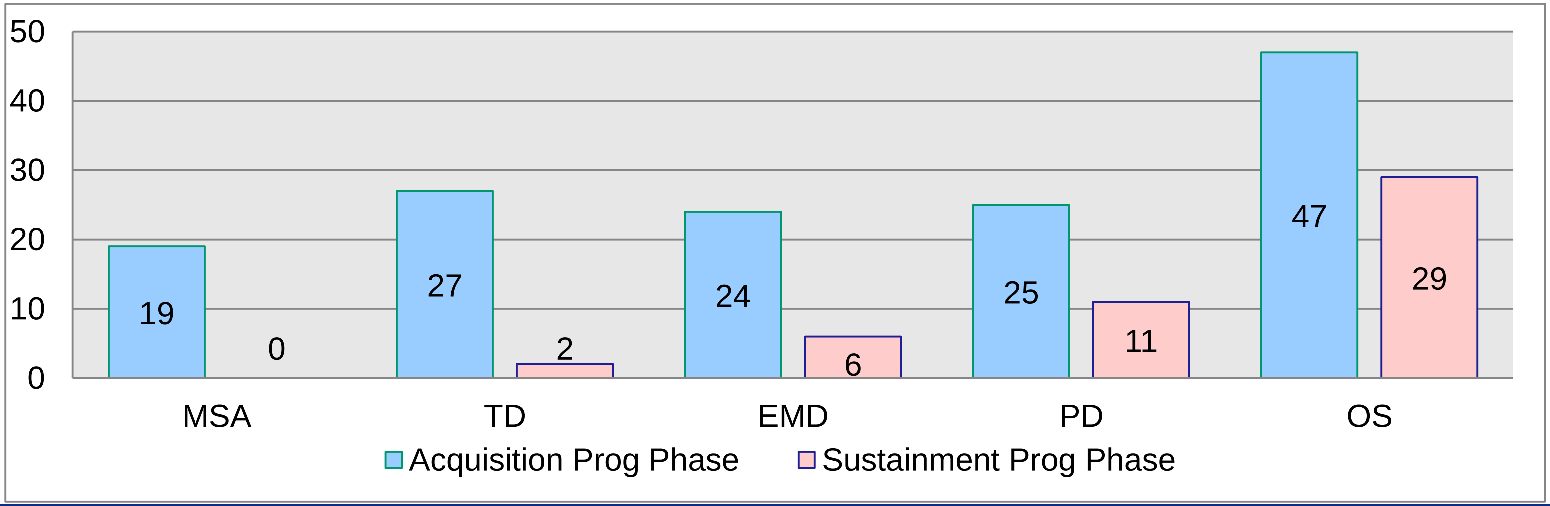
Personnel and Programs



- 97 Programs
- 900 Personnel (Est)

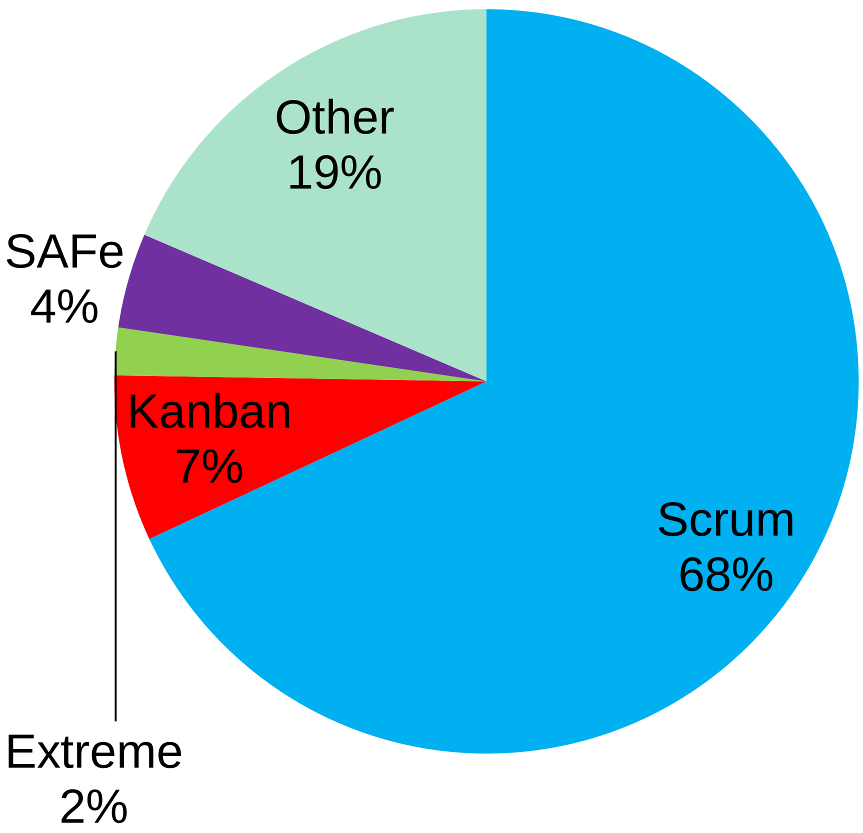
Agile Training Reported Funding





HQ AFMC/EN ASD Questionnaire Results (con't)

ASD Techniques in Use



Assessment:

- **Many Air Force organizations are pursuing their own education**
- **AFMC has a need for enterprise level agile education**
- **AFIT/LS assisted with gap analysis and ASD course development**
- **More educational gap analysis is required; however, some tailored courses are likely to be needed**
  - **SMC/EN funds a Software Engineering Institute (SEI) ASD for Government programs course for SMC ASD training**
  - **AFLCMC/EN-EZ is developing an ASD workshop**

AFLCMC/EN-EZ Agile Software Development (ASD) Workshop

Guidance For Agile Avionics SW Development

How do I apply software engineering in an ASD environment?

How do can I support the PM's needs?

How can I track development progress in terms of functionality (Value!)?

How can I handle early discovery of issue?

How should I communicate with the contractor

How can I include the customer (e.g. war fighter, flight test, operational test, etc.)

How can I track development progress in terms of SWE (e.g., moving data throughout the SW system)?

Metrics!

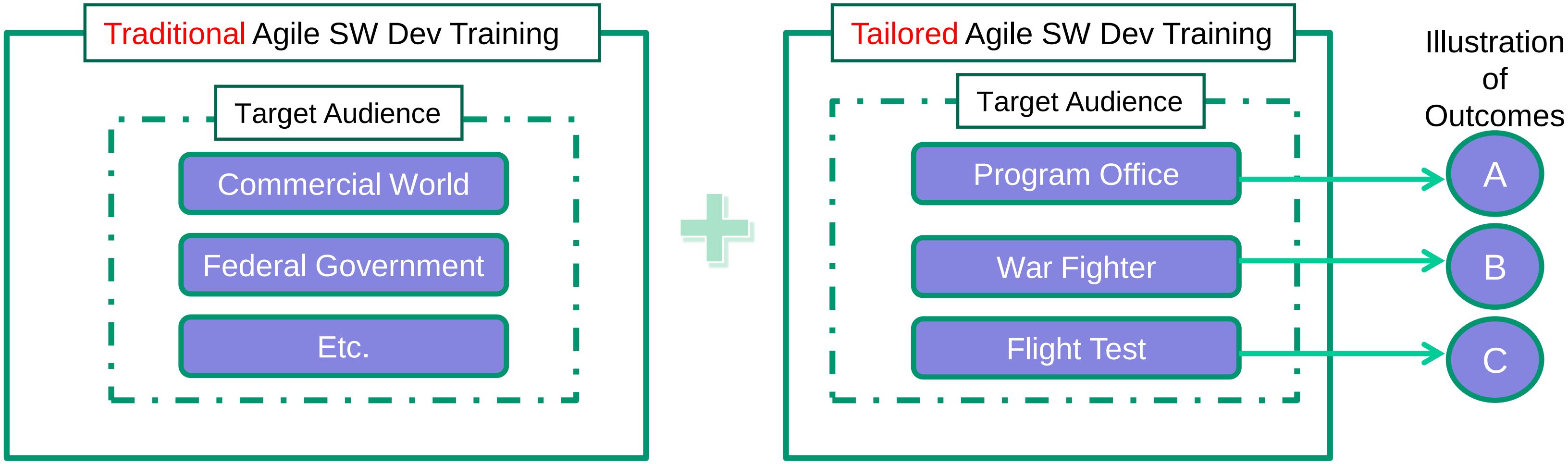
Guidance For Agile Avionics SW Development

- **Issue**
  - **Lack of guidance to help AF POs incorporate/transition agile SW procedures into the acquisition process**
    - **How to meet the intent of the of AFI 63-101**
    - **How to satisfy requirements of other processes (i.e., EVM)**
  - **Industry has pushed agile based SW development processes**
- **Goal**
  - **Establish agile aircraft systems SW development guidance & training focused on needs of the PO personnel**
  - **Establish best practices**
  - **Guidance on technical reviews**
  - **Understanding elements that impact cost, schedule, & performance**
  - **Etc.**

Agile Avionics SW Development

- Status
  - Commenced active participation in the Software Engineering Institute Agile Collaboration
  - Active membership in the NDIA Agile Working Group
  - Continuous involvement in the F-22 implementation of Scaled Agile Framework
  - Working with AFMC/ENS, SEI, and AFIT to establish training focused on the needs of the personnel in the imbedded avionics systems programs
    - Material based on best practices and lessons learned from participation in the above working groups and observations from F-22, B-2, F-15, and other programs
    - Including updated materiel in existing focus week training

Develop Training Tailored for DoD Aircraft Programs



A

- Illustration of agile tents aligned with DoD System Engineering
- Sample metrics to track SW development progress
- Approach to satisfy earned value management requirements
- Subset of documents generated for government accountability
- Early sustainment posture
- Etc.

B

—Expected role, availability . . .

—Etc.

C

—Examples of impacts to flight testing

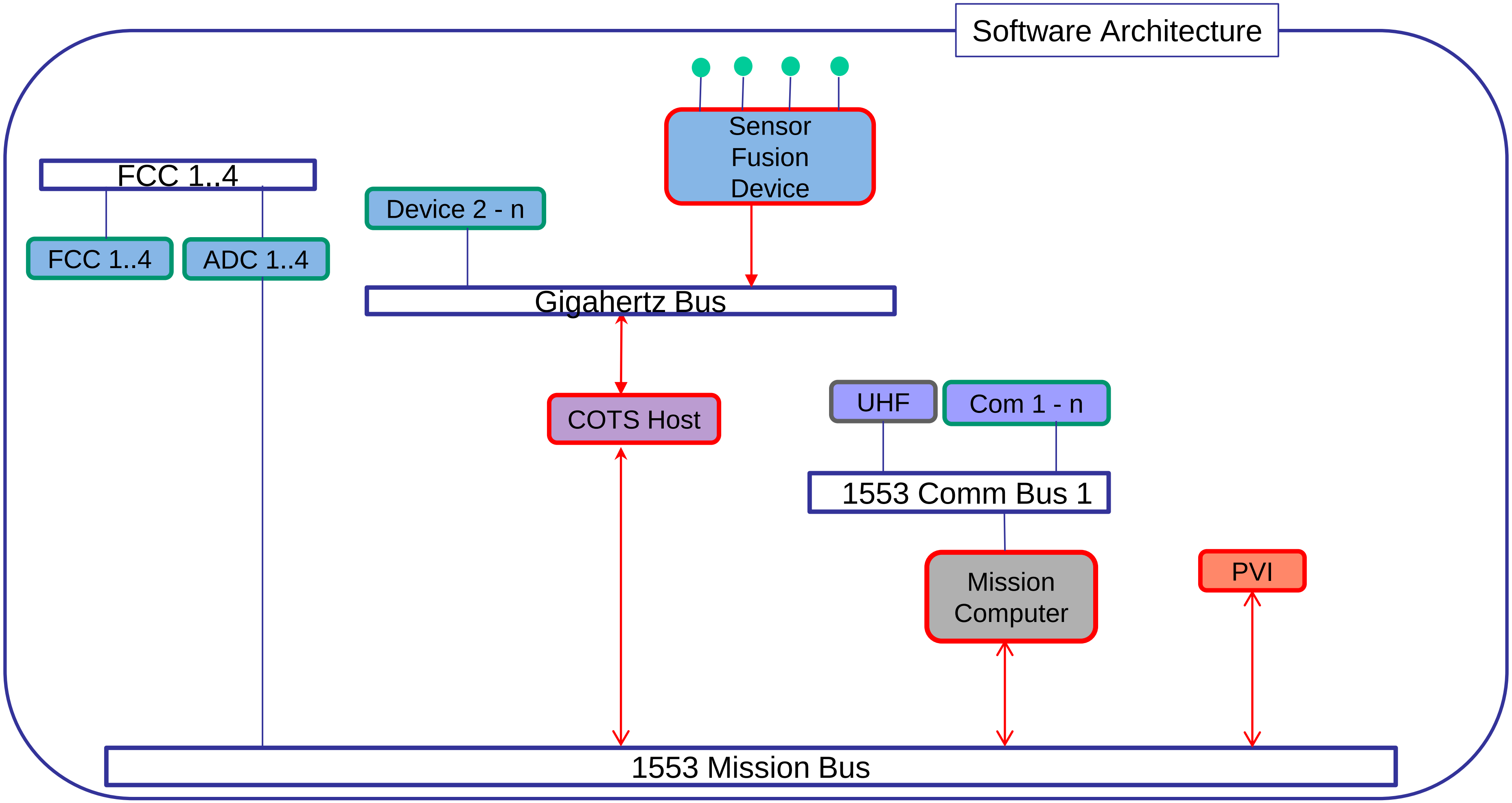
—Etc.

AFLCMC/EN-EZ SW Data Rights Strategy Process

Improve Acquisition of SW Data Rights

- **Issue**
  - **Non-availability of program SW data rights for sustainment – assertion supported by:**
    - **2011 AF Studies Board & Scientific Advisory Board reports**
    - **Table top discussions with 10 plus AFLCMC programs**
      - **No analysis executed to ID appropriate SW data rights**
- **Goal**
  - **Develop standard engineering analysis framework designed to ID, acquire, document, & retain appropriate SW data rights**
    - **Framework to include provisions for timely acquisition of government subject matter expertise congruent with utilization of acquired SW data rights**
    - **Cross organizational involvement (LCMC & AFSC) critical**
    - **Framework tenets included as part of core competency**

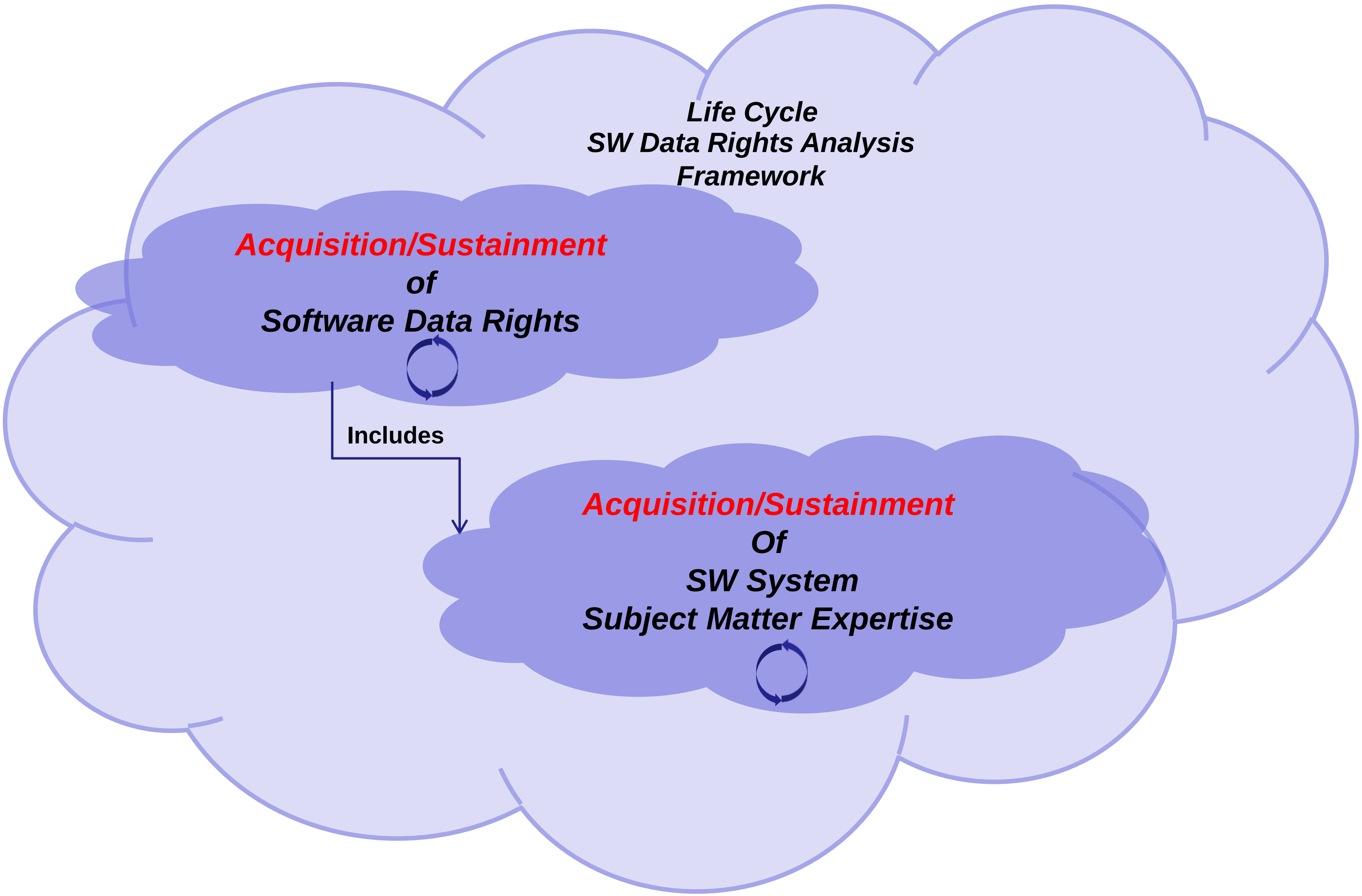
SW Data Rights Analysis Example: Isolate Mission Thread



DISTRIBUTION A. Approved for public release, distribution unlimited. (HQ AFMC-2017-0024)

SW Data Rights Analysis Example: Analyze Thread Elements

LRU/ICD	Sensor → Sensor Fusion Device	ICD	COTS Host	ICD	Mission Computer	ICD	PVI
Expected Change Rate	Low	Low	Low	Low	High	Mod	High
Gov't **Development** Funded	0%	100%	0%	100%	100%	100%	100%
SW Type	Complex Algorithm	N/A	COTS SW	N/A	OFP	N/A	OFP
…							
Expected Rights	Restricted	Unlimited	COTS SW	Unlimited	Unlimited	Unlimited	Unlimited
Needed Rights	TBD	GPR	COTS SW	GPR	GPR	GPR	GPR
Current Rights	Restricted	GPR	COTS SW	GPR	GPR	GPR	GPR
Comments	Needed rights pending analysis of winning bid	See fusion device			Organic Support	Organic Support	Organic Support


Life Cycle
SW Data Rights Analysis
Framework
Acquisition/Sustainment
of
Software Data Rights
Includes
Acquisition/Sustainment
Of
SW System
Subject Matter Expertise

Training

- Focus Week course
- Course material developed via SEI
- AFIT course in works

Questions?

Dr. Marc Shaver
HQ AFMC/ENS
(937) 257-5621
marc.shaver.4@us.af.mil

Mr. Andrew Jeselson
HQ AFMC/ENS
(937) 257-6460
andrew.jeselson@us.af.mil

Mr. Curtis Jefferson
AFLCMC/EZAS
(937) 656-4879
curtis.jefferson@us.af.mil

Helix: Understanding Systems Engineering Effectiveness through Modeling

Sponsor: DASD(SE)

By
Ms. Megan M. CLIFFORD and
Dr. Nicole HUTCHISON

25 October 2017
NDIA 20TH ANNUAL SYSTEMS ENGINEERING CONFERENCE
Washington, DC 20009

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. The SERC is a federally funded University Affiliated Research Center (UARC) managed by Stevens Institute of Technology consisting of a collaborative network of 22 universities. More information is available at www.SERCuarc.org

www.sercuarc.org

Background on Helix Research

- Helix is a multi-year longitudinal study building an understanding of the systems engineering workforce in the DoD, the Defense Industrial Base (DIB), and other sectors that perform systems engineering.
- From 2012-2016, Helix focused on three main research questions:
    1. What are the characteristics of systems engineers?
    2. How effective are those who perform SE activities and why?
    3. What are employers doing to improve the effectiveness of systems engineers?
- Most data collection has been through face-to-face, semi-structured interviews with systems engineers
- Reporting is done in an aggregated anonymous manner that does not reveal the identities of participating individuals or organizations

Helix Progress

- Research Methodology is based on a Grounded Theory approach
  - Initially open-ended, exploratory interviews intended to provide a broad variety of data
  - Analysis focused on identifying key patterns and themes
  - Further interviews explored the patterns identified
  - Analysis of career paths to understand the development of Systems Engineers
- **Main product of Helix is the first phase of *Atlas* – The Theory of Effective Systems Engineers**
  - Version 1.0 released December 2016

Helix Dataset

Participant Organizations

22

* 11 DoD/DIB

335

Participants Interviewed

Practicing Systems Engineers

92%

8%

Systems Engineers Peers

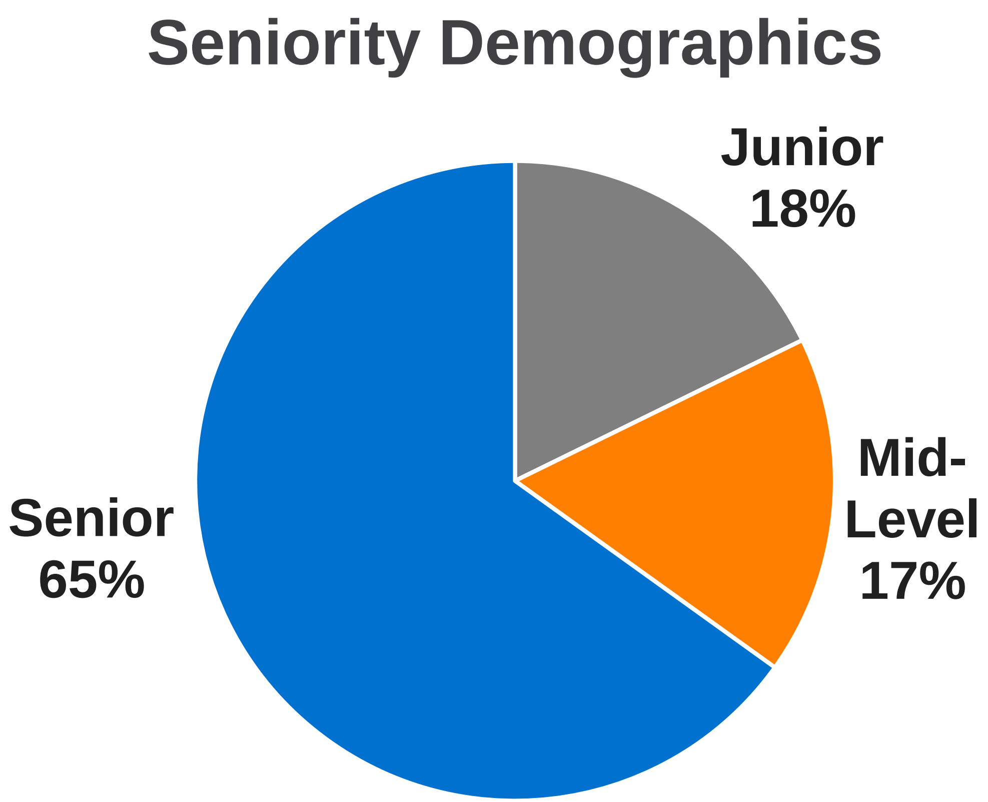
Pages of Transcripts

6000

270

Hours of Audio

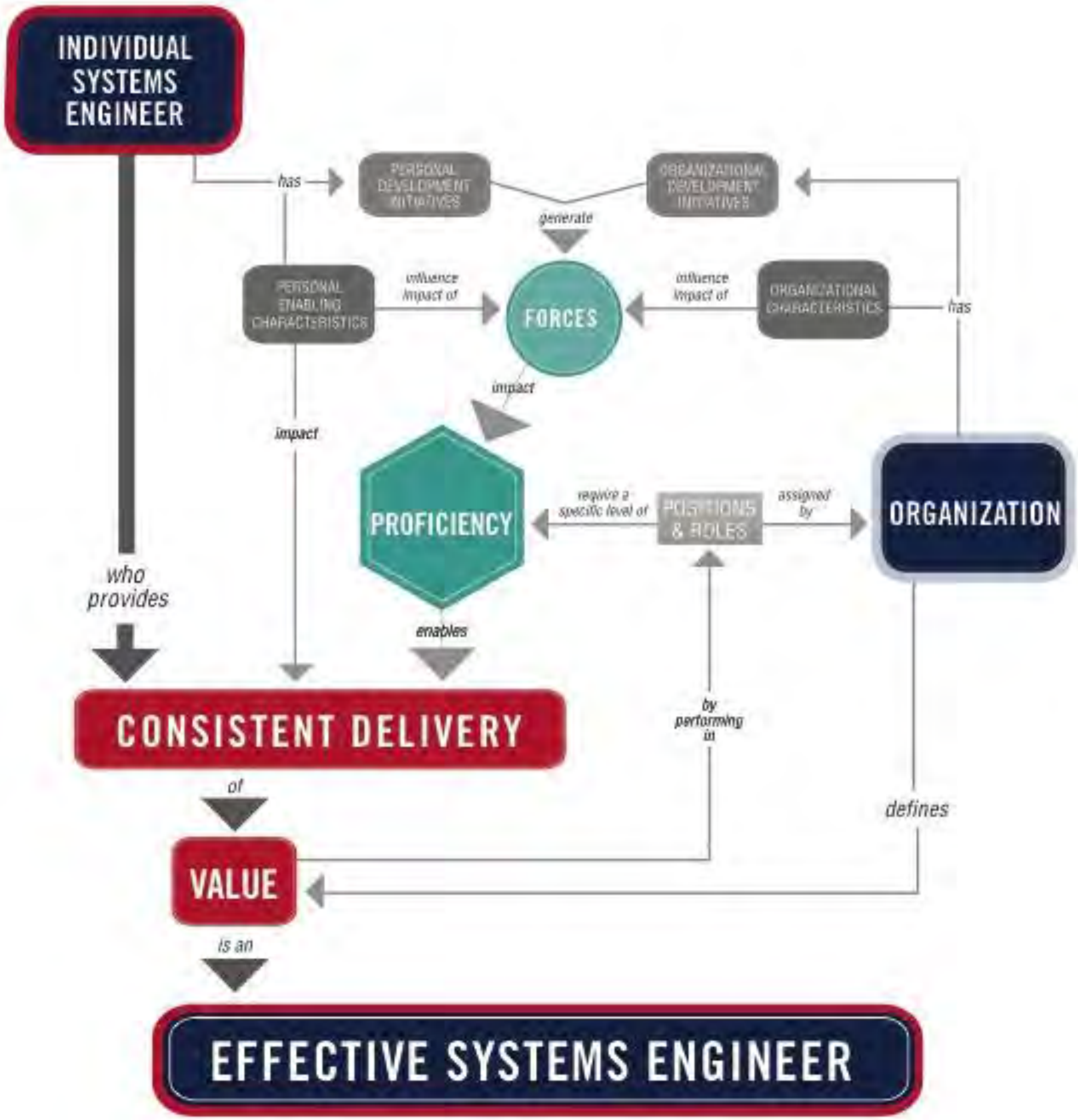
Seniority of Systems Engineers
Helix data



Why do we care about seniority?

It allows us to:

- Compare across individuals and groups at different parts of their careers
- Highlight differences in the way that senior systems engineers have developed and how junior and mid-level systems engineers are developing



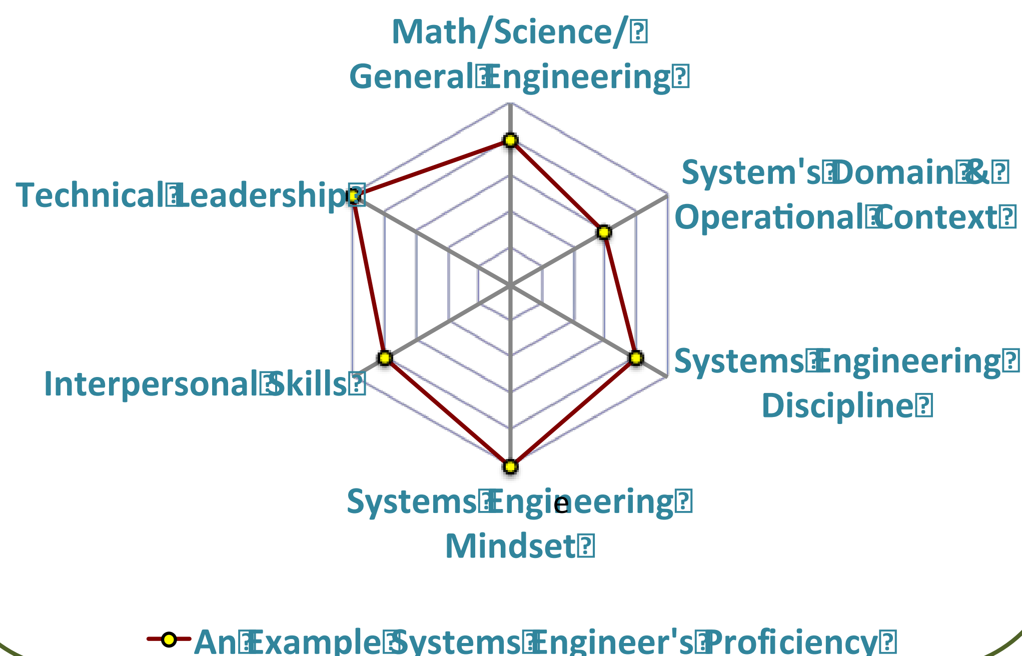
INDIVIDUAL SYSTEMS ENGINEER
has
PERSONAL DEVELOPMENT INITIATIVES
ORGANIZATIONAL DEVELOPMENT INITIATIVES
generate
PERSONAL ENABLING CHARACTERISTICS
influence impact of
FORCES
influence impact of
ORGANIZATIONAL CHARACTERISTICS
has
impact
impact
PROFICIENCY
require a specific level of
POSITIONS & ROLES
assigned by
ORGANIZATION
who provides
enables
CONSISTENT DELIVERY
by performing in
of
defines
VALUE
is an
EFFECTIVE SYSTEMS ENGINEER

Proficiencies, Forces, Characteristics

Forces that Impact Level of Proficiency
(may be generated by Personal and Organizational Development Initiatives)

Experiences	Mentoring	Education & Training

Proficiency of a Systems Engineer



Personal Enabling Characteristics
Self-Awareness
Ambition & Internal Motivation
Inquisitiveness
Lifelong Learning
Confidence, Persistence, & Focus
Professionalism & Respect
Creativity

Organizational Characteristics
Culture
Structure
Values
Appreciation of SE
Org. Definition of SE & Systems Engineer
Rewards & Recognitions
Career Growth Potential

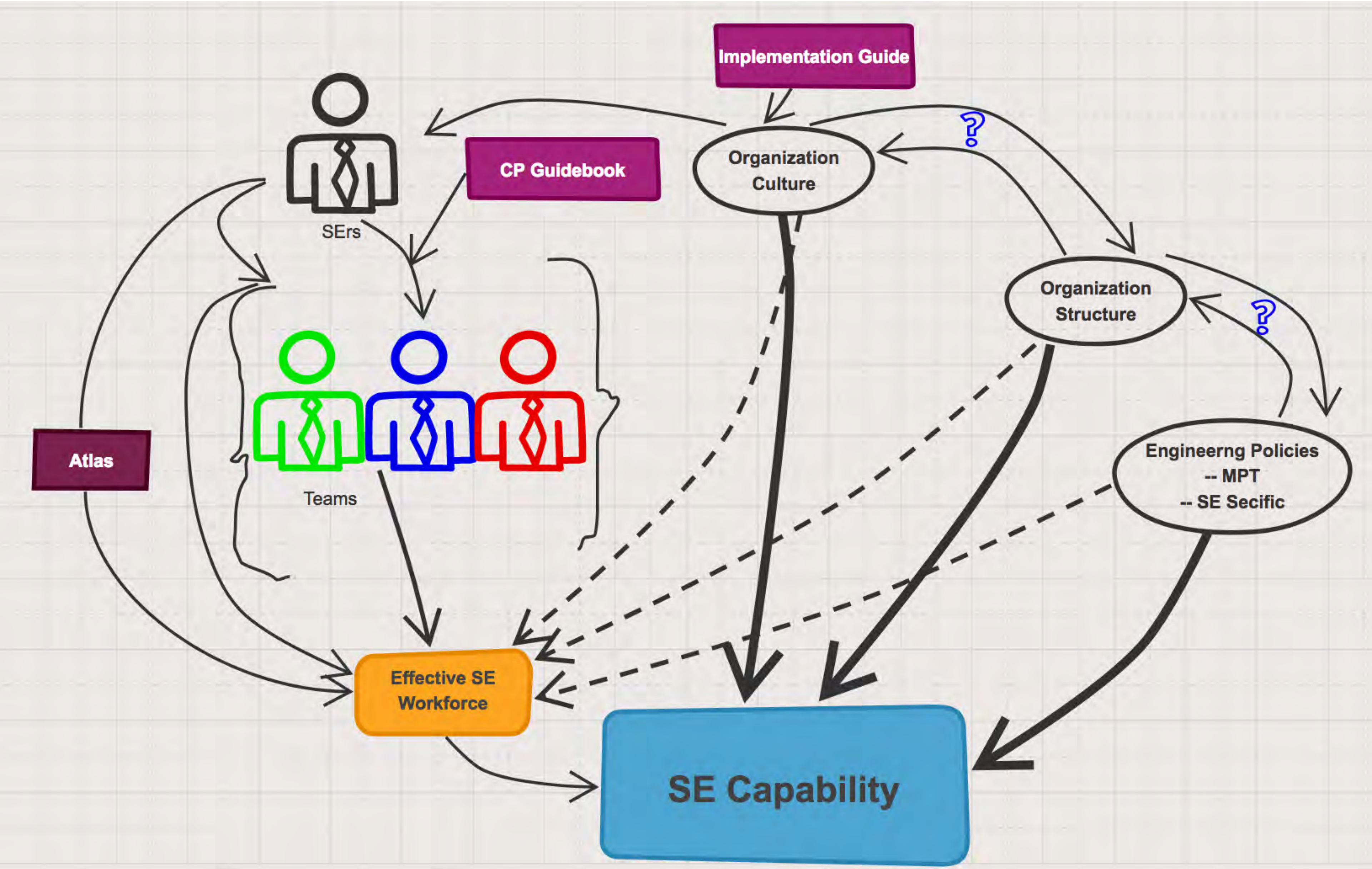
Current State of Helix

- How can organizations improve the effectiveness of their systems engineering workforce?
  - —Carried over from the previous work, and though we answered this slightly, it was not to depth that we wanted to, so continuing to pursue.
- How does the effectiveness of the systems engineering workforce impact the overall systems engineering capability of an organization?
- What critical factors, in additional to workforce effectiveness, are required to enable systems engineering capability?

Why Model Helix?

- Qualitative analysis tool
  - Further establish patterns and relationships
- Understand behaviors that general qualitative analysis does not provide
  - Assess effects of individuals and collective entities on system as a whole
- Predictive tool moving forward
  - Useful for exploratory purposes.

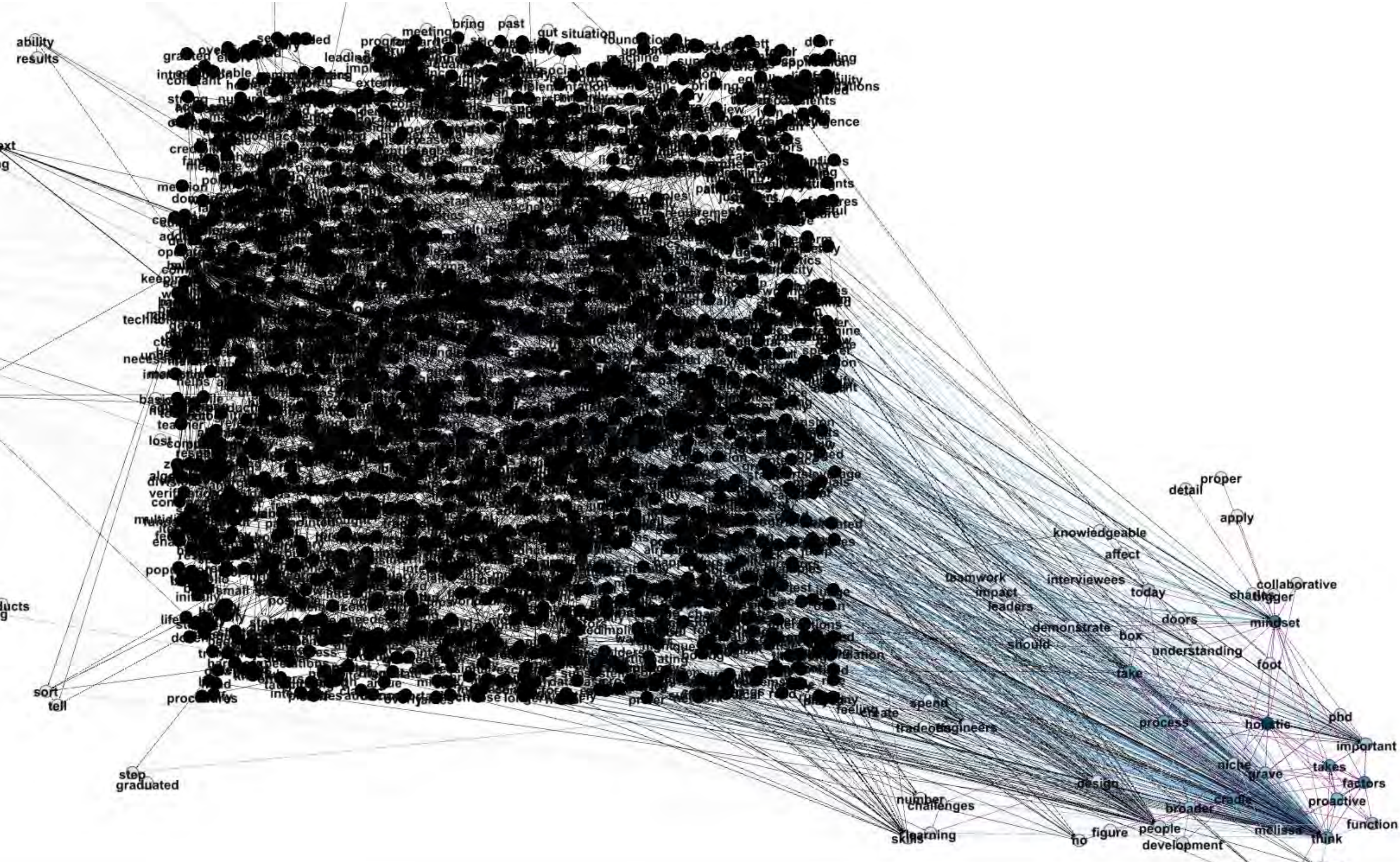
Overview Sketch



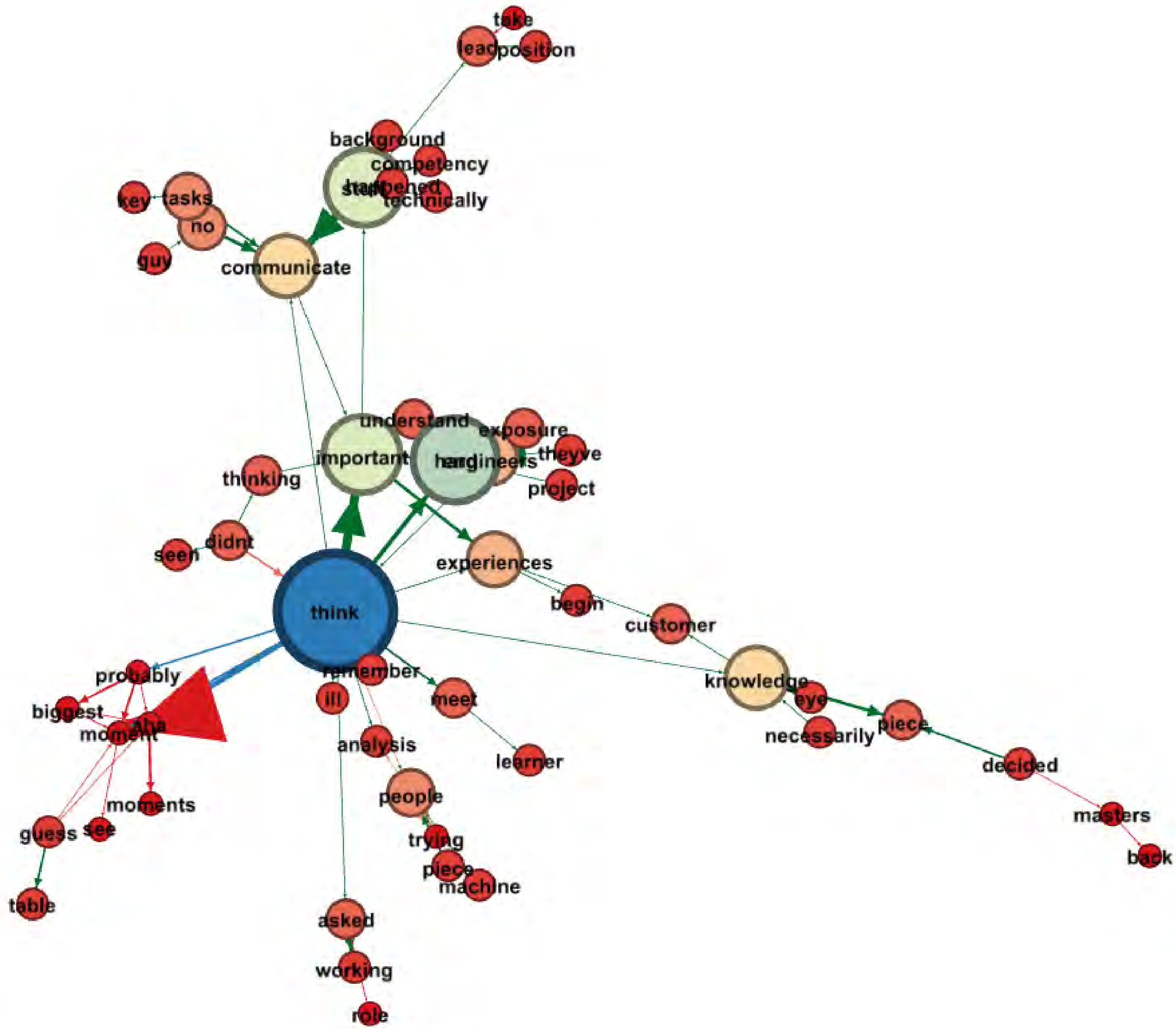
Modeling Helix

- Cluster Analysis, Syntagmatic and Paradigmatic
  - Deeper dive into the established proficiencies, forces, and characteristics (both personal and organizational) through cluster analysis, which will help further develop models.
    - Done within the 2017 work
- Modeling Career Path (Individual)
  - Utilize the grounded theory approach to then introduce the dynamism of numerous, both exogenous and endogenous, factors into an individual's career path and how they might best utilize their skill set, environment, and time to enhance their career path.
    - Partially completed with 2017 work
- Multilevel Model and Simulation (Organization)
  - Utilize the grounded theory approach to then introduce the dynamism of numerous criterion for an organization to enhance decision making to implement programs on growing and developing their systems engineering workforce and improve their overall systems perspective through the analysis.
    - Future work
- *Ontology*
  - *With over 6,000 pages of transcript, the team can engage in forming a higher level ontology for the community to have a streamlined discussion where little personal interpretation can be granted, therefore removing some human error.*

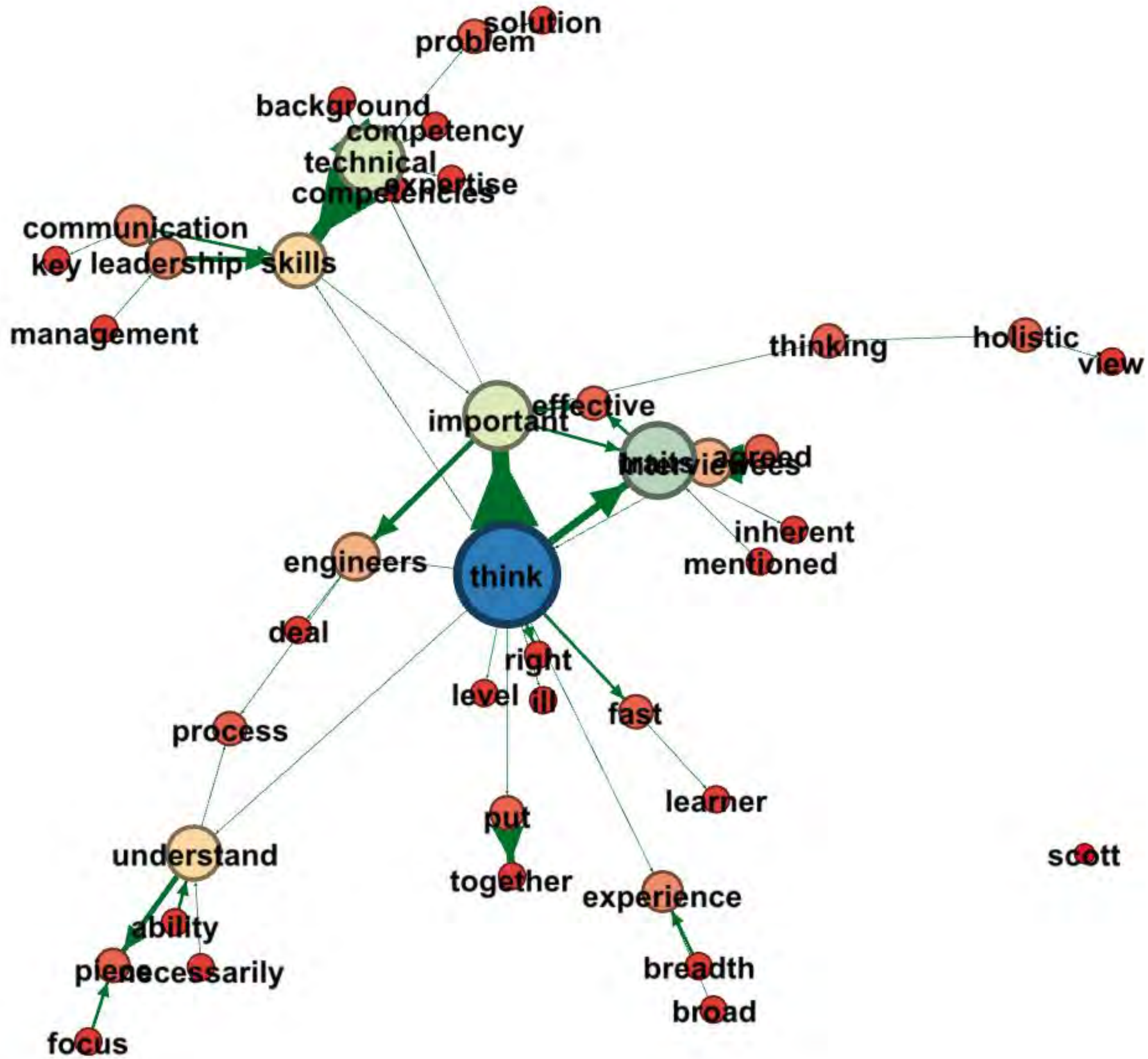
Cluster Analysis HELIX



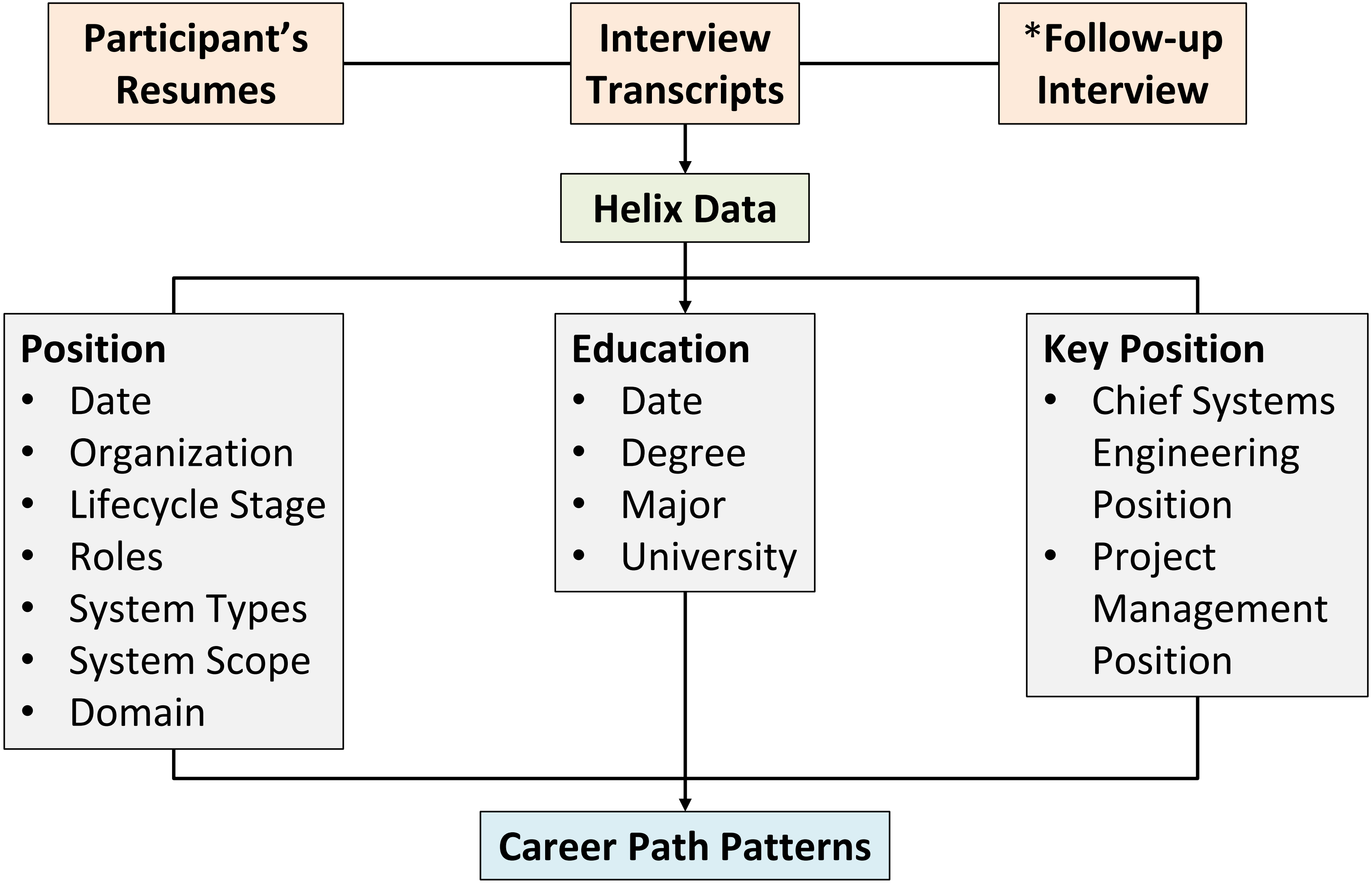
Cluster Analysis



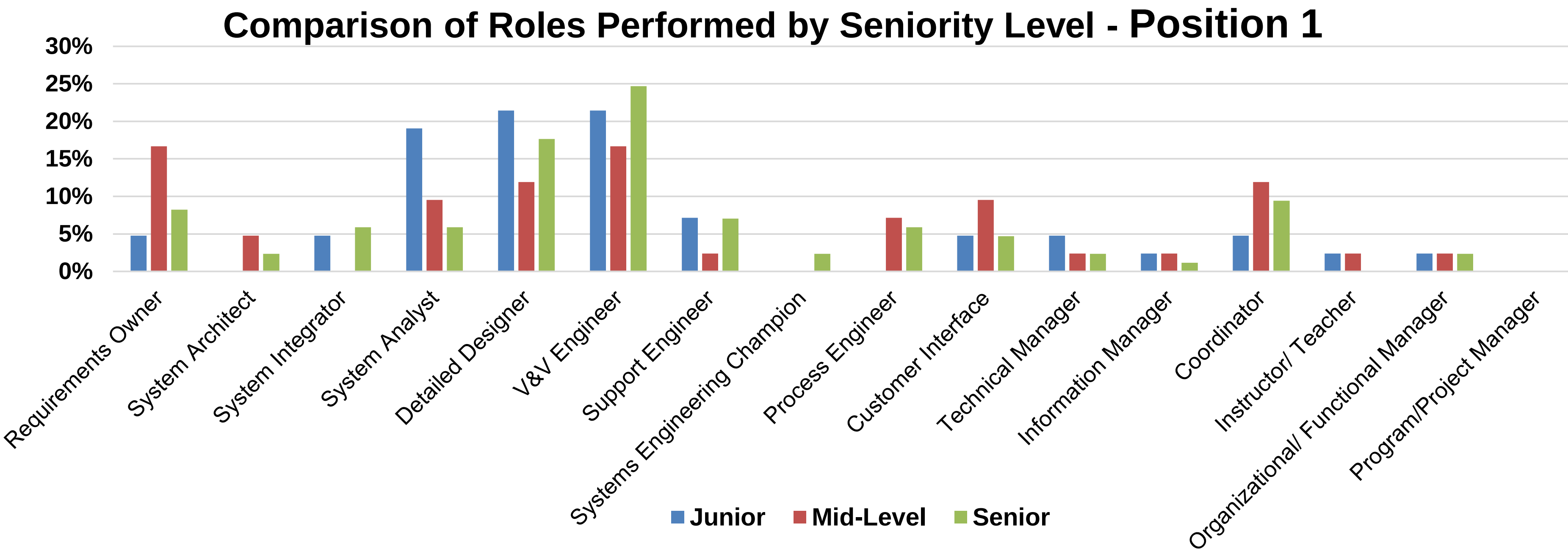
Cluster Analysis



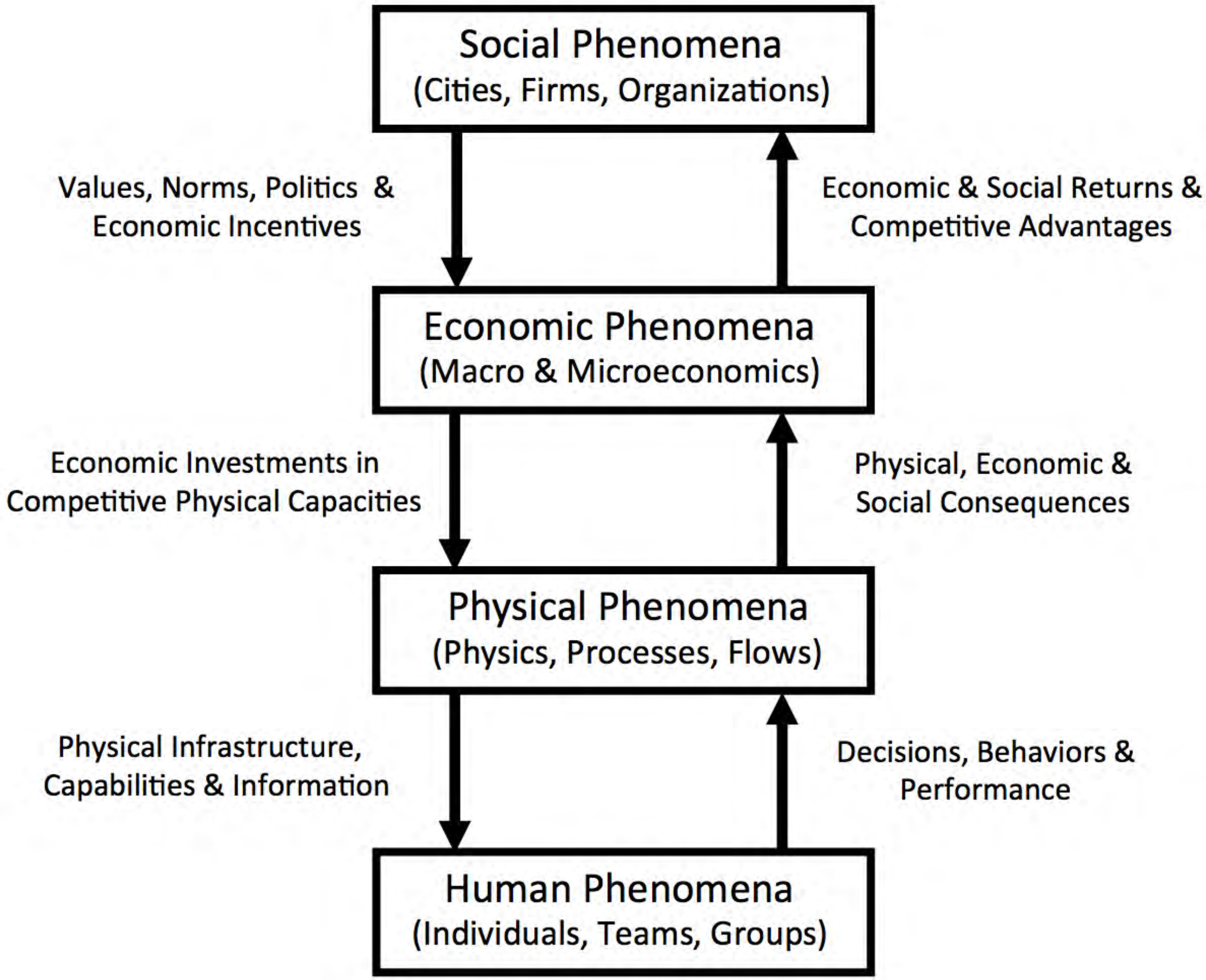
Methodology of Career Path Analysis



Modeling Effective Systems Engineers



Methodology for Multilevel Model (Framework) of Organization



Rouse, W.B., "Human interaction with policy flight simulators" In Applied Ergonomics, Issue 45, pp. 77-77, 2014

Constructing the Multilevel Model

- Step 1: Decide on the Central Questions of Interest
  - Organization's culture – need to understand impact on effective SE better than we do.
- Step 2: Define Key Phenomena Underlying These Questions
  - Policies and organizational structure, task behaviors and performance
- Step 3: Develop One or More Visualizations of Relationships Among Phenomena
  - Structures and roles affect employees movement within organization
- Step 4: Determine Key Tradeoffs That Appear to Warrant Deeper Exploration
- Step 5: Identify Alternative Representations of These Phenomena
- Step 6: Assess the Ability to Connect Alternative Representations
- Step 7: Determine a Consistent Set of Assumptions
- Step 8: Identify Data Sets to Support Parameterization
- Step 9: Program and Verify Computational Instantiations
- Step 10: Validate Model Predictions, at Least Against Baseline Data

Expected Outcomes

- In January, the Helix team will
  - Update Atlas (1.1)
  - Implementation Guide
  - Career Path Guidebook
- Included, the team will have set

Software Systems Maturity Analysis

Abstract ID: #19758

For:
NDIA
20^{th} Annual Systems Engineering Conference
23-26 October 2017

Prepared by:
Idaho National Laboratory (INL)
Christopher A. Dieckmann, ESEP
Systems Engineering Lead for National and Homeland Security Projects

Idaho National Laboratory

INL Systems Analyses & Engineering Contacts

Mitchell Kerman
Division Director
(208) 526-3631
mitchell.kerman@inl.gov

Ron Klingler
Department Manager
(208) 526-0183
ron.klingler@inl.gov

NDIA Presenter

Chris Dieckmann
Group Lead for
National & Homeland
Security Projects
(208) 526-5986
chris.dieckmann@inl.gov

John Collins
Group Lead for
Energy & Environment
Projects
(208) 526-3372
john.collins@inl.gov

Jody Henley
Group Lead for
Nuclear Projects
(208) 526-1979
jody.henley@inl.gov

Shyam Nair
Group Lead for
Process & Data Sciences
(208) 526-3071
shyam.nair@inl.gov

INL Systems Analyses &
Engineering Web Page
https://systemsengineering.inl.gov

INL/CON-17-42211

Core Functions – INL Systems Analyses & Engineering

1

- Concise Problem Definition
- Understanding Important Customer Needs
- Concise System/Project Boundaries
- Strategic Planning & Baselines
- "Concept" of Operations
- Stakeholder Buy-in
- Acquisition Strategy
- White Papers

2

- Technical, Functional, and Operational Analysis
- Requirements Elicitation, Clarification, Derivation, and Tracking
- Traceability, Change Control, and Impact Analysis
- Requirements Verification and Validation Planning

3

- Analysis of Alternatives
- Decision Metrics
- Organization Analysis & Visualization of Complex and Big Data
- Uncertainty Analysis & Probabilistic Risk Assessment
- Risk-informed Decision-making
- Integration of Viable Solutions
- Chemical Process Engineering & Analysis
- Chemical Process Control
- Computational Fluid Dynamics

4

- Risk Identification and Tracking
- Justification for Funding Contingency
- Risk Handling Strategy
- Risk Reduction Plan
- Risk-informed Path Forward

5

- Technology Maturity Analysis
- Technology Development Roadmap/Path Forward
- Roadblock Identification & Mitigation
- System Assessments (e.g., Energy Systems)

6

- Program & Project Integration
- Laboratory-wide R&D Integration
- Laboratories/Industries/ Universities Integration
- Integration of System Elements
- Systems of Systems Analyses

7

- Verification of System Performance and Functionality
- Validation of System Specification and Design Parameters
- Test Planning and Implementation

Software Systems Maturity Analysis Approach

- Customer Required Measurement of Tools / Capabilities
- ~ 10 Participating Companies Providing Tools / Capabilities
- Technology Readiness Levels (TRLs)
  - Accept criticism from participants
- Software Readiness Levels (SRLs)
  - Accept criticism from participants
- Maturity Gates (MGs)
  - Based on tailored version of generic TRL and SRL language
  - Criteria specific to products and platforms
  - Vetted with participants & gained acceptance
- Initial Rating of All Tools / Capabilities
  - Feedback discussed with participants
  - Goals outlined and road mapped for each participant

Maturity Gate Philosophy

Element / MG	Demonstration	Environment	Risks	SSCs (systems, subsystems and components)
MG1	Idea	None		Component
MG2	Theory	Correlational & mathematical	Good correlation of performance defined	Component
MG3	Performance Of Theory	Virtual simulated	Performance validates theory	Component
MG4	Performance of components in simulated system environment	Simulated operational environment, increased scale of operations	Performance is achievable within expected environment	Subsystem (component + environment)
MG5	Performance of subsystems working at same time	All parts of system running simultaneously but not yet integrated in simulated environment	Performance of system components can work at the same time without issues	Subsystem (multiple components + environment)
MG6	Performance of integrated system working together	Parts integrated in simulated environment working together	Performance of integrated system meets ops needs in simulated environment	System (integrated components + environment)
MG7	Performance of operational staff doing simulated tasks	Operationally simulated environment and missions, live streaming of data	Performance of integrated system by actual operators (non-developers) in simulated environment meets needs	System (system + operators + simulated mission)
MG8	Performance by operational staff doing actual tasks	Actual deployed system environment and missions	Applicable to actual systems and operators and tasking	System plus operators plus actual mission

INL/CON-17-42211

Idaho National Laboratory

Example Genericized MG Criteria

	Maturity Gate 2
MG2 Risks to Mitigate	
	Data to detect threat is not available
	Algorithms/analytics poor at detection/false alarm ratio
MG2 Exit Criteria	
	Identification of competing designs that have potential to detect threat
	Performance evaluation of competing designs to detect threat
	Data features that represent threat activity are defined
	Maturity Gate 3
MG3 Risks to Mitigate	
	Access to required data is not provided for testing
	Access to military network with appropriate sensor is not allowed as needed
	Data interfaces & needs for analytics to run on platform are not clearly defined
	Delay in platform documentation may impact development of ingest modules
	No interesting data available to exchange for cross-systems communications
	Different versions of platform software on remote VMs and central test system
MG3 Exit Criteria	
	Analytic/tool operate on the platform operating system at each participant facility
	Appropriate data sets delivered to support remote development
	Trial performance test in prototypical environment of selected design(s)

	Maturity Gate 4
MG4 Risks to Mitigate	
	Access to required data is not provided for testing
	Data interfaces & needs for analytics to run on platform are not clearly defined
	Delay in platform documentation may impact development of ingest modules
	Incompatibility of ingest language with analytic may lead to analytic failure
	May not operate at scale (cannot process data at scale)
MG4 Exit Criteria	
	Demonstration of analytic using representative data
	Demonstration of analytic using 30 days of captured data
	Issues defined in MG3 corrected and confirmed
	Strategy, requirements, architecture and design report for operations plan
	Test Plan defined functional performance demonstrated

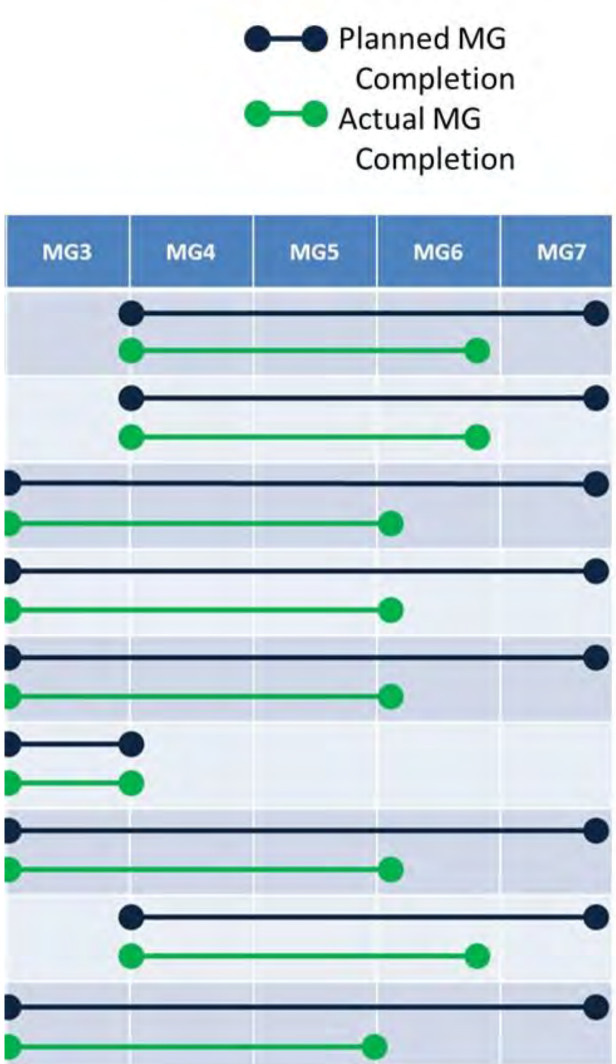
Maturity Gate Mapping

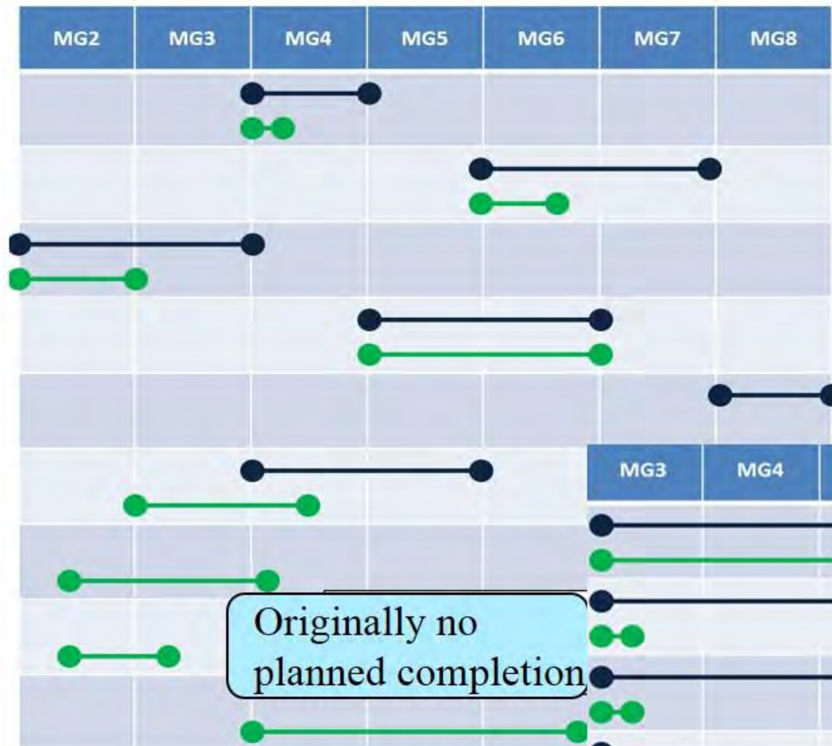
LEGEND:

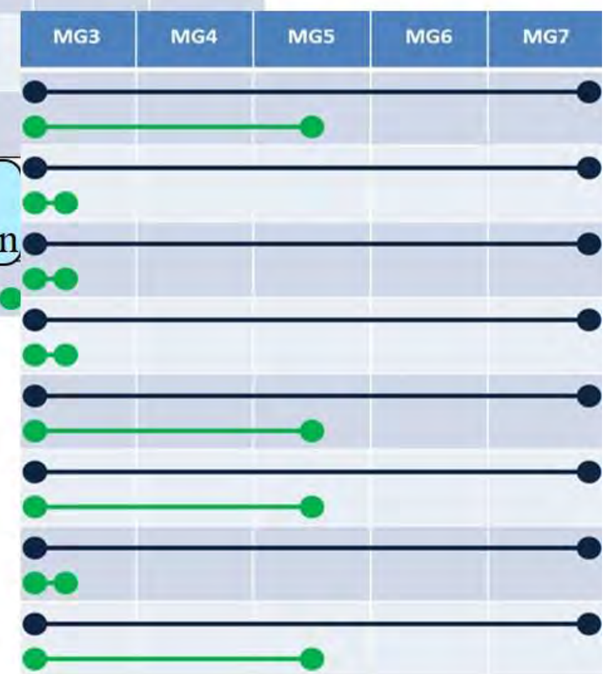
- RV = Resolved — Greater than 66% complete
- PR = Partially Resolved — Between 33% and 66% complete
- UR = Unresolved — Less than 33% complete
- NA = Not Applicable
- NI = Not an Issue

	Ktr1	Ktr1	Ktr2	Ktr2	Ktr3	Ktr4	Ktr4	Ktr5	Ktr5	Ktr6	Ktr7	Ktr7	Ktr7	Ktr7	Ktr7	Ktr8	Ktr8	Ktr9	Ktr10	Ktr10	Ktr10	Ktr10	Ktr10	Ktr10	Ktr10	Ktr10
	Tool / Capability 1	Tool / Capability 2	Tool / Capability 3	Tool / Capability 4	Tool / Capability 5	Tool / Capability 6	Tool / Capability 7	Tool / Capability 8	Tool / Capability 9	Tool / Capability 10	Tool / Capability 11	Tool / Capability 12	Tool / Capability 13	Tool / Capability 14	Tool / Capability 15	Tool / Capability 16	Tool / Capability 17	Tool / Capability 18	Tool / Capability 19	Tool / Capability 20	Tool / Capability 21	Tool / Capability 22	Tool / Capability 23	Tool / Capability 24	Tool / Capability 25	Tool / Capability 26
Maturity Gate 2	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**100%**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**
MG2 Risks to Mitigate	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	100%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
MG2 Exit Criteria	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	100%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
MG2-->MG3 Entrance Criteria	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Maturity Gate 3	**NA**	**NA**	**100%**	**100%**	**100%**	**NA**	**NA**	**100%**	**100%**	**NA**	**0%**	**NA**	**NA**	**80%**	**100%**	**100%**	**33%**	**NA**	**100%**	**29%**	**29%**	**100%**	**100%**	**100%**	**29%**	**29%**
MG3 Risks to Mitigate	NA	NA	100%	100%	100%	NA	NA	100%	100%	NA	NA	NA	NA	75%	100%	100%	100%	NA	100%	0%	0%	100%	100%	100%	0%	0%
MG3 Exit Criteria	NA	NA	100%	100%	100%	NA	NA	100%	100%	NA	0%	NA	NA	100%	100%	100%	0%	NA	100%	0%	0%	100%	100%	100%	0%	0%
MG3-->MG4 Entrance Criteria	NA	NA	100%	100%	100%	NA	NA	NA	100%	NA	0%	NA	NA	75%	100%	100%	0%	NA	100%	50%	50%	100%	100%	100%	50%	50%
Maturity Gate 4	**100%**	**100%**	**88%**	**88%**	**100%**	**0%**	**NA**	**NA**	**100%**	**100%**	**NA**	**NA**	**NA**	**50%**	**100%**	**0%**	**NA**	**100%**	**81%**	**0%**	**0%**	**81%**	**81%**	**81%**	**0%**	**0%**
MG4 Risks to Mitigate	100%	100%	50%	50%	100%	0%	NA	NA	100%	100%	NA	NA	NA	NA	100%	0%	NA	100%	100%	0%	0%	100%	100%	100%	0%	0%
MG4 Exit Criteria	100%	100%	100%	100%	100%	0%	NA	NA	100%	100%	NA	NA	NA	100%	100%	NA	NA	100%	100%	0%	0%	100%	100%	100%	0%	0%
MG4-->MG5 Entrance Criteria	100%	100%	100%	100%	100%	0%	NA	NA	100%	100%	NA	NA	NA	0%	100%	0%	NA	100%	63%	0%	0%	63%	63%	63%	0%	0%
Maturity Gate 5	**100%**	**100%**	**100%**	**100%**	**100%**	**NA**	**NA**	**NA**	**100%**	**100%**	**NA**	**100%**	**NA**	**0%**	**100%**	**NA**	**NA**	**100%**	**50%**	**0%**	**0%**	**50%**	**50%**	**50%**	**0%**	**0%**
MG5 Risks to Mitigate	100%	100%	100%	100%	100%	NA	NA	NA	100%	100%	NA	100%	NA	0%	100%	NA	NA	100%	100%	0%	0%	100%	100%	100%	0%	0%
MG5 Exit Criteria	100%	100%	100%	100%	100%	NA	NA	NA	100%	100%	NA	100%	NA	0%	100%	NA	NA	100%	50%	0%	0%	50%	50%	50%	0%	0%
MG5-->MG6 Entrance Criteria	100%	100%	100%	100%	100%	NA	NA	NA	100%	100%	NA	100%	NA	NA	100%	NA	NA	NA	40%	0%	0%	40%	40%	40%	0%	0%
Maturity Gate 6	**79%**	**79%**	**17%**	**17%**	**17%**	**NA**	**29%**	**NA**	**17%**	**71%**	**NA**	**100%**	**NA**	**NA**	**0%**	**NA**	**NA**	**67%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**
MG6 Risks to Mitigate	100%	100%	0%	0%	0%	NA	100%	NA	0%	100%	NA	100%	NA	NA	0%	NA	NA	100%	0%	0%	0%	0%	0%	0%	0%	0%
MG6 Exit Criteria	100%	100%	17%	17%	33%	NA	50%	NA	33%	75%	NA	100%	NA	NA	0%	NA	NA	NA	0%	0%	0%	0%	0%	0%	0%	0%
MG6-->MG7 Entrance Criteria	63%	63%	25%	25%	0%	NA	0%	NA	0%	50%	NA	NA	NA	NA	0%	NA	NA	50%	0%	0%	0%	0%	0%	0%	0%	0%
Maturity Gate 7	**13%**	**13%**	**14%**	**14%**	**14%**	**NA**	**0%**	**NA**	**14%**	**14%**	**NA**	**NA**	**NA**	**NA**	**14%**	**NA**	**NA**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**
MG7 Risks to Mitigate	0%	0%	NA	NA	NA	NA	0%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0%	NA	NA	NA	NA	NA	NA	NA	NA
MG7 Exit Criteria	13%	13%	13%	13%	13%	NA	0%	NA	13%	13%	NA	NA	NA	NA	13%	NA	NA	0%	0%	0%	0%	0%	0%	0%	0%	0%
MG7-->MG8 Entrance Criteria	0%	0%	0%	0%	0%	NA	NA	NA	0%	0%	NA	NA	NA	NA	0%	NA	NA	NA	0%	0%	0%	0%	0%	0%	0%	0%
Maturity Gate 8	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**0%**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**
MG7 Risks to Mitigate	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
MG7 Exit Criteria	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
MG7-->MG8 Entrance Criteria	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0%	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Planned and Actual MG Assessments







- 3 Groups of Tools
- Different Maturities
  - 2-3 3 4
  - 3-7 4-5
  - 4-7 5-6
  - 6-7 8

Conclusions

- TRLs / SRLs have been criticized for being not applicable – Solved by tailored MGs.
- Evaluate product status and progress against objective evidence – Proof / Plan to Prove.
- Pressure to field products vs risks from unresolved criteria in an earlier MG.
  - *Open risk items carried forward must have a coordinated risk mitigation plan.*
- When platforms change, readdress already completed maturity criteria.
  - *Risks carried forward with block releases must have a coordinated risk mitigation plan.*
- Block-released products need regular, planned releases with known capabilities.
- When changing directions to resolve issues, know where you are going before changing.
- Create accurate product documentation so capabilities & limitations are understood.
- Frequent discussions, shared portals, and remote test system access improved progress.
- Develop a plan for integrating products and assign a knowledgeable lead system integrator.
- Ensure participants understand the “big picture” and how they contribute.
- Understand users’ needs & develop information products whose displays match the needs.
- Plan for delays in getting approvals to operate on military networks.
- Ensure participants know whose comments and criticism require actions and whose do not.
- Ensure training is timely and audience has proper skills and knowledge to receive it.

INL/CON-17-42211

Questions?

Chris Dieckmann
Group Lead for
National & Homeland Security Projects
(208) 526-5986
chris.dieckmann@inl.gov

Software Complexity Model

Thuc Tran
School of Engineering and Applied Science
The George Washington University
ttran21@gwu.edu

NDIA Systems Engineering Conference 2017

Software Complexity Model

What is Complexity?

*“not easy to understand or explain **:** not simple ”*

“having parts that go together in complicated ways”

“having many varied interrelated parts, patterns, or elements and consequently hard to understand”

What is Software Complexity?

Software that is *“not easy to understand or explain **:** not simple ”*

Software *“having parts that go together in complicated ways”*

Software *“having many varied interrelated parts, patterns, or elements and consequently hard to understand”*

Software Complexity makes software difficult to understand and support

Source: https://www.merriam-webster.com/dictionary/complex

Software Complexity Model

Problem Statement

The lack of a comprehensive software complexity measurement framework leads to an increase of over 90% in software maintenance cost.

Research Objective

The research aims to measure the complexity of software applications through a comprehensive analysis using different dimensions of characteristics. The result will be a score which comprehensively represents the dimensions of software complexity.

Source: Software Maintenance Costs (Koskinen, 2015)

Software Complexity Model

Impacts of Software Complexity

- More than 90% of overall software lifecycle cost can be devoted to maintenance

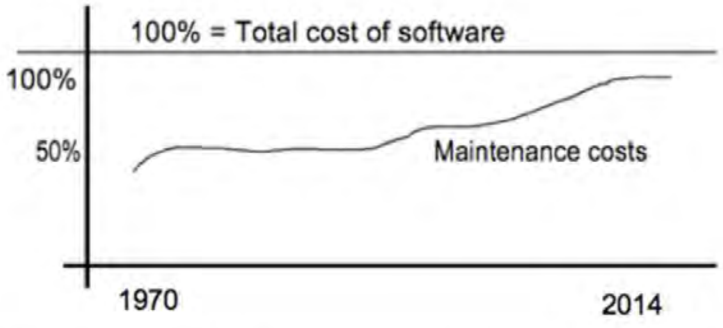


Figure 1: Development of Software maintenance costs as percentage of total cost

Year	Proportion of software maintenance costs	Definition	Reference
2000	>90%	Software cost devoted to system maintenance & evolution / total software costs	Erlikh (2000)
1993	75%	Software maintenance / information system budget (in Fortune 1000 companies)	Eastwood (1993)
1990	>90%	Software cost devoted to system maintenance & evolution / total software costs	Moad (1990)
1990	60-70%	Software maintenance / total management information systems (MIS) operating budgets	Huff (1990)
1988	60-70%	Software maintenance / total management information systems (MIS) operating budgets	Port (1988)
1984	65-75%	Effort spent on software maintenance / total available software engineering effort.	McKee (1984)
1981	>50%	Staff time spent on maintenance / total time (in 487 organizations)	Lientz & Swanson (1981)
1979	67%	Maintenance costs / total software costs	Zelkowitz *et al.* (1979)

Source: Software Maintenance Costs (Koskinen, 2015)
How to save on software maintenance costs (Vries & Burki, 2014)

Software Complexity Model

Impacts of Software Complexity

- Analysis of software accounts for nearly 50% of maintenance development

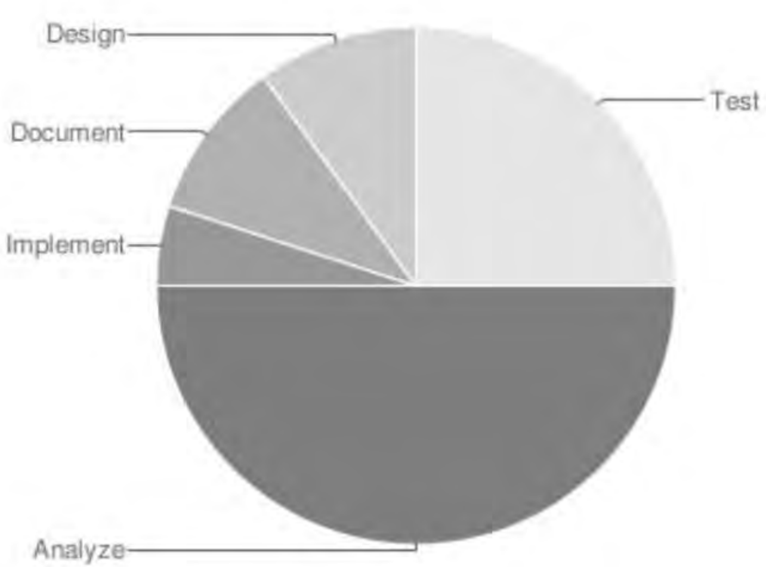
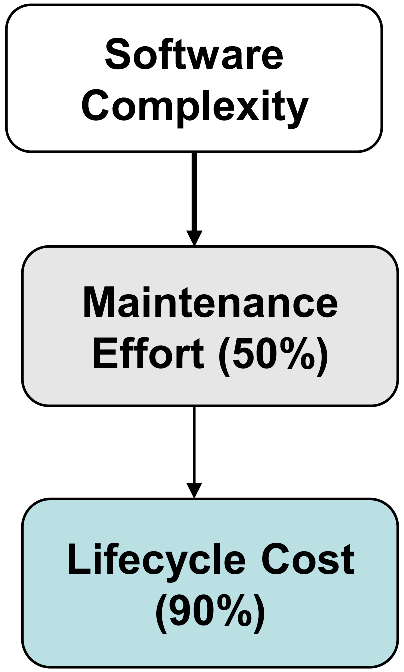


Figure 2: Analyzing is almost 50% of the total maintenance effort



Source: Software Development Practices, Software Complexity, and Software Maintenance (Banker et al, 1998)
How to save on software maintenance costs (Vries & Burki, 2014)

Software Complexity Model

Software Product Quality Model – ISO/IEC 9126 (2001)

- **Functionality –** The capability of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions.
- **Reliability –** The capability of the software product to maintain a specified level of performance when used under specified conditions.
- **Usability –** The capability of the software product to be understood, learned, used and attractive to the user, when used under specified conditions.
- **Efficiency –** The capability of the software product to provide appropriate performance, relative to the amount of resources used, under stated conditions.
- **Maintainability –** The capability of the software product to be modified. Modifications may include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications.
- **Portability –** The capability of the software product to be transferred from one environment to another.

Source: ISO/IEC 9126

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Software Complexity Model

Software Product Quality Model – ISO/IEC 9126 (2001)

Dimension	Sub-Dimension	Definition
Functionality	Suitability	• The capability of the software product to provide an appropriate set of functions for specified tasks and user objectives.
	Accuracy	• The capability of the software product to provide the right or agreed results or effects with the needed degree of precision.
	Interoperability	• The capability of the software product to interact with one or more specified systems.
	Security	• The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them.
	Functionality Compliance	• The capability of the software product to adhere to standards, conventions or regulations in laws and similar prescriptions relating to functionality.
Reliability	Maturity	• The capability of the software product to avoid failure as a result of faults in the software.
	Fault Tolerance	• The capability of the software product to maintain a specified level of performance in cases of software faults or of infringement of its specified interface.
	Recoverability	• The capability of the software product to re-establish a specified level of performance and recover the data directly affected in the case of a failure.
	Reliability Compliance	• The capability of the software product to adhere to standards, conventions or regulations relating to reliability.
Usability	Understandability	• The capability of the software product to enable the user to understand whether the software is suitable, and how it can be used for particular tasks and conditions of use.
	Learnability	• The capability of the software product to enable the user to learn its application.
	Operability	• The capability of the software product to enable the user to operate and control it.
	Attractiveness	• The capability of the software product to be attractive to the user.
	Usability Compliance	• The capability of the software product to adhere to standards, conventions, style guides or regulations relating to usability.

Software Complexity Model

Software Product Quality Model – ISO/IEC 9126 (2001)

Dimension	Sub-Dimension	Definition
Efficiency	Time Behavior	• The capability of the software product to provide appropriate response and processing times and throughput rates when performing its function, under stated conditions.
	Resource Utilization	• The capability of the software product to use appropriate amounts and types of resources when the software performs its function under stated conditions.
	Efficiency Compliance	• The capability of the software product to adhere to standards or conventions relating to efficiency.
Maintainability	Analyzability	• The capability of the software product to be diagnosed for deficiencies or causes of failures in the software, or for the parts to be modified to be identified.
	Changeability	• The capability of the software product to enable a specified modification to be implemented.
	Stability	• The capability of the software product to avoid unexpected effects from modifications of the software.
	Testability	• The capability of the software product to enable modified software to be validated.
	Maintainability Compliance	• The capability of the software product to adhere to standards or conventions relating to maintainability.
Portability	Adaptability	• The capability of the software product to be adapted for different specified environments without applying actions or means other than those provided for this purpose for the software considered.
	Installability	• The capability of the software product to be installed in a specified environment.
	Co-Existence	• The capability of the software product to co-exist with other independent software in a common environment sharing common resources.
	Replaceability	• The capability of the software product to be used in place of another specified software product for the same purpose in the same environment.
	Portability Compliance	• The capability of the software product to adhere to standards or conventions relating to portability.

Software Complexity Model

Software Product Quality Model – ISO/IEC 9126 (2001)

- Compliance is a part of every dimension and can be considered a dimension on its own
- *Note: The following displays all attributes from the ISO/IEC 9126 Product Quality Model, but not all dimensions / sub-dimensions will be used:*

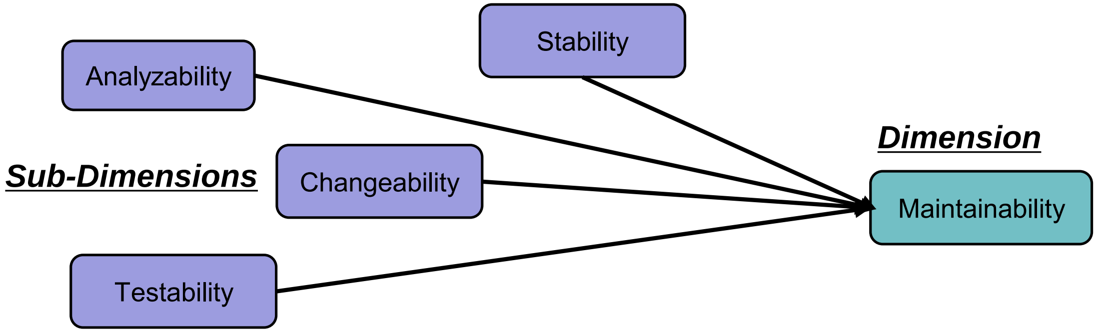
Dimensions	Sub-Dimensions
Functionality	• Suitability • Accuracy • Interoperability • Security • Functionality Compliance
Reliability	• Maturity • Fault Tolerance • Recoverability • Reliability Compliance
Usability	• Understandability • Learnability • Operability • Attractiveness • Usability Compliance
Efficiency	• Time Behavior • Resource Utilization • Efficiency Compliance
Maintainability	• Analyzability • Changeability • Stability • Testability • Maintainability Compliance
Portability	• Adaptability • Installability • Co-Existence • Replaceability • Portability Compliance

Dimensions	Sub-Dimensions
Functionality	• Suitability • Accuracy • Interoperability • Security
Reliability	• Maturity • Fault Tolerance • Recoverability
Usability	• Understandability • Learnability • Operability • Attractiveness
Efficiency	• Time Behavior • Resource Utilization
Maintainability	• Analyzability • Changeability • Stability • Testability
Portability	• Adaptability • Installability • Co-Existence • Replaceability
Compliance	• Functionality Compliance • Reliability Compliance • Usability Compliance • Efficiency Compliance • Maintainability Compliance • Portability Compliance

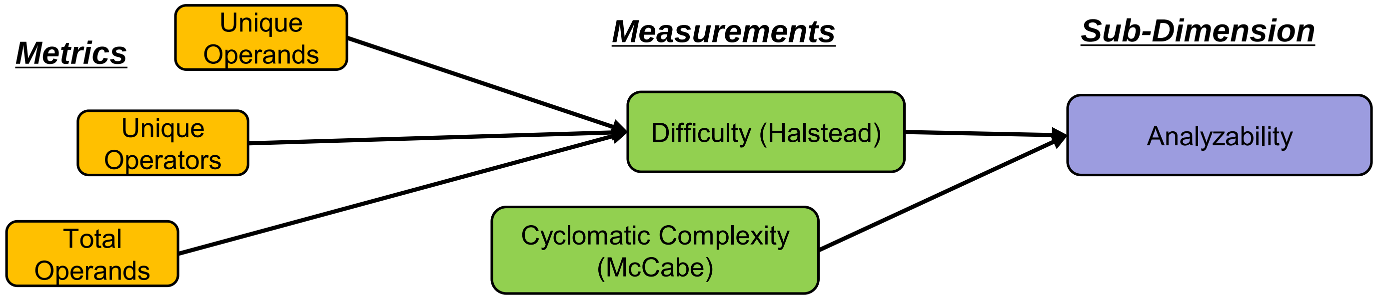
Software Complexity Model

Software Product Quality Model – ISO/IEC 9126 (2001)

- **Dimensions** are comprised of **Sub-Dimensions**



- **Sub-Dimensions** are comprised of various **measurements**
- **Measurements** may use many different **metrics**



Software Complexity Model

Software Metrics

- Software Metrics identify a ***value*** that represents a characteristic of the software
- Software Metrics contribute to the evaluation of Software Measurements

Metric Category	Metric Type	Metric
Complexity	Size	• Lines of Code
	Interface Complexity	• Number of Attributes and Methods
		• Number of Local Methods
	Structural Complexity	• McCabe Cyclomatic Complexity
		• Weighted Method Count
		• Response for a Class

Source: ARISA Compendium of Software Quality Standards and Metrics - Version 1.0

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Software Complexity Model

Software Metrics

Metric Category	Metric Type	Metric
Architecture and Structure	Inheritance	• Depth of Inheritance Tree
		• Number of Children
	Coupling	• Afferent Coupling
		• Coupling Between Objects
		• Change Dependency Between Classes
		• Change Dependency of Classes
		• Efferent Coupling
		• Coupling Factor
		• Data Abstraction Coupling
		• Instability
		• Locality of Data
		• Message Passing Coupling
		• Package Data Abstraction Coupling
	Cohesion	• Lack of Cohesion in Methods
		• Improvement of LCOM
		• Tight Class Cohesion

Software Complexity Model

Software Metrics

Metric Category	Metric Type	Metric
Design Guidelines and Code Conventions	Documentation	• Lack of Documentation
	Code Conventions	

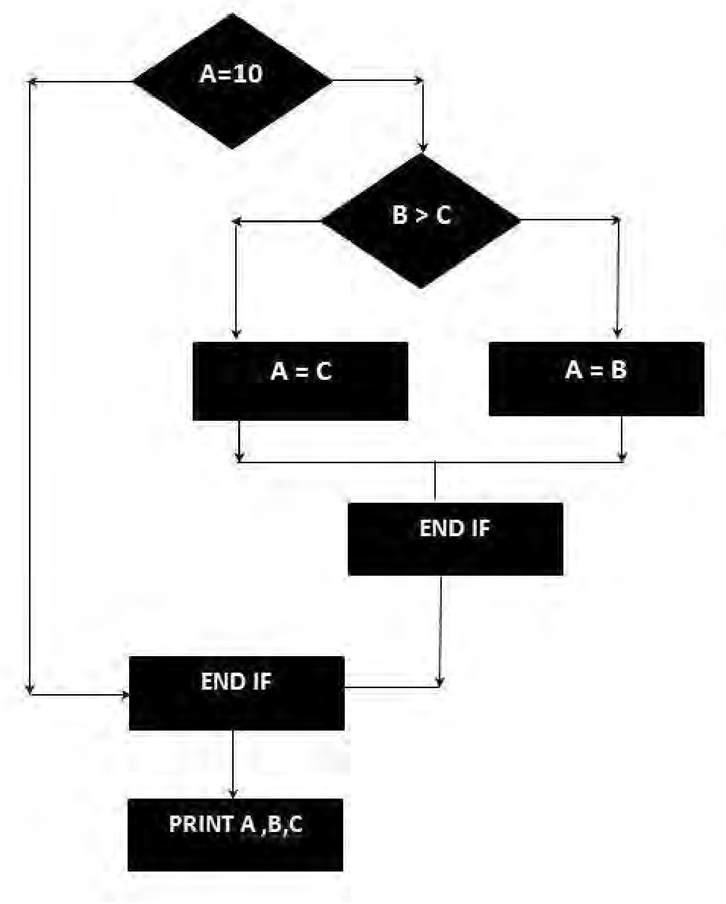
Source: ARISA Compendium of Software Quality Standards and Metrics - Version 1.0

Software Complexity Model

Cylcomatic Complexity

Example Complexity:

```
IF A = 10 THEN
 IF B > C THEN
   A = B
 ELSE
   A = C
 ENDIF
ENDIF
Print A
Print B
Print C
```



v(G) = e – n + p

v(G) = cyclomatic number
e = edges
n = nodes
p = connected components

v(G) = 8 – 7 + 2 = 3

e = 8
n = 7
p = 2

Source: https://www.tutorialspoint.com/software_testing_dictionary/cyclomatic_complexity.htm

Software Complexity Model

Software Science Metrics

```
void sort ( int *a, int n ) {
    int i, j, t;
    if (n<2) return;
    for (i=0; i<n-1; i++) {
        for (j=i+1; j<n; j++) {
            if (a[i] > a[j]) {
                t = a[i];
                a[i] = a[j];
                a[j] = t;
            }
        }
    }
}
```

Operators			
<	3	{	3
=	5	}	3
>	1	+	1
-	1	++	2
,	2	for	2
;	9	if	2
(	4	int	1
)	4	return	1
[]	6		

Operands	
0	1
1	2
2	1
a	6
i	8
j	7
n	3
t	3

Source: http://www.win.tue.nl/~aserebre/2IS55/2011-2012/10.pdf

Software Complexity Model

Software Science Metrics

	Total	Unique
Operators	N1 = 50	n1 = 17
Operands	N2 = 30	n2 = 7

n1 = unique operators
n2 = unique operands
N1 = total operators
N2 = total operands

Program Length (N) = N1 + N2
Vocabulary Size (n) = n1 + n2
Volume (V) = N * log2(n)
Difficulty (D) = (n1 / 2) * (N2 / n2)
Level (L) = 1 / D
Effort = D * VOL
Time (T) = E / 18
Bugs (B) = V / 3000

n1 = 17
n2 = 7
N1 = 50
N2 = 30

Program Length (N) = 80
Vocabulary Size (n) = 24
Volume (V) ≈ 392
Difficulty (D) ≈ 36
Level (L) ≈ 0.027
Effort = 14112
Time (T) = 784 (s)
Bugs (B) ≈ 0.1306

Source: http://www.win.tue.nl/~aserebre/2IS55/2011-2012/10.pdf

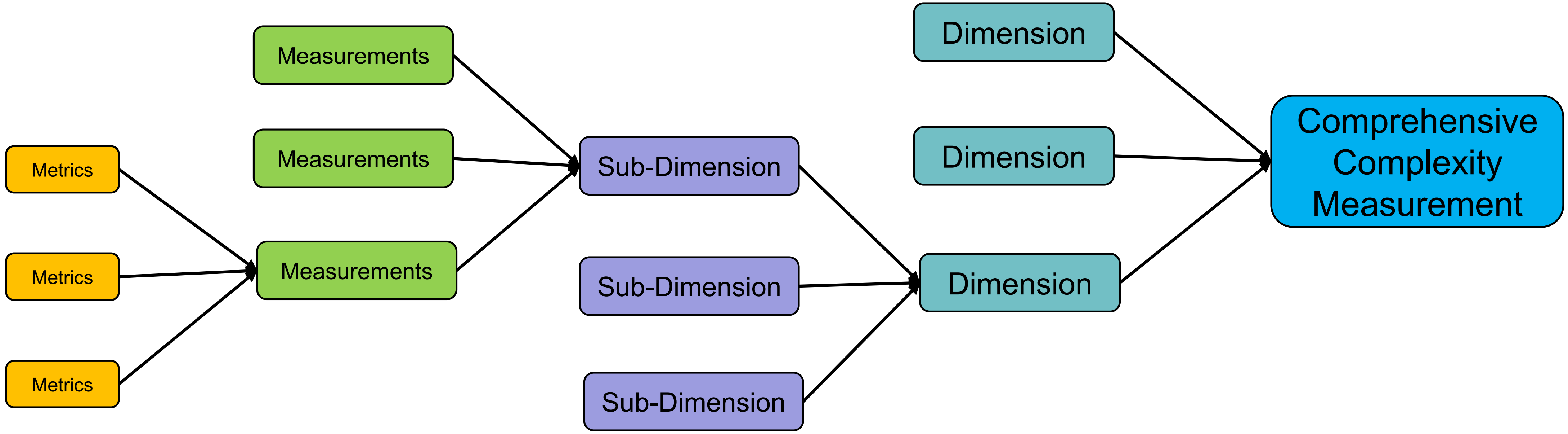
Software Complexity Model

Comprehensive Complexity Measurement

- Software Metrics identify a value that represents a characteristic of the software
- Metrics are used to calculate Software Measurements
- Software Measurements are used to evaluate Sub-Dimensions
- Sub-Dimensions are then used to evaluate Dimensions
- Dimensions can then be used to calculate a Comprehensive Complexity Measurement

Software Complexity Model

Comprehensive Complexity Measurement

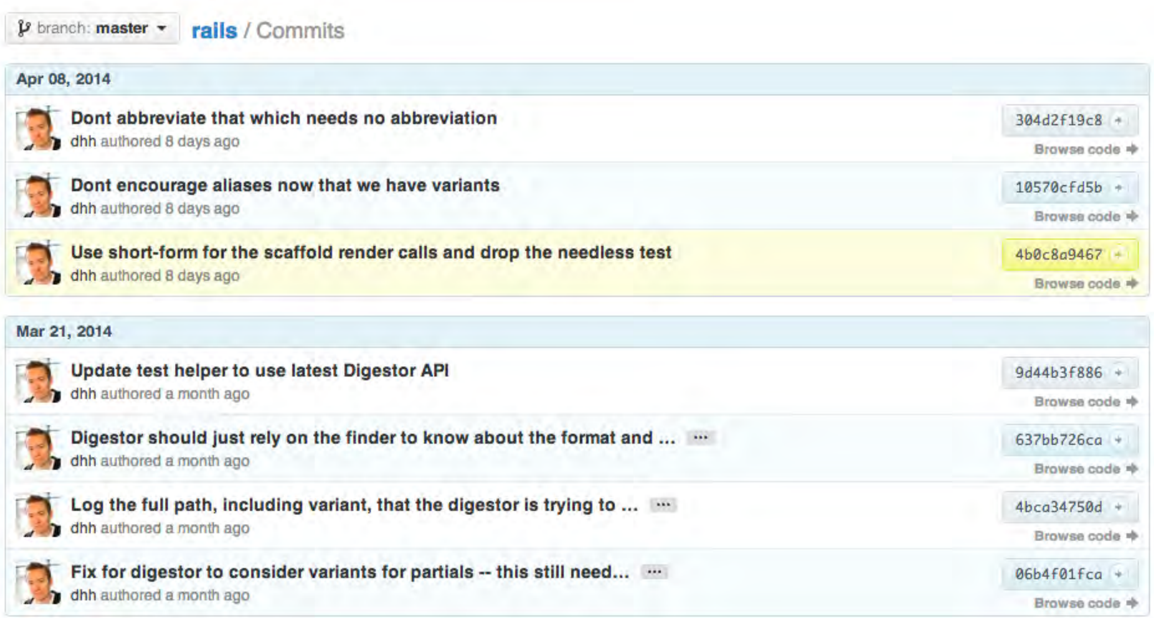


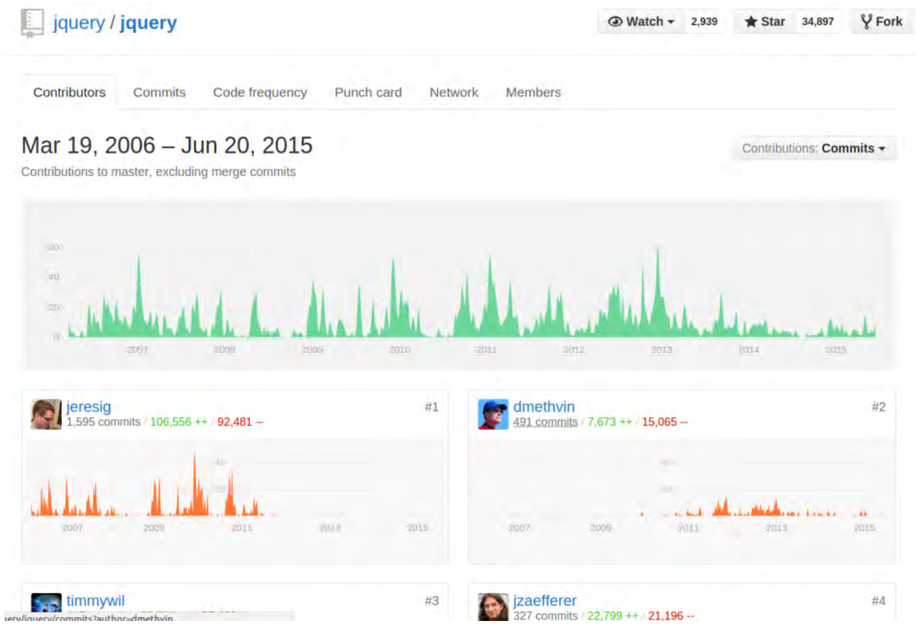
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Software Complexity Model

Implementation

- Now we have a current score and a desired score, **so what?**
- The framework can then **recommend** changes that most significantly reduce the delta score; bringing the **current system** closer to the **most optimal system**
- **This can eventually be operationalized with a system like GitHub, a version control system that tracks changes *over time***





THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Questions

References

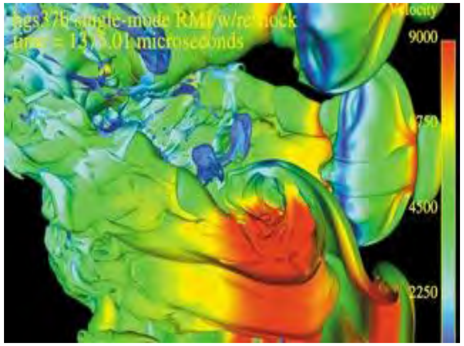
- Scalet et al., 2000: ISO/IEC 9126
- Carlson, A. (n.d.). *University of Washington*. Retrieved 6 21, 2017, from Paul G. Allen School of Computer Science and Engineering: http://courses.cs.washington.edu/courses/cse403/96sp/coupling-cohesion.html
- Chidamber, S. R., & Kemerer, C. F. (1994, June). A Metrics Suite for Object Oriented Design. *IEEE Transactions on Software Engineering, 20*(6), 476-493.
- *Cyclomatic Complexity*. (n.d.). Retrieved 6 21, 2017, from tutorialspoint: https://www.tutorialspoint.com/software_testing_dictionary/cyclomatic_complexity.htm
- Halstead, M. (1977). *Elements of Software Science.* New York, NY: Elsevier.
- Holzmann, G. (2007, December). Conquering Complexity. 111-113.
- *https://www.merriam-webster.com*. (2017, 6 21). Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/complex
- Kafura, D., & Henry, S. (1981, September). Software Structure Metrics Based on Information Flow. *IEEE Transactions on Software Engineering, SE-7*(5), 510-518.
- McCabe, T. J. (1976, December). A Complexity Measure. *IEEE Transactions on Software Engineering, SE-2*(4), 308-320.
- *Measurement of Halstead Metrics with Testwell CMT++ and CMTJava (Complexity Measures Tool)*. (n.d.). Retrieved 6 21, 2017, from verifysoft: http://www.verifysoft.com/en_halstead_metrics.html
- Misra, S., Akman, I., & Colomo-Palacios, R. (2011). Framework for evaluation and validation of software complexity measures.
- Ortu, M., Destefanis, G., Murgia, A., Marchesi, M., Tonelli, R., & Adams, B. (n.d.). The JIRA Repository Dataset: Understanding Aspects of Software Development.
- Serebrenik, A. (2017, 6 21). Software Metrics. *Software Evolution*.
- Shao, J., & Wang, Y. (2003). A new measure of software complexity based on cognitive weights. *CCECE 2003 - Canadian Conference on Electrical and Computer Engineering*.
- Stevens, W., Myers, G., & Constantine, L. (1974, June). Structured Design. *IBM Systems Journal, 13*(2), 115-139.
- *The Halstead Metrics*. (n.d.). Retrieved 6 21, 2017, from Virtual Machinery: http://www.virtualmachinery.com/sidebar2.htm
- Weyuker, E. (1988, September). Evaluating Software Complexity Measures. *IEEE Transactions on Software Engineering, 14*(9), 1357-1365.

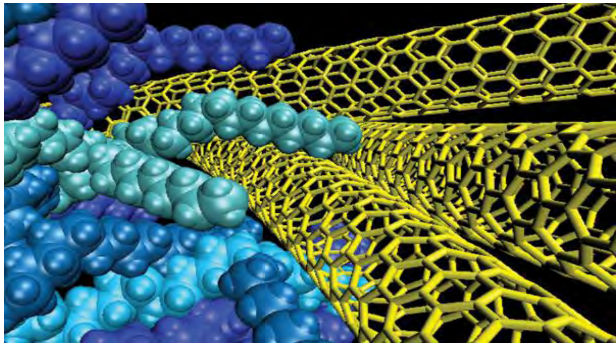
References

- Debbarma, M. K., Debbarma, S., Debbarma, N., Chakma, K., & Jamatia, A. (2013). A Review and Analysis of Software Complexity Metrics in Structural Testing. *International Journal of Computer and Communication Engineering*, *2*(2), 129–133. https://doi.org/10.7763/IJCCE.2013.V2.154
- Dehaghani, S., & Hajrahimi, N. (2013). Which factors affect software projects maintenance cost more. *Acta Informatica Medica*, *21*(October 2012), 63–66. https://doi.org/10.5455/aim.2012.21.63-66
- Gui, & Scott, P. D. (2008). New coupling and cohesion metrics for evaluation of software component reusability. *Proceedings of the 9th International Conference for Young Computer Scientists, ICYCS 2008*, 1181–1186. https://doi.org/10.1109/ICYCS.2008.270
- Holvitie, J., & Leppänen, V. (2014). Illustrating software modifiability - Capturing cohesion and coupling in a force-optimized graph. *Proceedings - 2014 IEEE International Conference on Computer and Information Technology, CIT 2014*, 226–233. https://doi.org/10.1109/CIT.2014.112
- Husein, S., & Oxley, A. (2009). A coupling and cohesion metrics suite for object-oriented software. *ICCTD 2009 - 2009 International Conference on Computer Technology and Development*, *1*, 421–425. https://doi.org/10.1109/ICCTD.2009.209
- Kafura, D., & Reddy, G. R. (1987). The Use of Software Complexity Metrics in Software Maintenance. *IEEE Transactions on Software Engineering*, *SE-13*(3), 335–343. https://doi.org/10.1109/TSE.1987.233164
- Klemola, T., & Rilling, J. (2003). A Cognitive Complexity Metric Based on Category Learning. In *The Second IEEE International Conference on Cognitive Informatics, 2003. Proceedings.* (pp. 106–112).
- Kushwaha, D. S., & Misra, A. K. (2006). Improved cognitive information complexity measure: a metric that establishes program comprehension effort. *ACM SIGSOFT Software Engineering Notes*, *31*(5), 1–7. https://doi.org/10.1145/1163514.1163533
- Allen, E. B., Khoshgoftaar, T. M., & Chen, Y. (2001). Measuring coupling and cohesion of software modules: an information-theory approach. *Proceedings Seventh International Software Metrics Symposium*, (561), 124–134.
- Keshavarz, G., Modiri, N., & Pedram, M. (2011). A Model for the Controlled Development of Software Complexity Impacts. *International Journal of Computer Science and Information Security, 9*(6).
- Mancoridis, S., Mitchell, B. S., & Rorres, C. (1998). Using Automatic Clustering to Produce High-Level System Organizations of Source Code. *Program Comprehension, 1998. IWPC '98. Proceedings., 6th International Workshop*.
- Mitchell, B. S., & Mancoridis, S. (2006). On the automatic modularization of software systems using the Bunchtool. *IEEE Transactions on Software Engineering*, *32*(3), 193–208.
- Yau, S. S., & Collofello, J. S. (1980). Some Stability Measures for Software Maintenance. *IEEE Transactions on Software Engineering*, *SE-6*(6), 545–552.

Exceptional service in the national interest

Sandia National Laboratories





Harnessing the Beast:

Using Model Based Systems Engineering (MBSE) to Manage Complex Research Software Environments

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXX X

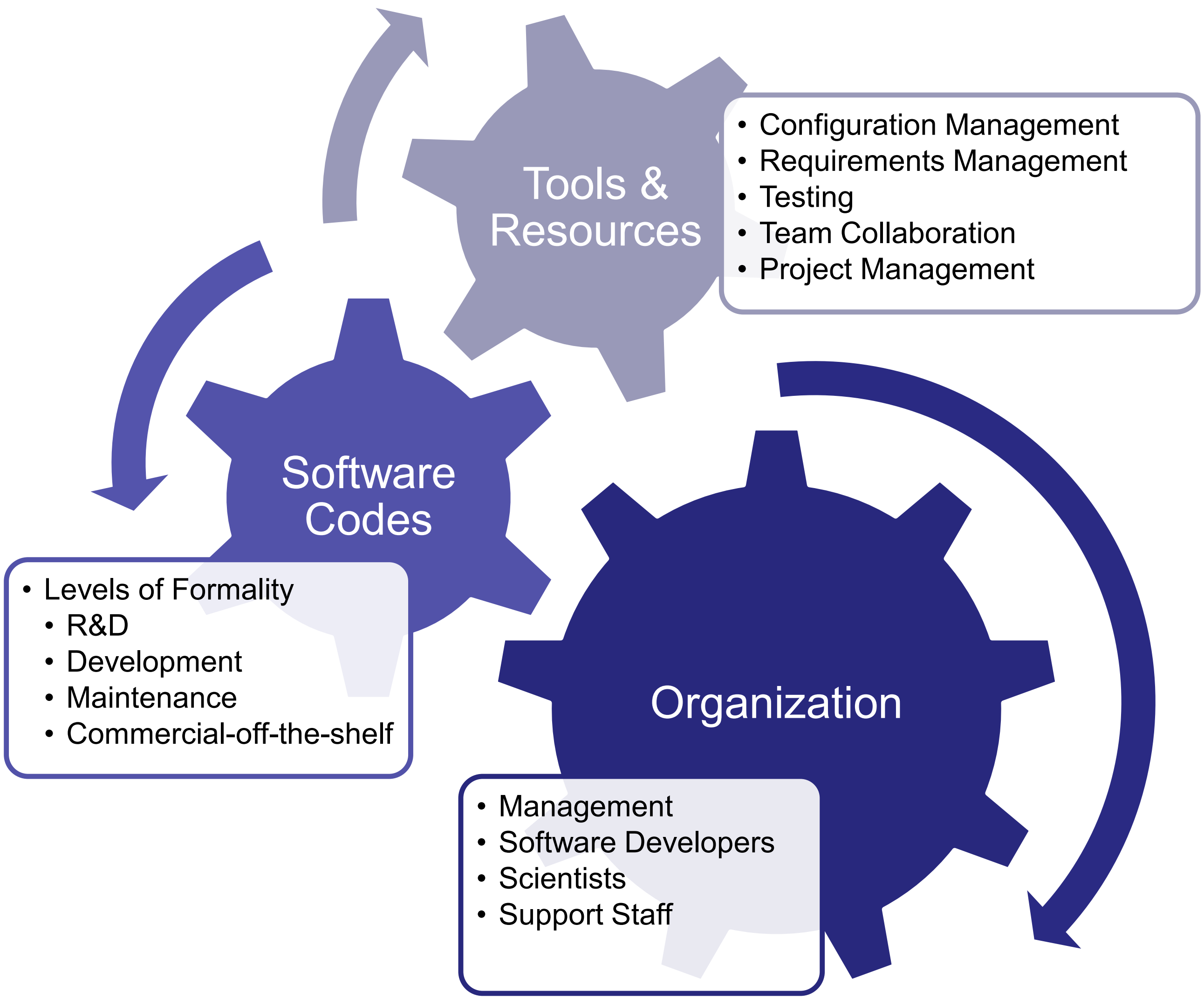
Introduction

- Background
  - Software engineering
  - Software process improvement
  - Project management
  - Capability Maturity Model Integration (CMMI)
    - Appraisals (software & systems)
    - Implementation (software & systems)
  - Systems engineering
    - Model based systems engineering (MBSE) in non-traditional environments
  - Data analysis
    - Decision support
    - Impact analysis
    - Performance monitoring

Complexity

The state or quality of being intricate or complicated.

- For this presentation, we are focused on system complexity, not software complexity.



Managing the Complexity

Product Issues

- Software integration
- Transition from research to development
- Support tools
- Programming languages
- Product quality (*and all the "ilities" that come with it*)
- Competing requirements
- Independent designs

People Issues

- Conflicting customer needs
  - Internal and external to the system
- Plethora of code teams
  - Experience levels
  - Funded from within and outside the system
- Multitude of managers
- Multiple physical locations
- Organizational structure changes

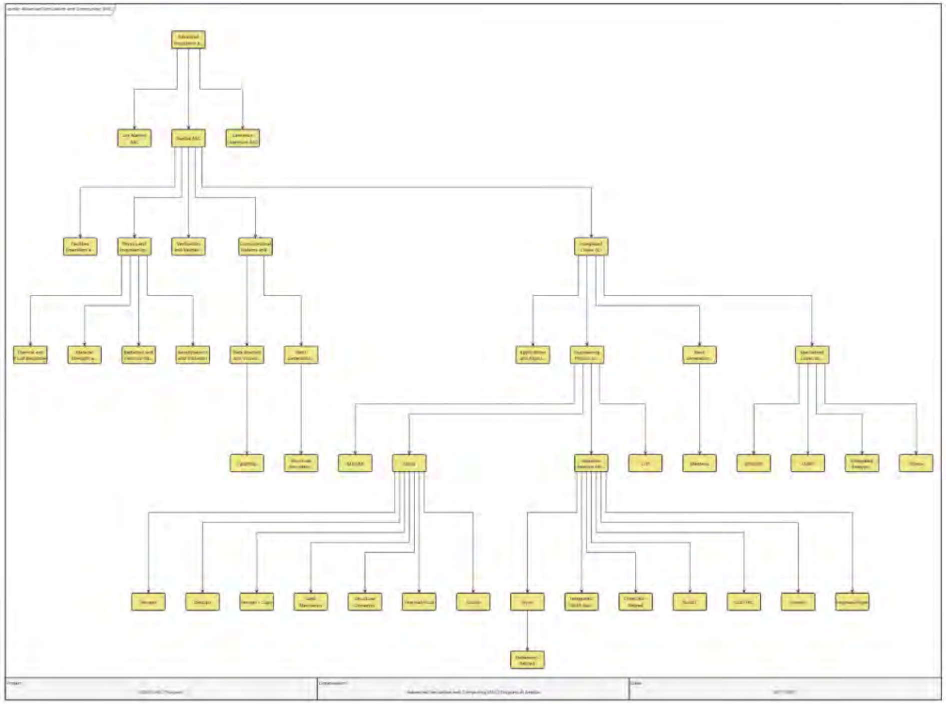
Complexity Management: “As-Is” State

- Management Structure and Hierarchy
  - Software codes and teams are chunked into five different program elements
  - Program element management reports to a program director
- Dependence on Tribal Knowledge
- Meetings
  - Design Reviews
  - Peer Reviews
  - End-user Office Hours
- Agile Software Development Methods
- Support Tools

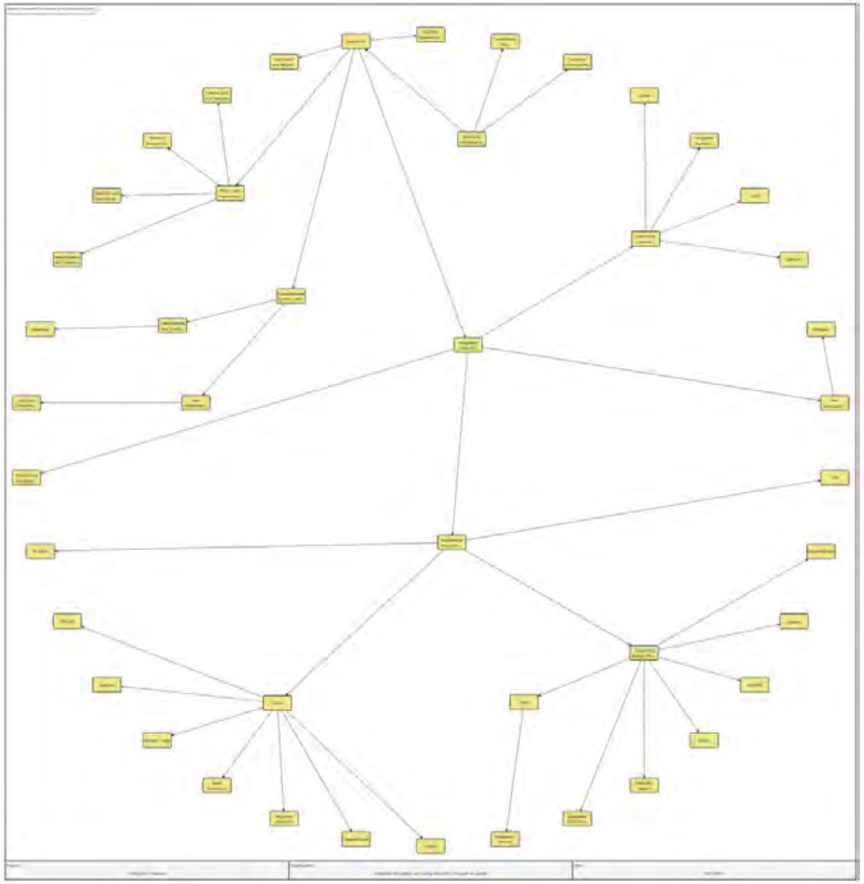
Complexity Management: “To-Be” State

- Resilient Architecture for Migration and Sustainability of Software (RAMSS)
  - Use Model-based Systems Engineering (MBSE) to model the organizational system
    - Model people, software codes, interfaces, etc.
    - Use Vitech’s GENESYS tool to manage the organizational model
  - Use outputs from the model to inform data visualizations
    - Support management decision and impact analyses
    - Provide situational awareness to clearly demonstrate the current environment so that changes impacting the future are based upon fact
    - Inform prioritization of software process improvement efforts
    - Use Tableau to develop dashboard visualizations that pull from the MBSE model

RAMSS Operational Architecture

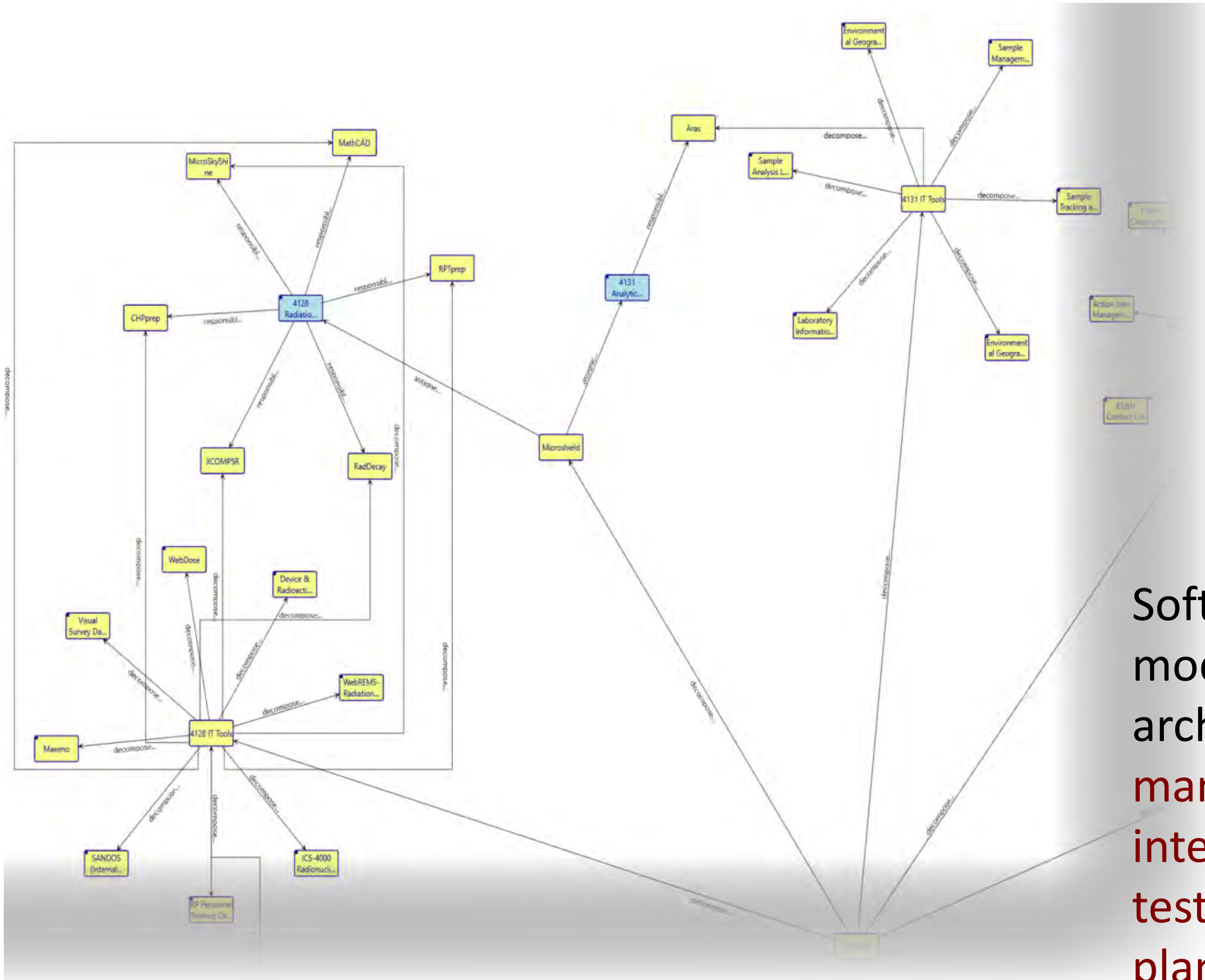


Different views of organizational structure provide insight into areas with more complexity.



Organizational models are part of the operational architecture and will be used to manage programmatic requirements, capabilities, and processes.

RAMSS System Architecture



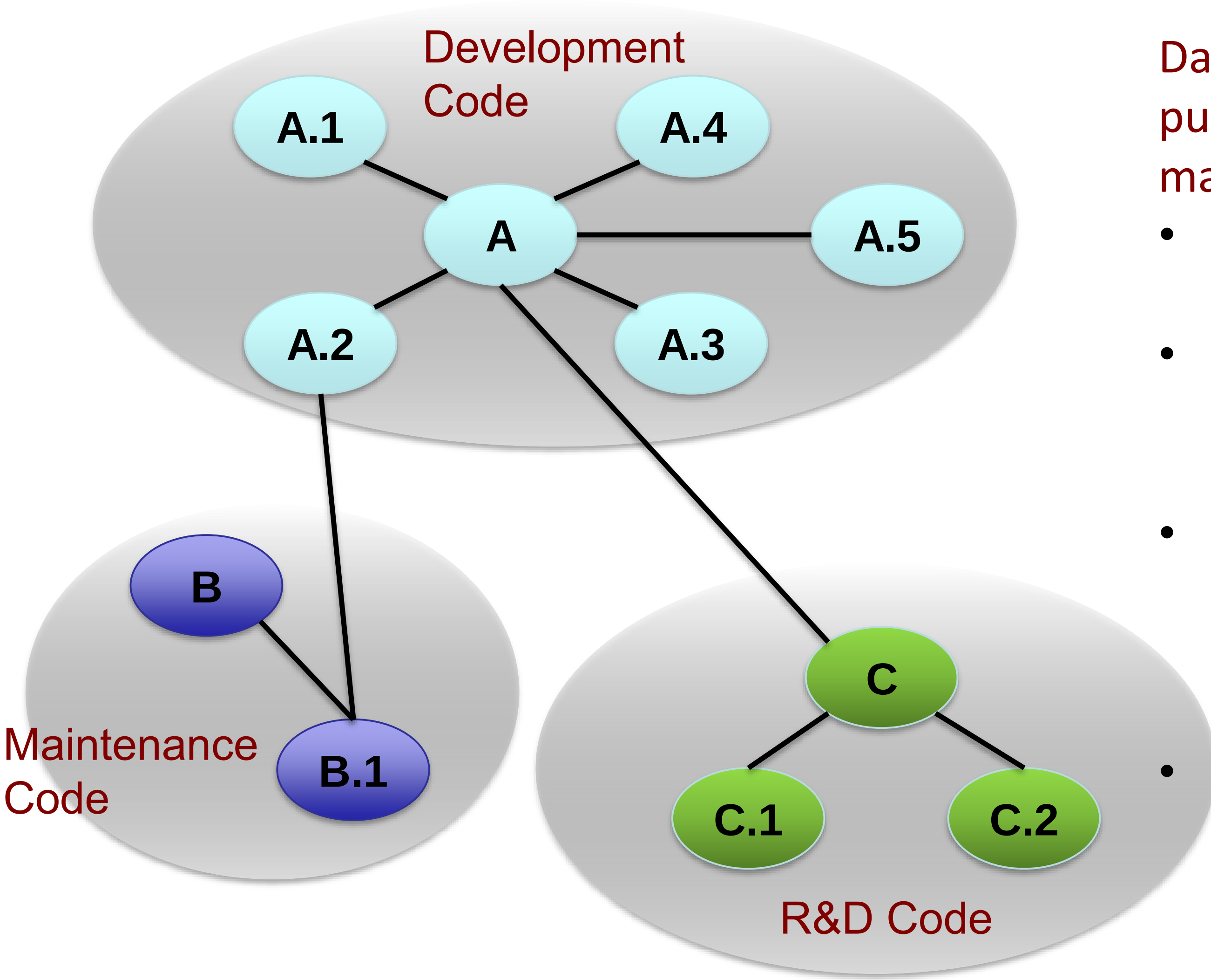
A documented system architecture provides visual insight not available in the “As-Is” state.

Software components modeled within the system architecture will be used to manage software code integration and assimilation, test integration, and release planning.

RAMSS System Architecture Attributes

- Interfaces
- Assessment results
- Graded risk levels
- Code type (maintenance, development, R&D, COTS, etc.)
- Primary code uses
- Tools associated with code development
- Test methods and types
- Team leadership information
- Code development languages and environments
- More to be discovered…

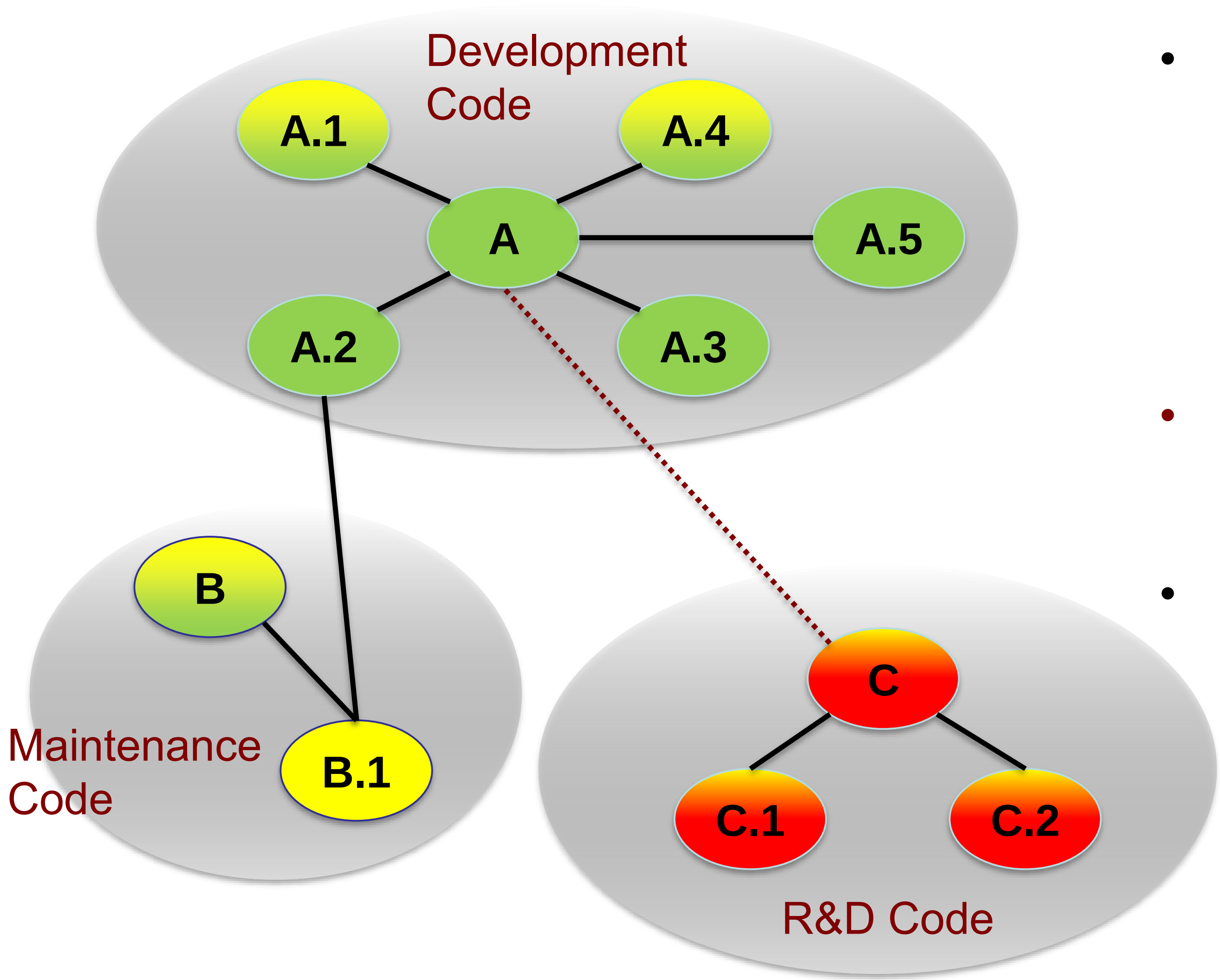
RAMSS Data Analytics



Data from the MBSE tool is pulled to inform management decisions.

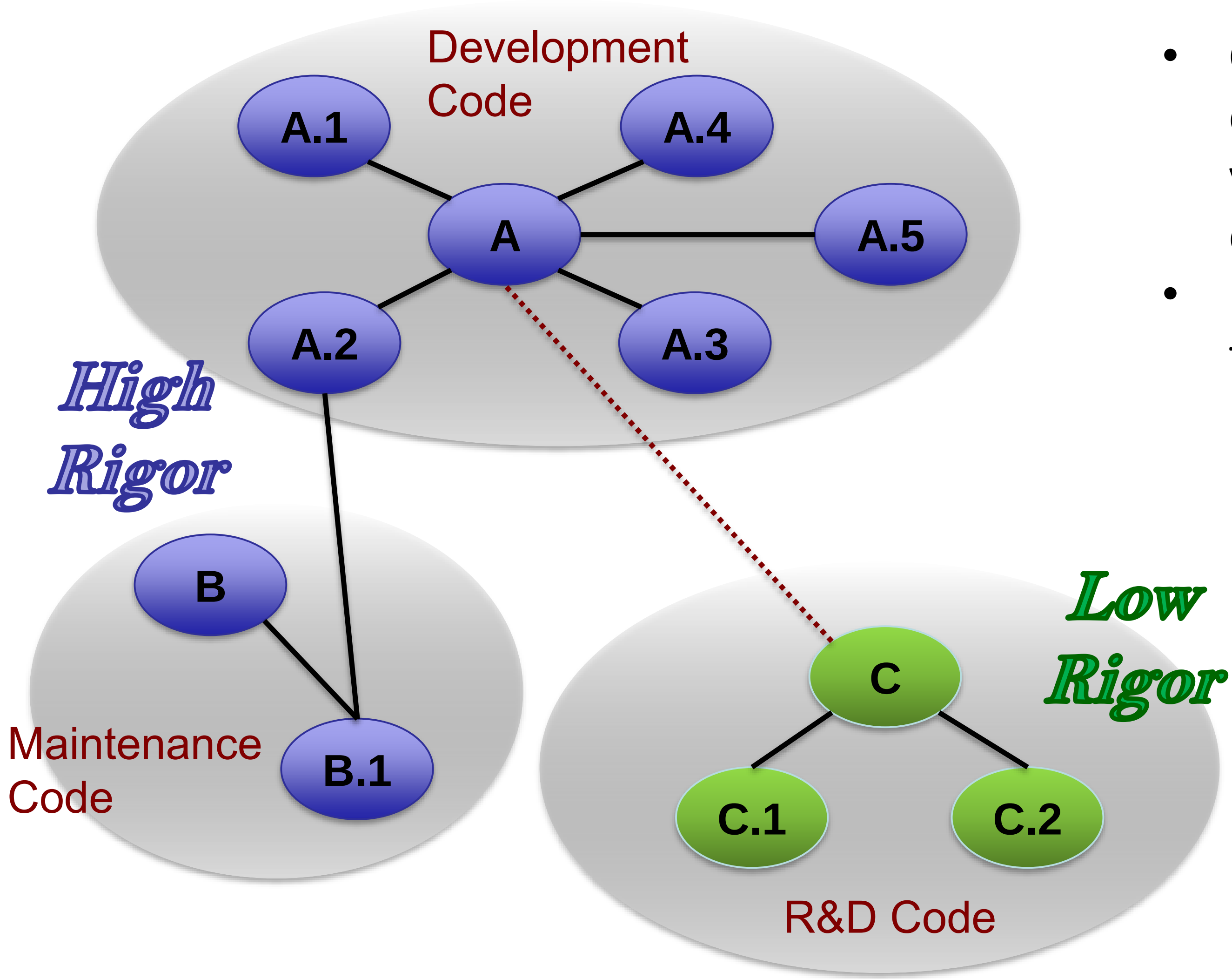
- Readiness of R&D codes for development
- Areas where cross-team integrated testing may benefit the product line
- Identification of areas where software development processes may need to be aligned
- Etc.

RAMSS Data Analytics - Transition



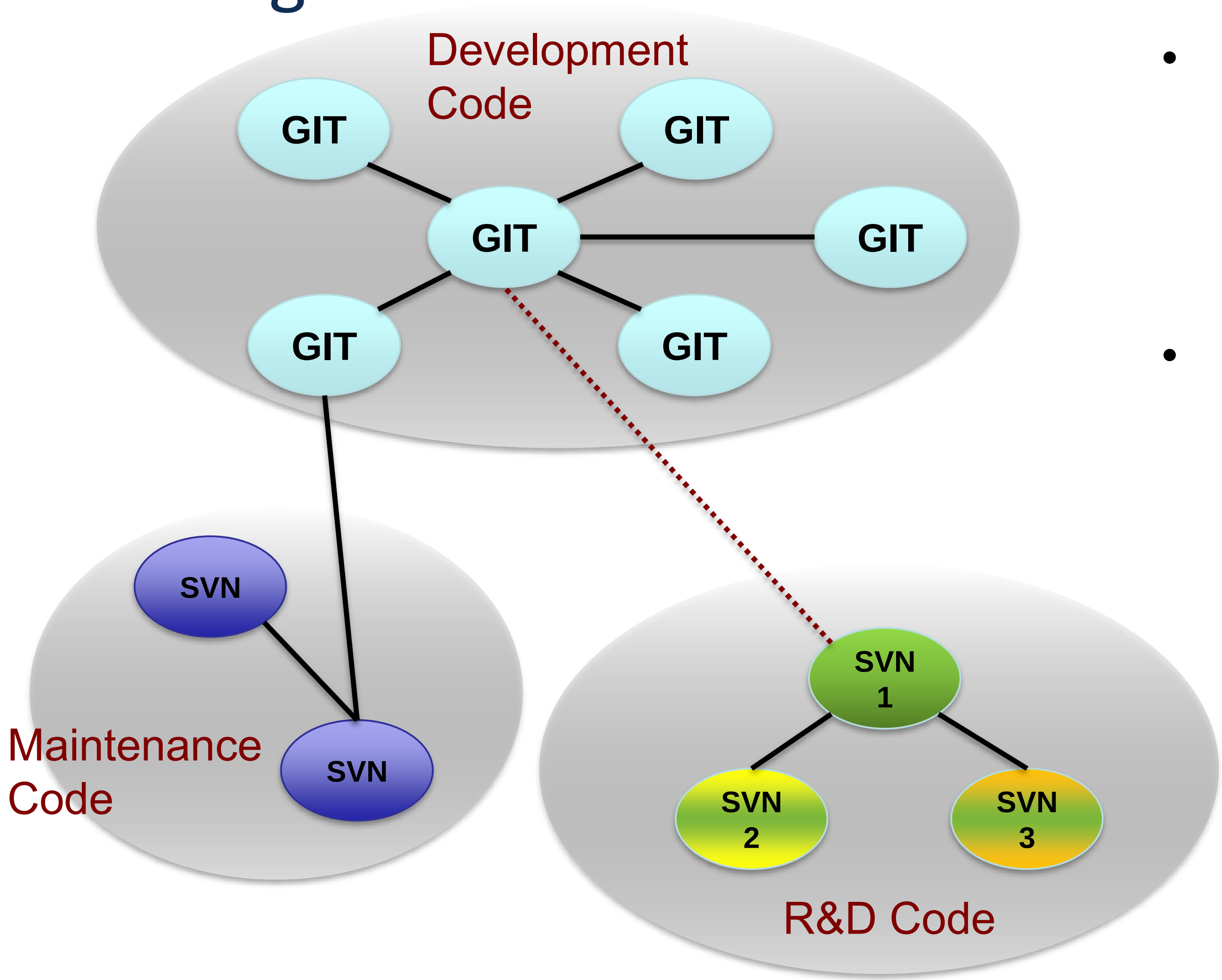
- Information pulled from the model provides insight needed for transitioning R&D code into a development environment.
- "Readiness" can be gathered from past assessment data.
- Risk management

RAMSS Data Analytics - Process



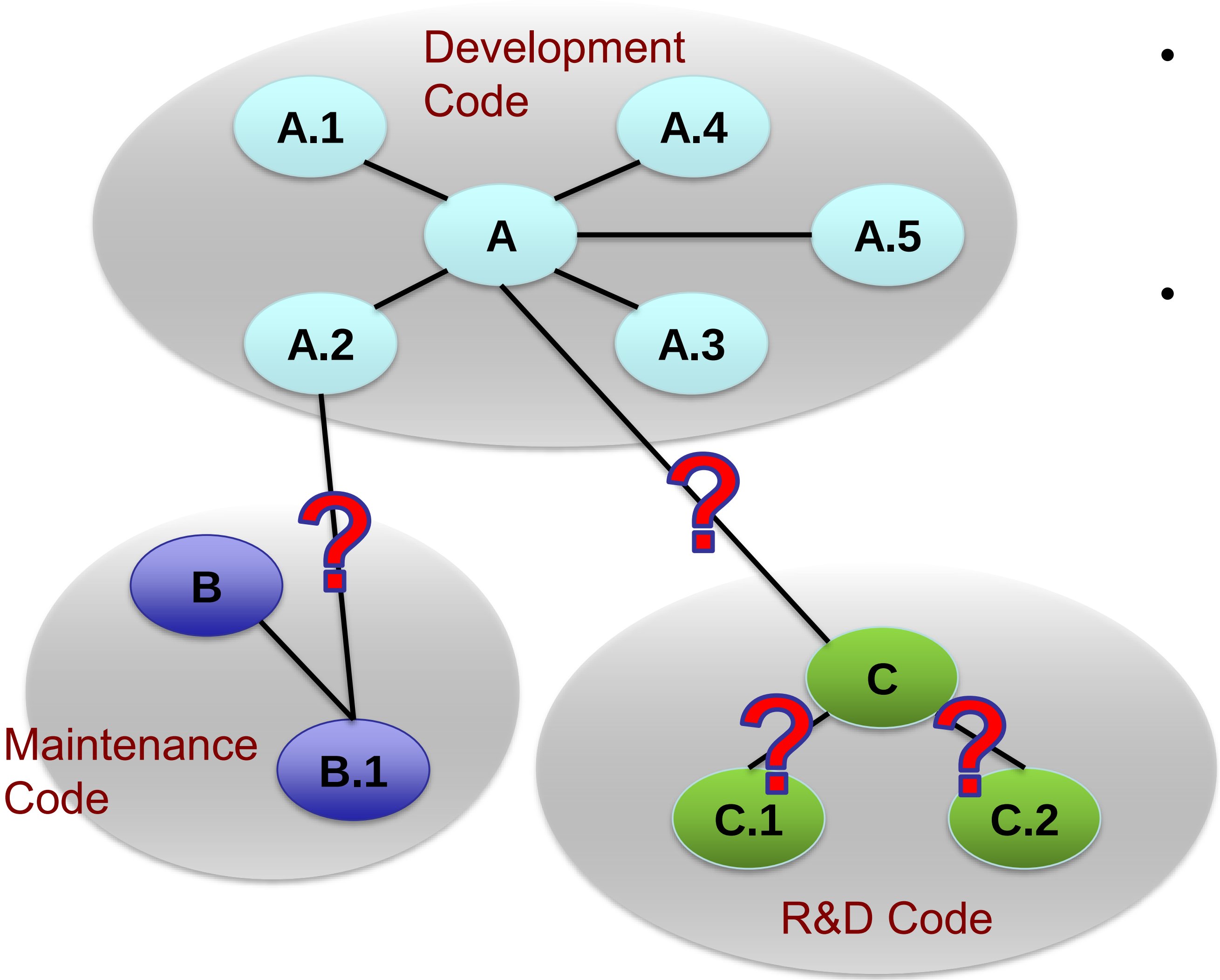
- Code team development processes vary based upon their development phase.
- Integration requires teams to align some:
  - Rigor levels
  - Processes
  - Tools

RAMSS Data Analytics – Configuration Management



- Configuration management influences code releases, code integrity, and code integration.
- When codes interface, configuration management decisions need to be made.

RAMSS Data Analytics - Testing



- Testing often creates bottlenecks with code integration and data transfer.
- Visualizations help understand where these bottlenecks occur and where to develop test strategies to avoid issues.

Comments & Questions

Jennifer Turgeon

Sandia National Laboratories

505-284-3630

jturgeo@sandia.gov