Strategies for Moving from Waterfall Acquisitions

Carnegie Mellon University
Software Engineering Institute

FAA V&V TIM
11/15/2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-1043

Objectives of Today's Meeting

FAA Interests (Based on a Prior Conversation):

- Future Trends in Software Engineering
- Contracting using an Agile Approach
- Specifying Requirements for Agile Projects
  - Sharing Risk with Contractors
- Providing Needed Discipline for Agile Projects
- Moving V&V to the Left via New Approaches
- Identifying Tooling / Testbeds for Use

Providing Safety to the Flying Public

CMU SEI is a DoD R&D Federally Funded Research and Development Center

Established in 1984 at Carnegie Mellon University (CMU)

Charged to improve the state of the practice of software engineering and cybersecurity

Added AI Engineering in 2018

Collaborates with CMU and broadly in academia, government, and industry

Capable of conducting both fundamental research and classified work

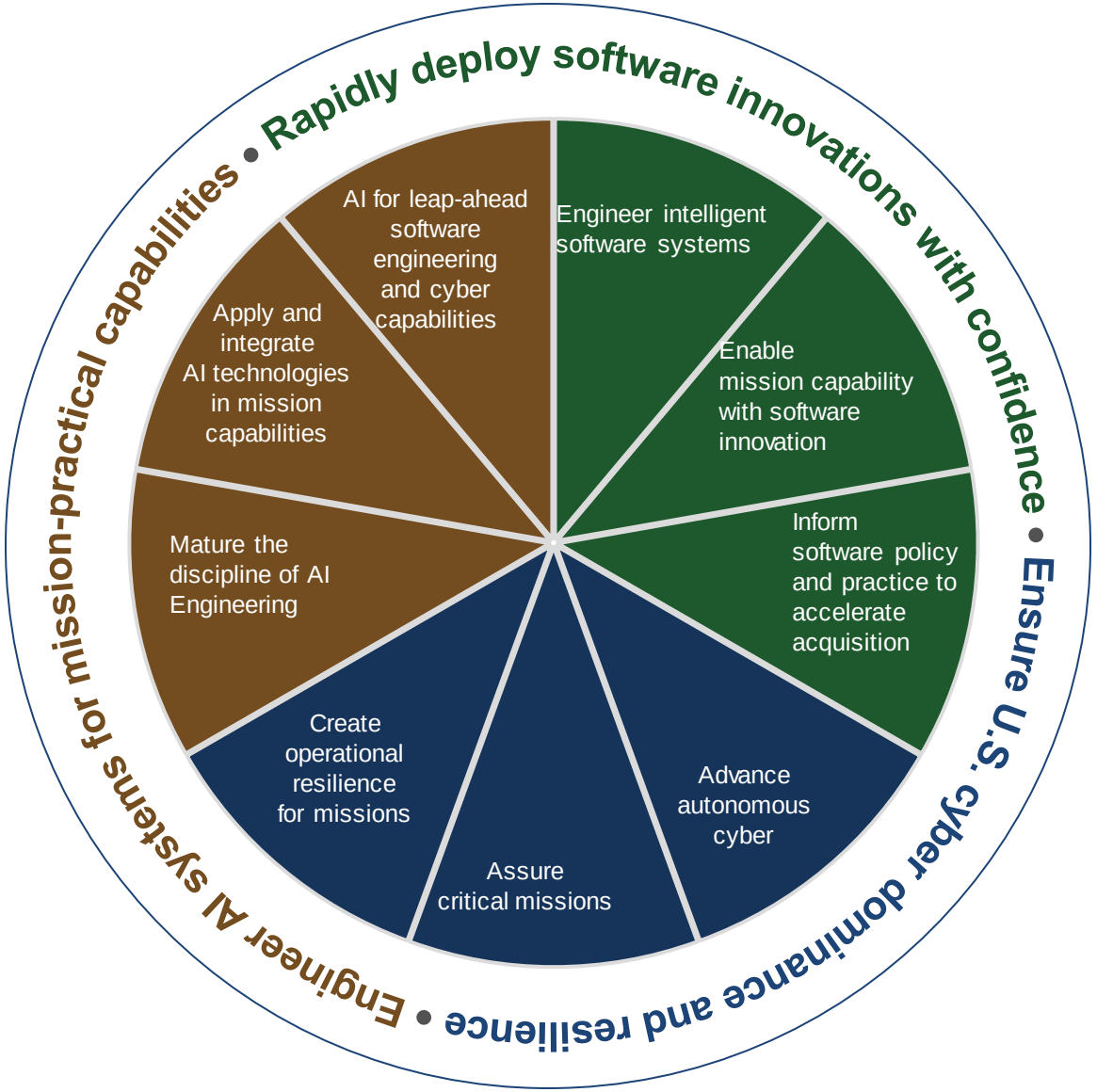
~610 staff members

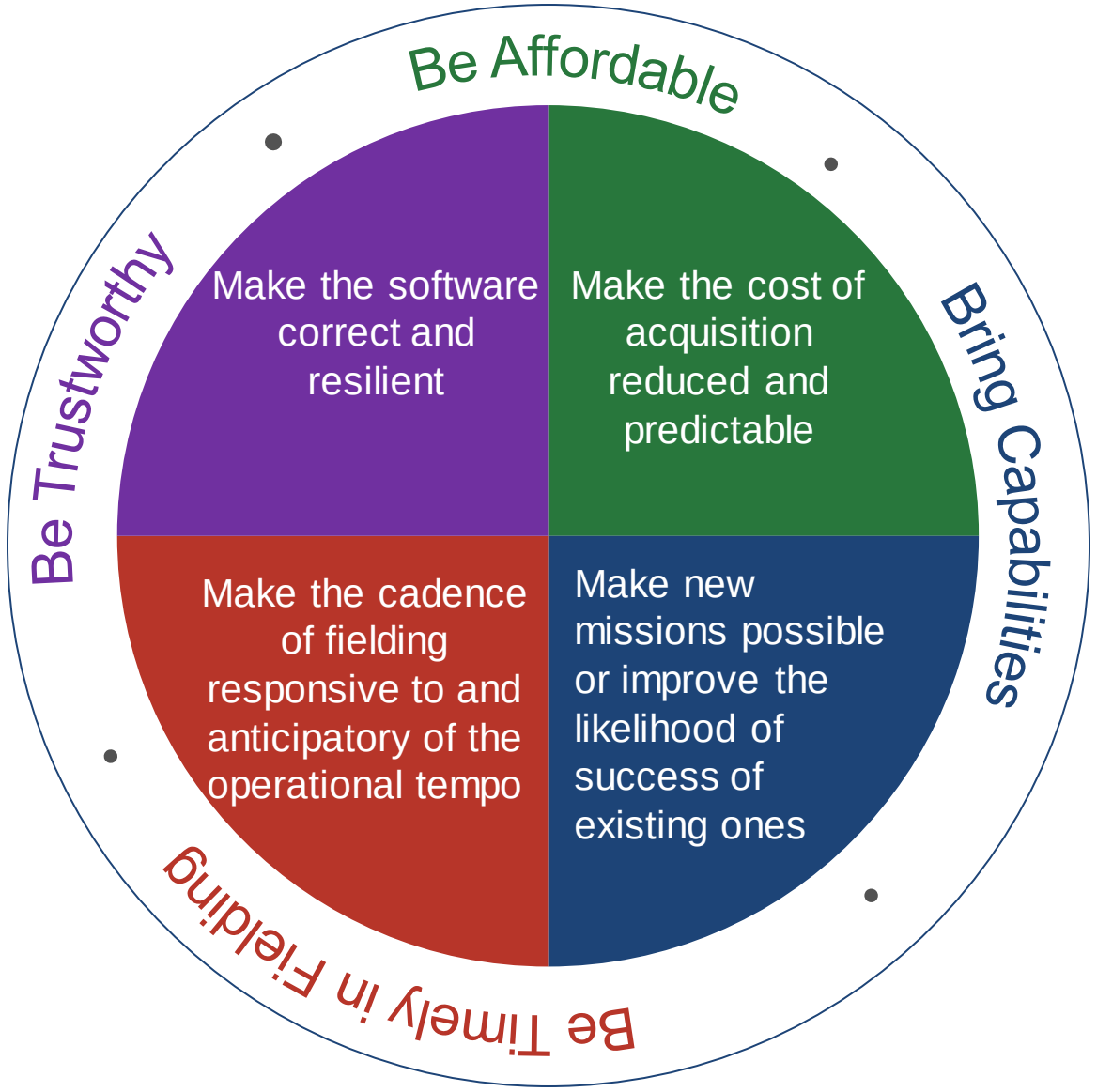
FY20 total funding $140M Offices in Pittsburgh and DC, with locations near customer facilities in MA, TX, and CA

Our Technical Work Portfolio connects:

- Software Acquisition & Engineering
- Cybersecurity & Resilience
- Emerging AI Approaches

For Greater Business / Mission Impact





The SEI **Helps Government Customers to:**

- Integrate efforts across multiple customer stakeholders
- Provide independent and unbiased analysis and recommendations
- Fill research gaps as needed for difficult problems
- Enable organizational transformation to Agile, DevOps, and Cloud
- Accelerate customer efforts to achieve government mandates e.g.: 'move to the cloud'
- Consider impacts of decisions on software acquisition, engineering, and cyber ops lifecycle

CMU SEI History with FAA

PWP #	Dates	FAA Contact	Area of Work	Key Deliverables
6-427A3	9/2019-6/2022	S. Mandalapu	Use of Machine Learning to Find the Worst-Case Execution Time of Avionics Software	FAA Reports / AI/ML Prototype Model
6-427B1	4/2018-9/2019	I. Venetos	Research in Self Adaptive Networks and Systems and Design Assurance Methods for Mixed Trust Environments	Reports and Self-Adaptive Network Demonstration
6-427A2	9/2015-9/2017	S. Mandalapu	Identifying Assurance Issues and Safety Risks of using Virtual Machines in Avionics Systems	Reports Discussing Assurance Issues for VMs, Available Assurance Tools, Timing and Verification Techniques, Potential Cyber Issues
6-427A1	9/2014-9/2016	S. Mandalapu	When is Software Too Complex to Certify?	FAA Report / Complexity Assessment Method

SEI support for FAA's Research Organizations

A National Agenda for Software Engineering Research and Development (NA4SE): Architecting the Future of Software Engineering

Anita Carleton, John Robert
November 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

CMU SEI Released Study on the Future of Software Engineering R & D: Vision, Research Focus Areas, Research Roadmap

The CMU SEI National Agenda for Software Engineering R&D Study is now live on our website. https://sei.cmu.edu/news-events/news/article.cfm?assetId=741319

CMU Software Engineering Institute Asserts Bold Vision for Engineering Future Software Systems

Summary of Study Findings

1. **Maintaining national software engineering proficiency is a strategic advantage**. Software engineering affects everything, because software is everywhere.

2. **Maintaining national software engineering proficiency requires sustained research.** New types of systems will continue to push beyond the bounds of what current software engineering theories, tools, and practices can support.

3. **Maintaining national software engineering proficiency requires fostering strategic partnerships.** We need to enable strategic partnerships and collaborations to drive innovation in software engineering research among industry, research laboratories, academia, and government.

4. **Maintaining national software engineering proficiency requires sustained investment.** We must ensure policy makers recognize the benefits of software engineering as a critical national capability.

5. **The vision of software engineering needs to change.** The current notion of a software development pipeline will be replaced by one where AI and humans collaborate to continuously evolve the system based on programmer intent.

6. **Focusing on re-assuring systems will enable continuous and rapid incorporation of new capability.** Because software is ubiquitous there is an increasing need for software to continuously evolve to include new capability.

7. **New design principles are needed for societal-scale systems.** The growing recognition of software's impact is generating new quality attribute requirements for which better design approaches are needed.

8. **The software engineering workforce needs to be (re-)conceived.** We need to better understand the nature of the needed workforce and what to do to foster its growth.

Emerging Vision of the Future of Software Engineering

The current notion of software development will be replaced by one where the software pipeline consists of humans & AI as trustworthy collaborators that rapidly evolve systems based on programmer intent.

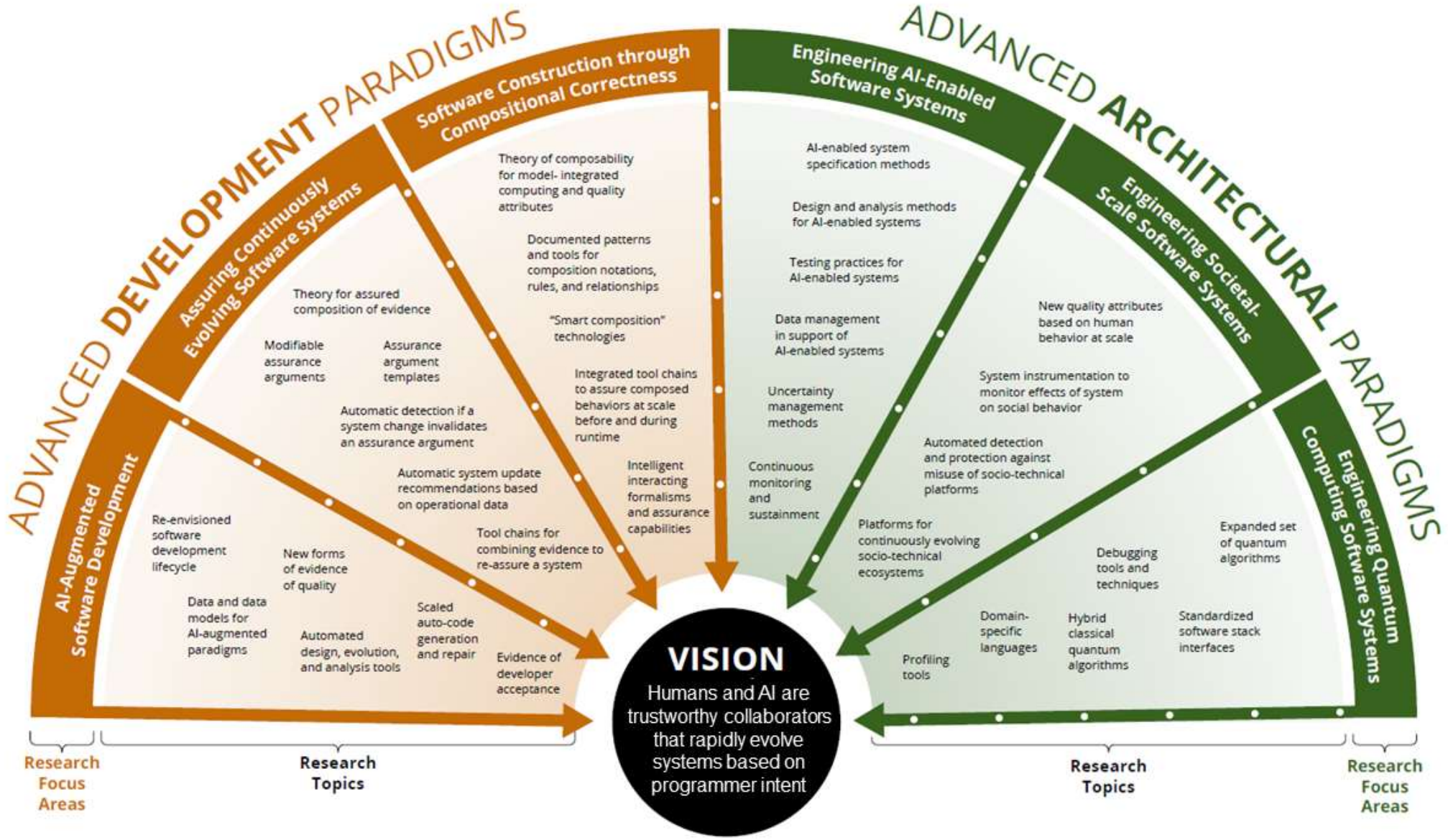
Advanced development paradigms lead to efficiency & trust at scale.

- Humans leverage trusted AI as a workforce multiplier for all aspects of software creation & sustainment.
- Formal assurance arguments are combined & analyzed to assure & efficiently (re)assure continuously evolving software.
- Enhanced software composition mechanisms enable predictable construction of systems at increasingly large scale.

Advanced architectural paradigms enable the predictable use of new computational models.

- Theories & techniques drawn from social sciences are used to design large-scale socio-technical systems, yielding more predictable outcomes.
- AI & non-AI components interact in predictable ways to achieve enhanced mission, societal, & business goals.
- New analysis & design methods facilitate the development of quantum-enabled systems.

Software Engineering Research Roadmap (10-15 Year Horizon)



Research Focus Areas: Development Paradigms

AI-Augmented Software Development

The focus of this research area is on what AI-augmented software development will look like at each stage of the development process & during continuous evolution, where it will be particularly useful in taking on routine tasks.

Assuring Continuously Evolving Systems

The goal of this research area is to develop a theory & practice of rapid & assured software evolution that enables efficient & bounded reassurance of continuously evolving systems.

Software Construction through Composition

This research area focuses on methods & tools that enable the specification & enforcement of composition rules for component-based technologies & platforms that allow both the creation of required behaviors & the assurance of these behaviors.

Research Focus Areas: Architectural Paradigms

Engineering AI-Enabled Software Systems

This research area focuses on exploring which existing software engineering practices can reliably support the development of AI systems, as well as identifying & augmenting software engineering techniques for systems with AI components.

Engineering Societal-Scale Software Systems

This research area leverages the social sciences to develop new software engineering approaches that enable predictable behavior of software systems consisting of people as system components.

Engineering Quantum Computing Software Systems

Our goals in this research area are to first enable current quantum computers to be easily programmed, & then enable increasing abstraction as larger, fully fault-tolerant quantum computing systems become available.

Recommendations

Our goal is to catalyze change that advances software engineering, which in turn will lead to more trustworthy and capable software-reliant systems in the future. Advancing software engineering requires supportive policy, research funding, researchers, practitioners, and cross-fertilization with other research communities.

Research recommendations are necessary to catalyze change.

1. Enable AI as a reliable system capability enhancer.
2. Develop a theory and practice for software evolution and re-assurance at scale.
3. Develop formal semantics for composition technology.
4. Mature the engineering of societal-scale socio-technical systems.
5. Catalyze increased attention on engineering for new computational models, with a focus on quantum-enabled software systems

Enactment recommendations focus on institutional obstacles, including economic, human, and policy barriers.

6. Investment priorities should reflect the benefits of software engineering as a critical national capability.
7. Institutionalize ongoing advancement of software engineering research.
8. Develop a strategy for ensuring an effective workforce for the future of software engineering.

Policy & Practice Enabling Agile Acquisitions

Eileen Wrubel, Nanette Brown
November 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Policy & Practice Enabling Agile Acquisitions

The SEI provides data-driven analysis and technical leadership in support of software acquisition policy modernization.

A major area of work is execution and empirical study of pathfinder programs which support true *evidence-based policies,* e.g. for:

- Agile / iterative software practices (Can DoD programs deliver capabilities on radically faster cycle times?)
- Single software appropriation (How is modern software practice supported when programs don't have to budget separately for software RDT&E, O&M, and procurement?)
- Consumption-based pricing models (How can we effectively marry elastic pricing / consumption models, e.g. for Cloud services, with traditional processes?)

…and building out guidance to support execution on topics like **architecture**, **technical debt**, **DevSecOps organizational models**

Impact

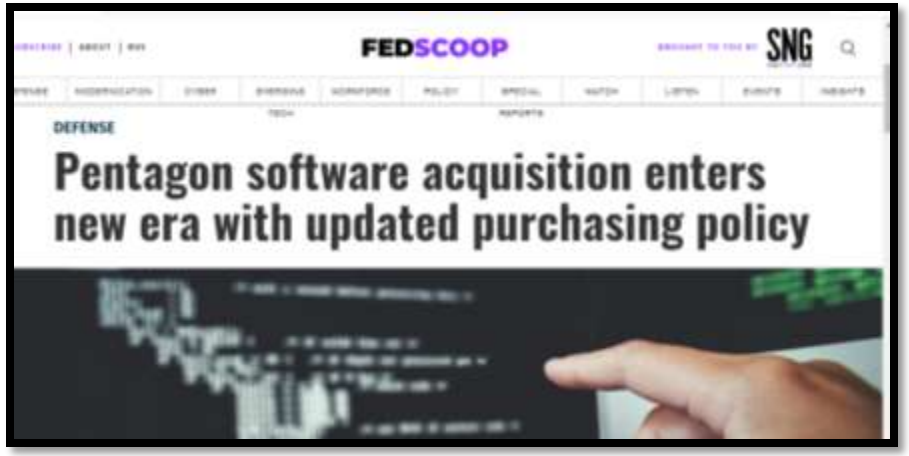
SEI technical teams advised the DoD in the development, piloting, testing, and updating of the DoD's Software Acquisition Pathway, issued in 2020.

Our work is applicable to, and being used by, **programs across the Department**

Our team is working with many of the early adopters to continue to **learn and improve** the process & guidance

The policy is already supporting programs at delivering at much faster rates

Customer appreciates our team's "Superlative ability to rapidly translate … complex technical matters into ideas that can be readily communicated to the most senior audience in DoD and Congress."



"Software acquisition, widely seen as a 'nightmare' in the Pentagon, is getting a major update…"

"'You want to work at a pace that allows the users to deliver,' she said of software teams trying to bring new tools to the department."

Shift-left testing and digital engineering

FY20 National Defense Authorization Act Section 231, Objective:

"The Secretary of Defense shall establish a digital engineering capability to be used – for the development and deployment of digital engineering models for use in the defense acquisition process; and

to provide testing infrastructure and software to support automated approaches for testing, evaluation, and deployment throughout the defense acquisition process"

SEI's Role:

Collaborate with and advise the office of the Director, Operational Test and Evaluation (DOT&E) to improve its capabilities to assess the readiness of cyber-focused components in a an environment of continuous development and delivery

NDAA Sec231 Implementation Approach

Leadership

- Digital Engineering /Workforce Policy & Guidance Team - Philomena Zimmerman, Thomas Simms - R&E/EP&S
- Infrastructure Team - Ryan Norman - R&E/TRMC
- T&E Demo – Amy Henninger – DOT&E

Activities

- Select 4 – 10 Candidate Demo Programs
  - Satisfy Statute Requirements, Provide a Range of Digital Engineering Implementations and Applicable / Interesting Scenarios:
    The Program is using DE technology "Y" to accomplish testing "Z" in order to achieve benefit "A".
  - Outreach Mechanisms - Branch of Service Liaisons, DOT&E staff, Agile Pilot programs, Networking, Data Call
- Collect program data through interviews, document review, observation

Deliverables

- Infrastructure Plan
- Workforce Plan
- Comparative Analysis (Case Study) Report

NDAA Sec231Observations

Infrastructure and Ecosystems

Characterizing Digital Engineering (DE) Capabilities, Usage and Adoption Paths

Continuous Authority to Operate (cATO)

Digital Engineering's Impact on Shifting OT to the Left

Enabling bolder, faster, more adaptive acquisition of software-enabled capability

	Software Acquisition Pathways	Software Engineering Measurement & Analysis
Problem to be Solved	Identify new acquisition innovations to field software enabled capability to deliver at the speed of relevance by changing acquisition to be rapid, iterative, and continuous.	Investigate and apply new analytical methods to improve understanding and decision making of systems and acquisition, development and sustainment processes
Technology	Application of continuous delivery activities throughout the acquisition lifecycle including automation that connects acquisition business toolchains to development toolchains.	Statistical, machine learning, and causal learning techniques combined with experimental and quasi-experimental designs; creating and managing datasets relevant to mission and agency needs
Outcomes	•Develop and apply tools that automate acquisition practices and dataflow. •Updated acquisition guidance and practices •Acquisition guidance to support new/disruptive technologies and methods •Improved competition and innovation (broader ecosystem with new innovators)	• Decision support algorithms, models, and prototypes • Curated datasets • Causal knowledge to enhance decision making efficiency and effectiveness • Automated metrics to inform data driven decisions

Skills	•Acquisition strategy, contracting, and planning
	•Enterprise systems
	•Prototyping of acquisition approaches and tools
	•Intellectual property strategies
	•Acquisition, sustainment policy development
		• Data science
		  ○ Quantitative analytical expertise including machine learning and statistics
		  ○ Data management
		  ○ Experimental design
		• Prototype development
		  ○ Data visualization
		  ○ Statistical and ML programming and tools
		• Qualitative analytical methods
		  ○ Expert judgment elicitation
		  ○ Text analysis
		•Enterprise data strategies

Agile In Government

Will Hayes
November 2021

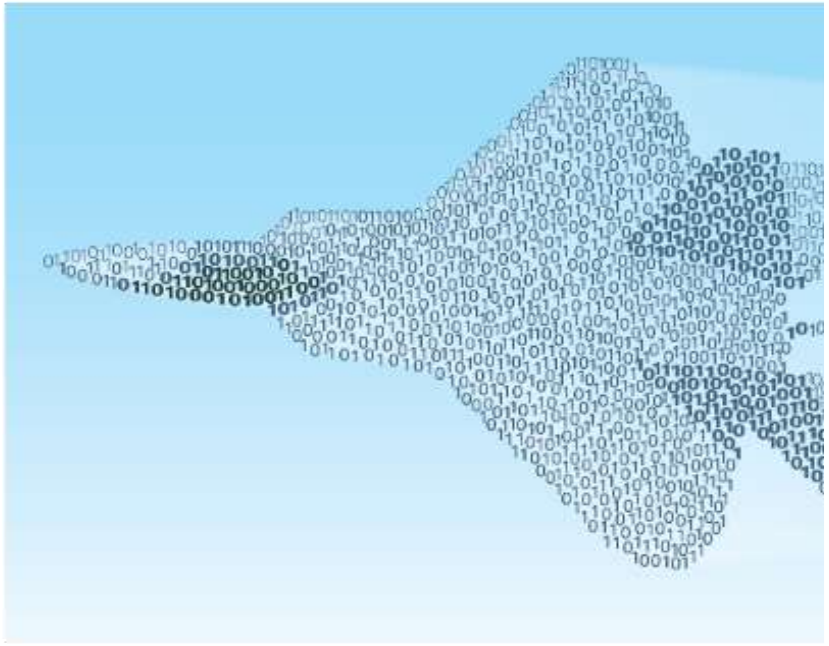
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Agile in High-Stakes Environments

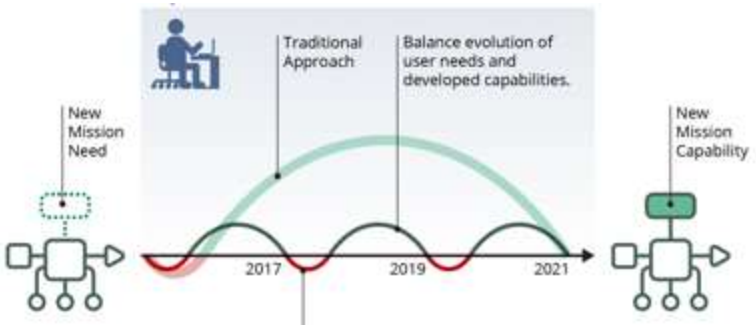
Orchestrating *Rapid Incremental Delivery* requires discipline

- Architecture
- Good Design
- Quality Code
- Effective Test
- Cyber Security
- Independent V&V

Poor Quality Does Not Scale



Enterprise-Scale Lean/Agile Delivery Capability



Scaling agility from the software project to the enterprise involves a host of socio-technical challenges

Enterprise Strategy Development - Expand rapid, incremental delivery models up and down the value stream. We deploy agile and lean strategies beyond software development to strategically improve enterprise capabilities:

- Measuring flow and delivery of value
- Simulation-rich CI/CD pipelines
- Systems Engineering discipline applied as intended, to the process and product
- Proactive accumulation of assurance information required for certification

Rapid Engineering Adoption - Implement best-of-breed incremental methods in environments where high levels of engineering discipline are necessary in complex, mission-critical cyber-physical products.

Architecturally-Aware Product & Process - Apply systematic view of enterprise architecture to the design of the product pipeline. Understanding the critical interplay of these systems enables rapid innovation through incremental change and AI, ML, MBSE adoption.

Coaching - We advise leaders and teams through iterative adoption of Lean, Agile methods in complex government/industry collaborations. Shoulder-to-shoulder coaching builds lasting organic capability.

Training - Our experienced instructors provide engaging classroom and virtual workshops for organizational and cultural change. Custom design for alignment with enterprise context uses table top exercises with real challenges instead of toy examples.

Assessment - We assess organizations' breadth of diffusion as well as depth of infusion for Lean/Agile approaches. Building beyond an inventory of practices, we focus on unique readiness and fit for transition of new methods.

Organizational Design and Capability Evolution - We design and support path-finding efforts and pilots for the evolution of the enterprise. Orderly experimentation and enterprise adoption of promising changes support a sustained focus on capability delivery.

SEI Agile Virtual Schoolhouse

Content

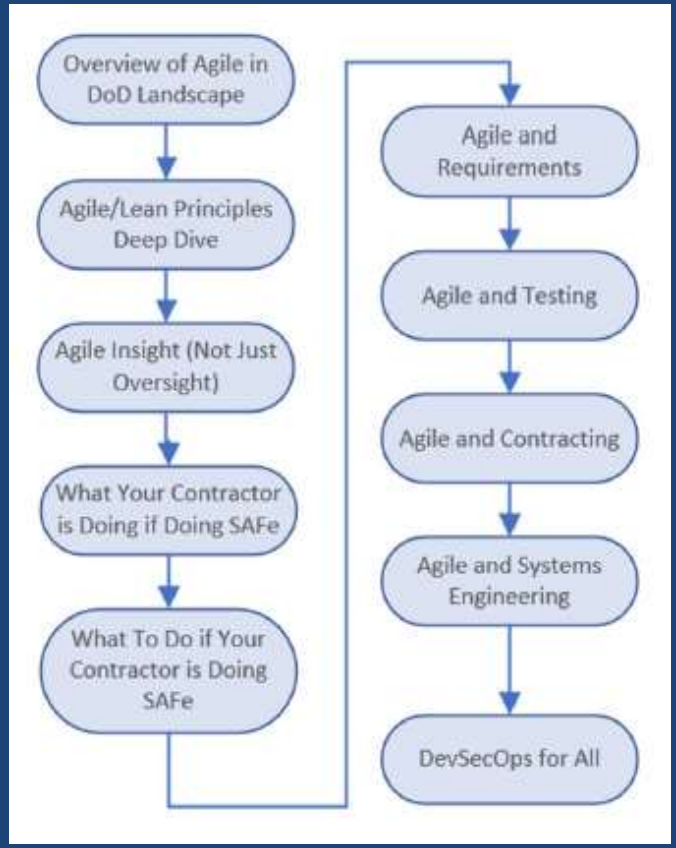
Each Agile Virtual Schoolhouse delivery is customized to address the goals of the audience. We often recommend that the learning begins with introduction to the Agile/Lean principles that inform organizational change. We then build upon those fundamentals by exploring how to implement principles into software-intensive programs.

Format

Each Learning Package has two key elements:

1. SELF-STUDY ASSIGNMENT: This is a curated collection of publicly available resources on the Agile topic to introduce key insights.
2. LIVE VIRTUAL CLASS: An SEI subject matter expert will deliver a two-hour online lecture and facilitate group discussion. This live interaction provides a richer exploration of how to implement insights introduced in self-study.

Sample
Learning Package Map



Publicly Available Example

NASA IV&V

Agile approach to assuring the safety-critical embedded software for NASA's Orion spacecraft

IEEE Aerospace Conference 2019

https://ieeexplore.ieee.org/document/8742095

Orion EM-1 Mission Overview

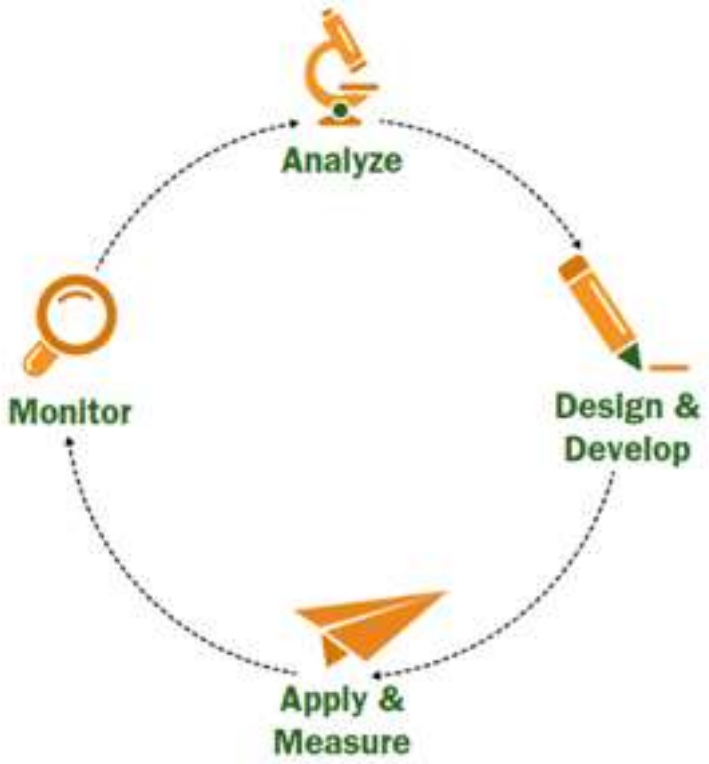
IV&V Program

DevSecOps Initiatives

Hasan Yasar

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

DevSecOps Innovations and Solutions



Analyze Analyze an organization's business goals, processes, and development/operational challenges to assess the status quo, bottlenecks, and areas that could get maximum impact from process improvement efforts.

Design & Develop - Develop a customized strategy and roadmap to improve organizational culture, process, and tools to support business needs and improve software development quality, transparency, and delivery while decreasing risk.

Apply & Measure - Provide tools and methods to enable process measurement capabilities. Apply a process improvement strategy according to the developed roadmap and measure the quantitative impact of DevOps on metrics for collaboration, quality, transparency, and process efficiency.

Monitor - Enable development managers and teams to independently monitor DevOps practices and engage in continuous data-driven improvements to tools and methods according unique organizational needs.

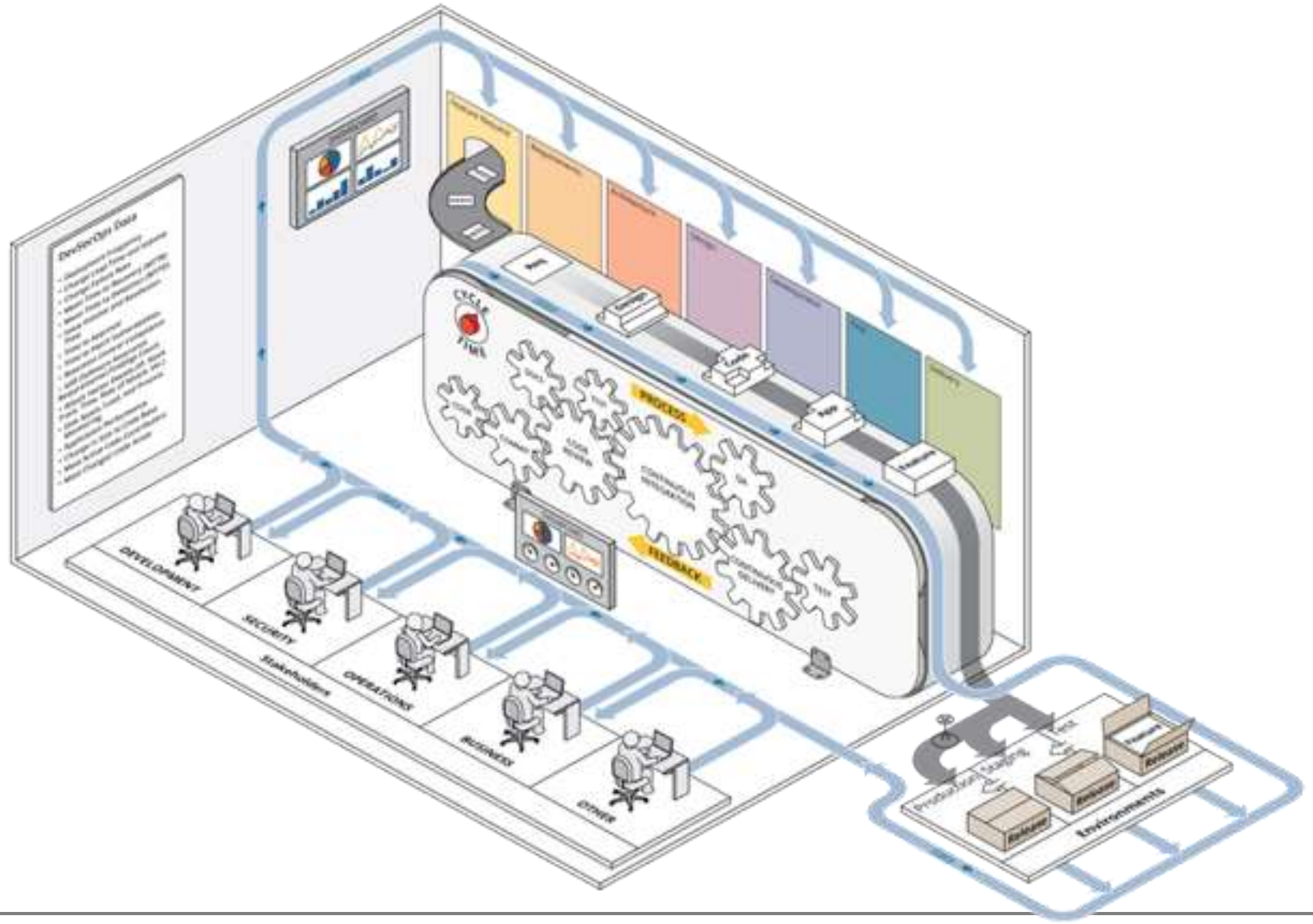
Training - We provide onsite or virtual courses that teach DevOps to managers, technical teams, and other stakeholder groups. We also offer advanced, hands-on DevOps training for development and operational teams that includes processes, tools, and practices.

Workshops - We conduct customized, hands-on workshops that provide comprehensive exercises to deliver practical training in DevOps tools and techniques throughout the SDLC, from inception to production.

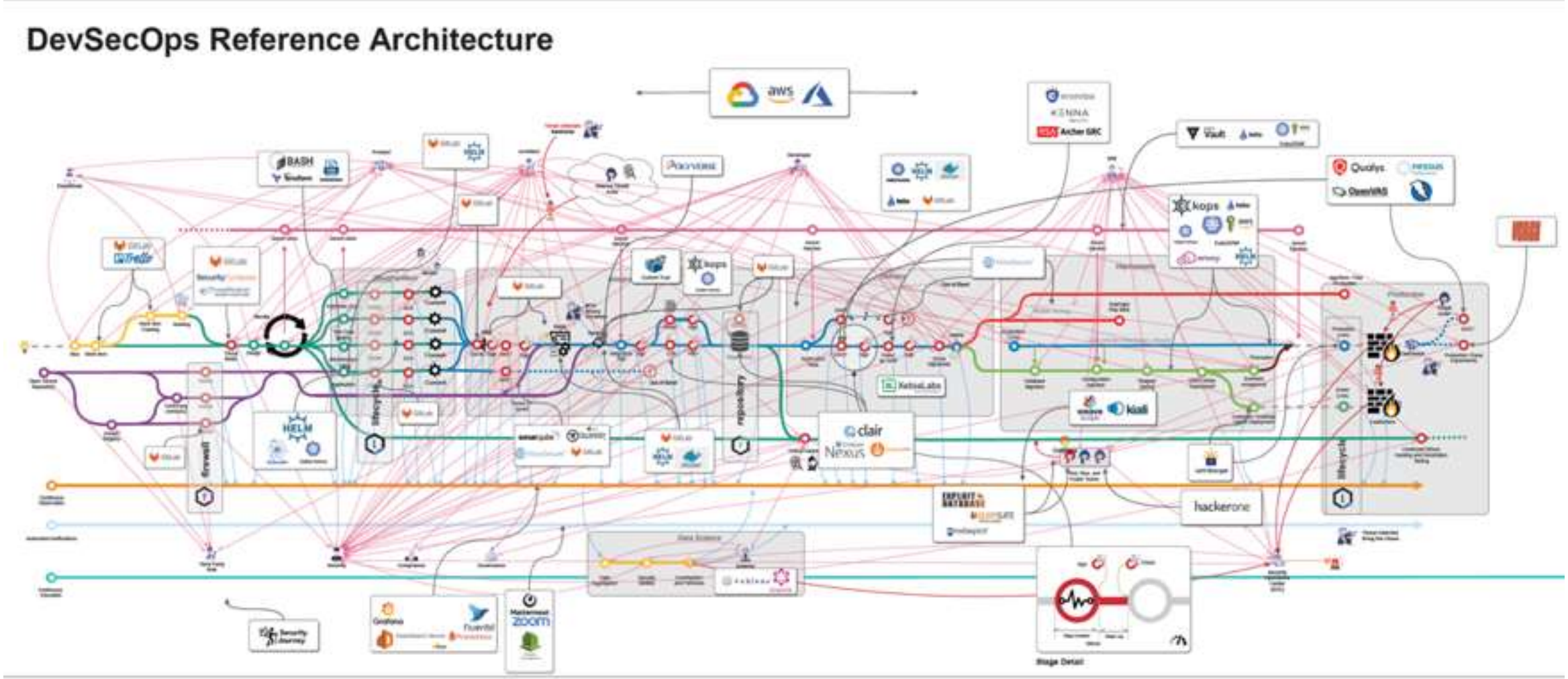
Mentoring - By collaborating closely with teams and stakeholders, we facilitate cultural integration and assist in establishing practical guidelines to improve existing DevOps strategies and enhance collaboration among organizational teams.

Engineering Support - Our highly experienced engineers assist in the implementation and measurement of DevOps tools and processes.

DevSecOps/SW Factory Concept



But It's getting really complicated to build



DevSecOps in Complex Systems

Emerging technology challenges: Incorporation of AI/ML models built, trained, tested, and validated within the pipeline

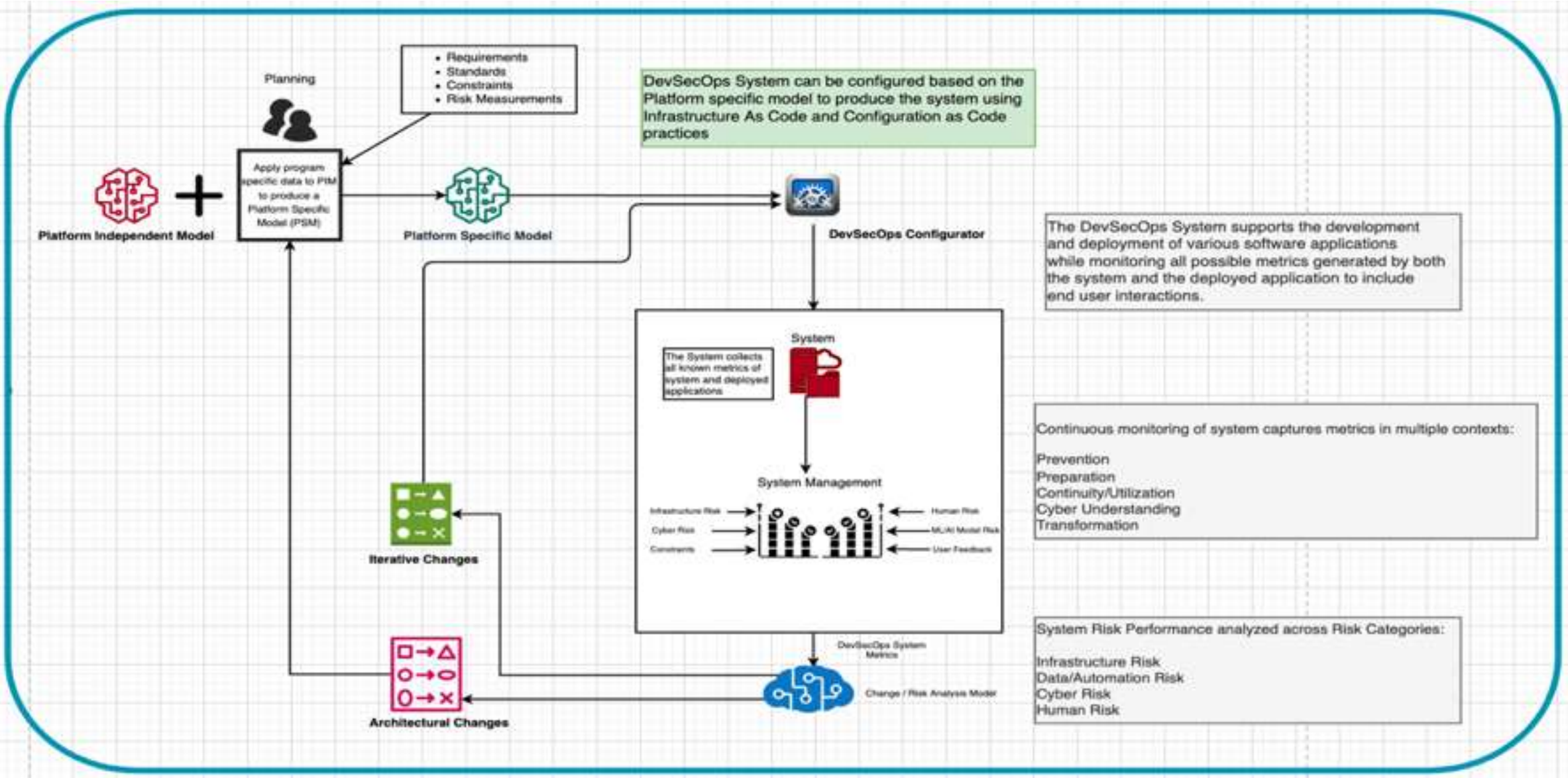
Hardware in the Loop challenges: Application to Large Highly Regulated, Cyberphysical Systems of Systems

Governance and collaboration challenges: Evolution of oversight, evaluation, and collaboration practices for nimble delivery of value

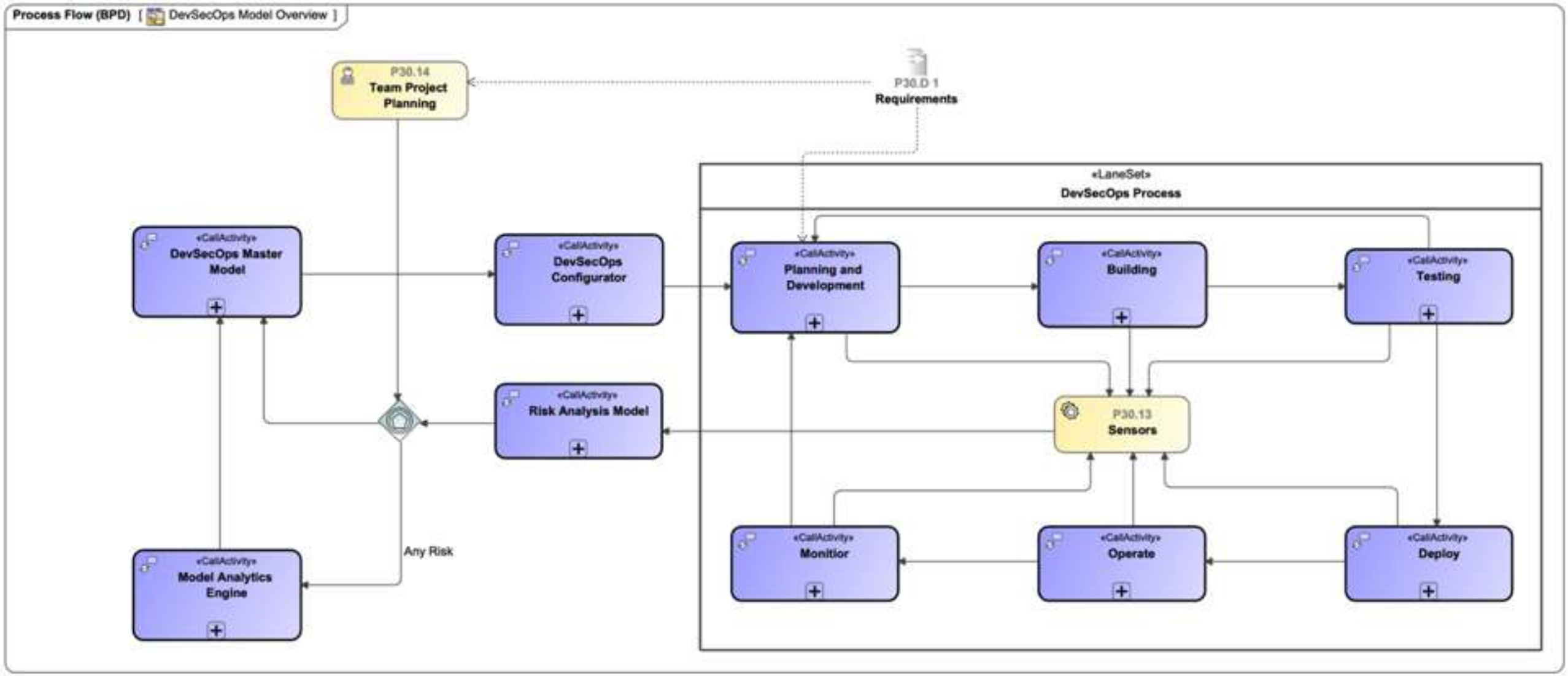
Architectural challenges: Compatible architecture that supports iterative and incremental development

Current Research Studies

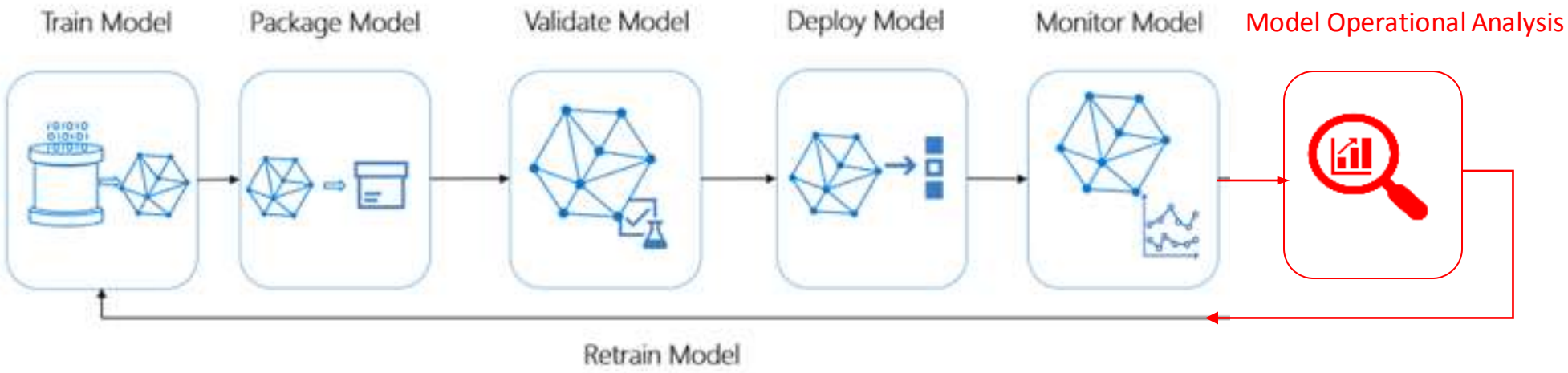
Resilience Engineering



Modelling DevSecOps environment



Integrate the Analyses performed by the Data Scientist into the MLOps pipeline



Model Operational Analysis should perform the first three steps of the model retraining process

1. [Analyze] Statistical analysis between the production data and development data
2. [Audit] Audit model performance
3. [Select] Integration of development and production data into a new development data set, with weights

Diagram Adapted from MS Azure MLOps Pipeline

Published Recent Papers

Security Impacts of Sub-Optimal DevSecOps Implementations in a Highly Regulated Environment ACM publication https://dl.acm.org/doi/10.1145/3407023.3409186

Guide to Implementing DevSecOps for a System of Systems in Highly Regulated Environments

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=638576

Closing Discussions

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

In Summary

The SEI is pleased to have a long-term relationship with the FAA

Working on past projects have benefited both the SEI and US citizens

- FAA is able to take advantage of research and methods sponsored by DoD
- SEI continues to learn about acquisition, engineering, governance, and resilience needed for safety-critical systems of systems

The SEI has a wide skill-set, how can we best help?

We are pleased to present BAA or other proposals, at FAA's request!

Background

Rapidly Deploy Software Innovations with Confidence

Photo: Adnan Akram, Aug 2019

Strategy	Representative Portfolio
Engineer intelligent software systems	• Assuring autonomous cyber-physical systems • Cyber physical system modeling and analysis • AI for continuous verification and validation • Real-time multicore systems
Enable mission capability with software innovation	• Automating architecture analysis and repair • Assuring ML/AI systems • Cyber resiliency code analysis for embedded systems • Securing tactical systems • Modernizing legacy systems
Inform software policy and practice to accelerate acquisition	• AI to improve mission decision making • DevSecOps for embedded mission-critical systems • Transform the acquisition ecosystem

Ensure Cyber Resilience

Photo: NOAA National Hurricane Center

Strategy	Representative Portfolio
Assure critical missions	• Measures of effectiveness for cyber assurance • Measures of cyber resilience • Continuous integrity assurance • Security-instrumented lifecycles • Data pipeline security • AI/ML supply chain risk mitigation • AI threat modeling
Create operational resilience for missions	• Identifying, responding to, and recovering from attacks on AI and autonomous capabilities • State-of-the-art cyberspace and cyber-kinetic simulators, platforms, and APIs • Mission-specific readiness development • Cyber monitoring and defense mechanisms • Methods to design in, build in, and rigorously quantify operational cyber resilience
Advance autonomous cyber	• Continuous and on-demand assessment and mitigation • Situational awareness using autonomy/ machine learning • Techniques to improve human-machine team performance • Methods for trust and explainable reasoning

Engineering AI Systems for Mission-Practical Capabilities

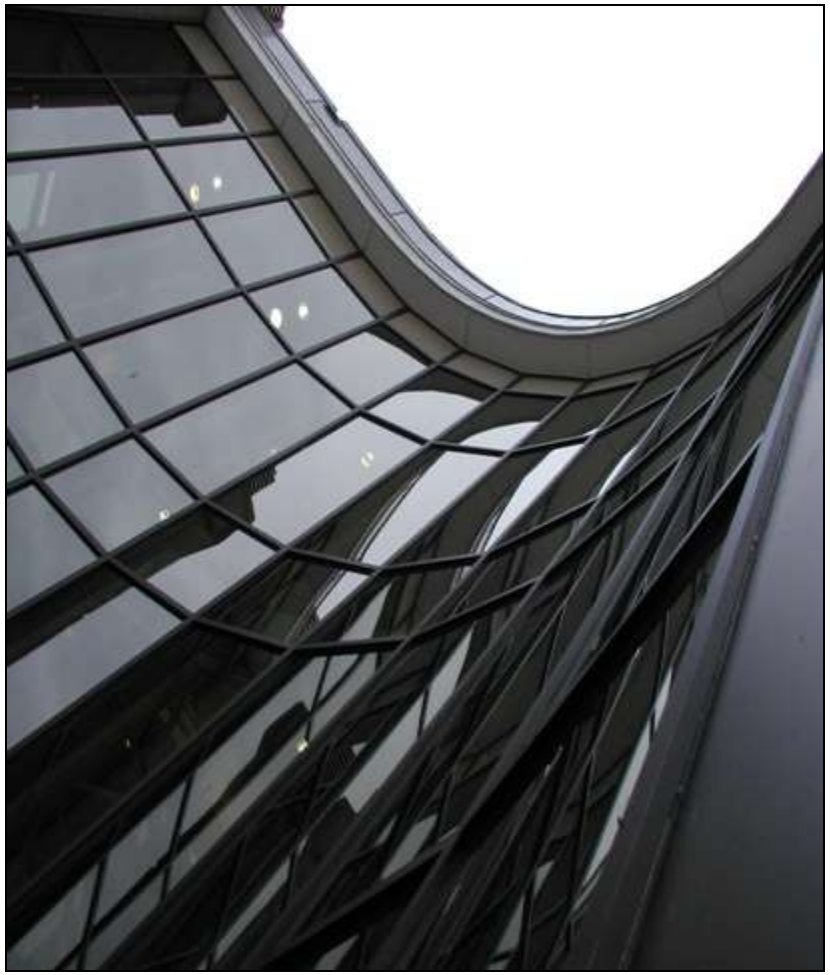


Photo: National Oceanographic and Atmospheric Administration

Strategy	Representative Portfolio
Mature the discipline of AI Engineering	• Mismatches in ML-enabled systems • Engineering of AI systems in an uncertain environment • Autonomous system design for human-machine teaming
Apply and integrate AI technologies in mission capabilities	• Application of principled imitation methods to real-world tasks • ML for patterns of life in video • AI for remote sensing
AI for leap-ahead software engineering and cyber capabilities	• Metrics for security, privacy, and scalability • Prototype tooling and a test harness for V&V • Improving human decision making with AI decision support systems • Computational graph/AI/ML primitives for HW/SW co-optimization • Best practices for AI-enabled cyber decision support system design • Practical neural network defenses