



**SYSTEMS ENGINEERING**  
Research Center

## **Quantitative Risk – Phase 1**

**A013 - Interim Technical Report SERC-2013-TR-040-1**

May 29, 2013

Research Team:

Dr. Roshanak Nilchiani, Dr. Stan Rifkin, Dr. Ali Mostashari,

Stevens Institute of Technology

Dr. Walt Bryzik, Dr. Gary Witus,

Wayne State University

# Report Documentation Page

Form Approved  
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>29 MAY 2013</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2013 to 00-00-2013</b>	
4. TITLE AND SUBTITLE <b>Quantitative Risk - Phase 1</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Stevens Institute of Technology, Systems Engineering Research Center, Castle Point On Hudson, Hoboken, NJ, 07030</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <b>A novel approach to technical risk identification and analysis for major weapons systems acquisitions is proposed. It is informed by the limitations of the current risk matrix. The approach is to examine representations of the evolving system design to locate sources of complexity and then inform the program manager as he/she makes technical choices among competing alternatives. Some of the alternatives will create more complexity and therefore more risk. The PM will then be able to balance risk and reward at the point of decision-? making deciding to engage risk at that moment by his/her choices. In addition we propose to rate or score the contractor + government organizations' abilities to master the complexity they have chosen so that the PM will know whether there is a match of product complexity with organizational capability. Future work will add dimensions of interconnections and interdependencies among risks timing delay order of risks and uncertainty.</b>					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>35</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

Copyright © 2013 Stevens Institute of Technology, Systems Engineering Research Center

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 H98230-08-D-0171. 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 author(s) and do not necessarily reflect the views of the United States Department of Defense.

#### NO WARRANTY

THIS STEVENS INSTITUTE OF TECHNOLOGY AND SYSTEMS ENGINEERING RESEARCH CENTER MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. STEVENS INSTITUTE OF TECHNOLOGY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. STEVENS INSTITUTE OF TECHNOLOGY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use by SERC, SERC Collaborators and originators : \* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

#### External use:\*

Academic Use: This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission, provided the copyright and "No Warranty" statements are included with all reproductions.

Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Systems Engineering Research Center attn: dschultz@stevens.edu

\* These restrictions do not apply to U.S. government entities.

## **ABSTRACT**

---

A novel approach to technical risk identification and analysis for major weapons systems acquisitions is proposed. It is informed by the limitations of the current risk matrix. The approach is to examine representations of the evolving system design to locate sources of complexity and then inform the program manager as he/she makes technical choices among competing alternatives. Some of the alternatives will create more complexity and therefore more risk. The PM will then be able to balance risk and reward at the point of decision-making, deciding to engage risk at that moment by his/her choices. In addition, we propose to rate or score the contractor + government organizations' abilities to master the complexity they have chosen, so that the PM will know whether there is a match of product complexity with organizational capability.

Future work will add dimensions of interconnections and interdependencies among risks, timing, delay, order of risks, and uncertainty.

## TABLE OF CONTENTS

---

<b>Abstract .....</b>	<b>3</b>
<b>Table of Contents.....</b>	<b>4</b>
<b>Figures and Tables .....</b>	<b>5</b>
<b>Challenges .....</b>	<b>6</b>
<b>1. Risk management is many processes .....</b>	<b>6</b>
<b>2. Forecasting risk is difficult and subjective .....</b>	<b>7</b>
<b>3. Risk identification is almost always post hoc.....</b>	<b>8</b>
<b>Our Approach and Its Justification .....</b>	<b>8</b>
<b>Summary .....</b>	<b>8</b>
<b>A. Objective Assessment.....</b>	<b>9</b>
<b>B. Quantifiable assessment.....</b>	<b>9</b>
<b>C. Aid in Decision Making .....</b>	<b>9</b>
<b>D. Time is a variable, risks are interconnected.....</b>	<b>9</b>
<b>E. Advances in Risk mangement: Where to Look.....</b>	<b>10</b>
<b>Connecting technical risk and types of complexity .....</b>	<b>13</b>
<b>A. A few definitions .....</b>	<b>13</b>
<b>B. How complexity manifests as technical risk .....</b>	<b>15</b>
B.1 Mechanisms and examples.....	15
B.2 Risk and Complexity Correlation.....	18
<b>C. Deriving Project Risk from Technical Complexity and Contractor Organizational Capabilities. 23</b>	
<b>D. Architectural-level Complexity Measures for Acquisition Systems: Summary of Case Studies 25</b>	
<b>E. Measuring Architectural Level Complexity: Initial Explorations .....</b>	<b>27</b>
<b>C. The fit between technical risk of the product and an organization's capability to manage it .. 30</b>	
<b>D. The places of case studies and quantitative data .....</b>	<b>30</b>
Examples and Some Case Studies .....	31
<b>IV. Next steps.....</b>	<b>34</b>

## FIGURES AND TABLES

---

<b>Figure 1.</b> DoD Risk Management Process (from <i>DoD Risk Management Guide</i> , 2006, p. 4) .....	7
<b>Figure 2.</b> Map of the leading scholars and areas of research in the complexity sciences.....	14
<b>Figure 3.</b> An output varying regularly about a mean value that is its target, showing the corrections that appear necessary at each time epoch when the measurement is made. (Beer, 1979), p. 60.....	16
<b>Figure 4.</b> Explosive behavior induced by the direct application of error corrections to a system that has reversed its input states by the time the correction is applied. (Beer, 1979), p. 60 .....	17
<b>Figure 5.</b> Traditional Risk Reporting Matrix {US Department of Defense (Office of the Undersecretary of Defense (Acquisition, 2006 #1)}.....	18
<b>Figure 6.</b> The Complexity-Risk spiral. Insignificant uncertainties and risks in combination with structural complexity escalate into a fragile situation and to a point of no return at which failure is certain. 19	19
<b>Figure 7.</b> Structural complexity and risk (uncertainty) correlation in the DARPA F6 program.....	20
<b>Figure 8.</b> F6 Simulation results showing that increased structural complexity leads to shorter time to failure in the system. ....	21
<b>Figure 9.</b> Logical relationship between structural and functional complexity .....	22
<b>Figure 10.</b> Complexity-Uncertainty-Risk Environment (CURE) Cube .....	23

## CHALLENGES

---

“It is not possible to know exactly how a particular design will perform until it is built. But the product cannot be built until the design is selected. Thus, design is always a matter of decision making under conditions of uncertainty and risk” [(Hazelrigg, 1998), quoted in (Deshmukh, 2010), p. 128].

---

### 1. RISK MANAGEMENT IS MANY PROCESSES

Defined in the *DoD Risk Management Guide* (2006, p. 1),

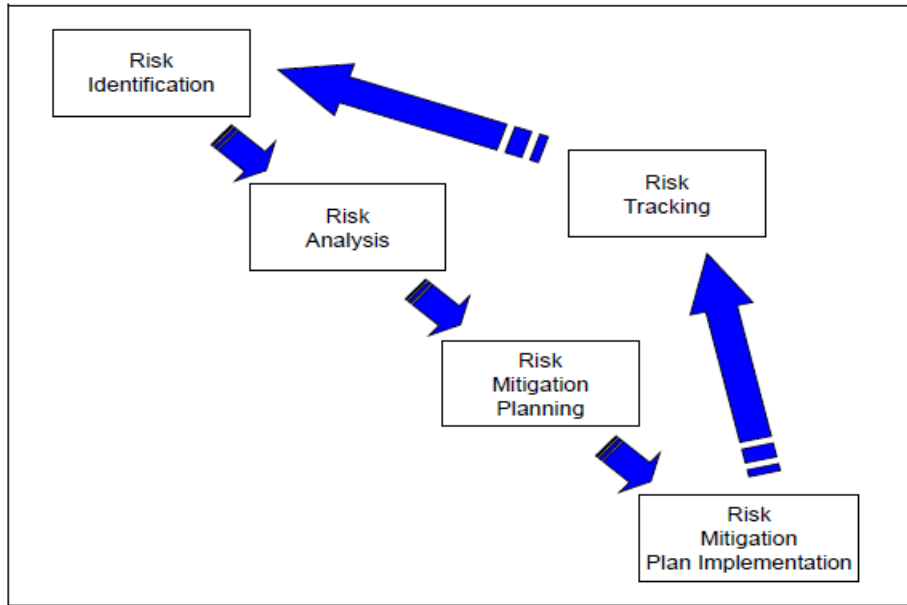
Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan,) .... Risk addresses the potential variation in the planned approach and its expected outcome.

Risks have three components:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at the present time of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to future root causes and their effects.

Further risk management is a number of processes:



**Figure 1.** DoD Risk Management Process (from *DoD Risk Management Guide*, 2006, p. 4)

Of these processes, which are the most important to practice, to "get right"? If we want to improve the management of technical risks, on which process(es) should we focus?

Our conjecture is that Risk Identification and Risk Analysis are key because, as in the Figure, everything else depends upon them. So, we are starting there.

## 2. FORECASTING RISK IS DIFFICULT AND SUBJECTIVE

As listed above, program management needs to collect and identify: future root causes, likelihood, and consequences. This is often, under the best circumstances, by assembling experts and asking them to converge on the three components. It is a group process and based on the extensive practical experience of the expert panel. It is necessarily subjective, based on the memories of the panel members and their analogic reasoning.

Tversky and Kahneman (see, for example, (Kahneman, Slovic, & Tversky, 1982)) are celebrated for their prospect theory, which explains how our biases interfere with our rational appraisals. They explain how our subjective judgments are susceptible to internal and also normative forces that cloud our perceptions and our reasoning. Accordingly, subjective assessments of technical risk are vulnerable to biases.

And this mentions nothing about the problem of using analogic reasoning, which is what expert team members often apply. The challenge in analogical reasoning is that the strength of the relevant similarities must outweigh the strength of any significant dissimilarity. But is that what happens when experts get together to evaluate risks? When one expert says, "This is just like Project X, so I can foresee



a risk of type A," is the analogy apt? Is it questioned? [Here is a list with examples of errors by analogy: <http://www.skeptdic.com/falseanalogy.html>]

Expert panels, in creating their subjective assessments, are susceptible to both biases and errors in analogical reasoning.

---

### **3. RISK IDENTIFICATION IS ALMOST ALWAYS POST HOC**

One part of the *Risk Management Guide* states, "Use a proactive, structured risk assessment and analysis activity to identify and analyze root causes, " (p. 5) and others state, "Use the results of prior event-based systems engineering technical reviews to analyze risks potentially associated with the successful completion of an upcoming review," (p. 5) and "During decomposition, risks can be identified based on prior experience, brainstorming, lessons learned from similar programs, and guidance contained in the program office RMP [Risk Management Plan]." p. 7.

Looking backwards to find risks is unassailable, except that it is applied by judgment and analogy and therefore subject to bias and error. For all of the looking backwards, the purpose is to predict the future. Where is the justification of the predictions?

## **OUR APPROACH AND ITS JUSTIFICATION**

---

---

### **SUMMARY**

Our approach is to characterize aspects of the technical products being developed in a way that would inform a program manager about to make decisions by weighing alternative technical courses of action. We would score or rank the alternatives based on the relationship that each alternative would incur future risk.

The result of our research would be a scorecard, dash board, or workbench that the program office operates before each major technical decision. The workbench would be fed information about the nature of the product alternatives and based on that would compute the relative attractiveness of each option with respect to incurring future risk.

In addition to examining characteristics of the product, the workbench would also scrutinize the match between the characteristics of the product and the characteristics of the developing organization, as risk can arise relative to an organization's capability to develop a certain product alternative.

As our research progresses, we intend to add capabilities to take into account the order and timing of decisions, their cascade effects, and the impact/influence of uncertainty.

We are taking this approach for a number of reasons:

1. The current method of risk characterization, measurement, and mitigation has not improved even though the Department of Defense has spent tens of millions of dollars on research to improve it. Evidently the research results have not proven useful.
2. We have all heard the remark, usually made informally by those who see many major weapons systems acquisitions, that by the time the real issues become visible it is very late and the effects have spread. We seek to identify risky courses of action at the time they are being considered for selection. This is very early in the unfolding of the systems development, hopefully in time to take alternative steps if unaddressed impacts are discovered.

---

#### **A. OBJECTIVE ASSESSMENT**

Our approach does not use any judgment, only objective measures of the product and of the organization's capability to create the product. Accordingly, we hope to circumvent the subjective biases that can be found in the current DoD risk identification and analysis practices.

---

#### **B. QUANTIFIABLE ASSESSMENT**

We seek to compute characteristics about the product alternatives and about organizational capability, so the outputs of our analysis would be quantities that would aid program management in making decisions among competing technical alternatives.

---

#### **C. AID IN DECISION MAKING**

Since our approach is a tool to be used during decision-making, we are not taking a retrospective view per se, but rather trying to give the PM information in order to avoid risk, that is, avoid encountering a state of nature that potentially would have unacceptably high likelihood and consequence.

---

#### **D. TIME IS A VARIABLE, RISKS ARE INTERCONNECTED**

There is no explicit time dimension in the current DoD risk management practice. We, on the other hand, see technical risks as largely interdependent/interconnected, so the order in which the technical decisions are considered matters. Accordingly, as our research progresses we intend to be able to present a program manager with the options during decision-making of understanding the effects of deferring or accelerating certain technical decisions.

In addition, time plays another important role in risk because time delay between cause and effect interferes with our ability to connect the two, our ability to reason about what the root causes are of untoward and/or unexpected program outcomes. Therefore, characterizing the time-dependent (that is, dynamic) flow through the program and technical product structures is crucial to identifying real, latent causes, not just their surface symptoms, such as cost and schedule over-runs.

---

#### **E. ADVANCES IN RISK MANGEMENT: WHERE TO LOOK**

A great deal of work already has been done on improvements to risk identification and risk analysis. For example, the DoD has sponsored:

The Software Engineering Institute's Risk Program for several decades.

University of Virginia's Center for Risk Management of Engineered Systems for several decades.

Research at the Air Force Institute of Technology and Naval Postgraduate School for decades.

Research and application at its FFRDCs, such as MITRE and Aerospace, for decades.

While the knowledge created at those institutions has varied, much of it centered on obtaining a more complete list of risks and better estimates of the likelihood and consequence. Evidently the fruits have not been powerful enough to change the written DoD guidance.

One could consult the major defense contractors, as for decades they have been actively managing the risks of developing weapons systems. We approached a few of them informally to ask if they would discuss with us their risk management methods. They responded that they considered their risk management practices to be competition sensitive and determinative of their commercial success and would not share them. We also approached a few industrial firms and received the same answer.

What about firms that deal in risk every day, such as insurance and investment businesses? Here the final report of a previous SERC research topic, valuing flexibility (RT-18), is dispositive (Deshmukh, 2010).

But what is the connection between valuing flexibility and risk? One parallel is that both attempt to characterize future uncertainties. After all, flexibility is about responses to future changes, some unplanned. "Most approaches for valuing flexibility depend on good estimation of uncertainty. However, estimating and characterizing uncertainty, even for foreseeable sources of [change], is difficult, especially in systems involving new technologies." p. 24

Investment advisors often use the technique of Real Options to find the best investment among alternatives, akin to what acquisition program managers must do at multiple points during development. Here are some weaknesses of Real Options in the DoD context (p. 62):

" Financial options' assumptions, such as no arbitrage condition, complete market condition and infinite liquidity, may not hold for the non-financial market.

"Without checking the assumption of Black-Scholes model, using the Black-Scholes formula does not make sense. For example, the strongest assumption of the model is the fact that uncertainty can be modeled in geometric Brownian motion and as a result the distribution of future status is [a] log-normal distribution. If the future environment cannot be modeled with this stochastic process and distribution, the Black-Scholes model is not valid.

[...]

"Almost all real options related literature assumes the risk-neutral decision maker implicitly or explicitly. This assumption need[s] to be check[ed] in [the] risk management sense."

Further, the report continues, with some overlap with the previous list (p. 64):

" Real options must be described in terms of specific technologies and the systemic domain in which they are to be developed. Financial analysis alone is insufficient to frame real options. This is quite difficult, when as yet undeveloped technologies are under consideration.

"Financial options are well-defined contracts that are tradable and individually valued, while real options are not: real options have no contract-specified exercise price or time. The usefulness of valuing every potential program alternative that provides flexibility is not clear.

"In military procurement programs, previous experiences associated with the development of similar technologies are not necessarily available. Hence, valuing real options on the basis of so called "comparables" becomes questionable because of the absence of available data.

"Real options are most often path-dependent. Hence, direct applicability of traditional financial options methodologies is not appropriate, as the underlying stochastic differential equations are not necessarily available.

"Real options in military acquisition programs are likely to be highly interdependent. Traditional financial option pricing methods fail here, again, because underlying stochastic differential equations may be unattainable.

"In military procurement programs, there may be no justifiable reason to accept the "no arbitrage assumption". In this case, general option pricing theory breaks down.

"There is typically no quantitative or qualitative reason to believe the real options have uncertainty in price that follow Brownian motion. That is, unlike in financial markets where there exist both quantitative and qualitative analyses that support by weak convergence in measure principles that suggests a limiting Brownian motion price process, there is typically no similar reasoning supporting the assumption of Brownian behavior. Hence, the semi-martingale arguments leading to the principal results of general option pricing are not applicable."

And this does not even address what may be the most difficult part of the application of Real Options in the DoD context: the necessity to assess the probability of each state of nature in the unfolding of future events. Investment analysts use historical information to estimate those probabilities, but there is little on which to base estimates of weapons systems development probabilities, especially of new capabilities.

In the end, we cannot rationally defend what some other communities, above, use to manage risk because their assumptions and sources of data match so little of our situation.

## CONNECTING TECHNICAL RISK AND TYPES OF COMPLEXITY

---

### A. A FEW DEFINITIONS

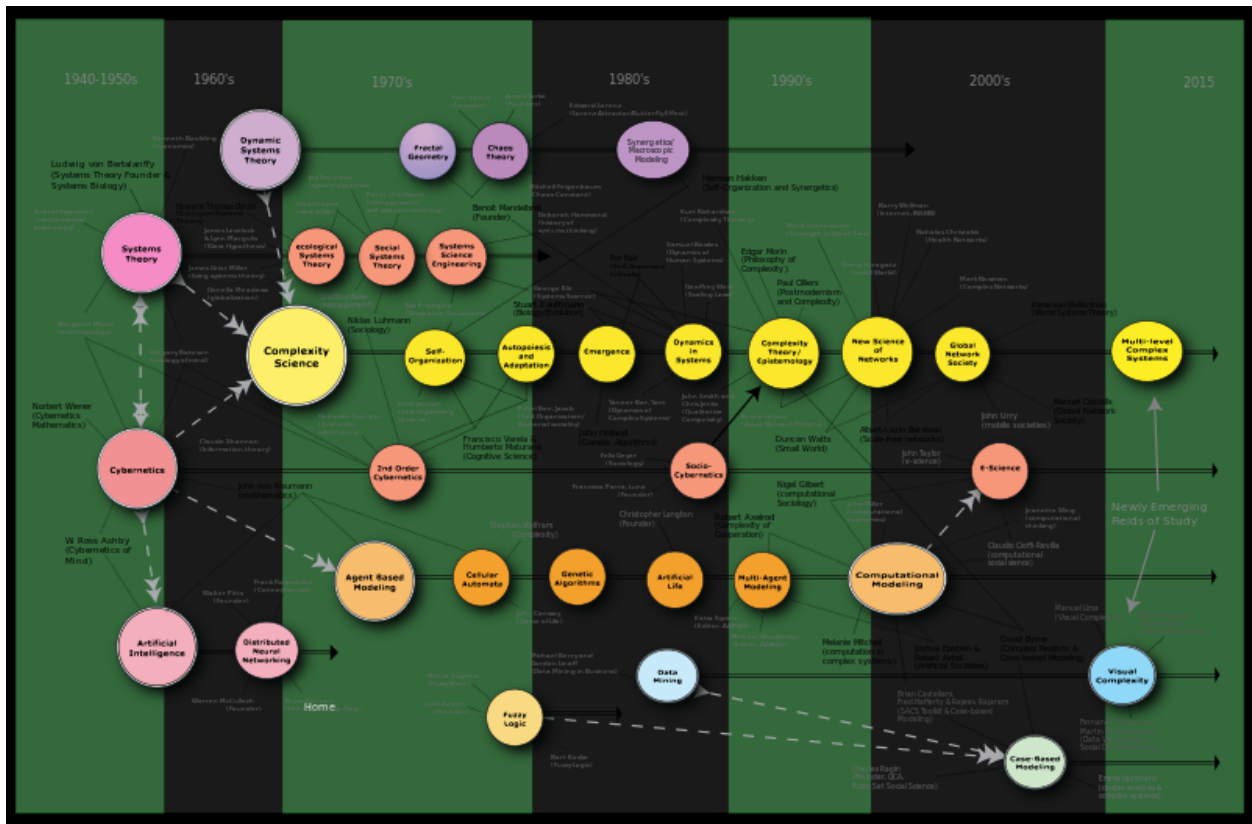
The field of complexity is rich and spans over the past half century in various fields of knowledge ranging from biological systems to cyber-physical systems. As it has been discussed by several researchers, a strong correlation can be observed between the complexity of the system and various ranges of failures, including catastrophic failures (Merry, 1995; Cook, 2000, Bar-Yam, 2003).

The term “complexity” has several definitions and various related aspects and characteristics in various domains of knowledge. We adopt the following definition:

*Complexity is the potential of the system to exhibit unexpected behavior (Willcox, 2011)*

Complex systems exhibit the potential for unexpected behavior with respect to variables of interest. The potential can manifest itself in certain situations and create the actual emergent behavior or stay hidden as a potential. Complex systems have non-linear interactions, circular causality and feedback loops. They may harbor logical paradoxes and strange loops. Small changes in a part of a complex system may lead to emergence and unpredictable behavior in the system (Erdi, 2008). It should be noted that complex systems are very different from complicated systems, and there is a tendency for mistake in using these terms interchangeably. Complicated systems often have many parts, however the interactions between parts and subsystems are often well known and linear, so they do not show emergent or non-linear behavior. In contrast, complex system may or may not have many parts, however, at least one non-linear behavior of feedback loop exists in the structure of the system that drives emergence and unknown unknowns in the system.

The increased complexity is often associated with increased fragility and vulnerability of the system. By harboring an increased potential for unknown unknowns and emergent behavior, the probability of known interactions that lead to performance and behavior in a complex system decreases, which in turn leads to a more fragile and vulnerable system. That is, the presence of complexity in a system, even a little complexity, can swamp the behavior of the familiar, linear interactions.



**Figure 2.** Map of the leading scholars and areas of research in the complexity sciences (<http://en.wikipedia.org/wiki/Complexity>).

As can be seen (but may not be able to read!) from this figure, there are many threads of research and many definitions of complexity. Our job is to pick and choose among the relevant threads of research which can contribute to the understanding of complexity at various milestones of acquisition programs, and identify the ones most applicable to characterizing technical risk.

At this early juncture, we can say only that we have not focused on the following areas in the diagram because we think they are not relevant to acquisition programs:

- Artificial intelligence (distributed neural networking)
- Agent-based modeling (cellular automata, genetic algorithms, artificial life, multi-agent modeling)
- Case-based modeling
- New science of networks
- Global network society

Fractal geometry  
Synergetics/macroscopic modeling  
Ecological systems theory  
Fuzzy logic

We are selectively making our way through the remainder to assess suitability to characterize technical risk based on what the government sees during the acquisition life cycle. Certain areas, such as emergence, are potent metaphors, but there is a connotation among complexity researchers that emergence is a property that cannot be sensed by looking at components, so for the moment we are not investigating emergence further.

We are looking closely at these kinds of complexity, in particular:

- *Structural* – The arrangement of pieces and parts that has loops, circuits, so that feedback is possible.
- *Dynamic* – The behavior of a system that unfolds as it executes. Here we look for delays and non-linearities.
- *Interface, interconnection* – How parts communicate and touch each other and whether that connection is across a barrier, whether there is a tight or loose connection, whether information is hidden inside the components, and whether the parts are of different "kinds."

---

## **B. HOW COMPLEXITY MANIFESTS AS TECHNICAL RISK**

---

### **B.1 MECHANISMS AND EXAMPLES**

One example of risk is interconnecting inhomogeneous elements. The term is meant broadly, as it could refer to trying to connect two systems that had never been connected before, even though each of them was mature in itself. The poster-child for this type of risk is DIVAD, the M247 Sergeant York "self-propelled anti-aircraft gun ([en.wikipedia.org/wiki/DIVAD](http://en.wikipedia.org/wiki/DIVAD)). Due to the urgent need for the capability, a decision was made by the Army to select a design that joined three commercial off the shelf systems: an Army M48 Patton tank chassis, a radar, and a cannon.

The three particular commercially off the shelf systems selected by the vendor had never been connected and the computer control system at the heart had not yet been developed. In the end, the tank was too slow to protect the ground vehicles it was intended to. The radar, while off the shelf, was off the shelf for an airplane! Airplane radars work internally by detecting movement. Clearly, a tank in the field was not (always) in motion and nor were its targets. The physical layout of the radar with



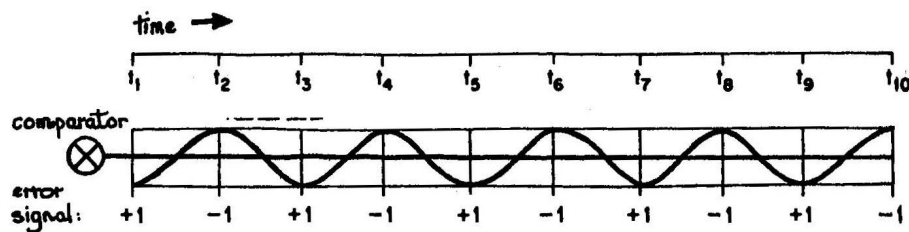
respect to the cannon had the cannon sometimes getting into the radar's line of sight. The tank's turret moved too slowly to track realistic air targets because, after all, it was never meant to. The list went on. And the program, comprised of commercial off the shelf systems, was cancelled.

How would our analysis have identified these risks? By looking for inhomogeneous interfaces.

A second type of complexity comes from feedback and delay. Feedback itself is a structural characteristic: it is a loop somewhere in the product being developed or in the organization creating the product. And the loop can amplify or dampen the signal passing through it, distorting the original (think of the child's game of "telephone"). And the transit may be delayed at points, which creates difficulty for us humans to reason about what causes the effects, the surface symptoms, that we see.

The field of system dynamics is awash in examples of loops and delays, and there is even something of a cottage industry in one particular example, the Beer Game<sup>1</sup>, in which a single instance of a change in a single signal causes the humans operating the game to respond in a way that causes oscillation that appears to be unable to be dampened. All of this due to the (underlying) structure of the system, illustrating that structure produces behavior.

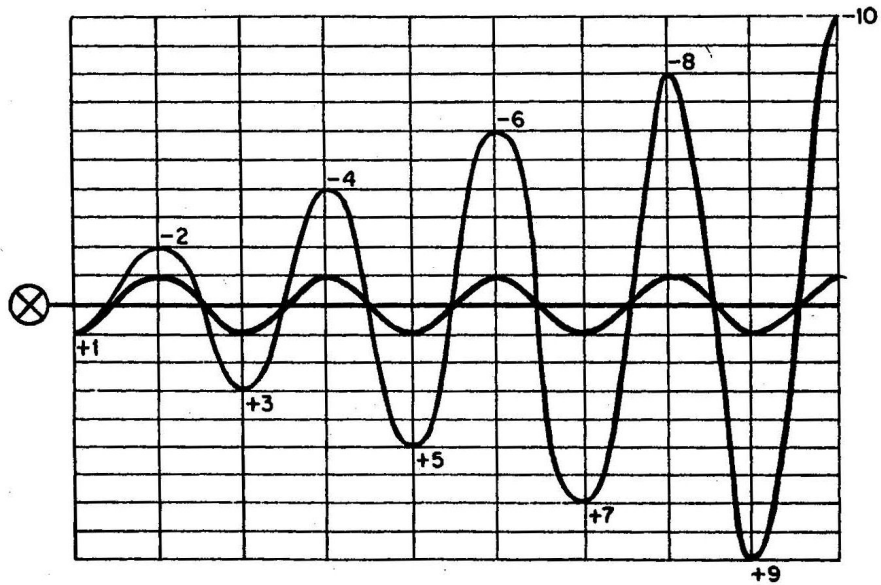
The example below comes from a book on business management (Beer, 1979), written to create interest in cybernetics. In this example are trying to construct a system that has even an output around the value 0, given an input single in the form of a regular sine wave:



**Figure 3.** An output varying regularly about a mean value that is its target, showing the corrections that appear necessary at each time epoch when the measurement is made. (Beer, 1979), p. 60

<sup>1</sup> <http://www.systemdynamics.org/products/the-beer-game/>

The approach is to generate a -1 when we see a +1 and generate a +1 when we see a -1. Here is what happens, according to that rule:



**Figure 4.** Explosive behavior induced by the direct application of error corrections to a system that has reversed its input states by the time the correction is applied. (Beer, 1979), p. 60

As seen, the system is "exploding." Why? Because the signal we generate to correct for the input is just one phase late, so instead of subtracting when it sees a +1, there is a slight delay and the negative signal we generate supplements an already negative signal, making it even more negative.

The important points are: this is common and is the result of the structure of the system, both static and dynamic. Our methods of risk identification and analysis would try to identify such connections and delay.

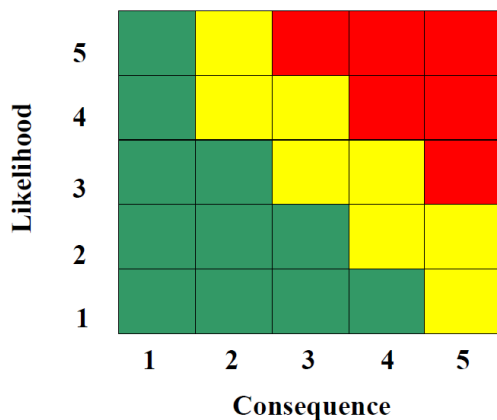
---

## B.2 RISK AND COMPLEXITY CORRELATION

Risk can be defined as “a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints.”{US Department of Defense (Office of the Undersecretary of Defense (Acquisition, 2006 #1, p. 1}.

For complex defense acquisition programs, often various types of risks exist that manifest themselves at different times throughout the acquisition process, including system development. These risks can be technical, programmatic or strategic in nature and can result in substantial cost overruns, delays, performance issues, reduced adaptability to changing requirements or even total cancellation of a project. One of the challenges with assessing risk using the traditional risk reporting matrices (See Figure 5) for complex systems acquisition is that neither the likelihood nor the true consequence of a risk can be objectively established. For one, there is substantial uncertainty around the interactions among different components of a system as well as uncertainties about how effectively various kinds of risks can be managed across a multiplicity of interfaces.

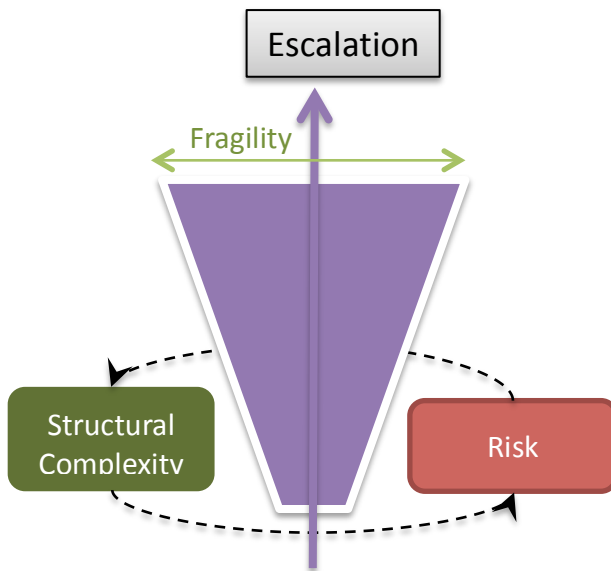
In this research we are proposing a fundamentally different approach to risk management, one that looks at how complexities within the technical and organizational realms result in uncertainties that can ultimately lead to risks in the system. The premise of this research is that in the realm of technical project risk, it is the complexity of the system combined with the experience/know-how of the contractors that determines system uncertainties and the resulting risks.



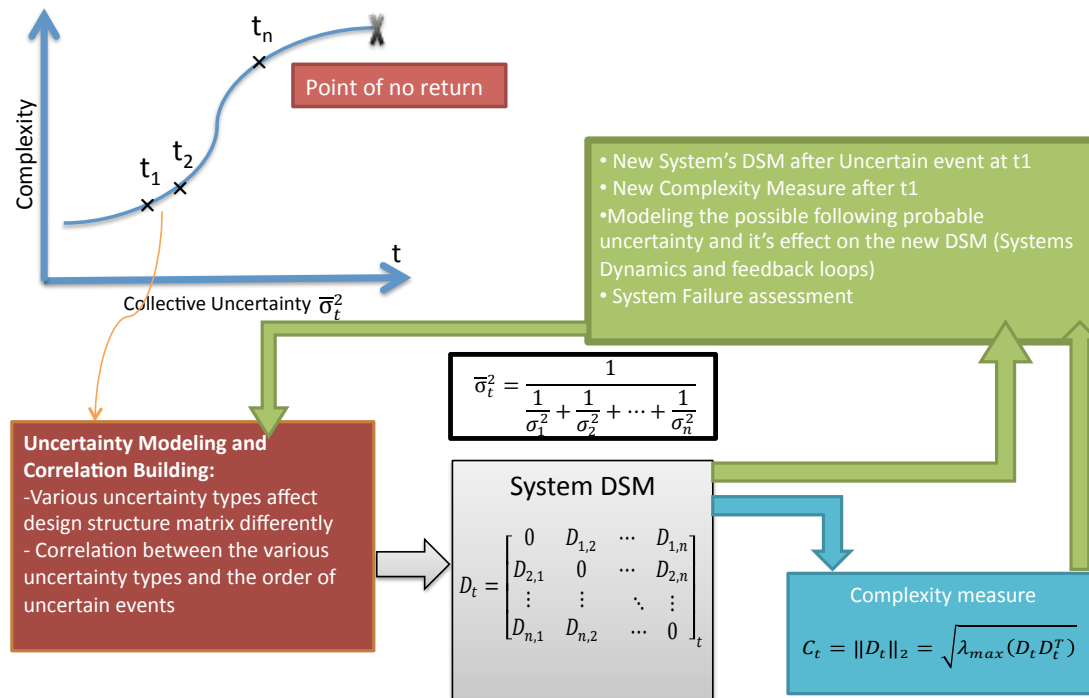
**Figure 5.** Traditional Risk Reporting Matrix {US Department of Defense (Office of the Undersecretary of Defense (Acquisition, 2006 #1}

The objective of this research is to link technical complexity with uncertainty and risk across different stages of the acquisition process, and dynamically quantifying and updating risk elements for decision-making on project continuation, modification or retirement.

Complexity may be the root cause of many unforeseen risks. Program/project complexity per se can generate negative consequences that may often take the project management team by surprise. Common and advanced methods of risk modeling, including, for example, Bayesian Networks, cannot predict the sort of emerging risks that manifest continuous ripple effects that unfold one after the other almost for the entire duration of the complex projects. This type of intimidating effect of complexity is not something one would like to have for the entire program duration, or perhaps at any time during the program, as the effect is one of being out of control, or, indeed, in the control of something unknown. Often the complexity manifests in risk and risk creates more complexity. This is known as complexity-uncertainty death spiral. In several case studies in our previous research, we have observed that the increase in structural complexity increases the risk and therefore occurrence of the minor undesired event. The unfolding of the first risk oftentimes affects the structure of the system in a manner that increases the structural complexity. The incremental increase in structural complexity again can contribute to the next risk to unfold and the spiral escalation can continue. We model this process by hybrid techniques and seek techniques that tackle the root cause of hidden risks that manifest in the form of a set of continuously mysterious (no clear root cause) risks. There is a very intricate relationship between structural complexity and fragility of complex Systems of Systems that can be the result of an escalation of overall system sensitivity, sometimes in a very short time period (Figure 6).

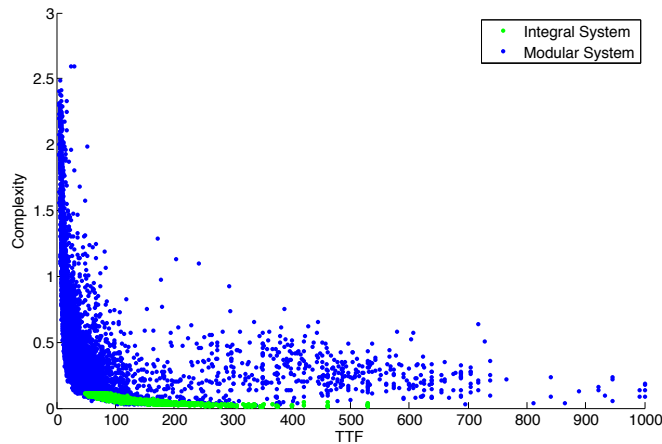


**Figure 6.** The Complexity-Risk spiral. Insignificant uncertainties and risks in combination with structural complexity escalate into a fragile situation and to a point of no return at which failure is certain.



**Figure 7.** Structural complexity and risk (uncertainty) correlation in the DARPA F6 program.

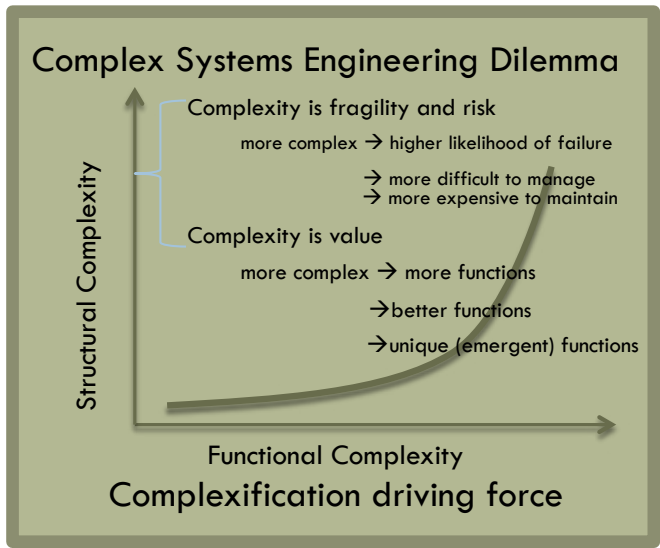
Figure 7 shows an example of the structural complexity metrics that we defined and used for the DARPA F6 program on fractionated space systems (Nilchiani, 2012). Fractionated space systems are a network of satellites in orbit that can consist of different number of heterogeneous satellites with various architectures flying in formation. Our research has shown a direct correlation between an increase in structural complexity and how fast a failure or risk in a network of these satellites propagates (such as a security attack on one of the satellites in the network). Figure 8 shows some of the results of the F6 simulation that connects the complexity measure of the system to the mean time to failure for various architectures of the fractionated space systems.



**Figure 8.** F6 Simulation results showing that increased structural complexity leads to shorter time to failure in the system.

According to some of our initial studies (Salado and Nilchiani, 2012; Efatmaneshnik and Nilchiani, 2012), the results of implementing some risk mitigation plans can create ripple effects through a project or system, increase the complexity of the system and therefore lead to making the program more vulnerable to known risks as well as the hidden uncertainties. Moreover, the existence of a minimum of only three interrelated risks with significant correlation can lead to a ripple effect that can remain hidden up until the last moment, when the negative consequences become fully developed and surface, overwhelming the system. Uncovering these types of hidden cause and effect relationships requires thorough structural monitoring of the system requirements and design as early as possible to uncover all the dependencies with a very high level analysis.

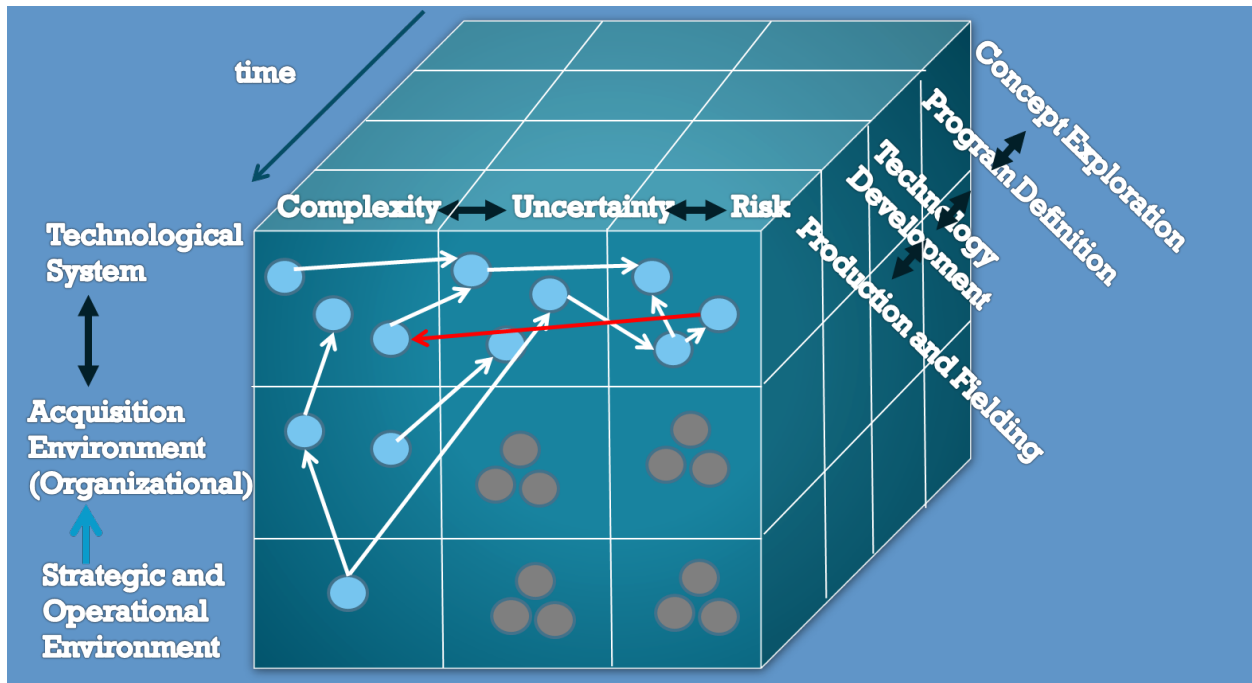
Additionally, as systems demonstrate more functional complexity, they can perform more sophisticated missions. However, the increased functional complexity can also result in an increased structural complexity for systems, which in turn increases risks of failures. While more complex functionalities are more likely to deliver higher values, structural complexity per se is not a positive attribute. More complex functions can require that structurally complex structures, which one after the other can act in unpredicted ways. In essence, functional complexity is the driving force behind complexification. Yet structural complexity is a cost on the system, because it increases the possibility of dramatic response to uncertainties, or fragility (Figure 9).



**Figure 9.** Logical relationship between structural and functional complexity

**C. DERIVING PROJECT RISK FROM TECHNICAL COMPLEXITY AND CONTRACTOR ORGANIZATIONAL CAPABILITIES**

A modified risk cube that looks at the causal relationships among technical systems complexity and organizational capability in dealing with technical and strategic complexity is presented in the complexity-uncertainty-risk environment cube of Figure 10.



**Figure 10.** Complexity-Uncertainty-Risk Environment (CURE) Cube

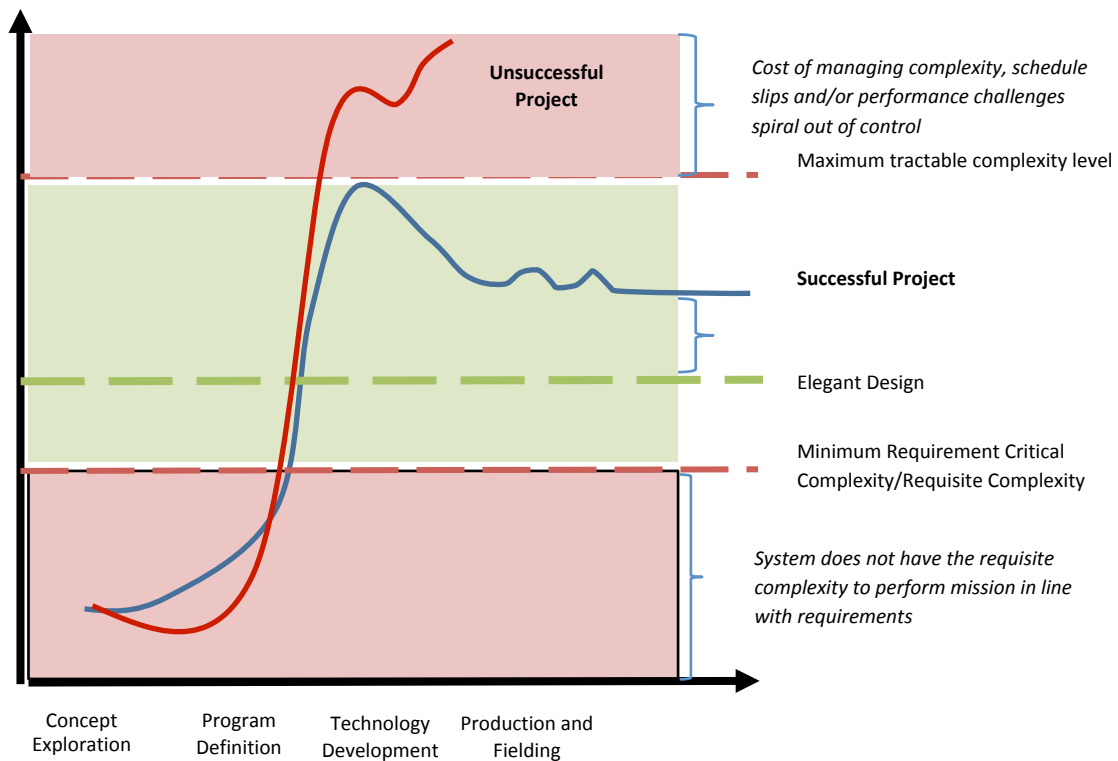
Here we can explore the interrelationships among various aspects of technological complexity across the acquisition process phases and explore the impact of organizational complexity (capability) as well as strategic (that is, higher level, as, for example, at the mission or campaign level) complexity on uncertainties and subsequently risk. The unfolding of the technical complexity depends on the inherent requirements complexity, the system design, and the capabilities of the contractor organization(s) to match their internal organizational complexity to manage the technical complexity. In our current research we are addressing only the top row of Figure 10, the technical aspects of the system and its creation and testing.

Figure 11, below, illustrates that below the minimum required critical complexity a system cannot perform the functions that are expected and above a maximum tractable complexity level, the system



development process can spiral out of control. It is the expertise, know-how and experience of the contractor organization, working with the government acquisition office, that can keep the development process within the boundaries of these two and stabilize the complexity level of a system. Thus, for the same system but different contractor + acquisition organizations, the graph in Figure 11 could have different forms.

*The key to acquisition risk management will therefore be to ensure a match between the unfolding technical complexity with the internal organization, know-how and expertise of the contractor(s) + acquirer in managing complexity.*



**Figure 11.** Complexity evolution throughout the systems acquisition lifecycle

**D. ARCHITECTURAL-LEVEL COMPLEXITY MEASURES FOR ACQUISITION SYSTEMS:  
SUMMARY OF CASE STUDIES**

The first step therefore in transitioning towards a complexity-centric risk assessment is to be able to measure systems complexity over the acquisition process. As it is possible that there is no detailed design in the early stages of the acquisition process, the measurement of complexity has to start at the architectural (high-level requirements) level. Tables 1 and 2 summarize the different types and planes of acquisition complexity at the architectural level. It should be noted that the following Tables summarize some of the major variables that contribute to the increased complexity of the system. However the list and variables may not be comprehensive and in phase 2 of the project, we are aiming at identifying the majority of variables that contribute to the complexity of the system

**Table 1.** Six types of complexity (Source: Sheard, 2012)

Six Types	
Structural: Size	Number of elements, number of instances, total cost, total number of requirements
Structural: Connectivity	Number of connections, density of connections, strengths of relationships, amount of conflict, distribution of connectedness
Structural: Inhomogeneity	Number of different types of entities, number of types of relationships, number of different areas within a space, diversity of sizes of elements or contractors or stakeholders
Dynamic: Short-term	Existence of loops/circuits, safety-criticality, tendency to blow up in operational time frame, seriousness of consequences of a mishap
Dynamic: Long-term	Evolution of purpose of an item, co-evolution of a variant and its environment, how much different the next iteration of a system might be
Socio-political	Fraction of stakeholder interests that are based on power, amount of disagreement among stakeholders, number of layers of management, changes of opinion of management or stakeholders, number of different cultures working together on a project, inhomogeneity of stakeholder utilities.

**Table 2.** Four planes of acquisition complexity (Source: Sheard, 2012)

Four Entities	
[Technical] System being built	Product, system, system-of-systems, tank, squadron, database, sensor, software algorithm.
Project or organization doing the building	Project, organization, program, tasks, team
Environment, both external systems and people	Customers, buyers, market, external technological system, future systems that need to interface with product
Cognitive: capacity of humans to understand, conceive of, build and operate the system.	Learning curve, uncertainty, confusion, operator skill set.

---

## **E. MEASURING ARCHITECTURAL LEVEL COMPLEXITY: INITIAL EXPLORATIONS**

Based on a comprehensive literature and state of the art review we have converged on the following five lenses for measuring complexity. Should these prove to be inadequate for our research, we will devise new ones based on our own observations of systems. We will explore which of the following lenses of complexity measurements applied to an architecture-level systems description can dynamically predict acquisition risk and improve mid-process decision-support

1. Requirement critical (algorithmic) complexity
2. Critical control path (cyclomatic) complexity
3. Dynamic architectural complexity
4. Structural complexity
5. Modified architectural-structural complexity

We will then explore how the experience of contractors + government plays a role in managing the complexity of the system in the acquisition process.

### **1) Requirement Critical Complexity**

Requirement critical complexity refers to the minimum amount of complexity a system needs to have in order to perform a desired set of functions in line with expressed requirements. Based on *Kolmogorov complexity* metric, it refers to the minimum set of architectural level components and linkages  $\{y\}$  that would address requirement set  $\{x\}$ . In other words, the requirement critical complexity of a system can be expressed as the minimal systems architecture  $\{y\}$  (minimum number and type of components and linkages) that would theoretically produce performance set  $\{x\}$ .

The determination of  $\{y\}$  given  $\{x\}$  is an important research question and this research will try to establish this threshold for various kinds of complex systems. The calculation of requirement critical complexity can be done either through modified structural complexity metrics that will be discussed further in this document.

### **2) Critical Control Path Complexity**

Based on the concept of cyclomatic complexity in software, the critical control path complexity metric measures the number of linearly independent control paths through a systems architecture graph. This number changes as the architecture (or the resulting design) changes over time and is estimated by the following equation:

$$CCP(t) = \sum n(t, i) - l(t, i) + p(t, i)$$

where  $CCP(t)$  is the critical control path complexity at time  $t$ ,  $n(t, i)$  is the number of nodes in the connected graph of the architecture expression for module  $(i)$ ,  $l$  is the number of linkages at time  $t$  in module  $(i)$  and  $p$  is the number of distinct connected components in the architectural flow graph. And the sum is over all modules.

### 3) UML-based Five-Views Dynamic Architectural Complexity (Lankford)

Rather than a single number, the UML-based Five Views Dynamic Architectural complexity metric allows the measurement of various system complexity metrics over time.

The five views complexity vector is calculated as follows:

$$C5V(t) = \begin{bmatrix} C_{class}(t, i) \\ C_{process}(t, i) \\ C_{component}(t, i) \\ C_{interfaces}(t, i) \\ C_{patterns}(t, i) \end{bmatrix}$$

Where:

Within

$C_{class}(t, i)$  = Number of classes and objects within each module at time  $t$

$C_{process}(t, i)$  = Number of processes and threads within each module at time  $t$

$C_{component}(t, i)$  = Number of components = the number of nodes

$C_{interface}(t, i)$  = Number of interfaces between each of these

$C_{patterns}(t, i)$  = Number of identifiable design patterns within each module

### 4) Simple Structural Complexity (Meyer)

Simple structural complexity can provide an easy to calculate way to capture how the complexity of a system is changing, by calculating changes in the number of parts (or sub-systems or systems), types of parts and number of interfaces over time.

$$C_{structural}(t, i) = \sqrt[3]{(N_p(t, i) \times N_y(t, i) \times N_x(t, i))}$$

Where

$N_p(t, i)$  = Number of parts/subsystems in subsystem/system  $i$  at time  $t$

$N_y(t, i)$  = Types of parts/subsystems in subsystem/system  $i$  at time  $t$

$N_x(t, i)$  = Number of interfaces in subsystem/system  $i$  at time  $t$

## 5) Modified Architectural-Structural Complexity (MASC)

The modified architectural-structural complexity is the most comprehensive measure of architectural complexity, taking into account size, type, interconnections and interfacial complexity of architectural modules into consideration. It is based on Kinnunen (2000). Modifying the simple architectural complexity equation for MASC we get:

$$C_{MASC}(t) = \sqrt[3]{\sqrt{[(N_p(t) \times N_y(t, i))] \times \sqrt[3]{[(N_f(t) \times N_{obj}(t) \times N_{op}(t))] \times N_x^{ICM}}}}$$

Where the arguments are respectively:

- Number of distinct types of objects/components
- Number of objects within each type
- Number of processes/functionalities affecting an object
- Number of objects/components affecting a process
- Number of operations per process
- Number of interfaces weighted with the interface complexity multiplier (ICM) (related to the integration readiness levels (IRLs) between different systems/subsystems).

It should be noted that these five types of architectural level complexity measures are our initial exploration of the relevant complexity measures of the technical system. Our research team may have to define novel measures based on the existing literature on complexity that may be more useful for different milestones of an acquisition program, and in particular characterizing the dynamic behavior of the architecture.

---

**C. THE FIT BETWEEN TECHNICAL RISK OF THE PRODUCT AND AN ORGANIZATION'S CAPABILITY TO MANAGE IT**

What accounts for one enterprise being able to create a complex product and another not? The primary conjecture, attributed to Ashby (Ashby, 1961), is that the enterprise that can construct a complex product has enough "variety" (he called it requisite variety) in the way it is organized and applies its resources. Variety is diversity, ability to react to various problems and opportunities, including unexpected ones.

Perhaps one of the most vivid illustrations of variety in this context was during the Apollo 13 manned space flight in 1970, when an oxygen tank aboard exploded, limiting power, causing loss of cabin heat, reducing the availability of potable water, and increasing the concentration of carbon dioxide in the cabin air. It was the mounting concentration of carbon dioxide that proved most troubling, as the astronauts would die of lack of oxygen if it were not reversed. A team on the ground was assembled and given the task of figuring out how to create a carbon dioxide removal system, given the constraints on-board. That the ground team succeeded was a tribute to its variety, its diversity of thought, as it quickly suggested and tested numerous options.

One of the biggest challenges in using variety to characterize organizations is that it is so difficult to observe, to measure. Two authors (Beer, 1979; Jaques, 2006) have suggested antidotes to this and we are exploring their methods.

---

**D. THE PLACES OF CASE STUDIES AND QUANTITATIVE DATA**

We are seeking to know what programs and organizations are "made of" that might inform the identification of risk. Our premise is that complexity is a major indicator of risk. In order to validate or invalidate the premise we need data. The most convincing data would be numeric, quantitative that showed the relationship between product complexity, say, and risk. If that data are not available, then we might use case studies.

Since we do not yet have quantitative data, we have indeed been reading case studies, supplied to us by the deep reservoir provided by our colleague, Dr. Gary Witus, at Wayne State University. At one stage he supplied 15 cases, some with multiple artifacts. Dr. Mostashari read them and in the end was not able to deduce anything general.

Dr. Witus responded to our request for additional case studies and we have not yet had a chance to absorb them, and it is a priority for our next steps.

At some point – earlier is better – we are going to need access to quantitative data that will help us confirm or deny the connection between some measure of complexity and technical program risk. This, too, is a priority for the next steps.

Both case studies and access to quantitative program information will help us steer where to look deeper, help us consider what programs are made of. In the end, it is possible that programs do not collect the measures of complexity that we think are the most indicative of risk, so we will have to work with programs on a pilot basis to install new measures and assess the ability of those measures to predict technical risk.

---

## **EXAMPLES AND SOME CASE STUDIES**

### **A-10 Thunderbolt II (Aircraft)**

Acquisition Organization: U.S. Air Force

#### **Risks and Weaknesses**

- **Technical:** Concurrent development of a new technology (the GAU-8/A gun system) and the aircraft at the same time with the aircraft architecture revolving around the armament system created delays in the acquisition process. Also the original structural design proved inadequate for the design life, and even fixes during production were inadequate for all but the latest aircraft produced.
- **Programmatic:** Overlooked problems associated with production readiness and contractor financial stability did not go away and had to be resolved far too late in the development program. Additional problems included loss of the Original Equipment Manufacturer (OEM), on-again/off-again decisions to retire the A-10, unstable funding for inspection and repair, and major personnel disruptions resulting from a BRAC decision. Critical “health of the fleet” structural inspections were not performed during sustainment, and a subsequent repair program failed to provide the desired level of life extension.

#### **Strengths**

Close attention to key mission characteristics (lethality, survivability, responsiveness, and simplicity) allowed the concept formulation and subsequent system design to result in an effective CAS aircraft, and design-to-cost goals kept the government and contractor focused on meeting the critical requirements at an affordable cost. The A-10 did not meet all its cost goals, but it came much closer to them than most major defense development programs did in that time frame or since then.

#### **Complexity Factors Leading to Risk**

- Low TRL technology at core of systems architecture (Interface complexity)



- Requirement changes rendering architecture inadequate (Requirement Complexity)  
Contractor technical and financial capability (Organizational Requisite Complexity)

**Source:** A-10 Thunderbolt II (Warthog) SYSTEMS ENGINEERING CASE STUDY , Air Force Center for Systems Engineering

## **C-5A Galaxy (Aircraft)**

Acquisition Organization: U.S. Air Force

### **Risks and Weaknesses**

- **Technical:** A Weight Empty Guarantee was included in the specification as a performance requirement and in the contract as a cost penalty for overweight conditions of delivered aircraft. The aircraft Weight Empty Guarantee dominated the traditional aircraft performance requirements (range, payload, etc.), increased costs, and resulted in a major shortfall in the wing and pylon fatigue life. The stipulation of a Weight Empty Guarantee as a performance requirement had far-reaching and significantly deleterious unintended consequences.
- **Programmatic:** The Total Package Procurement Concept (TPPC) employed by the government required a fixed-price, incentive fee contract for the design, development, and production of 58 aircraft. It included a clause giving Total Systems Performance Responsibility (TSPR) to the prime contractor. TPPC was invented to control costs, but it was the underlying cause of the cost overrun and limited the number of aircraft purchased under the original contract

### **Strengths**

The process for developing and documenting the system performance requirements involved the User (warfighter), planners, developers, and technologists from both the government and industry in a coordinated set of trade studies. It resulted in a well-balanced, well-understood set of requirements that fundamentally remained unchanged throughout the program.

### **Complexity Factors Leading to Risk**

- Detrimental hard requirement with cascading effect on mission critical requirements and architectural design (Requirement complexity)
- Weight, wing and pylon design conflict (Interfacial complexity)
- Faulty procurement concept (Organizational Process Complexity)

**Source:** C-5A Galaxy Systems Engineering Case Study, Air Force Center for Systems Engineering

## **F-111 (Aircraft)**

Acquisition Organization: U.S. Air Force and U.S. Navy

### **Risks and Weaknesses**

- **Technical:** The F-111 acquisition process suffered from a nearly impossible multi-role/multi-service requirement specification, and a protracted development cycle in which numerous serious technical problems had to be identified and corrected. Of the 1,726 total aircraft buy that had originally been planned in 1962, only 562 production models of seven different variants were completed when production ended in 1976. The F-111, like any complex weapon system development program, which provides new war-fighting capability, had areas of risk or deficiency that came to light during RDT&E even though there was perceived low risk in the design. The F-111 development program introduced concurrency (overlap) between design validation/verification and production to accelerate program
- **Programmatic:** Systems Architecture and Design Trade-Offs were not performed to achieve an F-111 design that was balanced for performance, cost and mission effectiveness (including survivability) and the attendant risk and schedule impacts. The F-111 suffered from poor communications between the Air Force and Navy technical staffs, and from over-management by the Secretary of Defense and the Director, Defense Research and Engineering, and it came under intense congressional scrutiny, which restricted the System Program Office (SPO) Director from applying sound systems engineering principles.

### **Complexity Factors Leading to Risk**

- Impossible requirements with severe conflicts (Requirement complexity)
- Inadequate verification and validation (Organizational Process Complexity)
- Multi-agency acquisition process (Organizational Process Complexity)
- Sociopolitical sensitivity (Organizational Process Complexity)

Source: F111 Systems Engineering Case Study, Air Force Center for Systems Engineering

### Additional Case Studies (read but not summarized here)

<u>Program</u>	<u>Risks and Weaknesses</u>
A-7D	High cost and schedule slip
CH-47D	Cost and schedule slip
F-4E	Unstable funding, vague authority
F-4M/K	High cost, delayed and poor performance
F-5E	Risk managed. Cost and schedule met
F-14	Cost overrun
RB-57D	High costs, performance problems and delays
RB-57F	Met cost, schedule and performance goals

## IV. NEXT STEPS

---

The most pressing need in this research is access to information on completed programs that will help characterize the connection between some definitions of complexity and the post hoc prediction/realization of technical risk.

In addition, we shall pursue more case studies, more literature, and more methods of characterizing complexity of products and organizations, including interviewing acknowledged experts.

## References

- Ashby, W. R. (1961). *Introduction to cybernetics*: Chapman & Hall.
- Beer, S. (1979). *The heart of the enterprise*. New York: Wiley.
- Deshmukh, A. (2010). RT-18: Valuing Flexibility, Phase I Progress Report. Hoboken, NJ: Systems Engineering Research Center.
- Hazelrigg, G. A. (1998). Framework for decision-based engineering design. *Journal of Mechanical Design*, 120(4), 653-658.
- Jaques, E. (2006). *Requisite organization: A total system for effective managerial organization and managerial leadership for the 21st Century* (2nd Revised ed.). Alexandria, VA: Cason & Hall.
- Kahneman, D., Slovic, P., & Tversky, A. (Eds.). (1982). *Judgment under uncertainty: Heuristics and biases*: Cambridge Univ. Press.
- Merry U. 1995. *Coping with Uncertainty: Insights from the New Sciences of Chaos, Self-Organization, and Complexity*. Praeger, London.
- Cook R. 2000. *How complex systems fail*. Cognitive Technologies Laboratory Publication, University of Chicago. Chicago, IL.
- Wilcox, K. et al. (2011), Stochastic Process Decision Methods for Complex Cyber-Physical Systems, META Program Final Report, Massachusetts Institute of Technology.
- Bar-Yam Y. 2003. *When systems engineering fails - toward complex systems engineering*. In proceedings of IEEE International Conference on Systems, Man, and Cybernetics, No 2, pp 2021- 2028.
- Erdi P. 2008. *Complexity Explained*. Springer-Verlag.
- Efatmaneshnik, M.; Nilchiani, R.; Heydari, B. "From Complicated to Complex Uncertainties in System of Systems," In Proceedings of IEEE Systems Conference, March 18-22, 2012, Vancouver, BC, Canada.
- Salado, A., Nilchiani, R. "Taxonomy and Categorization of Uncertainties in Space Systems with an Application to the Measurement of the Value of Adaptability," Session: SSEE-04, Space Systems Engineering and Space Economics I - Advances in Systems Engineering for Space Applications, Published in AIAA SPACE 2012 Conference, 11-13 Sep, 2012, Pasadena, California
- Nilchiani, R.; Heydari, B., "Quantification of the Value of Flexibility and theory of Emergent Modularity: Annual report," Annual report to DARPA F6 program, November 2012, Stevens Institute of Technology.