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)

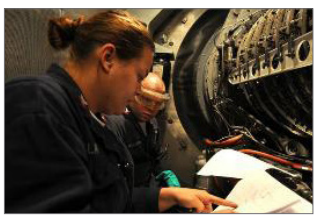
Demonstrating broad systems engineering community support, the conference is once again this year enjoying technical co-sponsorship by IEEE AES, IEEE Systems Council and the International Council on Systems Engineering.

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**

			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**

			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**

			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



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.



"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 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

Overcoming the Government-Industry Collaboration Obstacles

Patrick J. Martin, Ph.D.
Sr. Principal Research Engineer
patrick.j.martin@baesystems.com
Technology Solutions



10-26-2017

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

The Future of System Development
Rapidly Evolving Threats

Technology is democratized

OpenStack | AWS | Raspberry Pi | BitBucket

Github | ArduPilot | OpenSource Hardware | OpenRobotics

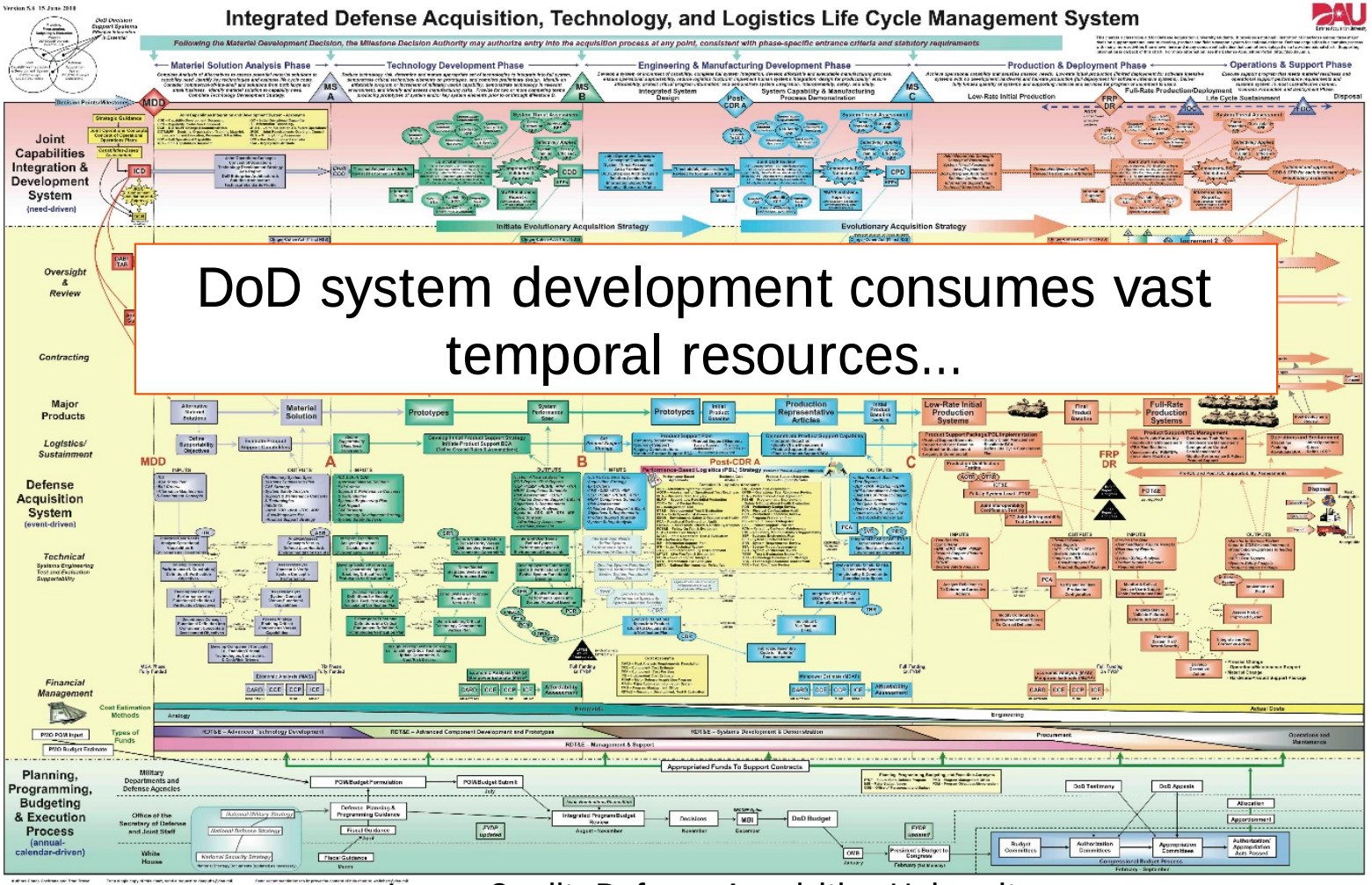
Near-peer and insurgent adversaries rapidly adapt tools and tactics



© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

The Future of System Development
Unsustainable Processes



DoD system development consumes vast temporal resources...

Image Credit: Defense Acquisition University

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

The Future of System Development
Unsustainable Processes

...and time IS money.

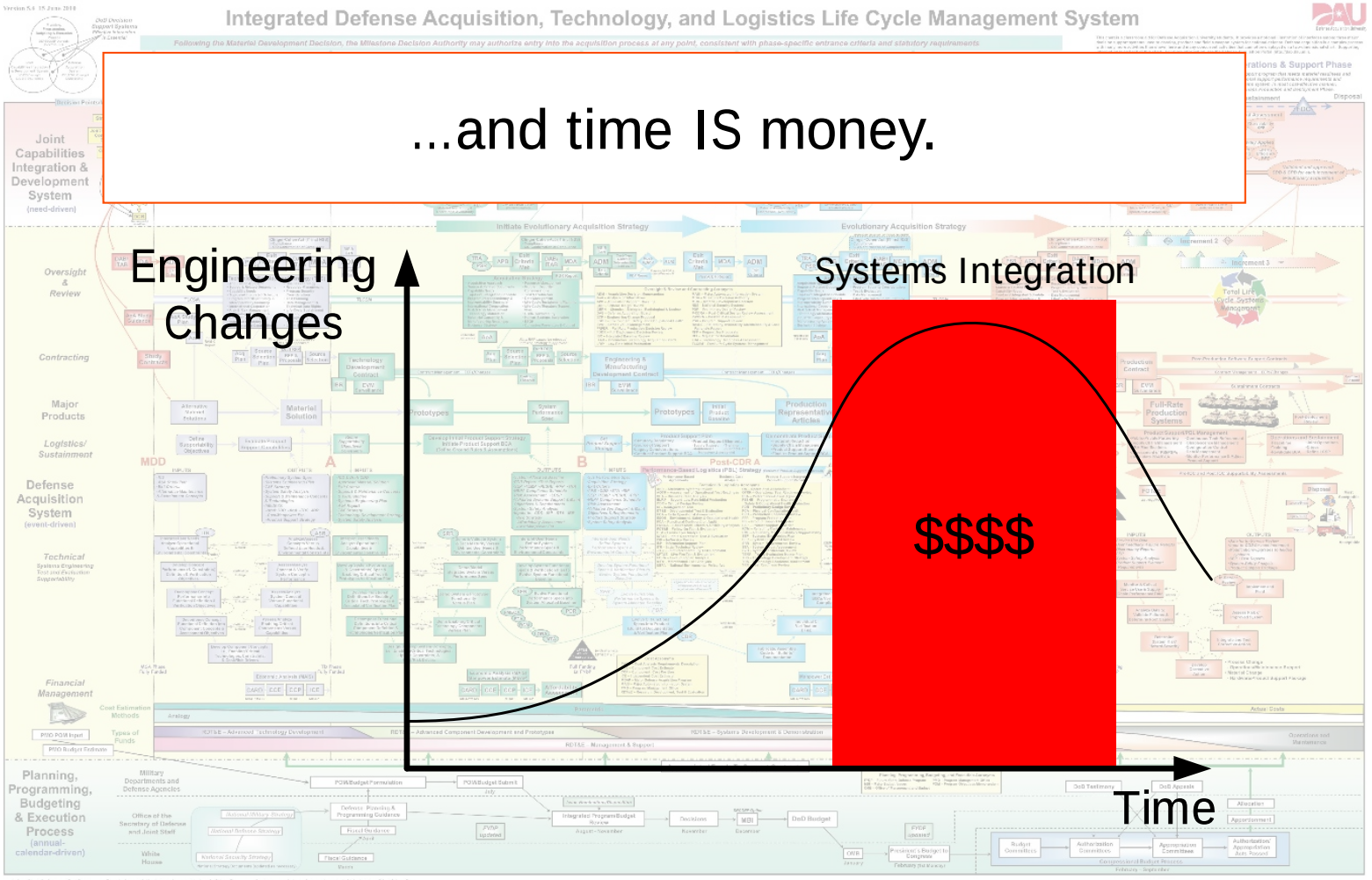


Image Credit: Defense Acquisition University

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

The Future of System Development

Developing, testing, and deploying engineered resilient systems will require **collaboration** across the DoD community

Technological Hurdles

- Security
- Scalability
- Flexibility

Policy Hurdles

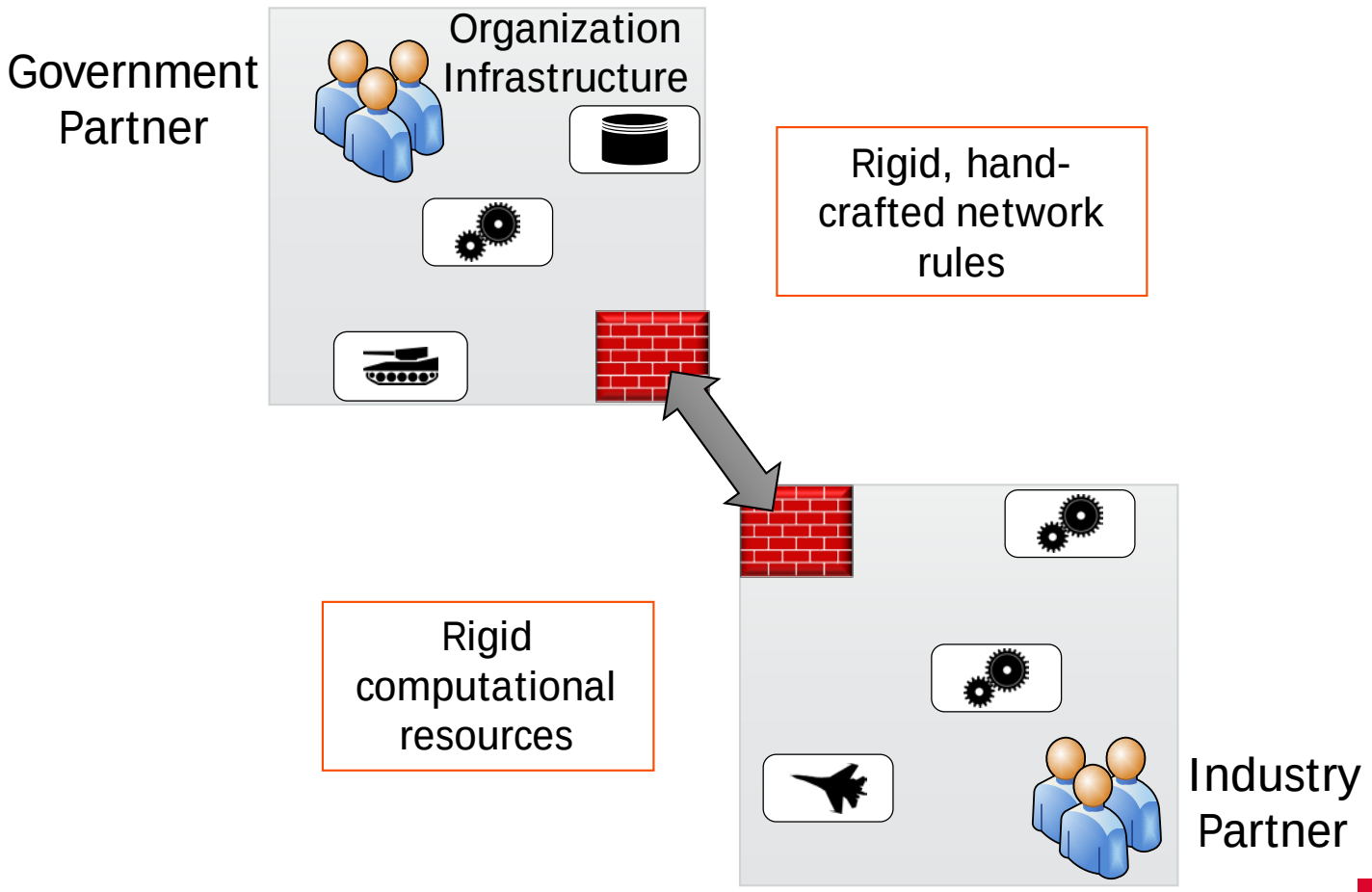
- Security
- Legal
- Business

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Collaboration Challenges

Partner collaboration is ad-hoc
Multiple IT and security organizations involved

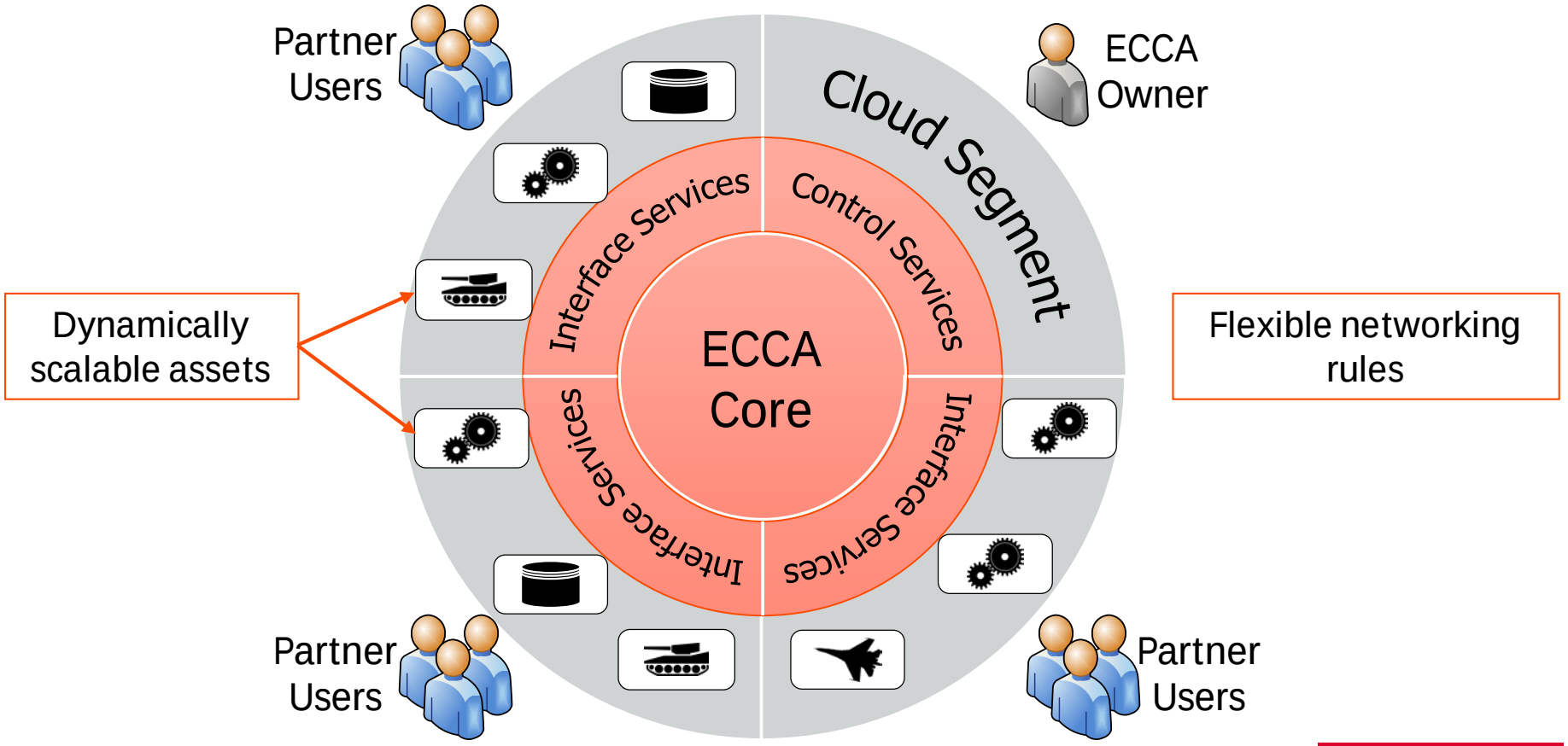


© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ERS Cloud Computing Architecture (ECCA)

ECCA provides a **collaborative analysis environment** for industrial, academic, and government partners



© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

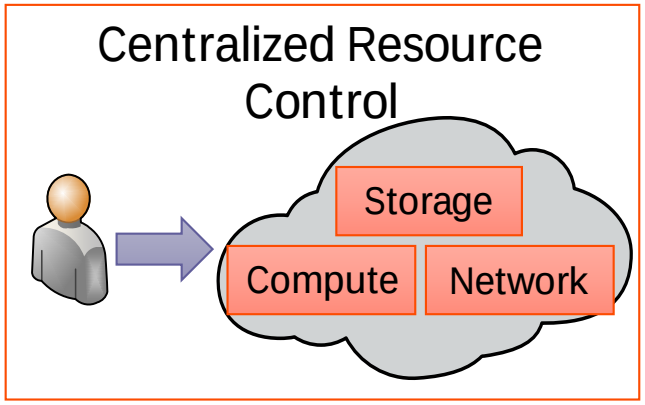
ERS Cloud Computing Architecture (ECCA)
Benefits and **Risks**

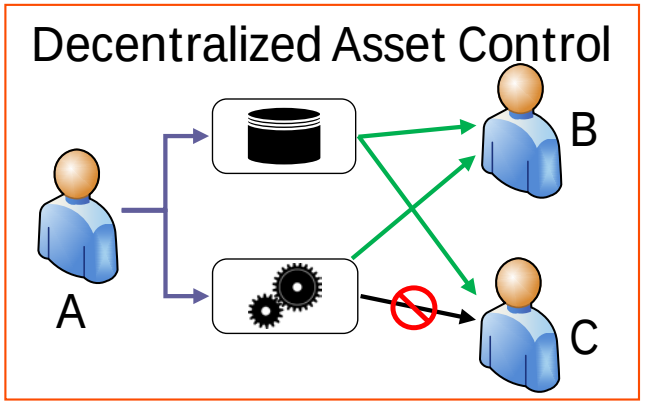
What we want...	What we need to worry about...
Controlled access to M&S capabilities	Standard network security risks
“Programmable” analysis applications	IP Leakage, Side channel exfiltration
Rapid capability sharing with DoD customers	Malicious assets
Discovery of strategic partners	Cloud computing resource overrun

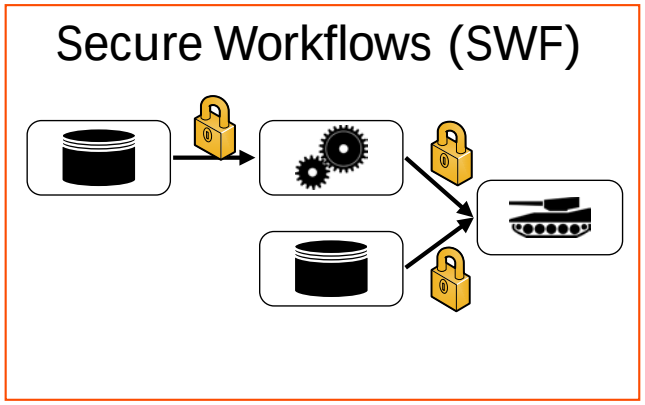
© 2017 BAE Systems

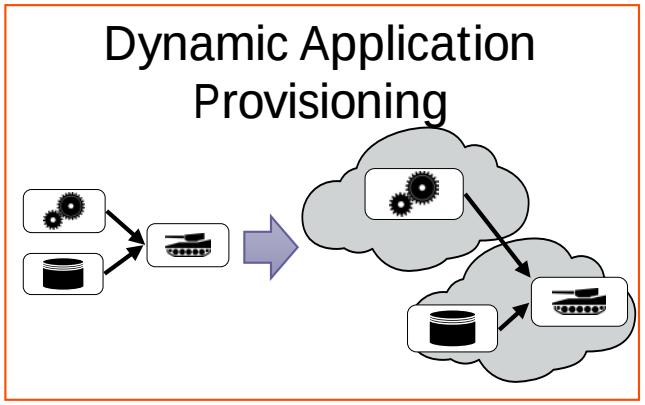
BAE SYSTEMS
INSPIRED WORK

ECCA High Level Concepts







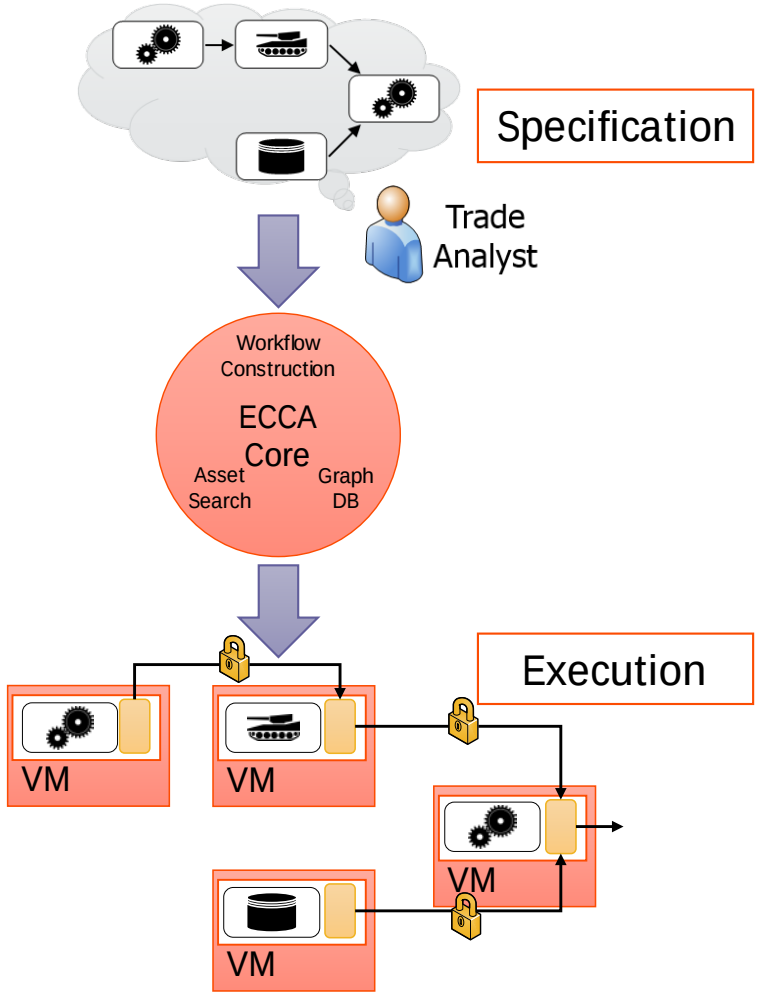


© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA IP Protection Strategy

- Encryption at-rest and in-motion
- Partners locally control access to their M&S assets
- Leverage recent cloud computing advances to enable:
  - Isolation of runtime assets
  - Automatic generation of secure software defined networks

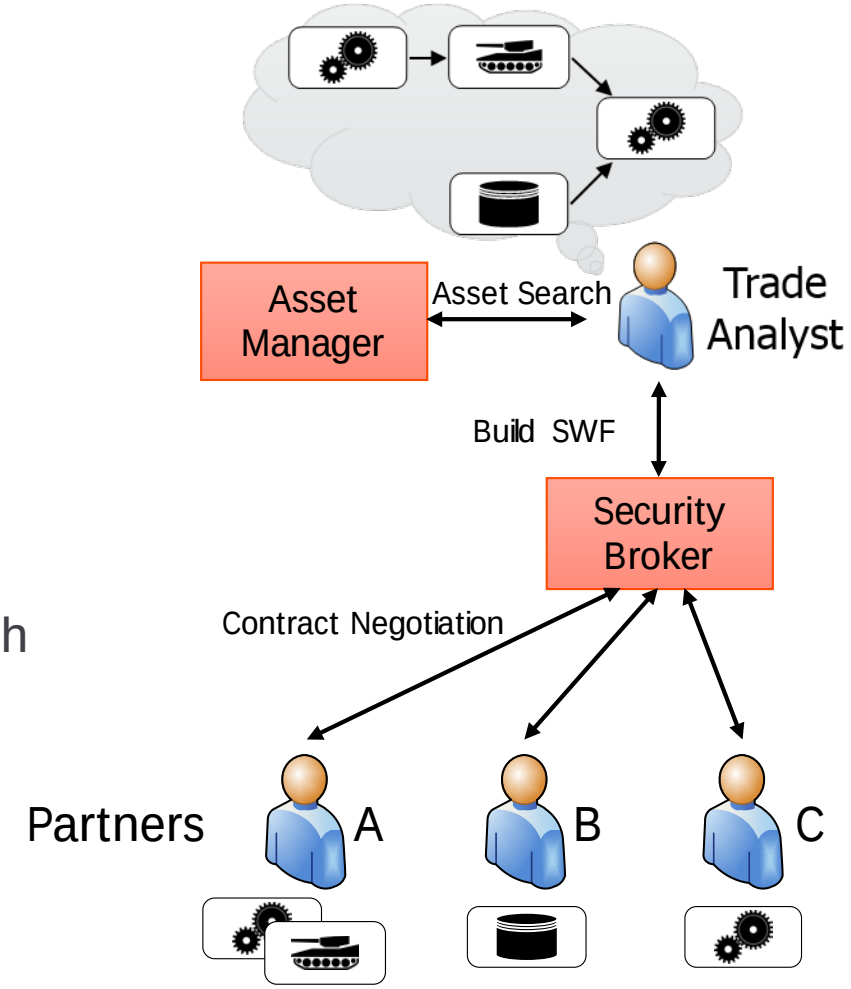


© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Secure Workflows

- AoA applications involve multiple organizations and their assets
  - Interactions must be agreed upon by the entities involved
- The Secure Workflow (SWF) is:
  - A model of an authorized analysis application…
  - …where assets are attached with limits set by Asset Owners (e.g. call limit, timing)

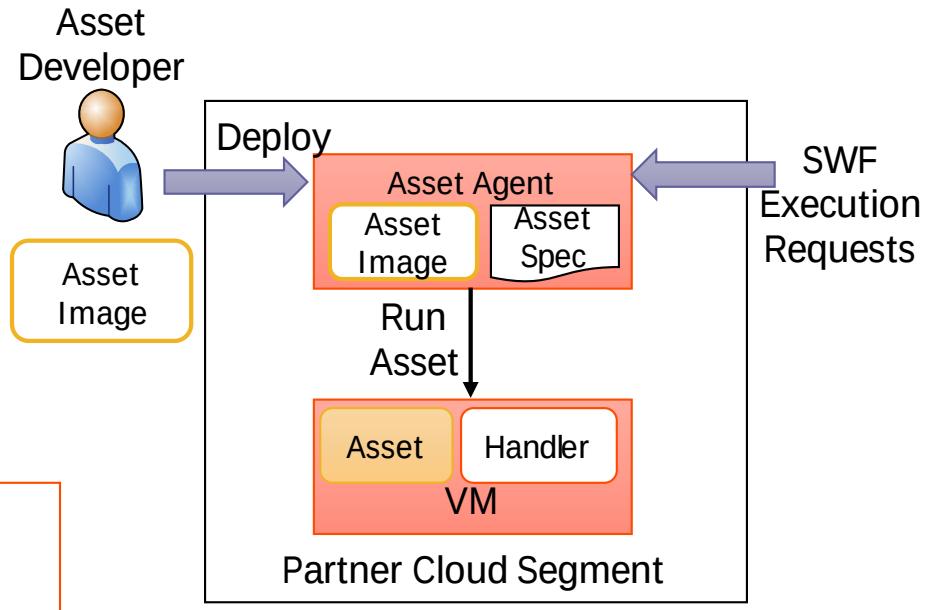


© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Asset Management

- Challenges:
  - Assets are heterogeneous
  - Assets could be malicious
  - ...but still need collaboration
- ECCA Solution: Asset Agents



Maintain asset containers

Publish asset meta-data

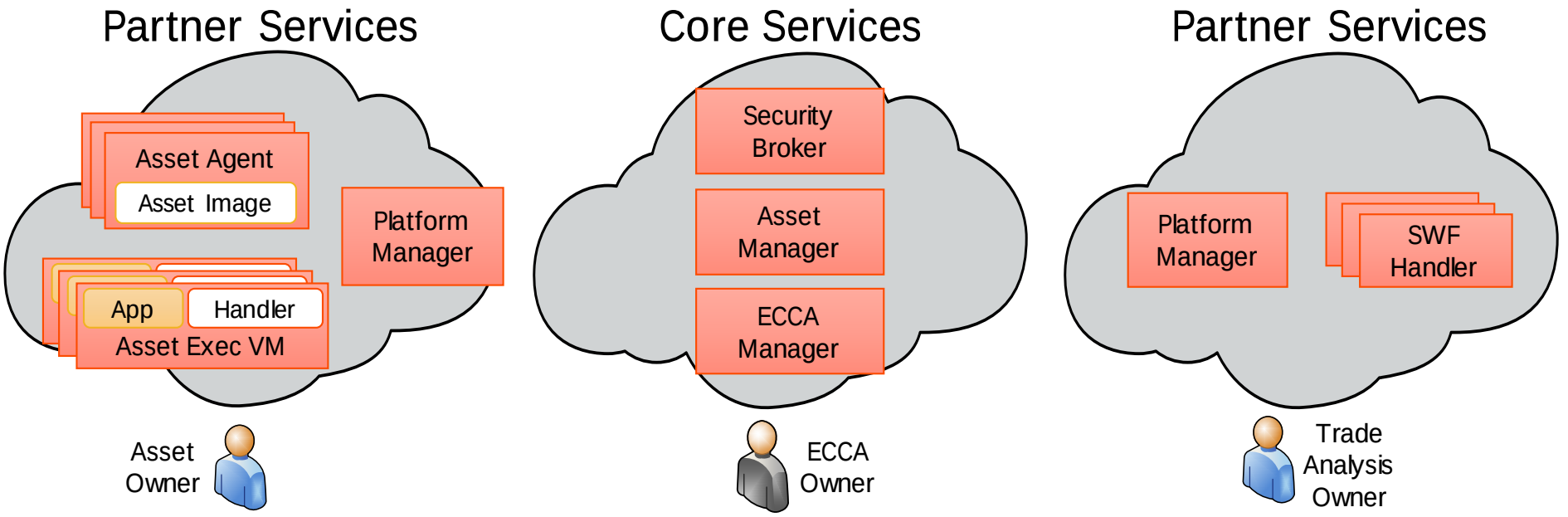
Isolate with automatically generated handlers

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Design

Distributed, Micro-service Architecture



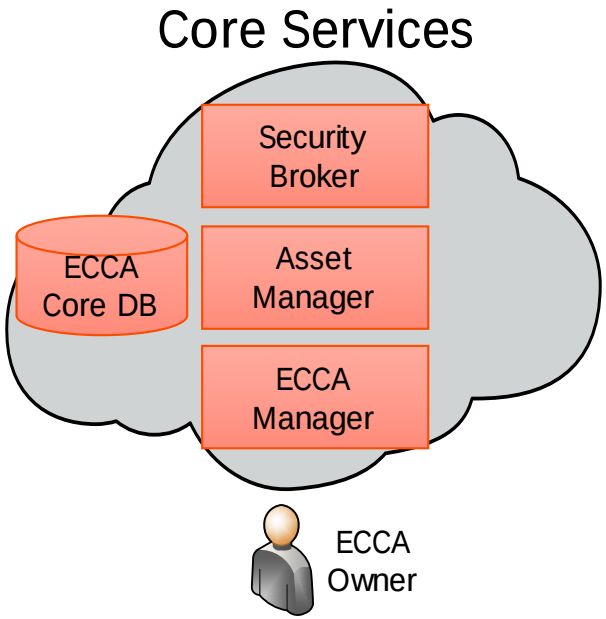
ECCA services manage cloud segment federation

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Design
Core Services

Security Broker
- Manages allowed ECCA entities in graph DB
- Orchestrates the SWF execution



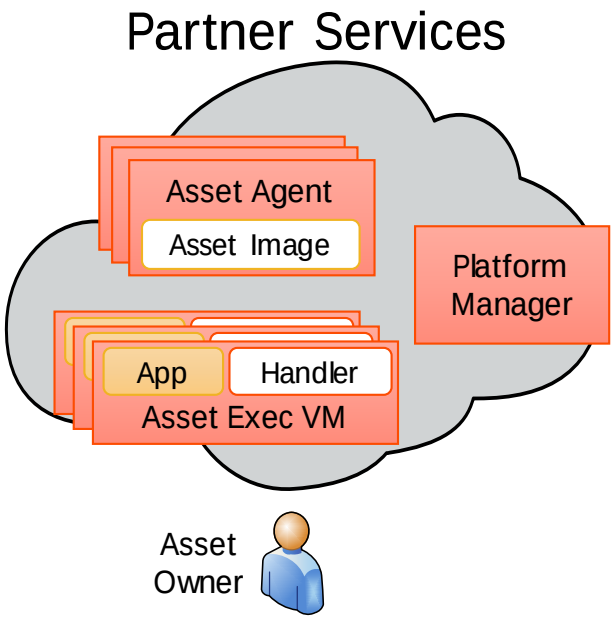
Asset Manager
- Facilitates asset meta-data searches in the ECCA Core DB

ECCA Manager
- Controls allowed Partner organizations
- Controls resources available for AoA applications

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Design
Partner Services: Asset Management



Platform Manager
- Interfaces to ECCA
- Enables peering among other Partner cloud segments
- Enables Asset publishing

Asset Agent
- Maintains a Partner asset within their cloud segment

Asset Execution Infrastructure
- Virtual Machine(s) execute Asset App
- Handler service isolates Asset App
- Supervisor manages Asset Apps based on SWF constraints

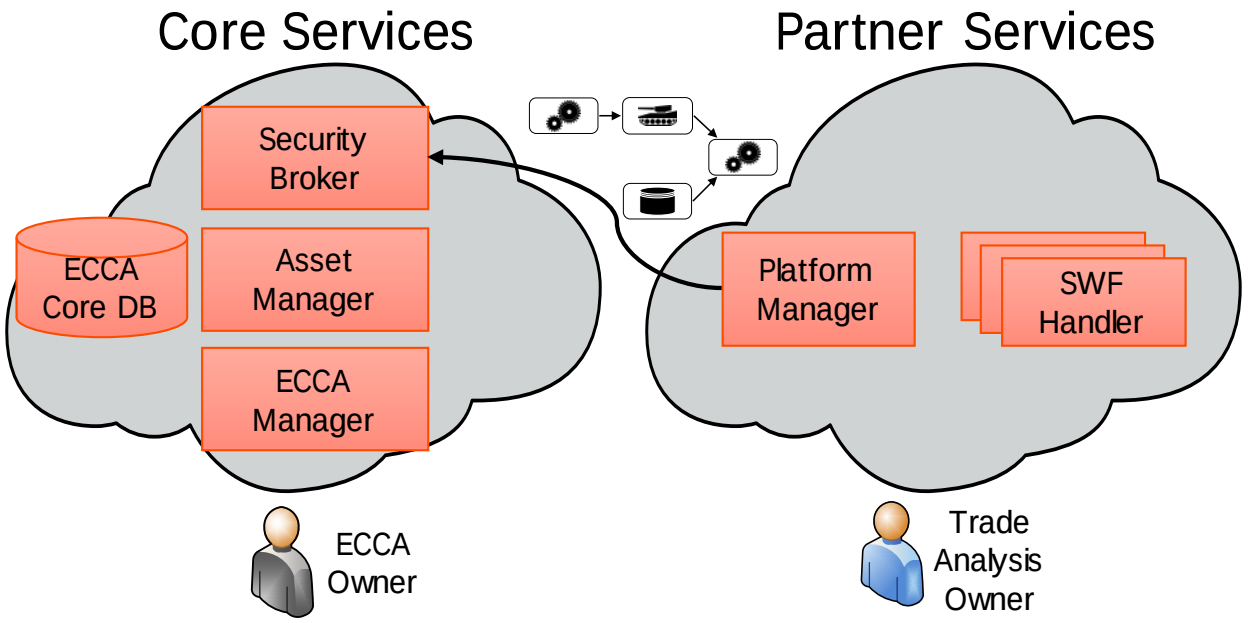
© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Design
Partner Services: SWF Management

Platform Manager
- Maintains SWF with the Security Broker

SWF Handler
- Enable construction of SWF from deployed assets within ECCA
- Submit initial data and received SWF results

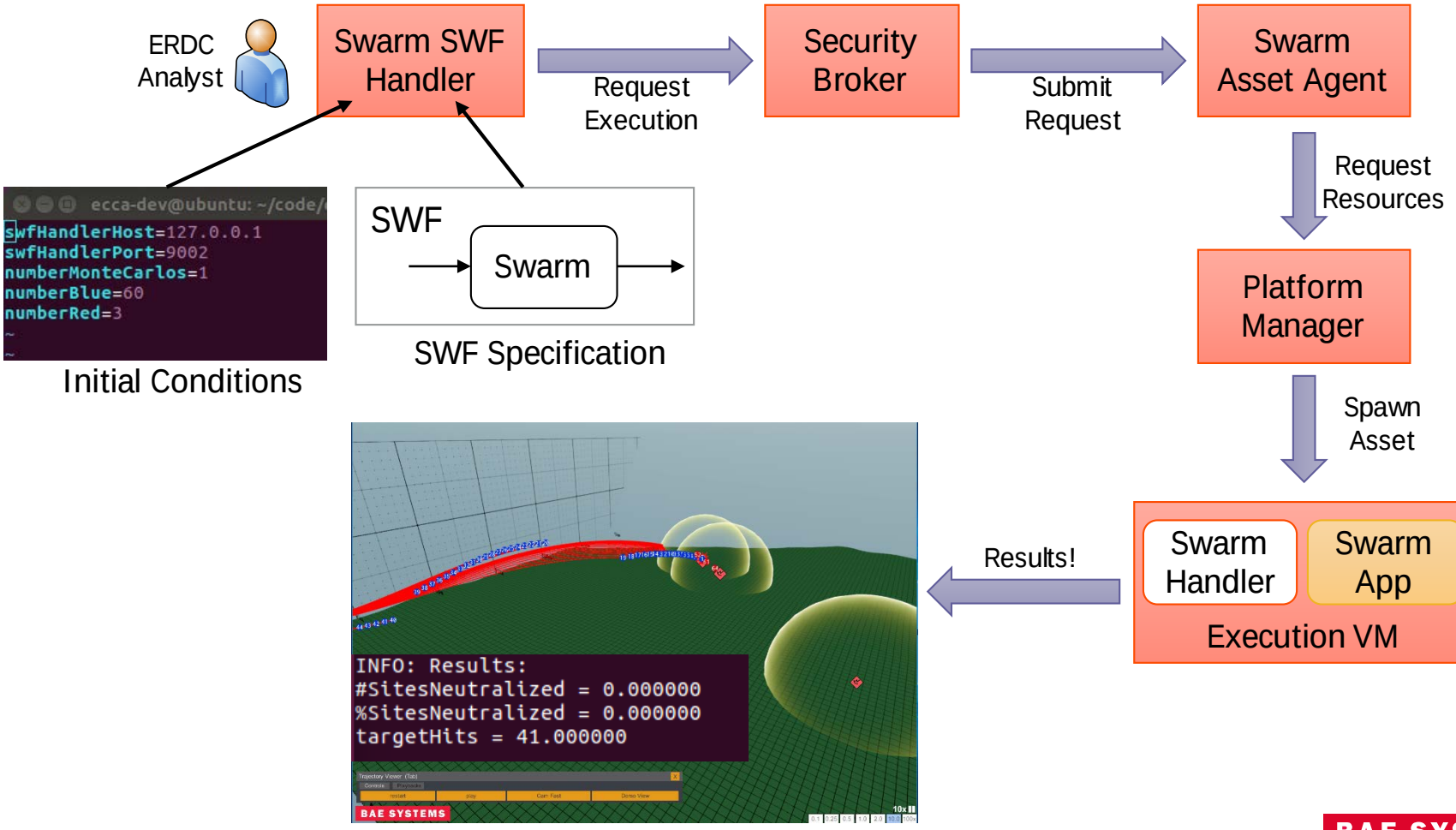


© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Program Status

ECCA lab prototype is live…



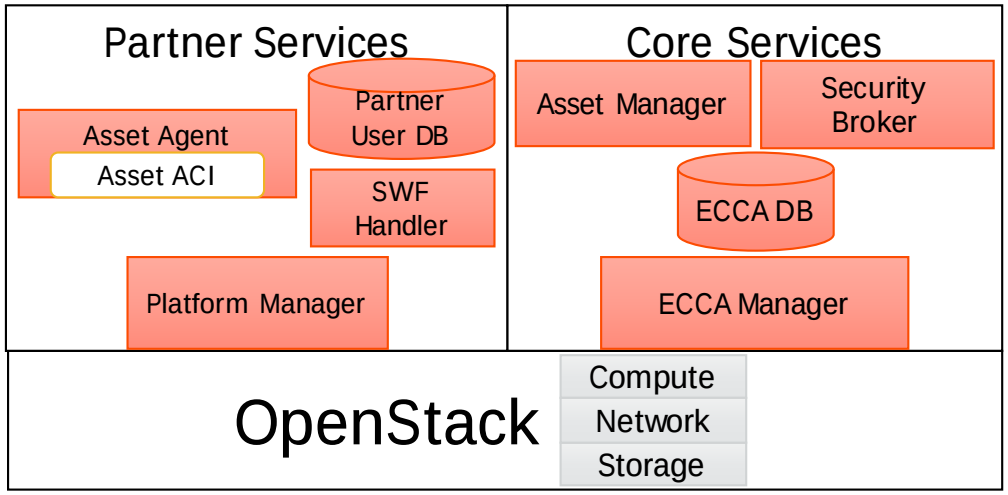
© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

ECCA Program Status

...more work remains to go to prime time!

Integration and test on OpenStack:



Further R&D:

- Cross Cloud Peering Mechanisms
- Commercial Tool Integration
- “ERS Language”
- Asset Reputation and Trust

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Conclusion

- Dynamic threats call for rapid DoD system design, test, and evaluation processes.
- ECCA is the first step to facilitate secure collaboration among DoD partners.
- This collaborative environment will provide tools for decision makers and engineers to develop, assess, and (re)engineer resilient systems.

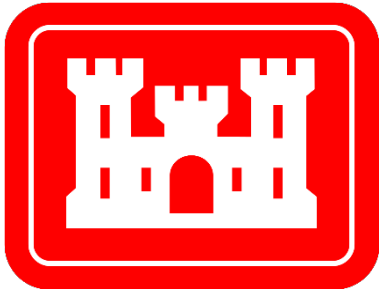
© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Acknowledgements

- The ECCA Team:
  - Brent Baker, Collin Blakley, Greg Eakman, Rob Ross, Bill Sexton, Chris Wentland

- This research effort was funded by the US Army Corp of Engineers ERDC



© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Thank you!

© 2017 BAE Systems

Solving Cybersecurity Skills Shortage With Apprenticeships and Certifications

NDIA

20th Annual Systems Engineering Conference

Girish Seshagiri

19734

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Topics

- Why We Are Here
- Ubiquitous Software Defects, “Patch and Pray”, What is at Stake
- Swiss/German Dual Track “Learn and Earn” Model
- DoL Registered Apprenticeships
- Community Initiative Center of Excellence for Secure Software (CICESS)
- Takeaways and “ASKs”

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Takeaways

- **Sense of urgency** to address unsustainable trends and exploit rare economic development opportunity to create hundreds of thousands of middle class jobs
- Industry/government/academic coalition led by industry to address **"skills gap"** and talent pipeline
- Connect education directly to a job through a dual learn and earn **registered apprenticeship program (Because "Nothing Else Works")**
- Develop **skilled workforce** based on validated competencies and industry standard certifications
- Apprenticeships are good for business with **positive return on investment**

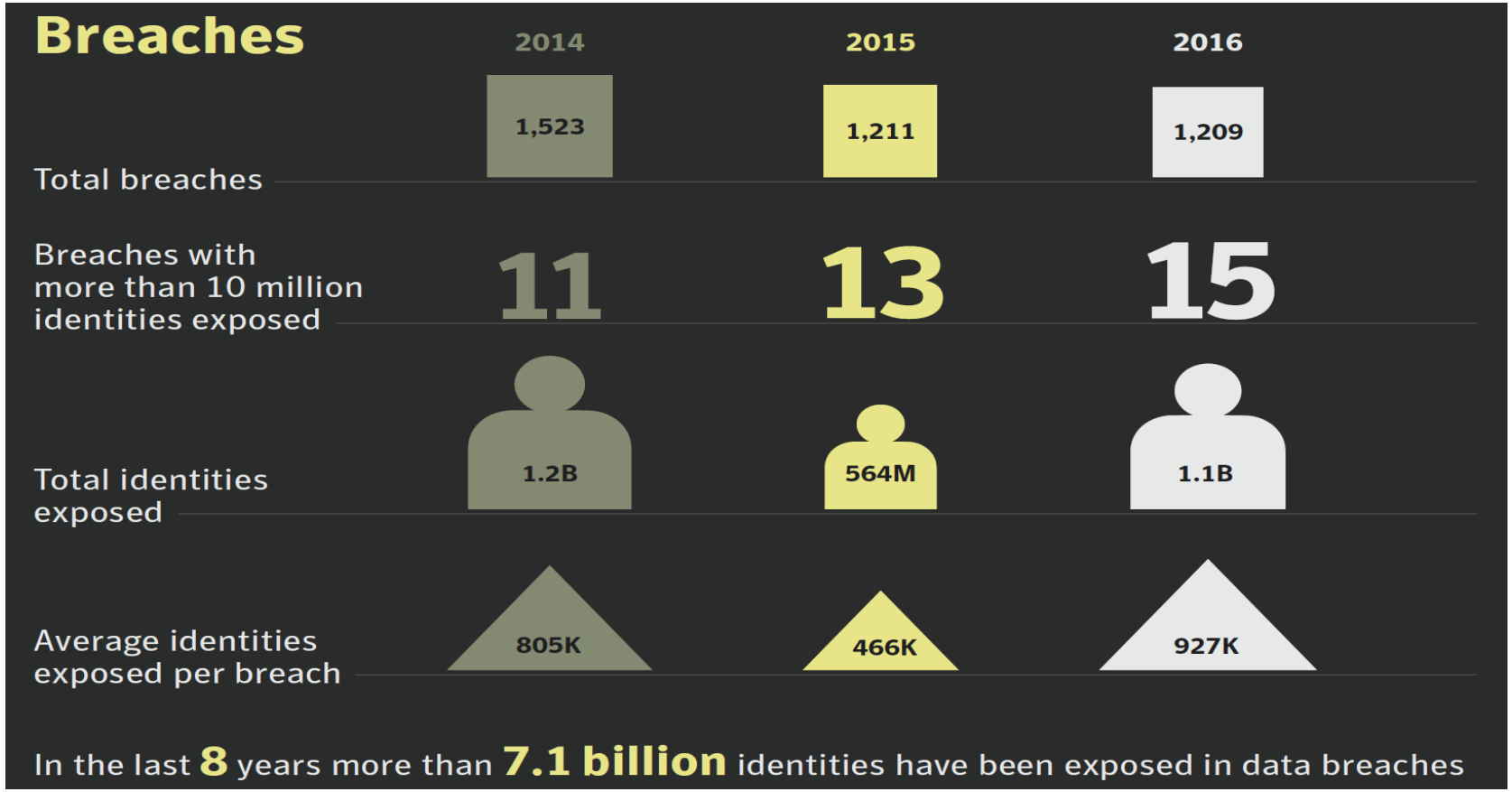
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Why We Are Here

- Increasing number of cyber attacks against critical infrastructure
- 90% of attacks are successful by exploiting defects in software
- Software developers not trained to deliver software with fewer vulnerabilities
- 1.5 million cybersecurity jobs currently unfilled
- High youth unemployment and large number of under-employed people
- Student debt > 1.0 trillion
- Cost of status quo

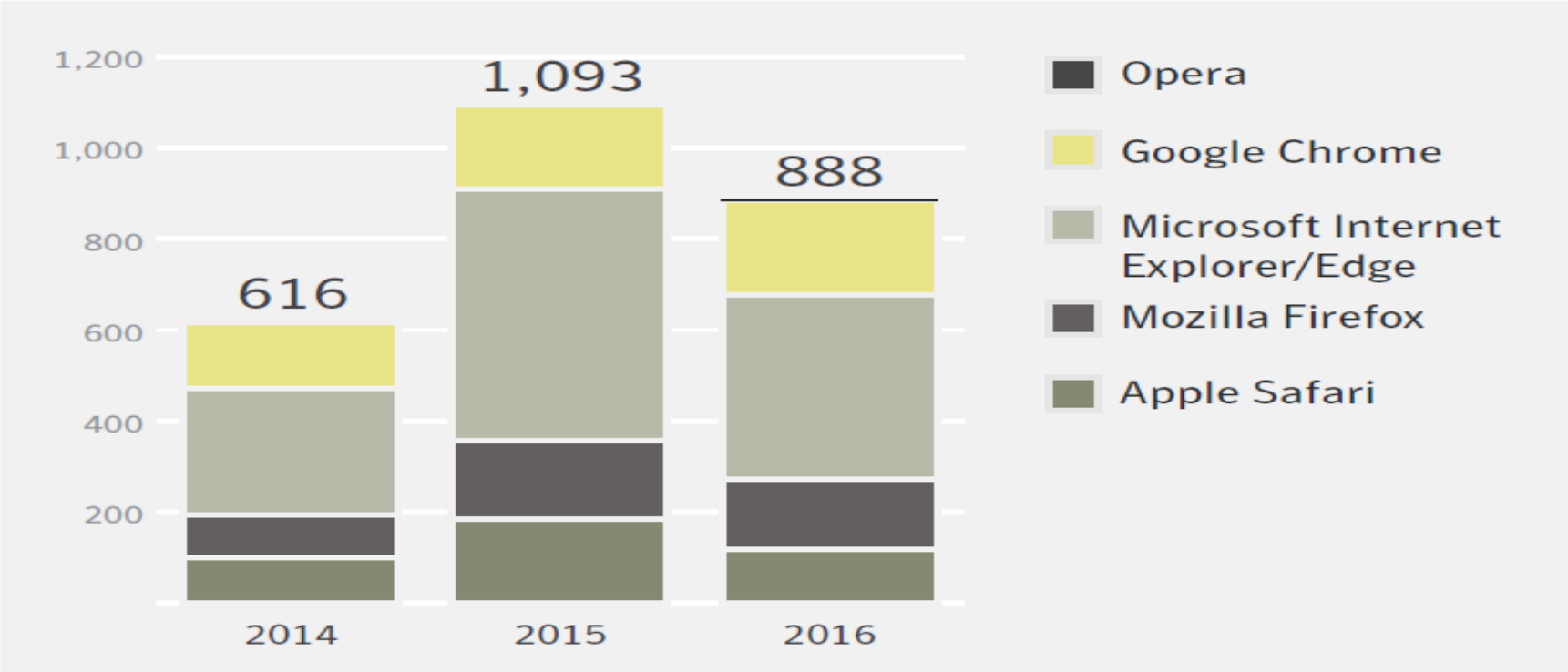
(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Personal Identity Breaches



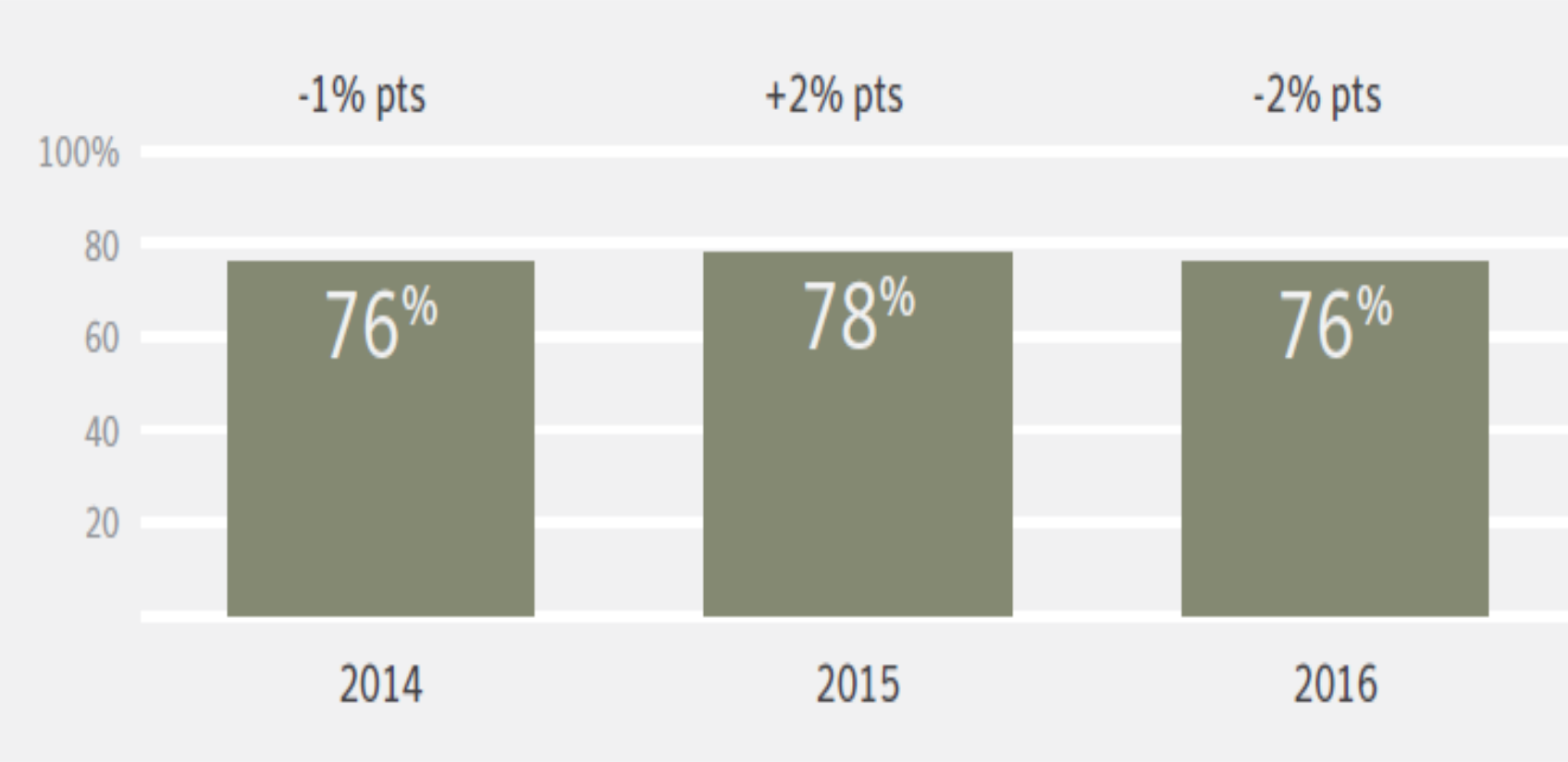
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Browser Vulnerabilities



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Websites with Vulnerabilities



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 1

Microsoft Patch Tuesday

On Tuesday, September 12, Microsoft released fixes for more than 80 security issues in multiple products, including Windows, Office, Microsoft .NET Framework, Flash, Internet Explorer, and Edge.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 2

Apache Struts Vulnerability Exploited in Equifax Breach

Equifax has acknowledged that the massive breach that exposed personal information of as many as 143 million people was due to a failure to apply a patch for a vulnerability in Apache Struts. A patch for the flaw was released on March 6, 2017. The Equifax breach occurred in "mid-May" 2017.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 3

Adobe Security Updates

Adobe has released updates to address security issues in Flash Player, ColdFusion, and RoboHelp for Windows. The Flash updates, available for Windows, Mac, Linux, and Chrome OS, address two critical memory corruption flaws. The ColdFusion update includes fixes for four flaws, and the RoboHelp update fixes two flaws

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 4

Patches dominate the Top of the News this week.

Bill Murray speaks for many when he writes: "The cost to tolerate or remediate a design, recording, or coding error goes up exponentially with the time to its discovery. **There is something fundamentally wrong with an industry in which the toleration, indeed the institutionalization, of late discovery and remediation of error is as it is in ours."**

And John Pescatore offers a path toward fixing that fundamental flaw in the software industry, describing a future where larger buyers of software (government, for example, along with the Business Roundtable) set a much higher bar for application security testing at multiple stages of the development life cycle, both for custom software they develop and for every package they buy, with **substantial contractual penalties for vendors who fail**.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake - 1

Some US States Are Going Back to Paper Ballots

In the wake of rising concerns about the security of electronic voting systems, several US states are returning to the use of paper ballots for their elections. Georgia will pilot a paper-ballot system in elections this fall.

FDA Approves Pacemaker Patch, Announces Recall of Abbott/St. Jude Medical Devices

The US Food and Drug Administration (FDA) has announced a recall of more than 450,000 pacemakers because they require a firmware update to address several security issues. The recall applies to several models of pacemakers manufactured by Abbott, formerly known as St. Jude Medical. Patients must visit their doctor's office where the update can be installed while the device is in backup mode. The flaws could be exploited to gain unauthorized access to vulnerable devices and issue commands to modify the pacemaker's settings and functionality.

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake - 2

Car Safety Vulnerability Lies in the Way CAN Handles Error Messages

A vulnerability in the Controller Area Network (CAN) that exists in most new automobiles could be exploited to shut down components of the car, including safety systems. Any component connected to the car's CAN bus could be affected. The issue is not one that can simply be patched because it lies in the CAN bus messaging protocol standard. Components that send too many error messages are disconnected from the CAN, so if attackers can spoof error messages to appear to be coming from a targeted component, that component could be shut off from the CAN.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake -3

National Infrastructure Advisory Council Report - A Pre 9-11 Moment

"There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack, [for the nation] to organize effectively and take bold action," said the US National Infrastructure Advisory Council report. The report lists 11 recommendations, including "establish separate, secure communications networks specifically designated for the most critical cyber networks; ... identify best-in-class scanning tools and assessment practices; ... [and] establish clear protocols to rapidly declassify cyber threat information."

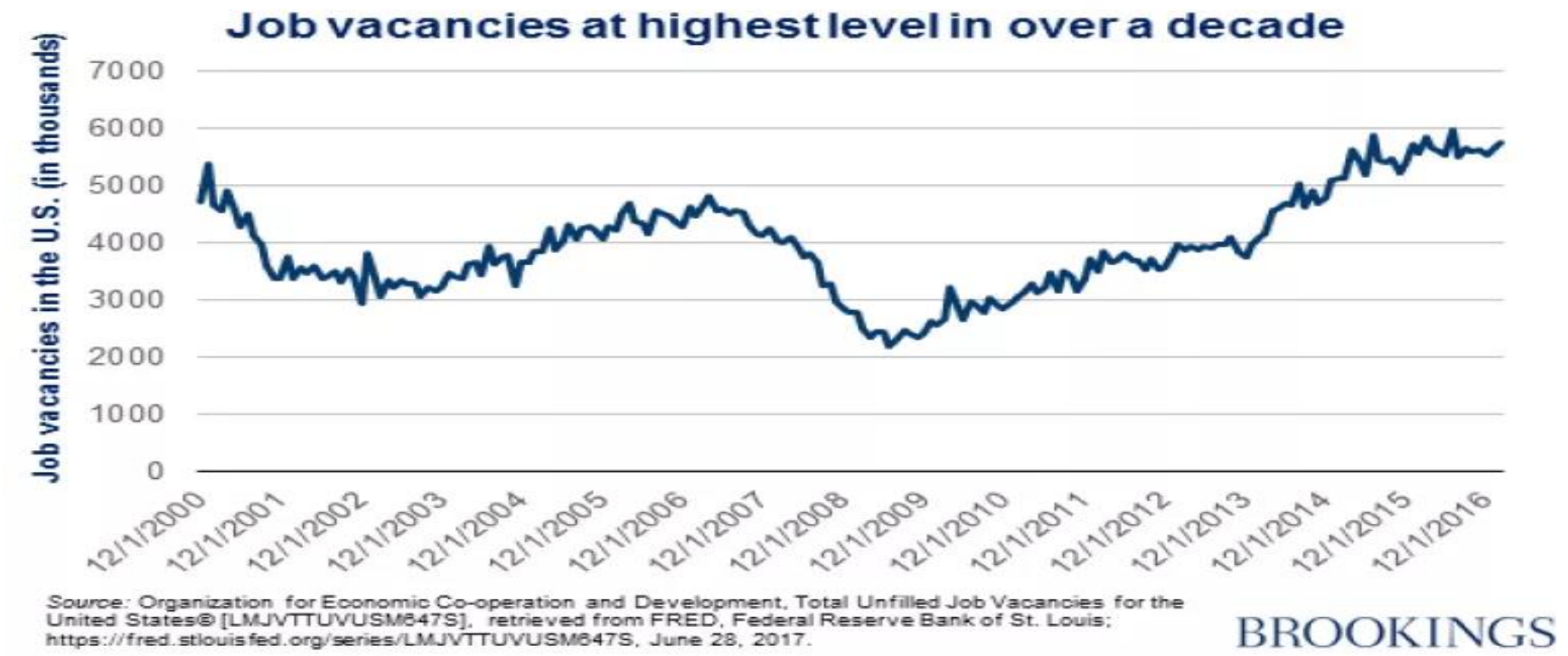
(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake - 4
IoT Risks



(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Total Number of Unfilled Jobs

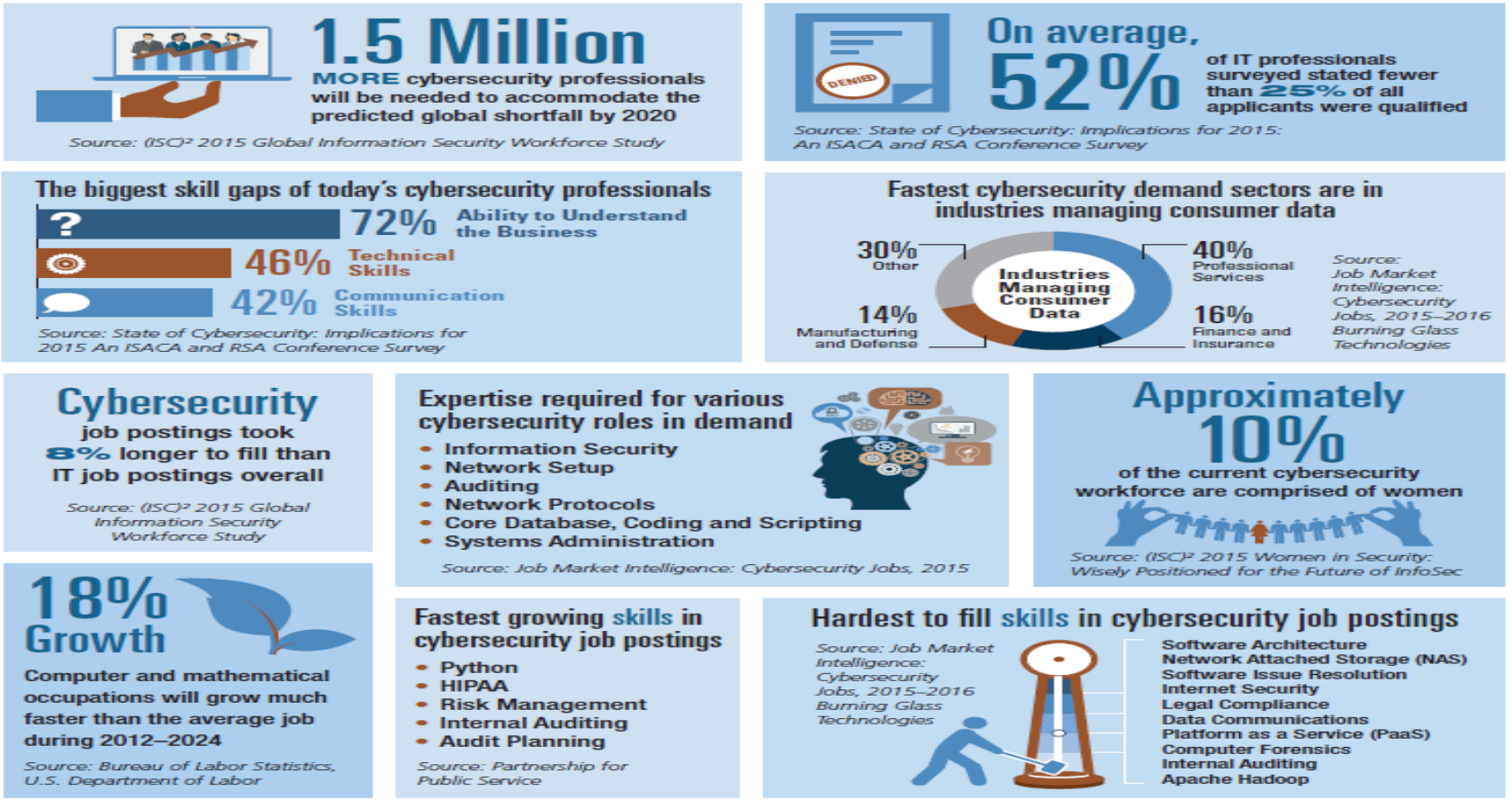


Source: Organization for Economic Co-operation and Development, Total Unfilled Job Vacancies for the United States© [LMJVTTUVUSM647S], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/LMJVTTUVUSM647S, June 28, 2017.

BROOKINGS

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Cybersecurity Skills Shortage



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Cybersecurity: the Hottest New Major In College

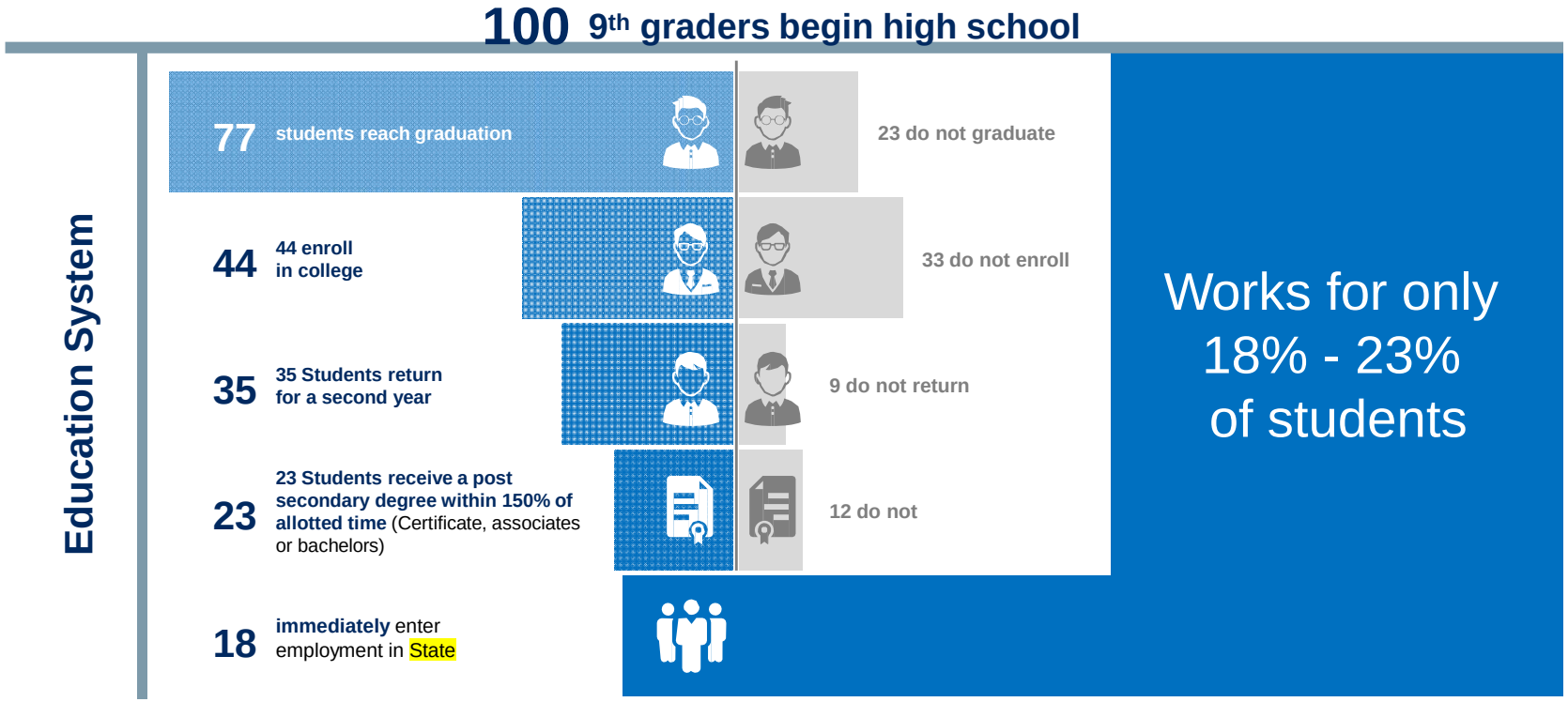
Large numbers of US colleges have added undergraduate cybersecurity majors, cybersecurity concentrations to other majors, and master's degree programs in cybersecurity. Most colleges, however, do not know what to teach, and **many are teaching students only how to admire the cybersecurity problem, but not how to fix it.** Further, computer science graduates don't learn secure coding or other technical cybersecurity topics. None of the top ten undergraduate computer science and engineering programs at American universities (as ranked by the U.S. News & World Report) required its students to take a cybersecurity course in order to graduate.

Read more in:

- www.villagevoice.com: How Cybersecurity Became 2017's Hot New Major

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Educational System's Challenge



The challenge: How do we prepare the talent needed by business to be globally competitive

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Cost of Status Quo

Item	Cost
Two-year and four-year college	$400 billion per year
Post-secondary workforce education and training	$600 billion per year
Skills gap	$160 billion per year
Time for new employees to reach full productivity	> Five months on average
Replacing an employee	Ranges from 6 to 24 months of the position's salary

Source: Georgetown University Center on Education and the Workforce

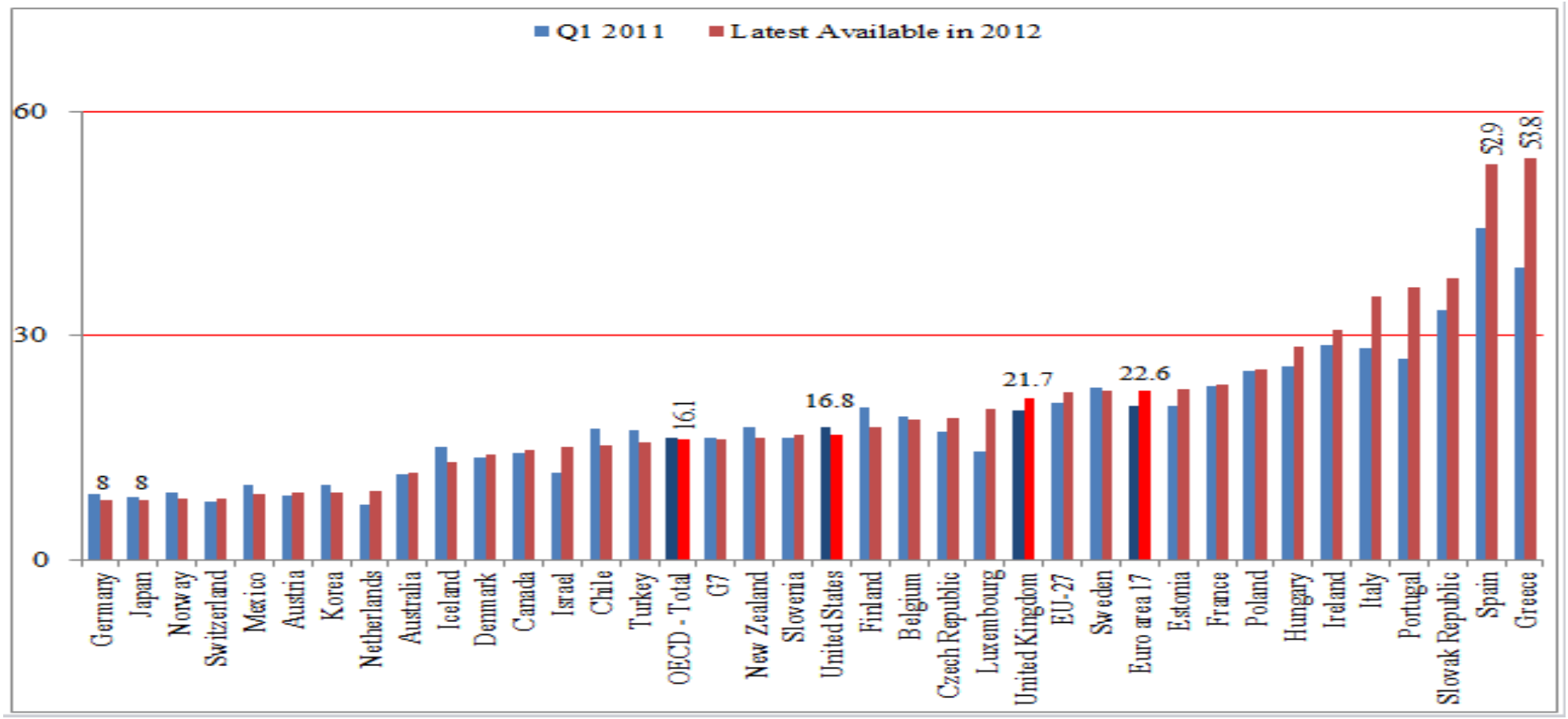
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Swiss Dual Track Vocational Education and Training Model



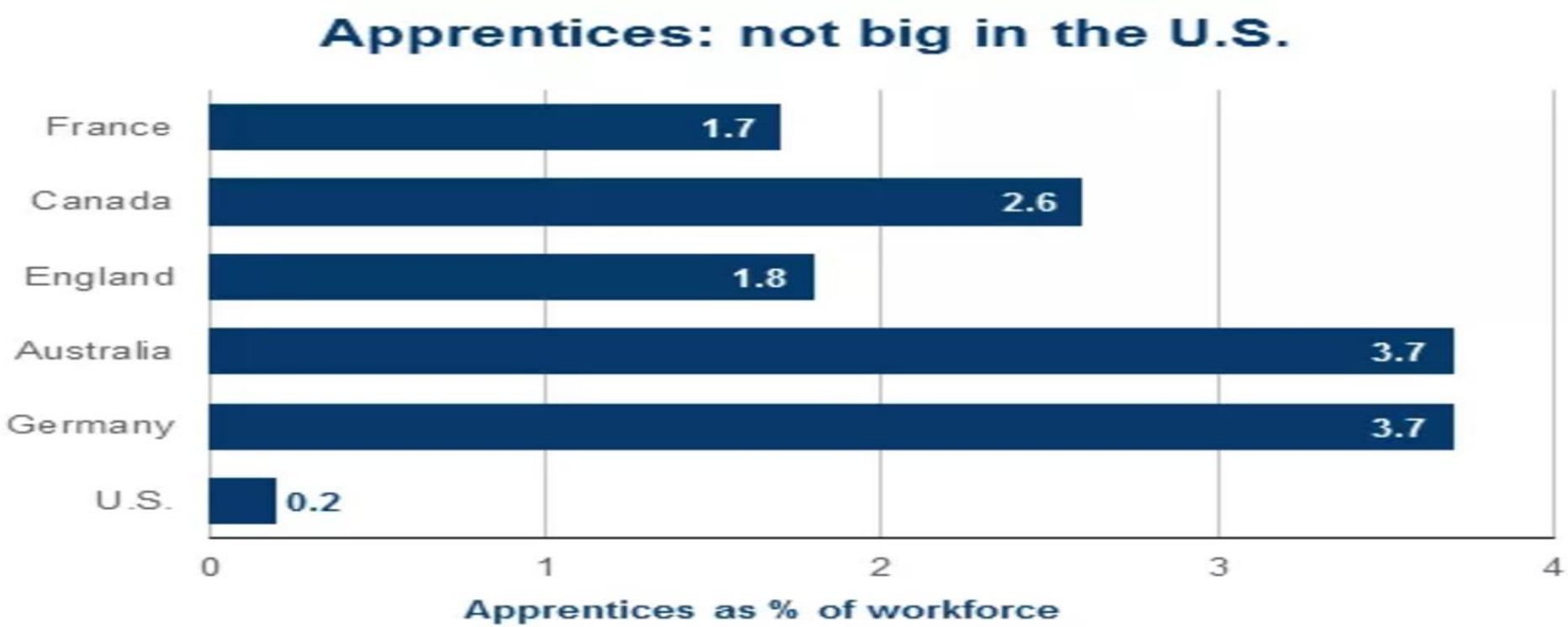
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Youth Unemployment



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Apprenticeships in the U.S.



Source: Robert Lerman, "Are Employers Providing Enough Training? Theory, Evidence and Policy Implications," prepared for National Academy of Sciences, 2015

BROOKINGS

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

US Department of Labor Initiative

ApprenticeshipUSA

- An exciting national renewal and reimagining of registered apprenticeship
- Learn, borrow and steal from Europe
- Expand in new, non-traditional industries and occupations
- $165 million in new funding for Registered Apprenticeship

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

DoL Registered Apprenticeship Requirement

5 Core Components of Registered Apprenticeship

Employer Involvement Is Integral	Employer is the foundation for the RA program and must be directly involved and provider of OJT
Structured On-the-Job Training with Mentoring	Minimum of 2,000 hours Structured and Supervised
Related Training and Instruction	**144 hours recommended per year** Parallel | Front-loaded | Segmented Options
Rewards for Skill Gains	Increases in skills brings about increases in earnings
National Occupational Credential	Nationally recognized credential showing job proficiency. Sponsor certifies individual is fully competent for career.

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Employer-Led Collaborative Design



© iShpi Information Technologies, Inc. (DBA iSHPI). All Rights Reserved

Why Apprenticeships?

Because Nothing Else Works

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CICESS

- Community Initiative Center of Excellence for Secure Software
- Solving Cybersecurity Skills Shortage With Apprenticeships and Certifications
- Launched successfully in Fall 2015, partnering with Illinois Central College and the Peoria Public Schools

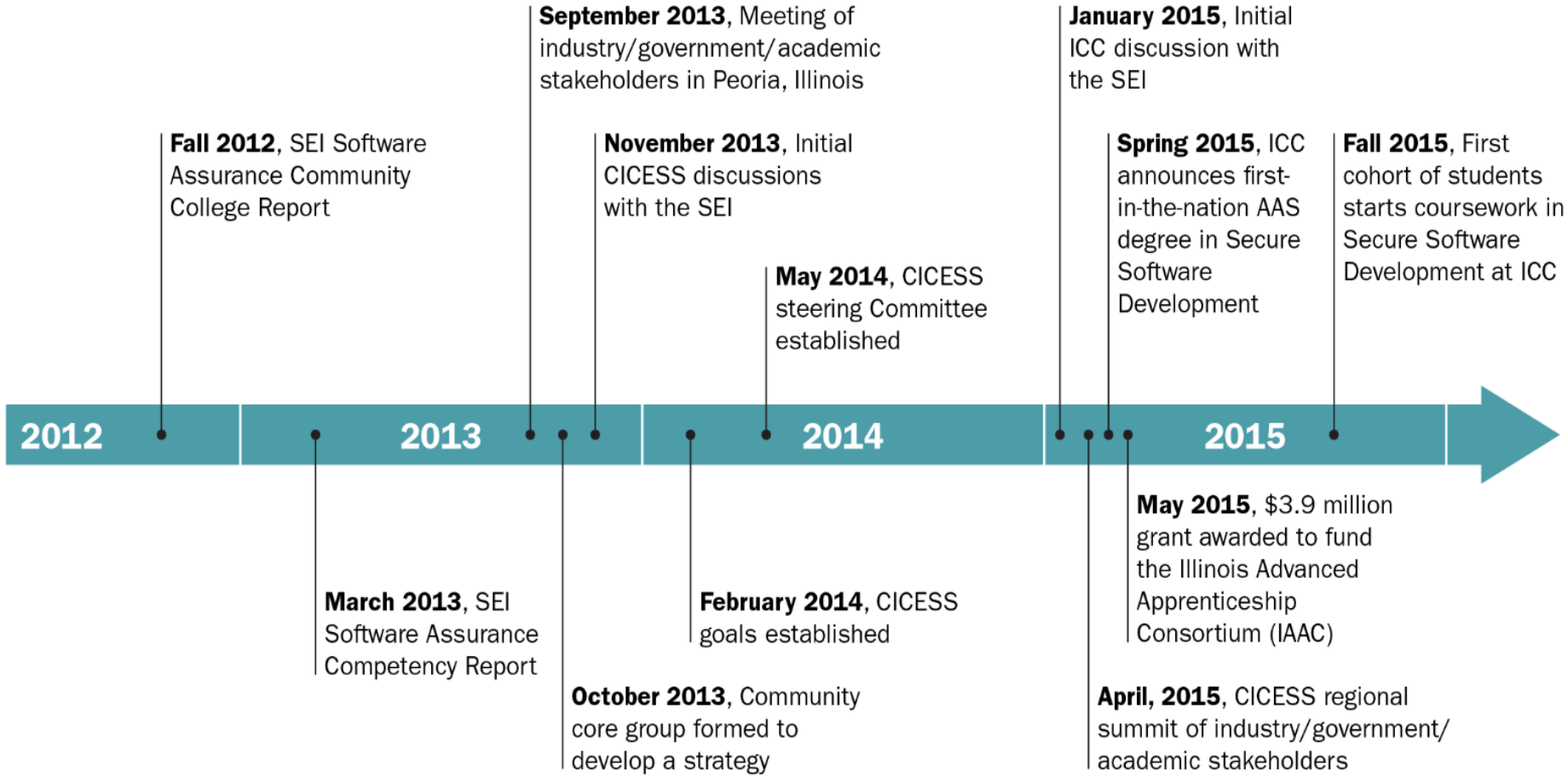
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

A Unique Collaboration – Industry, Government, Academe



CMMIDEV /5 SM
Exp. 2017-03-07 / Appraisal #21757
(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Timeline for the Community College and Industry Apprenticeship Program



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CICESS Design – 1

- Standard academic curriculum leading to first-in-the-nation AAS Degree in Secure Software Development
- Berger Aptitude Test (B-Apt) for Computer Programming for entry to the apprenticeship program
- Standard apprenticeship curriculum based on Carnegie Mellon University Software Engineering Institute (CMU/SEI) process models
- Validate secure software development competencies – $(ISC)^2$ CSSLP, SEI PSP Developer certifications

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CICESS Design – 2

- Alternating blocks of weeks of academic instruction and apprenticeship on-the-job training in the dual model
- Recurring and one-time-only fees from participating employers for ongoing program administration, apprenticeship curriculum development, and train-the-trainer materials
- Guidelines for minimum hourly wages for the apprentices with flexibility to meet varied human resources practices of participating employers

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Apprenticeship Dual Model
Computer Programing (Secure Software)

2-3-year dual model "learn and earn" program

On the job training	Class room instruction
Employment contract executed between company and apprentice	Full time student AAS degree in Secure Software Development at local community college
Dual work study model with increasing hours under company supervision and mentorship as training progresses	Dual work study model with more classroom hours at the beginning
Standard apprenticeship topics defined by industry and aligned with Carnegie Mellon University / Software Engineering Institute	Curriculum created by Carnegie Mellon University and adopted to meet industry requirements

Practicum examination and standard industry certifications to validate competency

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Secure Software Development AAS Degree

CS I: Programming in Java

CS II: Programming in Java

CS III: Advanced Programming in Java

Structured Query Language

Introduction to Relational Database

C# Programming

Mobile Application Programming

Introduction to Computer Security

Secure Coding

Introduction to Assured Software Engineering

Database Administration

Structured System Analysis

Two electives in computer programming, web, or networking, depending on employer needs

Students must also take 19 credit hours in general education courses.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Alignment with Federal Initiatives

- DHS Cybersecurity Workforce Framework
- NSA Centers of Academic Excellence
- NIST Cybersecurity Education
- DoL American Apprenticeship Initiative
- DoL Registered Apprenticeship standards

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CICESS Value Proposition

- Augmentation of your current workforce development methods
- Ability to plan for and satisfy future needs for hard-to-fill secure software developers
- Ability to build a secure software talent pipeline that includes women and minorities who are trained, mentored, and certified
- A cost-effective solution to training and retaining new workers in secure software development
- High retention rates when apprentices become full-time employees

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Takeaways/"ASKs"

- Act with a **sense of urgency** to address unsustainable trends and exploit rare economic development opportunity to create hundreds of thousands of middle class jobs
- Develop industry/government/academic coalition led by industry to address cybersecurity **"skills gap"** and talent pipeline
- Take immediate steps to connect education directly to a job through a dual learn and earn **registered apprenticeship program**
- In your community, develop **skilled workforce** based on validated competencies and industry standard certifications
- Stay on the message: Apprenticeships are good for business with **positive return on investment**

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Contact

Girish Seshagiri

girish.seshagiri@ishpi.net

703 426-2790

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

A Developing Science of Cyber Security – an Opportunity for Model Based Engineering & Design

October 26, 2017

Jerry M. Couretas, PhD

About Me - Cyber Modeling and Simulation

- 2016 – presentOSD C3CB Cyber Mission Model and Economics of Cyberspace Performance Working Group Lead
- 2013 – 2016 Coordinated OSD DM&SCO Cyber M&S Technical Working group for
- Editor-in-Chief of the Journal of Defense Modeling and Simulation
  - 7/2017 Cyber M&S Special Issue
  - 1/2018 Cyber Special Issue on Developing Science of Cyber Security






GREENLAND
CANADA
RUSSIA
UNITED STATES
CHINA
MEXICO
BRAZIL
ARGENTINA

Hackers Are Targeting Nuclear Plants, U.S. Says

By NICOLE PERLROTH

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

The joint report was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the severity of the threat.

The report did not indicate whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims' computers into the con-



DAVID EULITT/CAPITAL JOURNAL, VIA ASSOCIATED PR

The Wolf Creek nuclear plant in Kansas in 2000. Its operator was targeted by hackers.

cause of confidentiality agreements.

The origins of the hackers are not known. But the report indi-

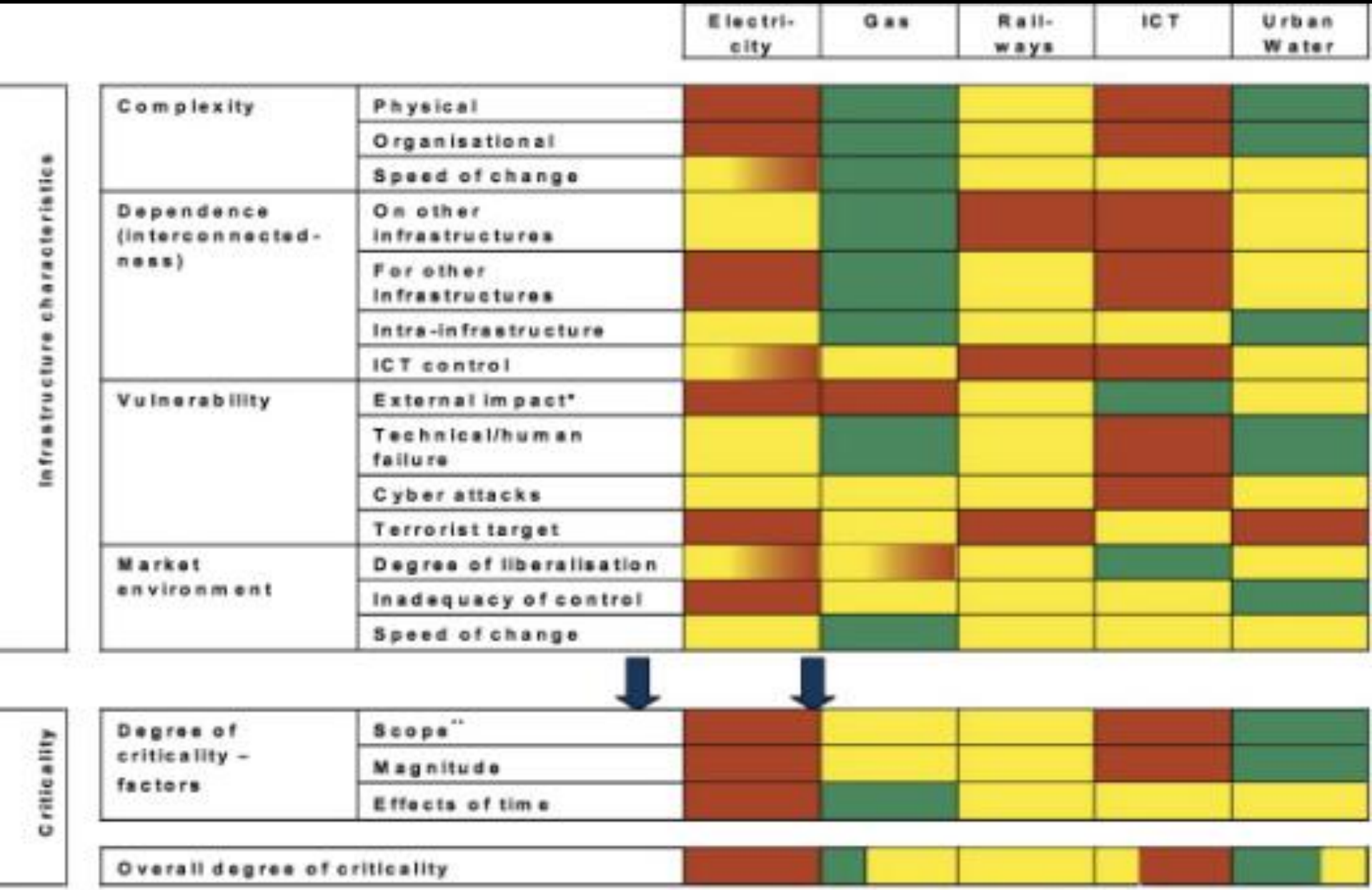
directed their victims' internet traffic through their own machines.

Energy, nuclear and critical manufacturing organizations

"We never anticipated that critical infrastructure control s tems would be facing advan levels of malware," Wellinghoff said.

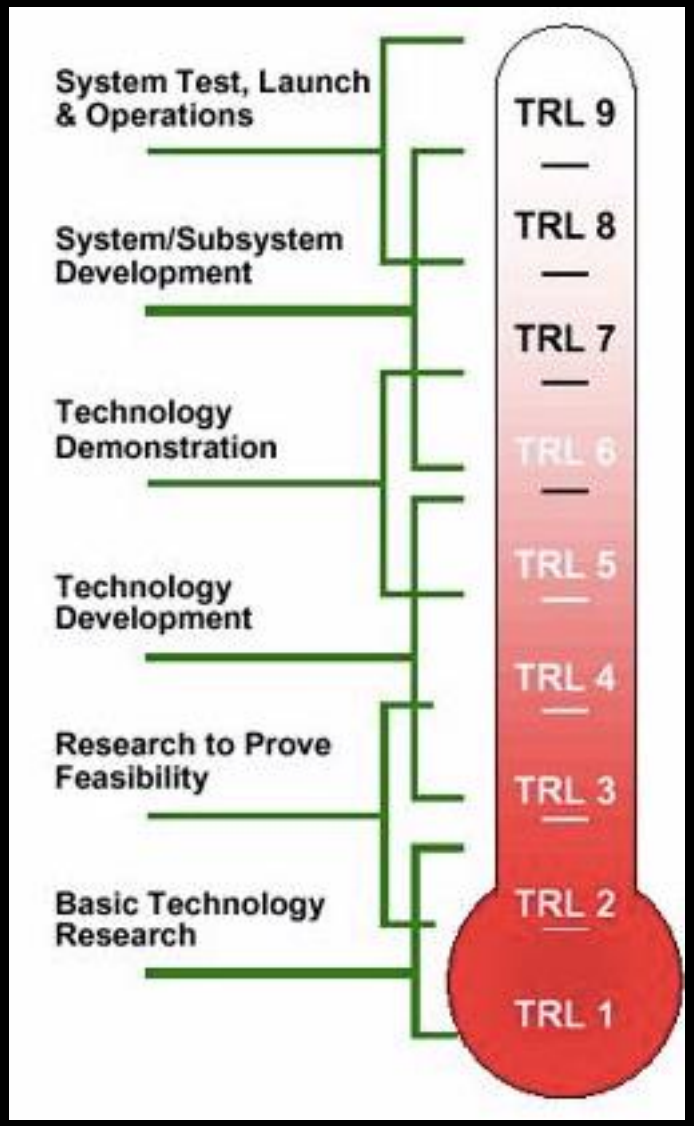



DISASTER
CITY
TEEX


Electri-city
Gas
Rail-ways
ICT
Urban Water
Infrastructure characteristics
Complexity
Physical
Organisational
Speed of change
Dependence (interconnected-ness)
On other infrastructures
For other infrastructures
Intra-infrastructure
ICT control
Vulnerability
External impact*
Technical/human failure
Cyber attacks
Terrorist target
Market environment
Degree of liberalisation
Inadequacy of control
Speed of change
Criticality
Degree of criticality – factors
Scope**
Magnitude
Effects of time
Overall degree of criticality

Cyber in the News
(Stoplight Charts)

M&S Work



NASA Technological Readiness Levels (TRLs)

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

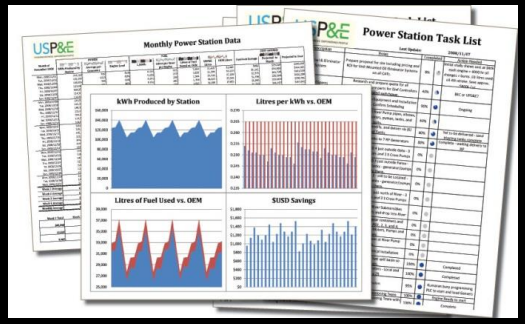
Contents

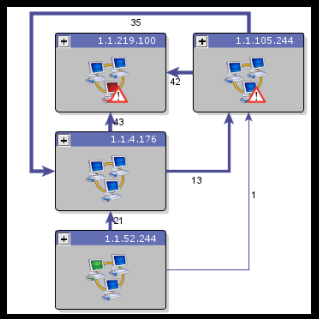
- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

The Scientific Underpinnings of Cybersecurity[1]

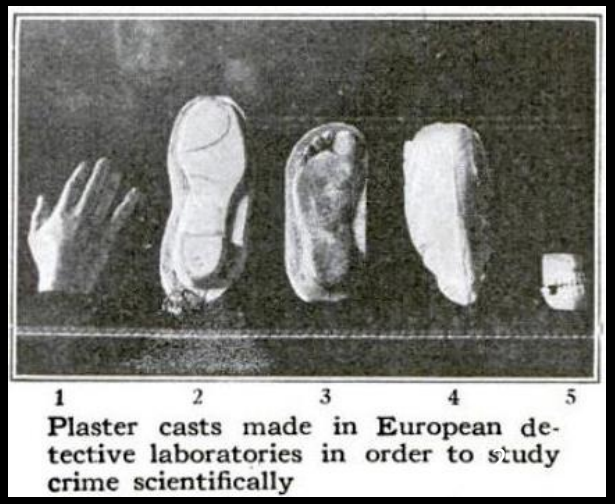
A science of security will develop

- a body of scientific laws
- testable explanations
- confirmation or validation of predicted outcomes





CyVision Network Layout


1 2 3 4 5
Plaster casts made in European detective laboratories in order to study crime scientifically

[1] https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023

Scientific Approach to Cybersecurity

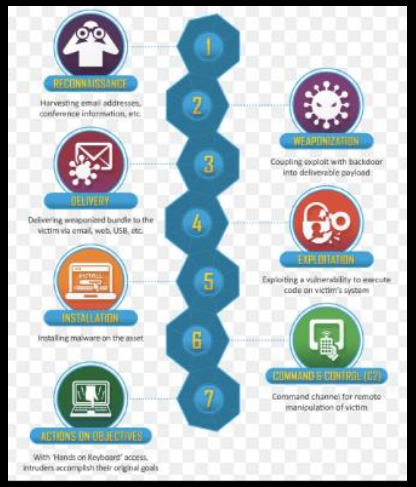
There are strong and well-developed bases in the contributing disciplines:

- mathematics and computer science
- human sciences[1]



A scientific approach to cybersecurity challenges expands understanding of

- systems
- defenses
- attacks
- adversaries





[1] https://www.amazon.com/Research-Methods-Cyber-Security-Thomas/dp/0128053496

National Academy of Science & Cyber Research

Findings included

- Interdisciplinary program examples – U of Bochum
- Questions current research
  - High frequency publishing vs quality
  - Enabling results
- Longer research projects may help

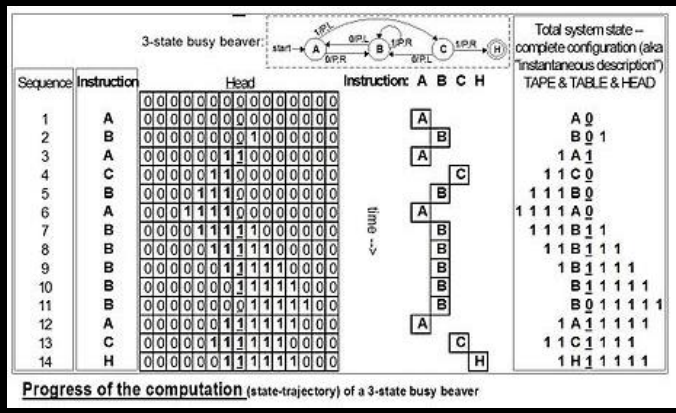
[1] https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023

Example Transitions from Art to Science

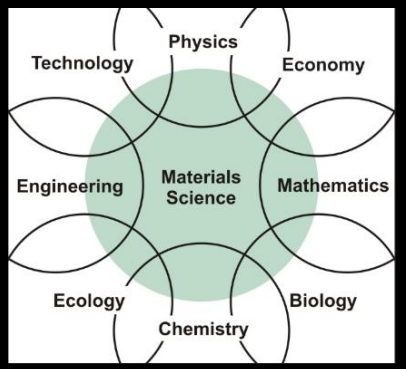
- ***Cyber Security Science***
  - 1700s– 1960s – complex industrial systems with integrated timing handled by respective operators
  - 1960s – 1980s – Systems Theory (e.g., Wymore, Zeigler …) texts introduced
  - 1990s – 2000s – micro computers increased number of entities to point where scale and scope of new systems introduce overall security / safety issues
  - Early 2000s – present – "cyber" introduced as topic in security circles
  - Next step ?

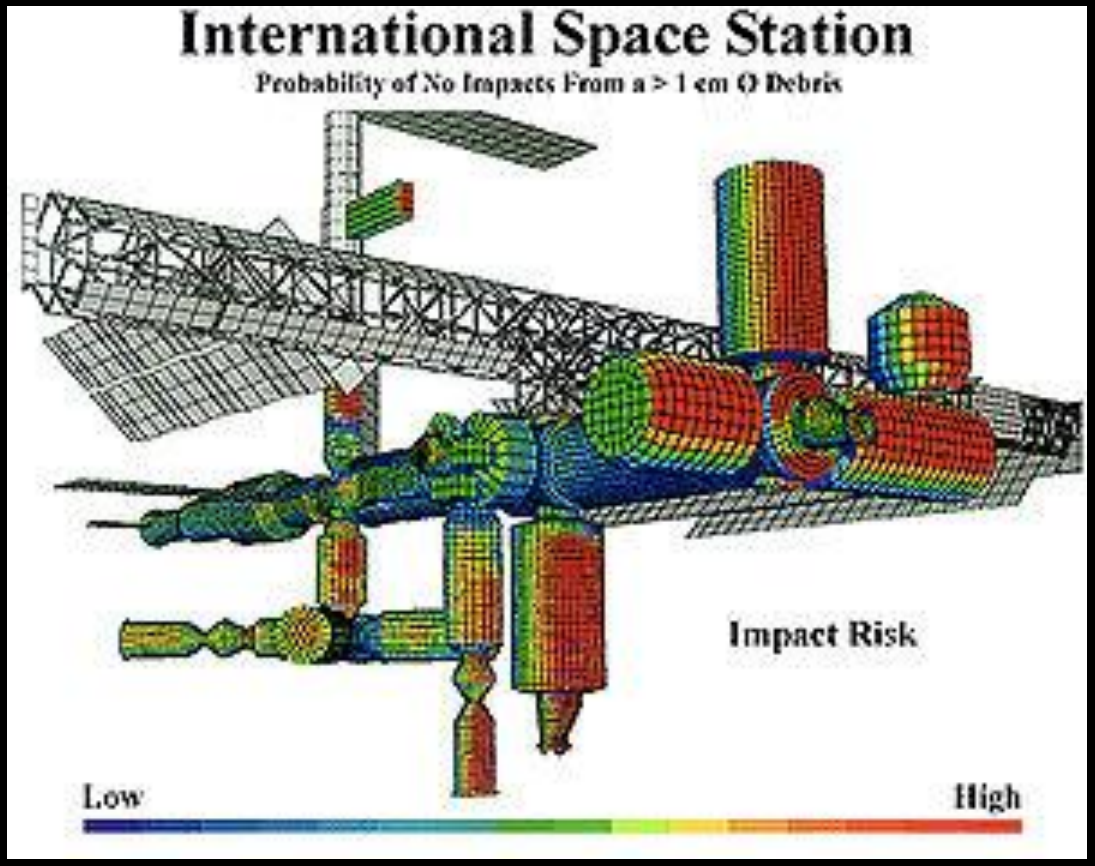


- Computer Science
  - Pre History – 1930s – "computer" was a person who used various devices (e.g., Abacus, analytical engine, etc.)
  - 1930s – 1950s – algorithms (e.g., Church-Turing, …), N. Wiener's "Cybernetics," identified as independent domain
  - 1950s – 1970s – development of computer science curricula and specialized literature (e.g., first PhD ~ 1965)
  - 1970s – present – "Computer Science" with provable hypotheses



- Material Science
  - Pre History to 17th Century – Alchemy
  - 17th Century – 1960s – Metallurgy
  - 1960s – present - Material Science
  - ➢ Still recipe based





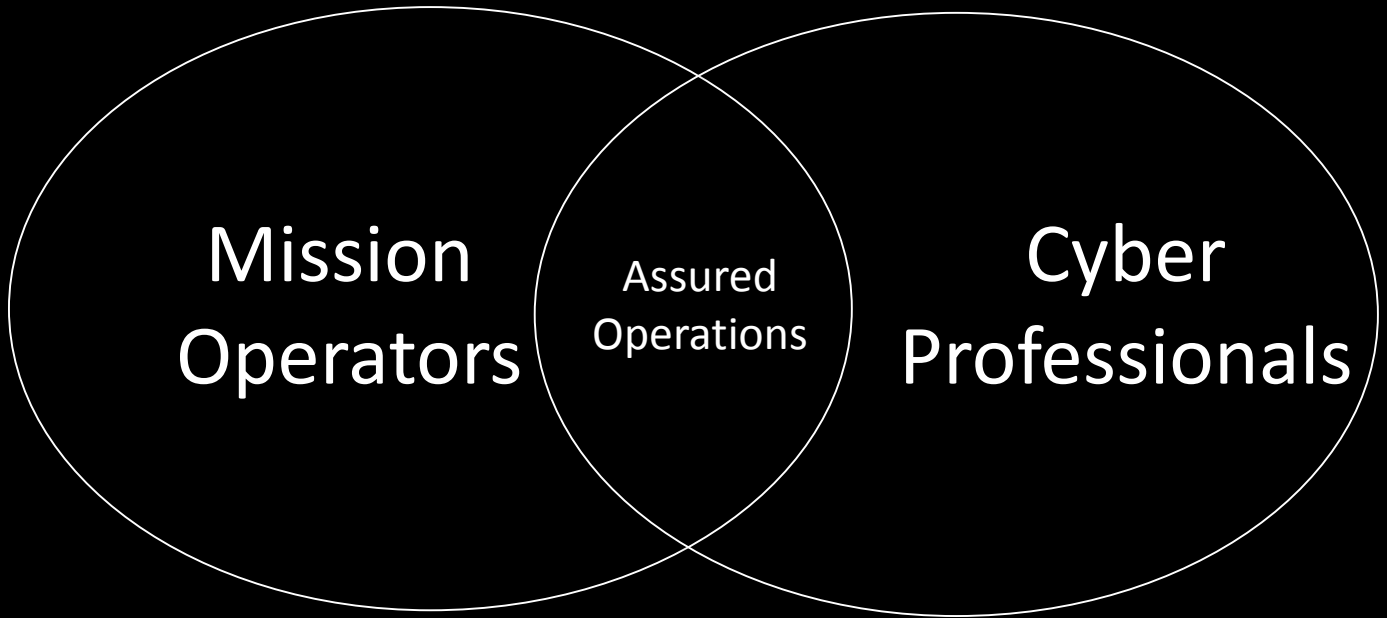
We have built high risk, complex systems, for new domains

Hard Problems are what M&S is For

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Cyber Mission M&S Communities



Cyber for Others

Cyber for Cyber

Cyber for Others, C4O

- Recognise cyber attack indicators
- React – call C4C

Cyber for Cyber, C4C

- Block network attacks
- Mitigate network attacks
- Reconstitute networks

Military Activities & Cyber Effects (MACE)[1]

Military Effects(C4O)

Cyber Effects (C4C)

	Deny	Degrade	Disrupt	Destroy	Digital Espionage
Interruption	✓	✗	✓	✗	✗
Modification	✓	✓	✓	✓	✗
Degradation	✗	✓	✓	✗	✗
Fabrication	✓	✓	✗	✗	✓
Interception	✗	✗	✗	✗	✓

[1] Bernier, M. (2015). *Cyber Effects Categorization - The MACE Taxonomy.* DRDC Center for Operational Research and Analysis. TTCP JSA TP3 Cyber Analysis

Example Cyber Mission Use of Standards

- OASIS standards address IA to protect
  - CybOX (Cyber Observable eXpression)
  - STIX (Structured Threat Information eXpression)
  - TAXII (Trusted Automated eXchange of Indicator Information)

- *Cyber Range Interoperability Standard (CRIS) to connect different range emulations*[1]

  - SISO Training Standards

[1] http://www.dtic.mil/ndia/2014/test/Ferguson.pdf

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

2015 Business Blackout

Lloyd's of London scenario looked at a U.S. power grid failure



[1] https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

… and, while a major cyber attack is unlikely …

Cyber attacks, including against industrial control systems, are a continuing phenomena

Date	Event name	Detailed description	Actors	Motivation	Methodology	Outcome
April 1999 (Milhorn, 2007)	**Gazprom – Russian gas supplier**	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorised Access
July 1999 (National Safety Transport Board, 2002) (Wilshusen, 2007)	**Bellingham**	Over 250,000 gallons of gasoline leaked into nearby creeks and caught on fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb. and April 2000 (Jill Slay, 2008) (Wilshusen, 2007)	**Maroochyshire**	A recently fired employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers and the grounds of a hotel.	Insider attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001 (US House of Representatives, 2005 (SCADA)[1] Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems, 2005	**California**	A hacking incident at California Independent System Operator (CASO) lasted two weeks, but did not cause any damage.	External attack	Unknown and contained	Deliberate	Thwarted
August 2005 (GAO Report, 2007)	**Daimler Chrysler**	Thirteen Daimler-Chrysler US auto manufacturing plants were taken offline for about an hour by an internet worm. An estimated $14m in downtime costs.		Spyware Installation	Zotob Worm and MS05-039 Plug n-Play	Infection
Infection	**Brown's Ferry**	Loss of recirculation flow on a US nuclear reactor down for maintenance caused a manual scram. A worm exploited a buffer overflow flaw in the widely used MSSQL server during the scram.		Unknown	Slammer Worm and Buffer Overflow	Non-industrial control systems targets
Oct 2006 (Wilshusen, 2007)	**Harrisburg**	Hackers gained access to a water treatment plant through an infected laptop.	Targeted Threat Agent	Mischief	Compromised Laptop	Server used to run online games
Jan 2008 (Maras, 2012)	**Lodz**	Attacker built a remote control device to control trains and tracks through distributed field devices. Four trains were derailed with zero deaths. A disgruntled employee installed malicious code on a canal control system.	Targeted Threat Actor, Accident or Insider Attack	Mischief	Altered Universal Remote	Mayhem, Criminal Damage
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the E.ON Kingsnorth power station which caused a 500MW turbine to take an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Project

Insurance Concepts & Systems Engineering for Cyber

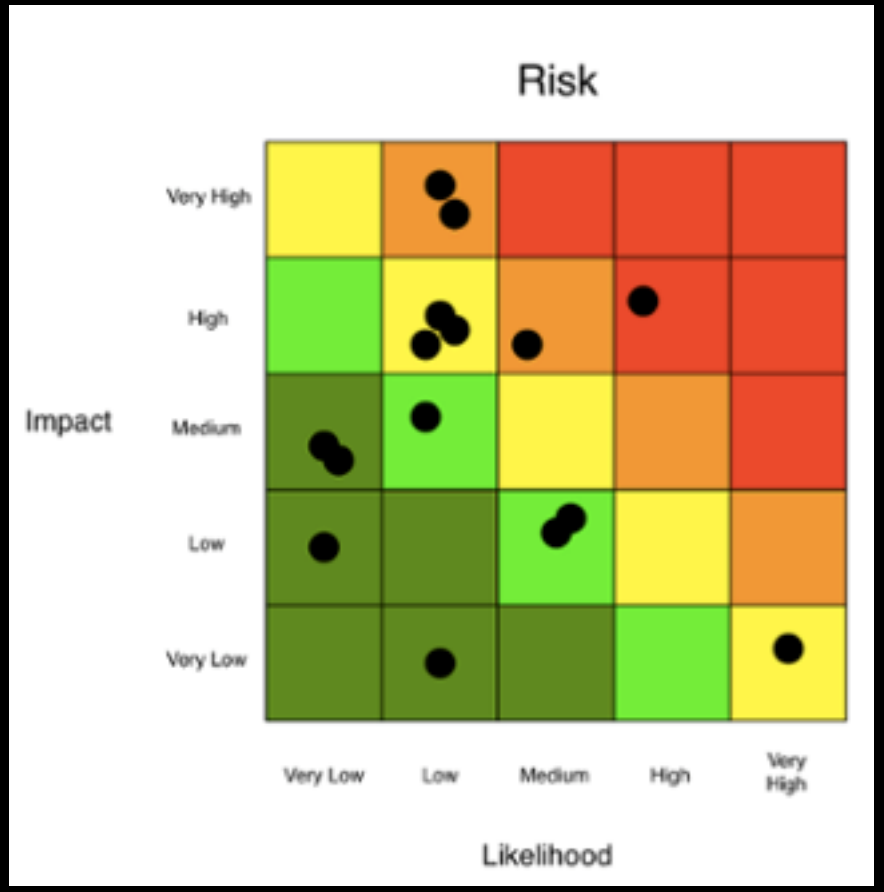
- Böhme & Schwartz (2010) provide an excellent summary of cyber insurance literature and define a unified model of cyber insurance that consists of 5 components:
  - the networked environment
  - demand side
  - supply side
  - information structure
  - organizational environment

- In addition, the defining characteristics of cyber insurance are
  - interdependent security
  - correlated failure
  - information asymmetry

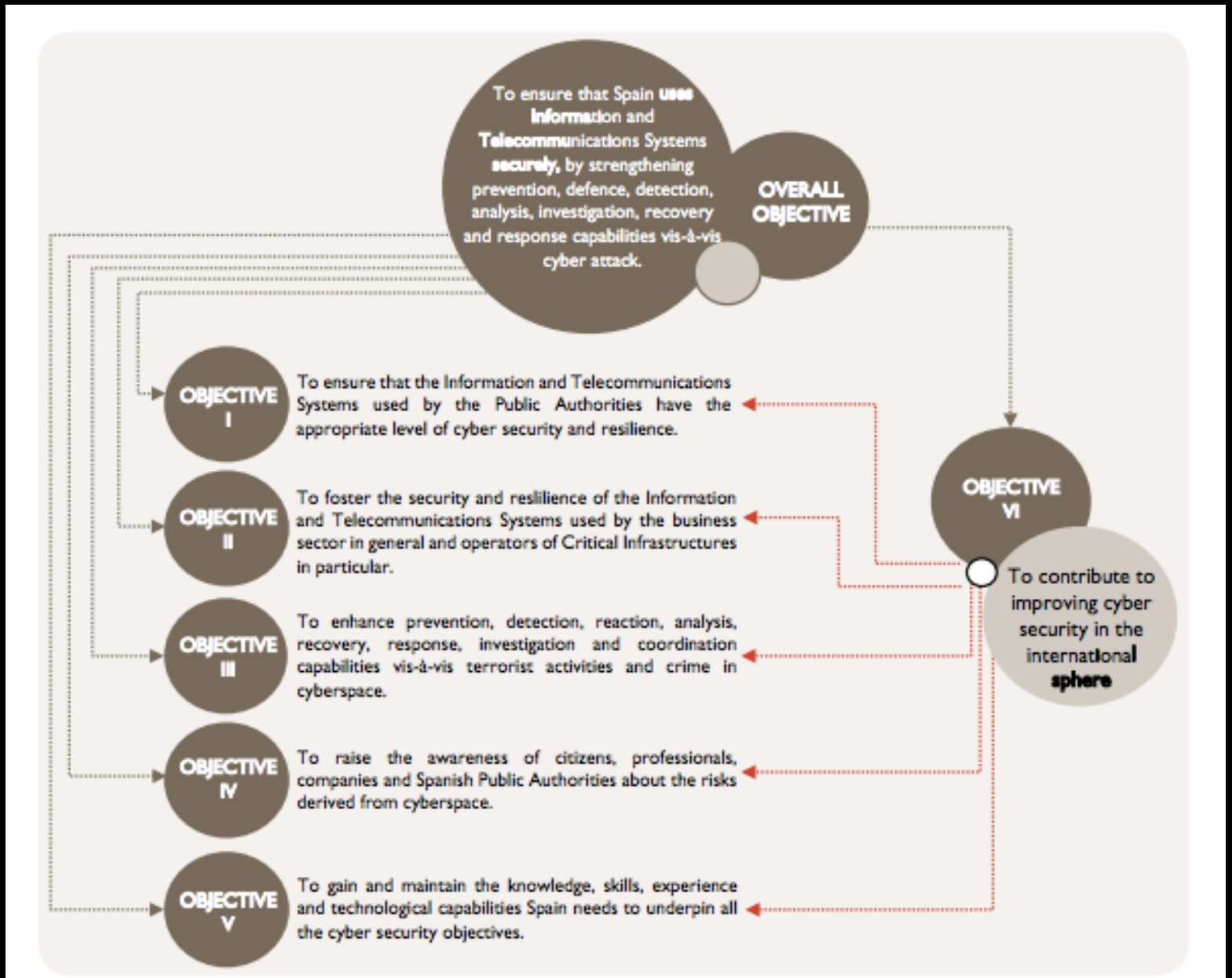
[1] http://mobile.royalgazette.com/business/article/20170714/ics-sees-ratings-as-key-for-cybersecurity&template=mobileart

Example Cyber Measurement Models

- Factor Analysis of Information Risk (FAIR) Model [1]
- "How to Measure Anything in Cyber Security Risk"[2]



1 http://www.fairinstitute.org/
2 http://www.howtomeasureanything.com/cybersecurity



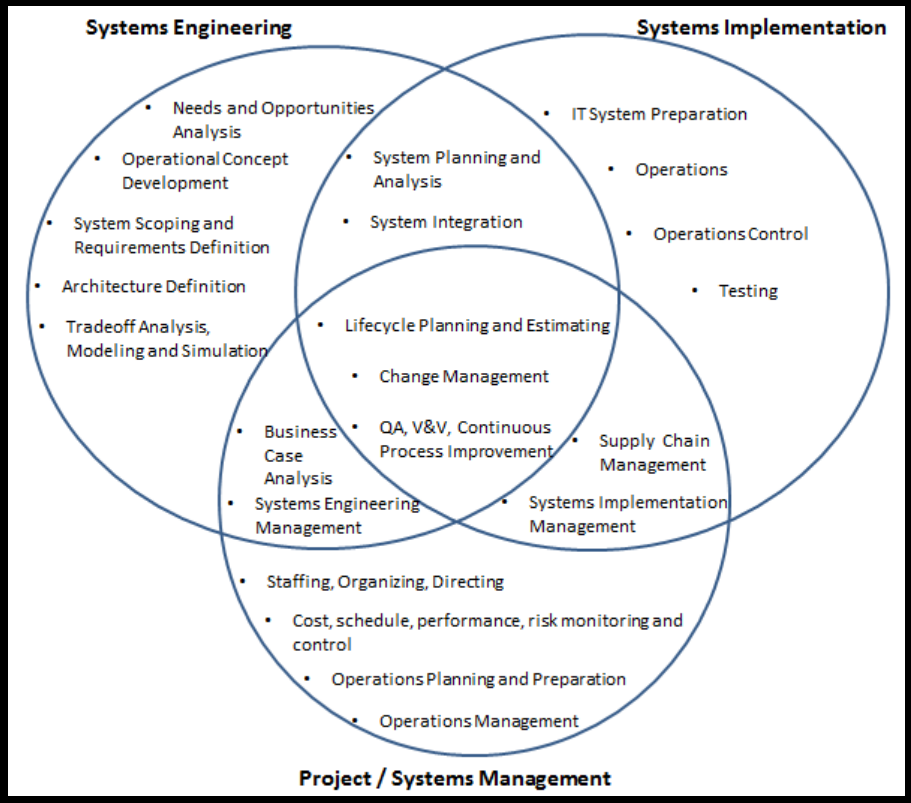
[1] https://www.enis

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Cyber Model Example - Introduction

- Build Enterprise Description Model
- Use Analytic Model



Enterprise Model

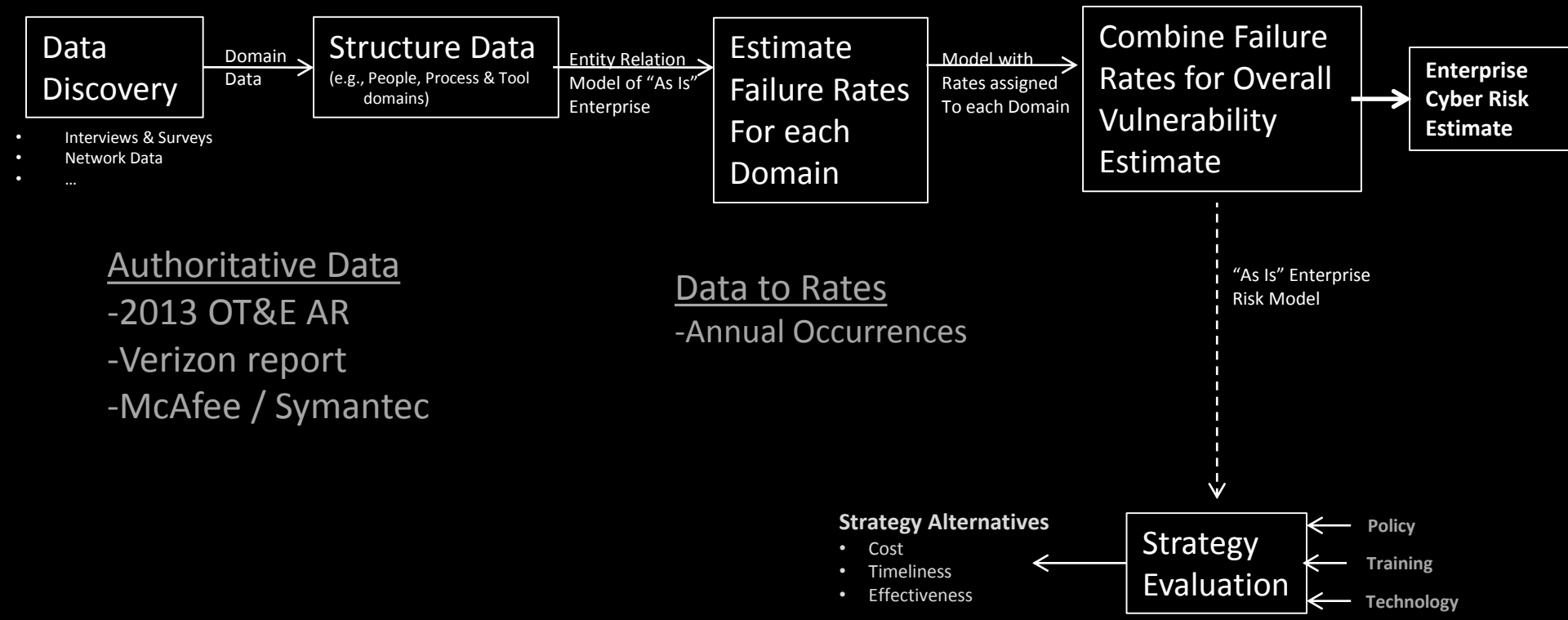
People manage enterprise due to the scope of information





[1] http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm

Enterprise Model Construction & Evaluation



Authoritative Data
-2013 OT&E AR
-Verizon report
-McAfee / Symantec

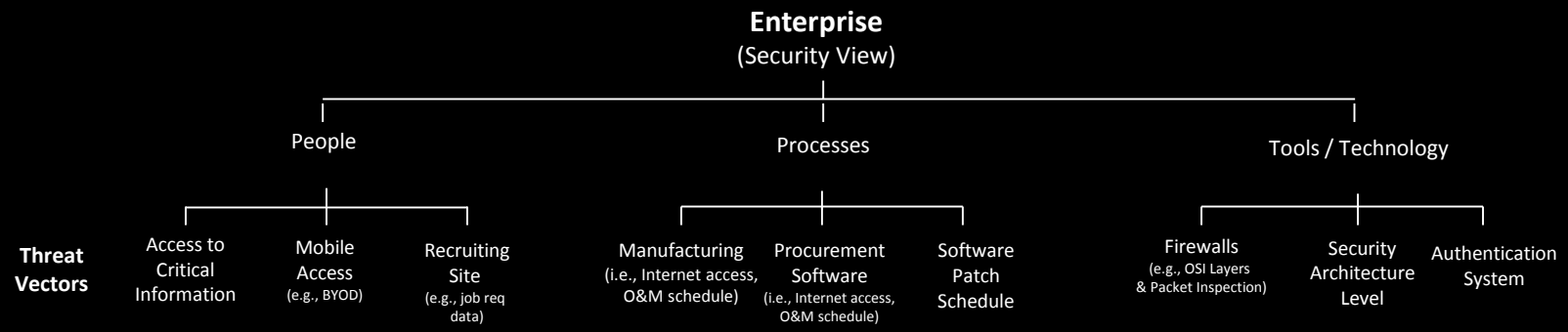
Data to Rates
-Annual Occurrences

Metrics
-Dollar quantifiable (e.g., Target, Nieman Marcus …)
-Media quantifiable (e.g., Snowden, Manning) – number of articles / exposure

Enterprise Model

(Populate with known Data)

People, Processes & Tools from Surveys / Interviews

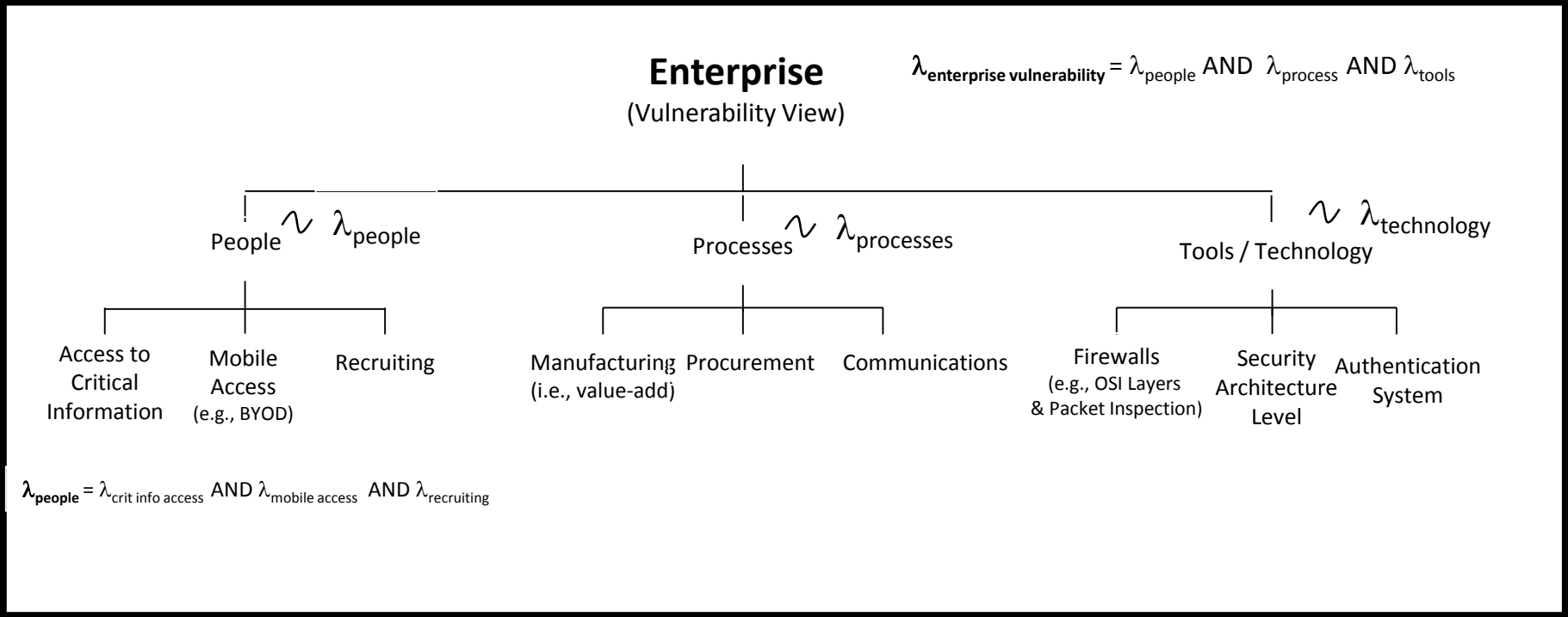


Q&A to Static Enterprise Model

Use the Q&A process to develop an information structure amenable to modeling:

	People	Processes	Tools
Who	• System Access		• User Authentication
What	• Personally Identifiable Information (PII) • Social Media	• Critical Information • High Volume (e.g., manufacturing)	
When	• System Access	• Maintenance Schedule • Patch Schedule • Software Updates	
Where	• Fixed Site • Mobile		
Why	• Business System access • Technology System Access		• Secure Sockets Layer (SSL)
How	• Recruiting • Screening		• Security Architecture Level • Firewall – monitoring & control

Enterprise Model & Parameterization
(organize respective failure rate estimates)

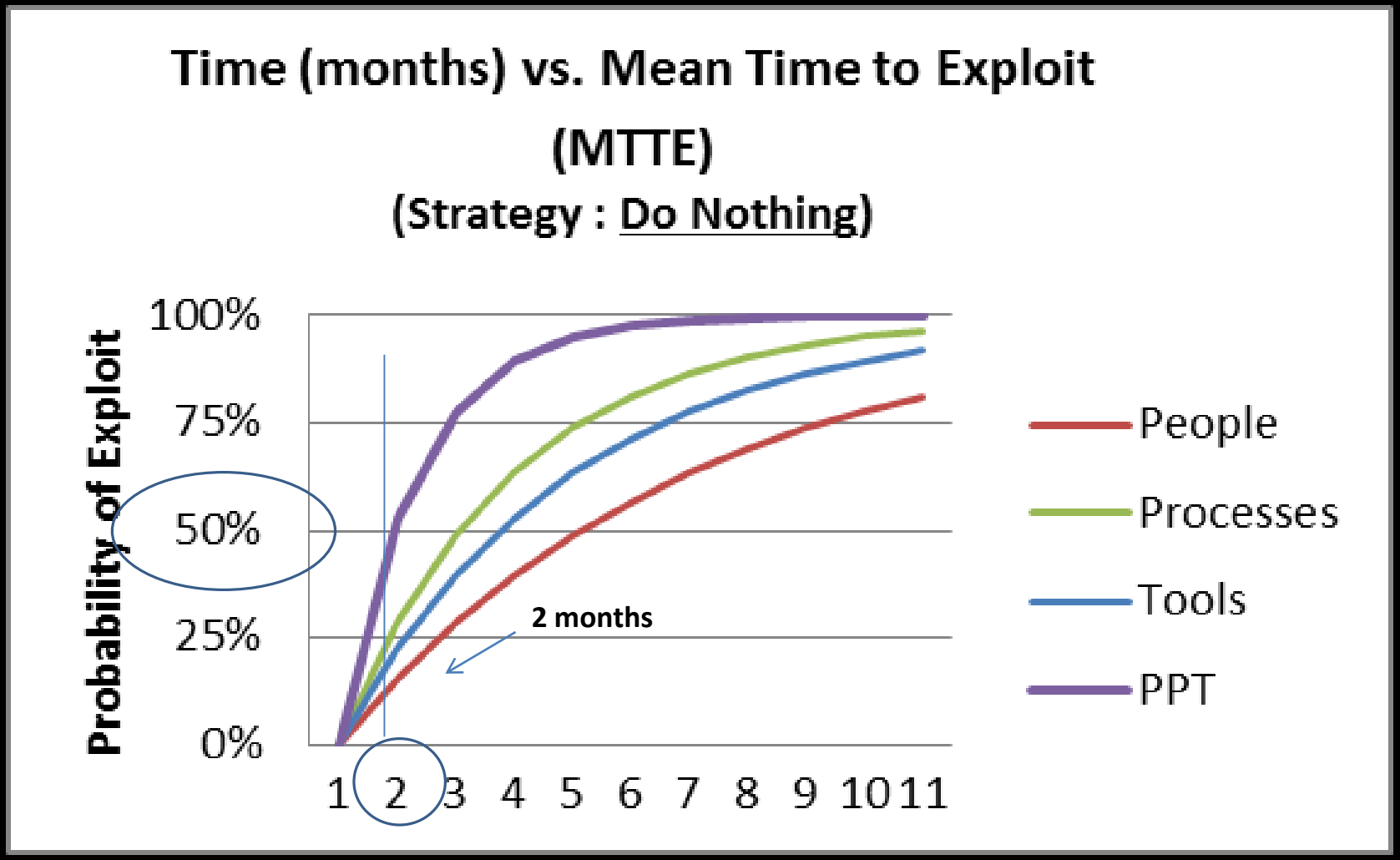


- λ is the failure rate for the respective domain (e.g., people, process, tool) or one of its components

- Exponential distribution results in “additive” combination of failure rates over the heterogeneous data for the respective domains

“As Is” Risk Estimation

(Strategy – “Do Nothing”)

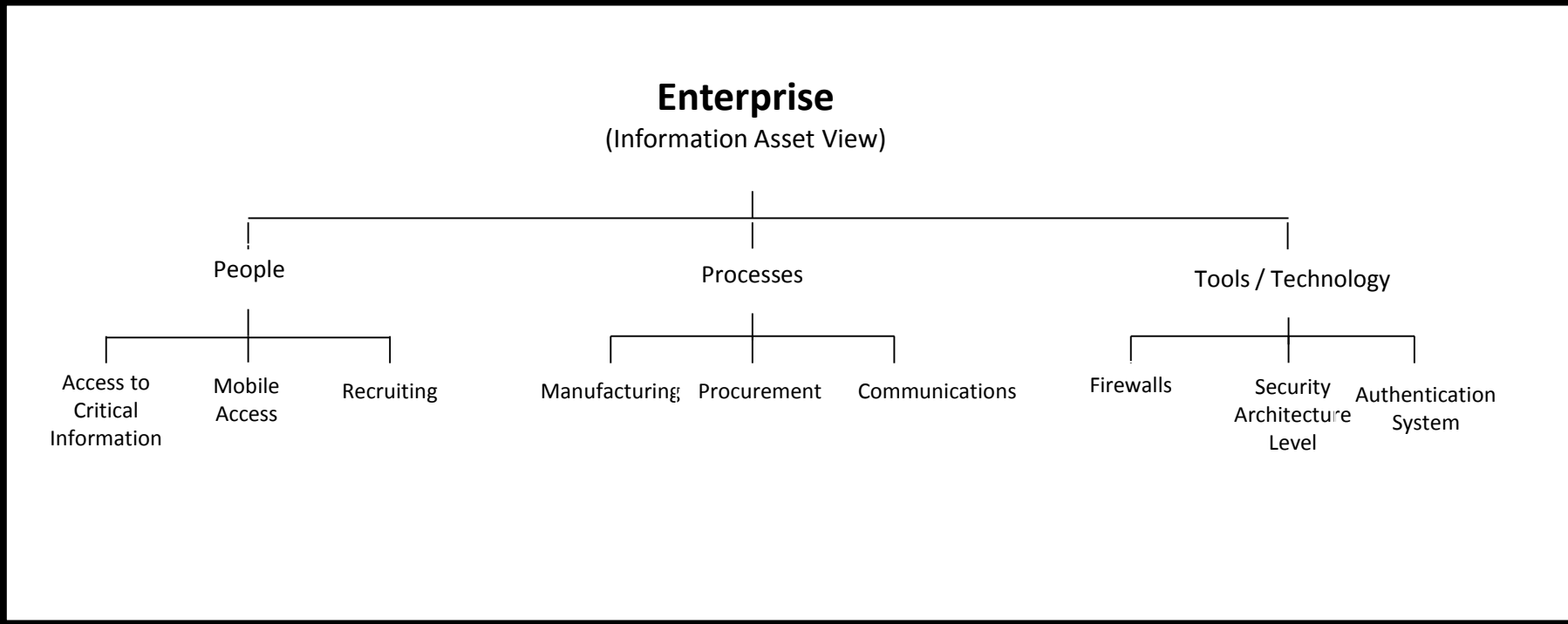


Example Countermeasures as Work Packages

Packages / Domain & Work Package		Cyber Enterprise Domain Affected by Work Packages			Work Package Time / Cost Estimate	
Work Packages		People (λ_{people})	Process ($\lambda_{process}$)	Tool (λ_{tool})	Implementation Time	Cost ($ K)
	Access	●	○	○	months	10's
Policy	Mobile Device	●	●	●	months	10's
	Critical Information	●	●	○	months	10's
	Phishing	●	○	○	weeks	10's
Training	Internet Use	●	○	○	weeks	10's
	Social Engineering	●	●	○	weeks	10's
	Firewalls	○	●	●	days	100's
Technology	M&C	○	○	●	days	100's
	Authentication	●	○	●	weeks	100's

- Work Packages provided as policy / training / technology "fixes" and affect cyber enterprise domains (i.e., people, processes and tools) independently
- Independent Work Package provision results in ready project plans in terms of time and cost estimates for improving enterprise resiliance

Model Based ⟺ Knowledge based



[1] "Artificial Intelligence and National Security" (http://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf)

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Nissan Quest / Ford Villager

- 7 Prototype builds
- 1000s of hours of testing / evaluation



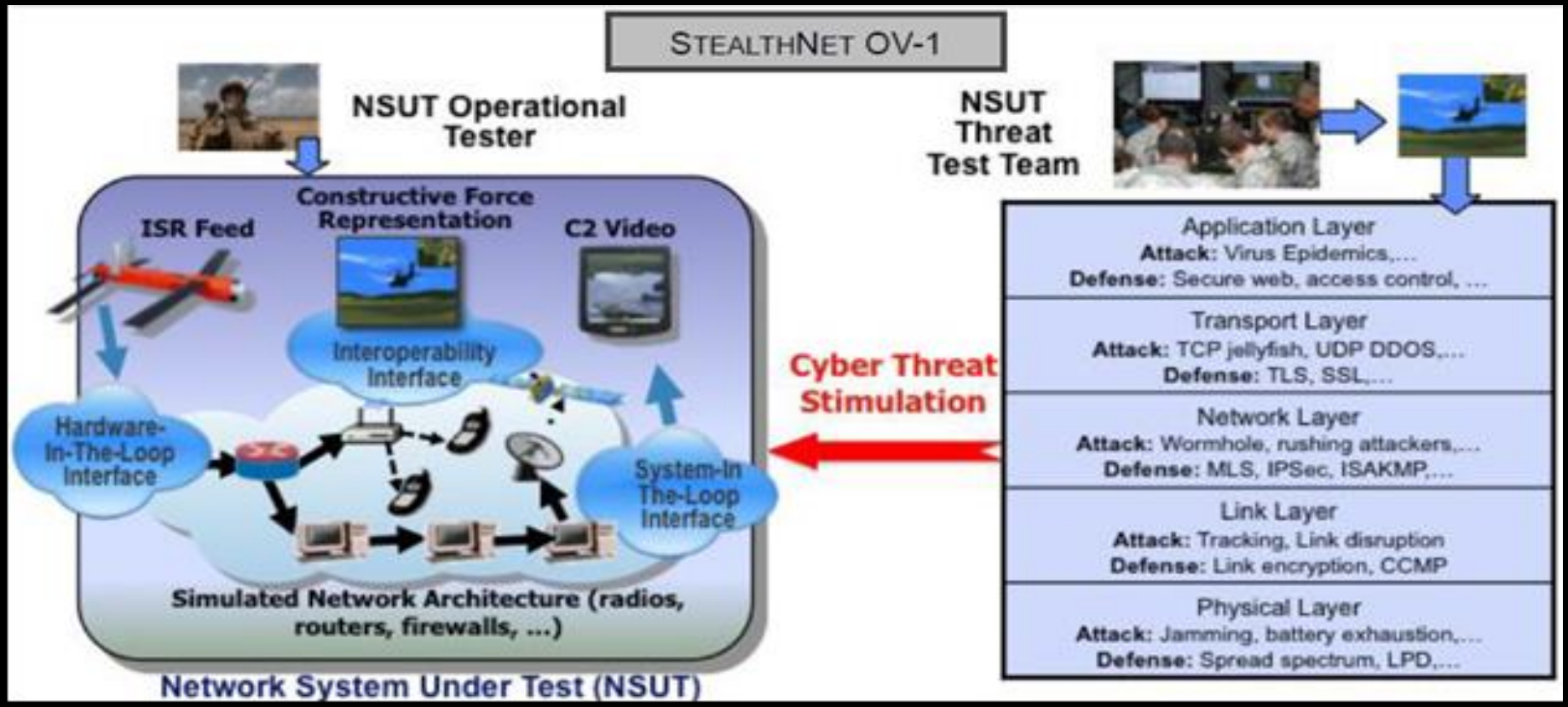
Death Valley Hot Weather Testing



Bemidji MN Cold Weather Testing



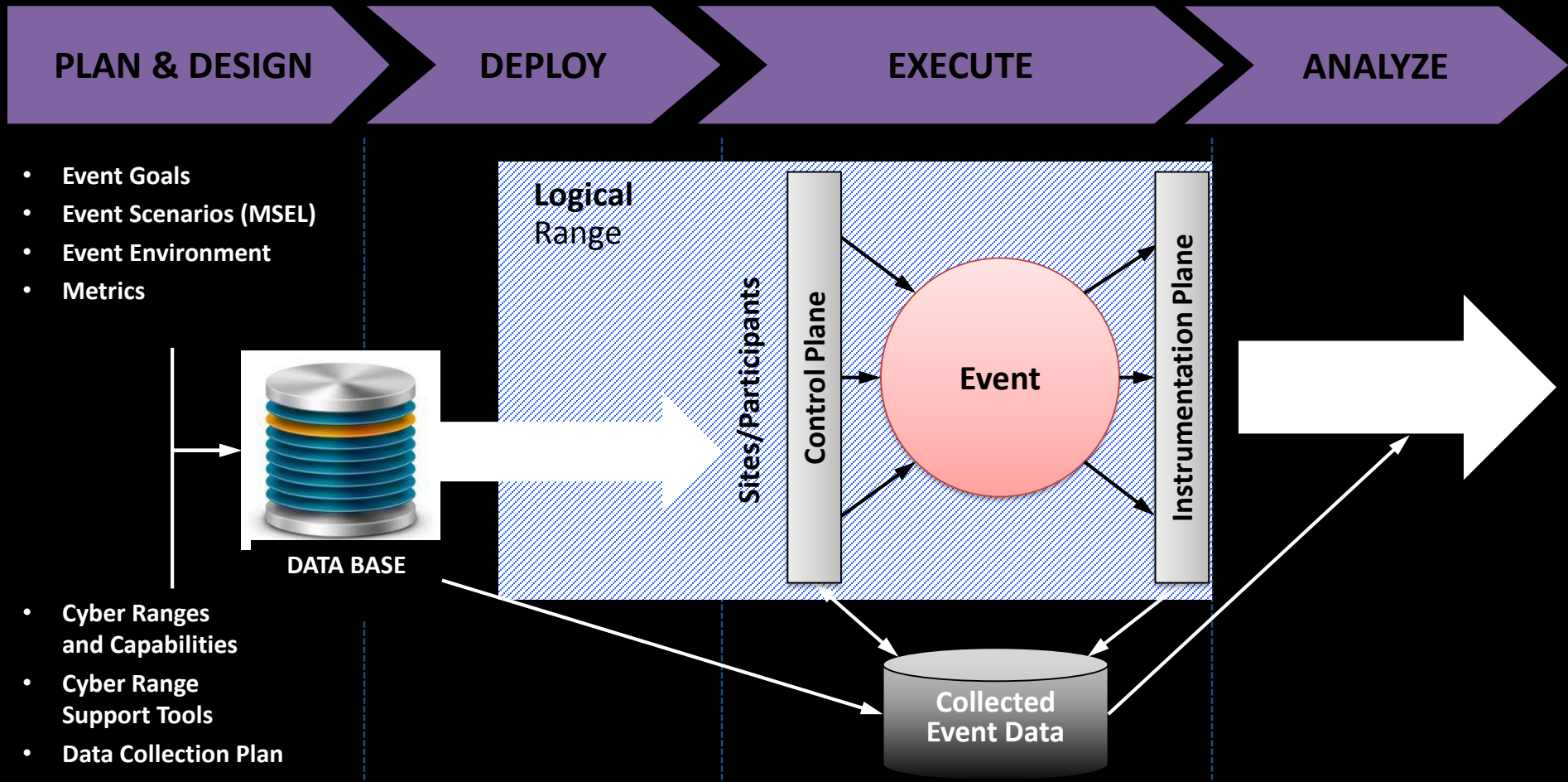
Cyber M&S / Test Example



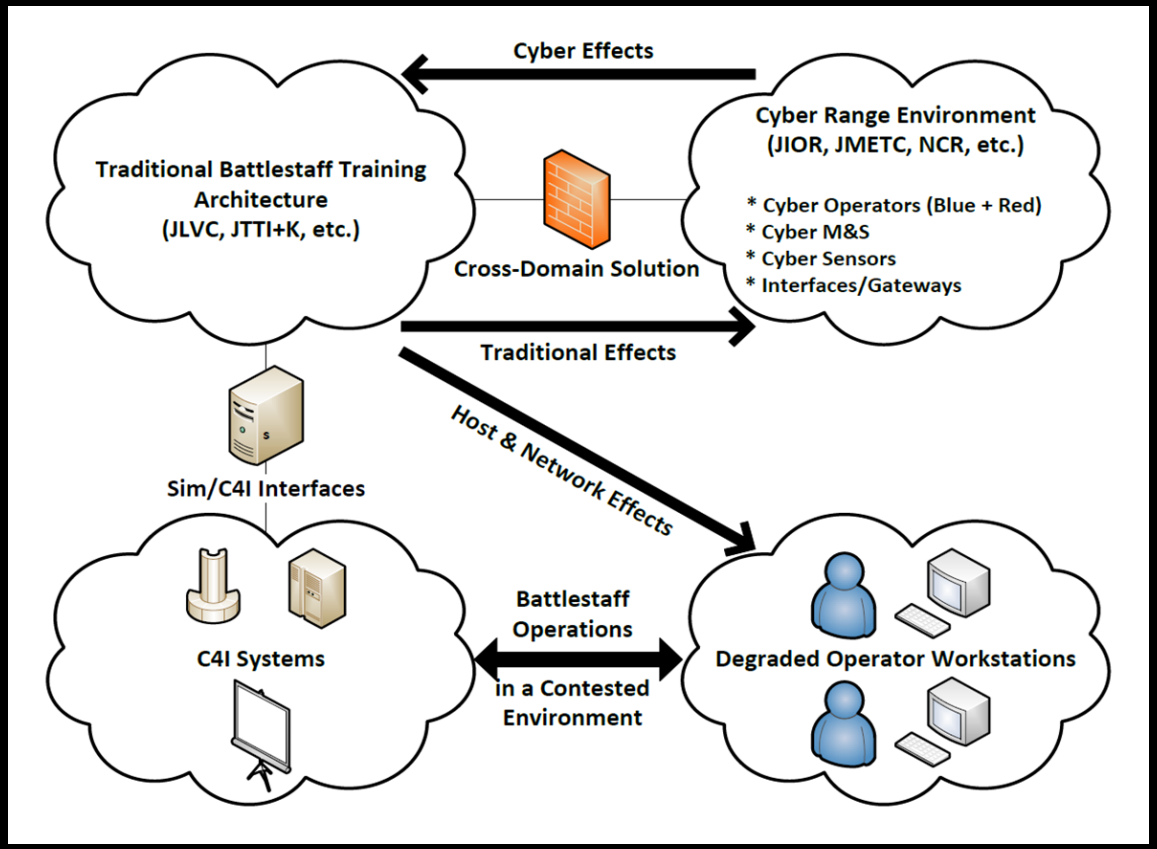
Network Emulation (StealthNet) injection into Network System Under Test (NSUT)[1]

[1] http://www.dtic.mil/ndia/2012/system/ttrack514951.pdf

Cyber-Range Event Process Overview



Cyber Operations Architecture Training System (COATS)[1]



Inject Cyber Range effects into Command Staff training simulations

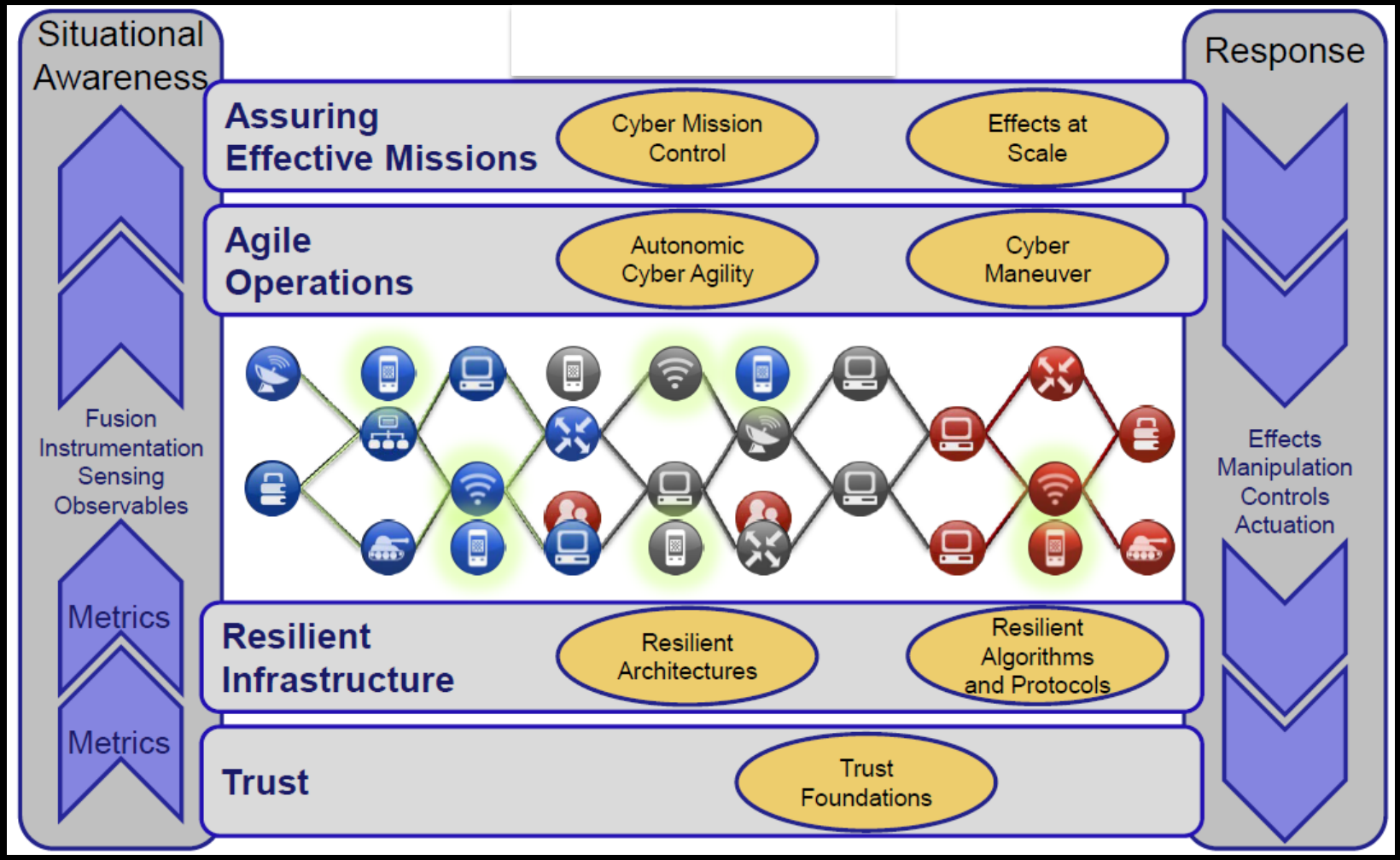
[1] 2015 I/ITSEC Best Paper (http://www.iitsec.org/about-iitsec/publications-and-proceedings/best-papers-and-tutorials-from-past-iitsec)



"I'm no expert, but I think it's some kind of cyber attack!"

Contents

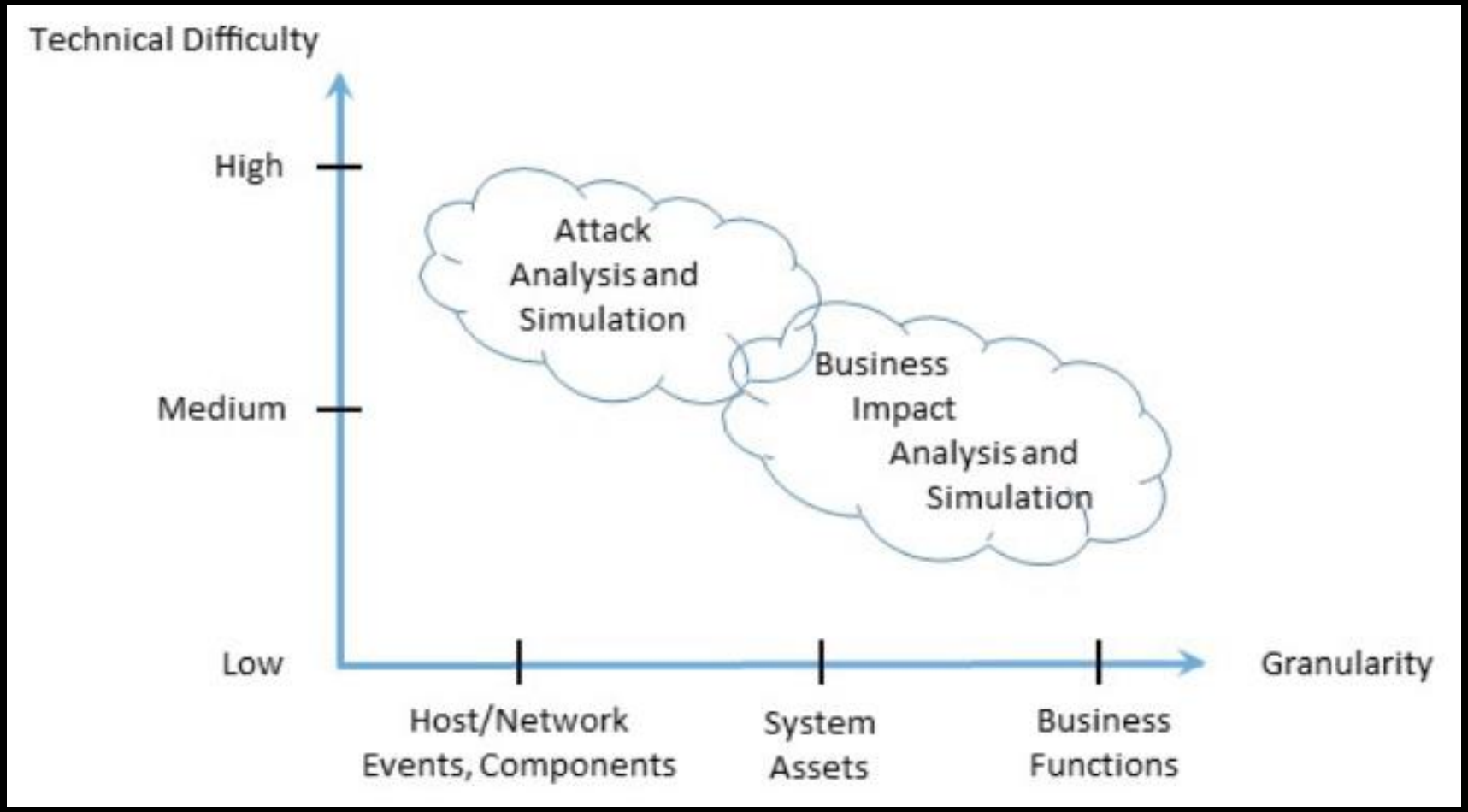
- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up



Cyber Mission Representation (DoD SBIR Conf – 2013)

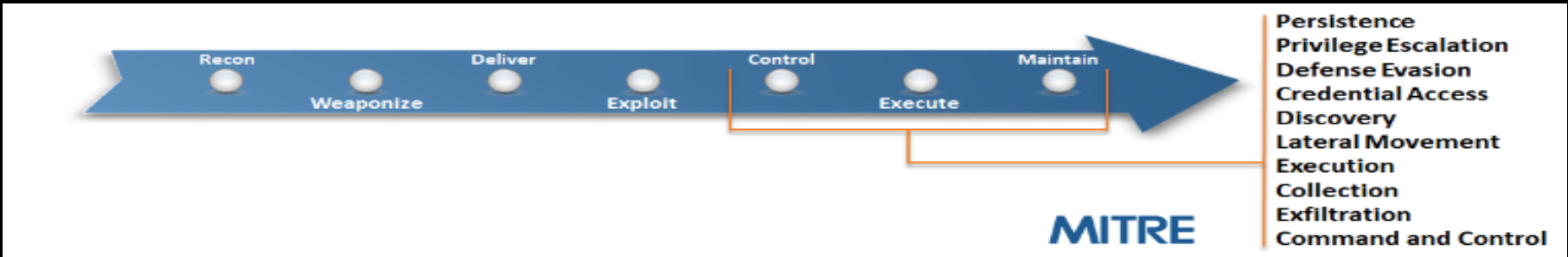
[1] https://www.dhs.gov/sites/default/files/publications/csd-sbir-2013-drsteven-king.pdf

Two major subspaces of cyber M&S problems



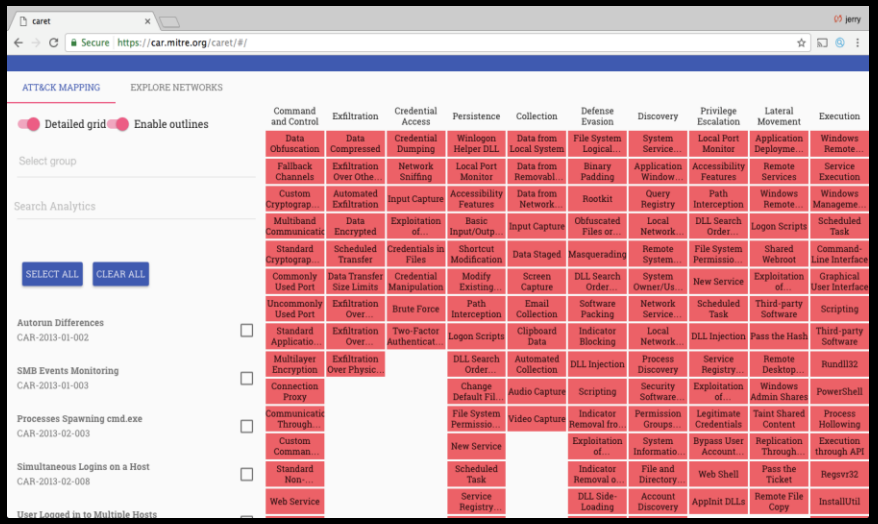
[1] NATO IST 094

MITRE & ATT@CK Framework[1]



- ATT@CK provides decomposition of cyber attack cycle

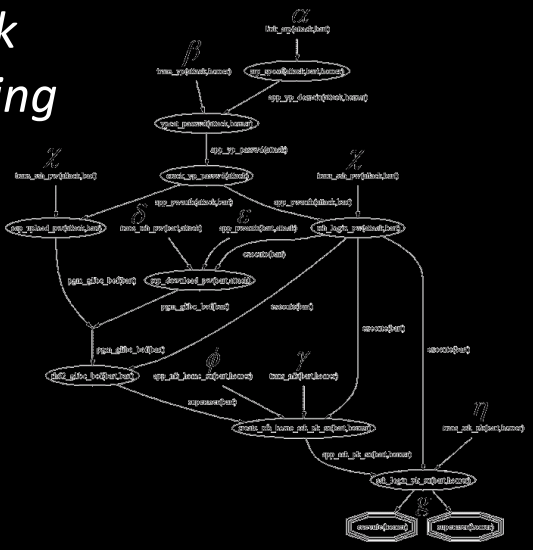
- CARET[2] expands ATT@CK to give more context on tactics, tools and threat groups



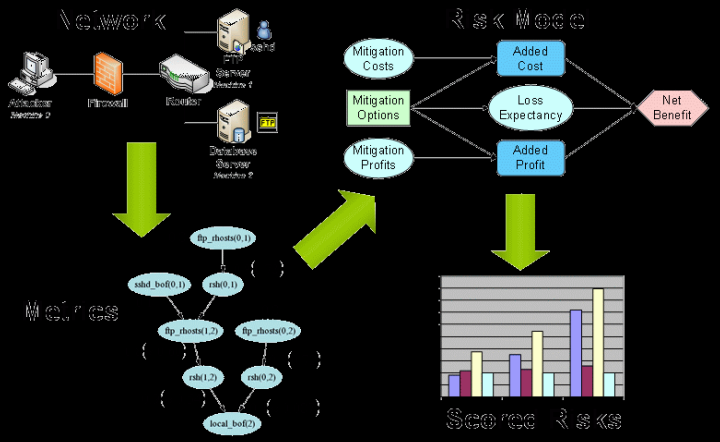
[1] https://attack.mitre.org/wiki/Main_Page
[2] https://car.mitre.org/caret/#/

Cauldron

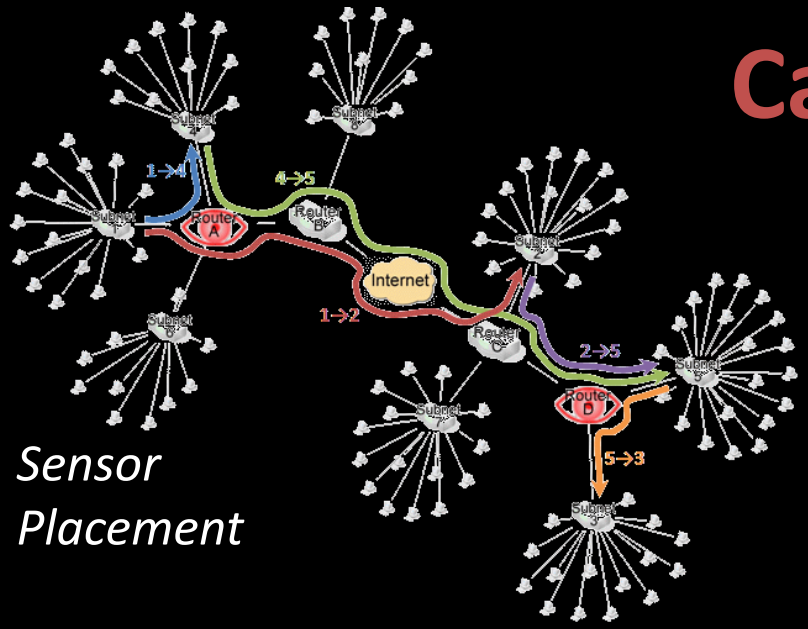
Network Hardening



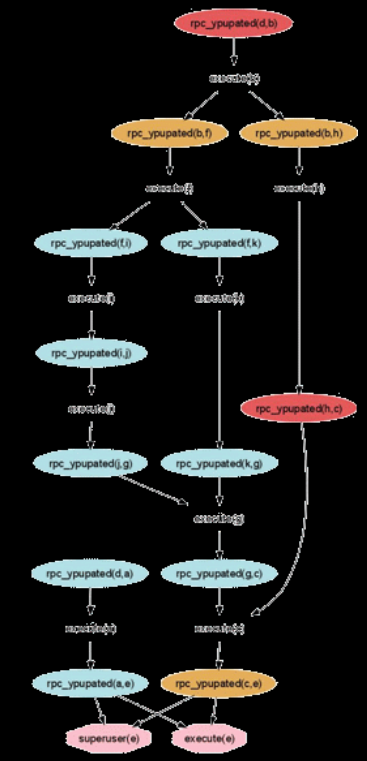
Security Metrics



Sensor Placement



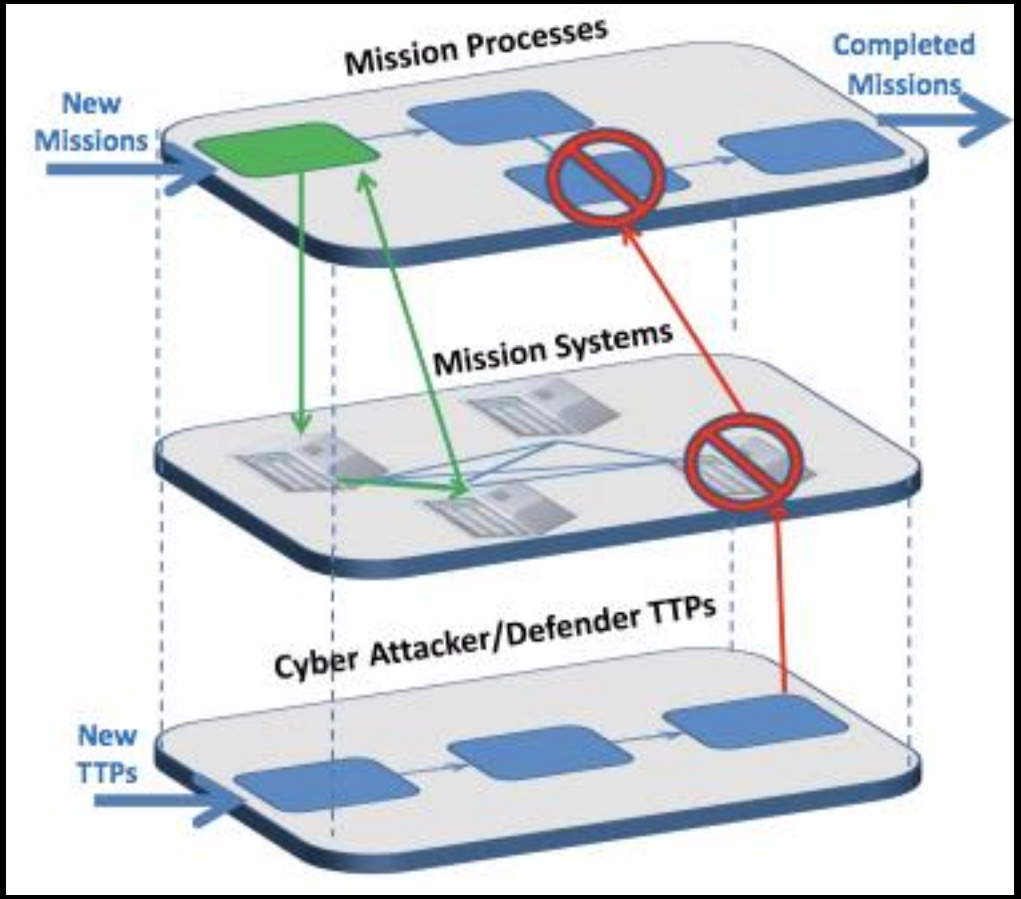
Alarm Correlation And Attack Response



Analyzing Mission Impacts of Cyber Actions (AMICA)[1][2]

For mission analysts, we seek to answer mission impact questions

For cyber defenders and analysts, we consider security posture



[1] 2015 NATO IST 128 Workshop (https://pdfs.semanticscholar.org/ff89/1d6348e2e2f01b3eef52126b45c64110a0a1.pdf)
[2] http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Wrap Up

Cyber Threads	Examples
People	• Mission Operators • Cyber Security Professionals • M&S Professionals that help design secure cyber systems
Process	• Insurance Evaluation • Assessment Frameworks • Knowledge Based Design • Range Testing • Modeling Process for Developing Secure Cyber Systems
Technology	• Attack / Dependency Graphs • Layered Network Simulators • Threat Frameworks



Trusted Supplier Steering Group

Managing Risk with Trusted ASICs: Introducing a Guidebook to Using Trusted Suppliers

NDIA Systems Engineering Conference
Oct. 26, 2017

Distribution Statement A: Approved for Public Release

Guidebook Abstract



This document seeks to guide those who would like to know how to specify and procure Trusted components within DoD or security-sensitive electronics. It details the scope of what types of products and services can be obtained under the current program of accreditation as well as options within the current program. Finally, it guides interested parties to other sources of information relevant to lowering risk and increasing security within electronic systems.

Entire systems can be brought down with a single unauthorized change of the smallest integrated circuit transistor or the loss of a key semiconductor supplier.

Distribution Statement A: Approved for Public Release

Presentation Preview



- Intro to Intrinsix
- Disaggregation Creates Supply Chain Risk
- DoD Responds with Trusted ASICs
- Risks, Rules, Realities
- Summary and Reasons for Guidebook
- Feedback/Questions

Distribution Statement A: Approved for Public Release

Introduction to Intrinsix

- Mixed-Signal SoC Design Services
- Team of ~60: Predominantly staffed with 15-20 year IC realization experts
- Trusted Design and Broker, Accredited since 2007, TSSG Member
- Supplier to advanced DoD and commercial semiconductor industry since 1986

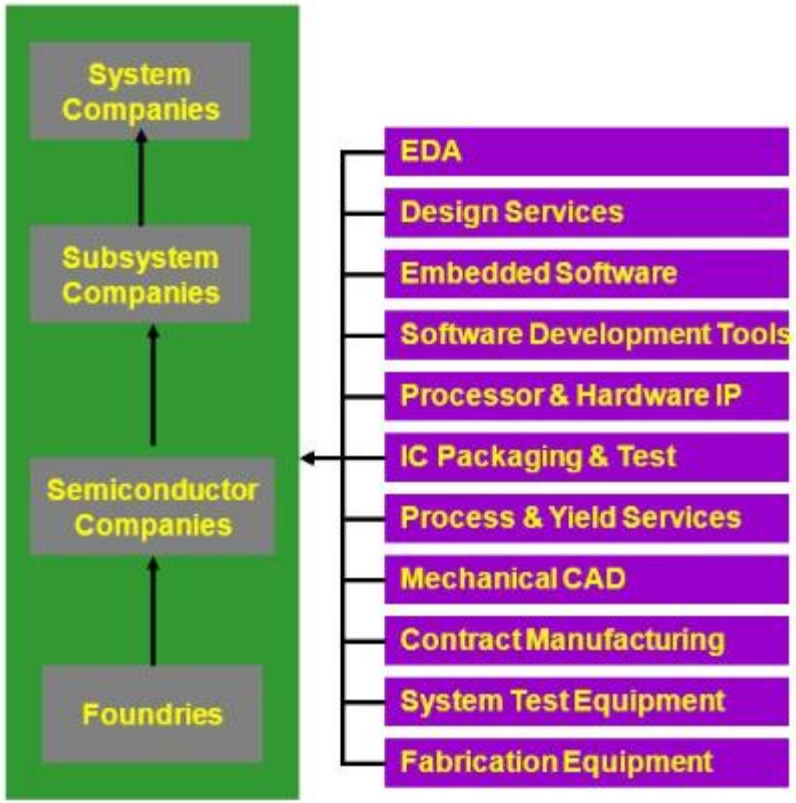


Intrinsix Corporate Headquarters
Marlborough, MA

Distribution Statement A: Approved for Public Release

Economics Drive Disaggregation

- Disaggregation multiplies risk as supply chain creates new links
- Systems companies' "in-house" or "captive" solutions lose competiveness over time
- ASIC Flows highly disaggregated and therefore inherently riskier



Distribution Statement A: Approved for Public Release

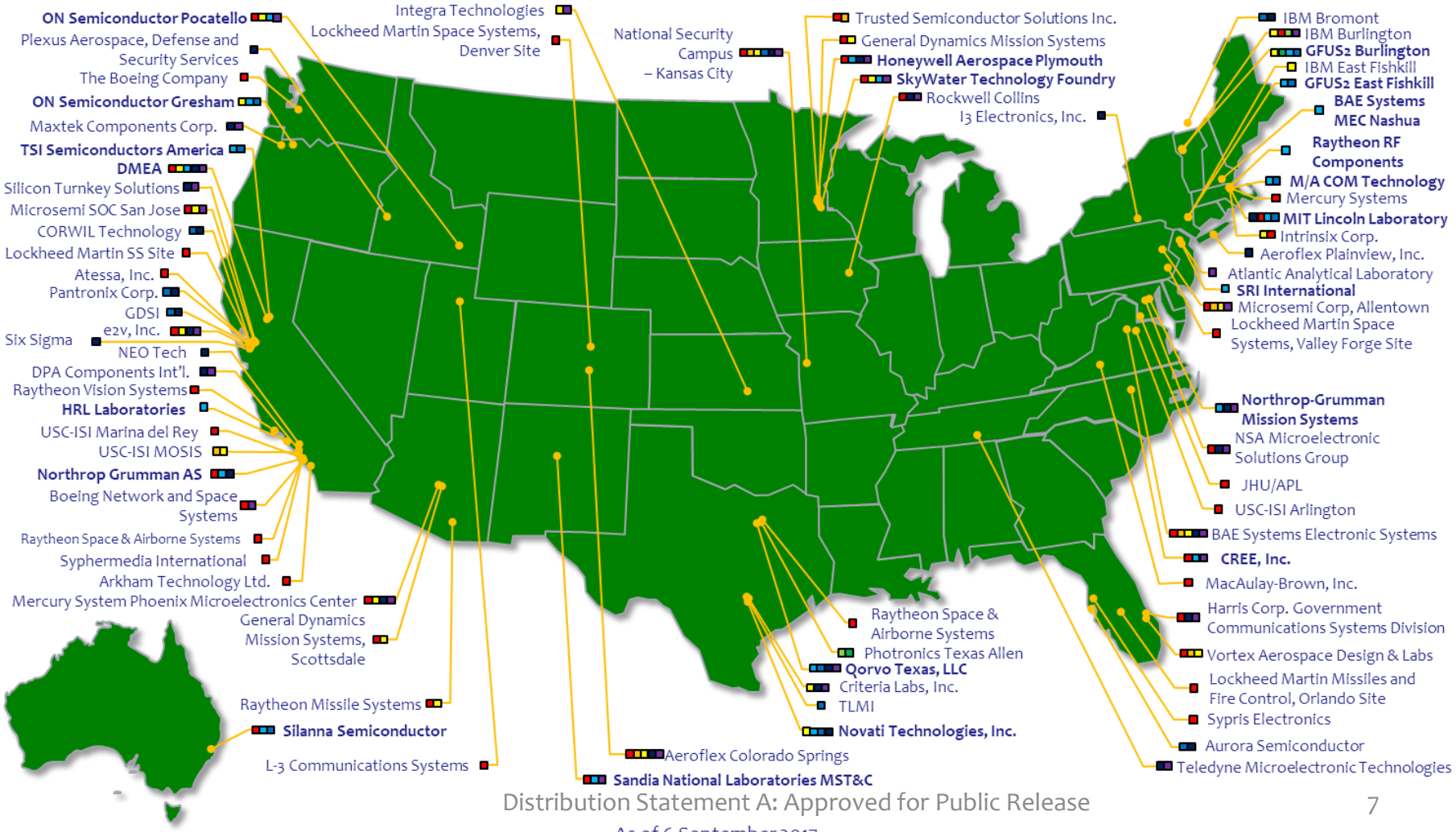
History of Trusted Accreditation



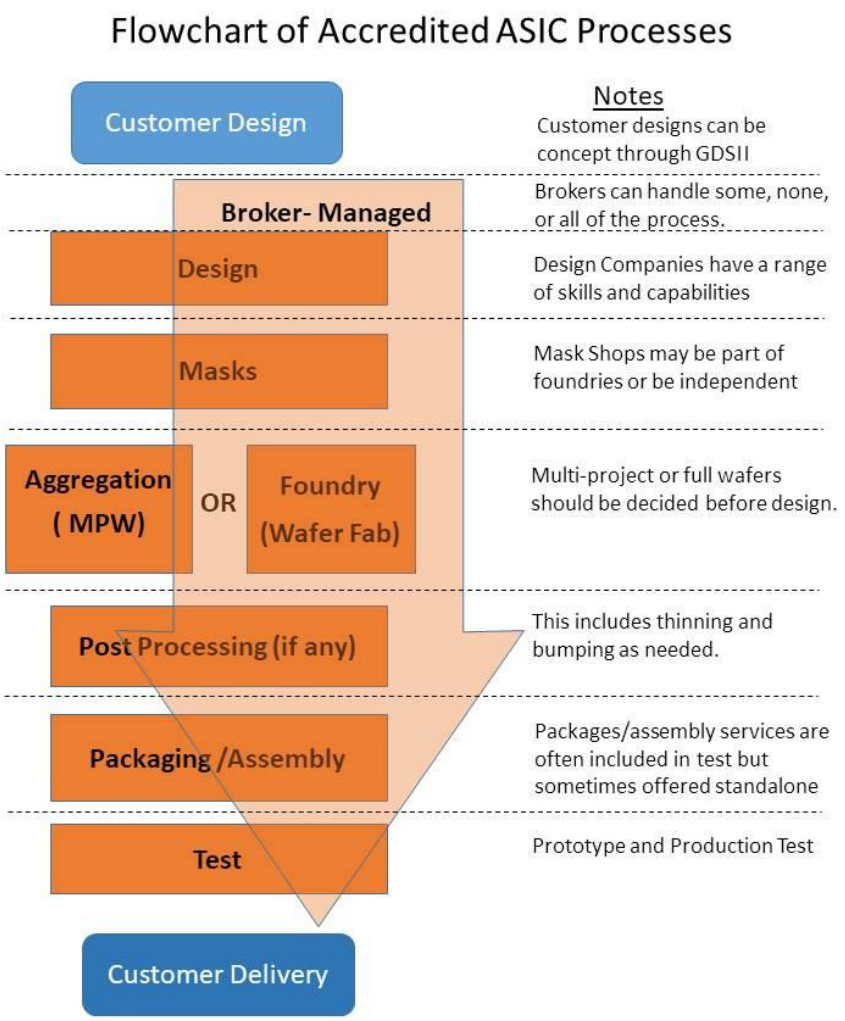
- **2003:** The Trusted Foundry Program Established
  - Administered and managed by the DoD Defense Microelectronics Activity (DMEA).
- **2005:** Defense Science Board Report highlights risk of "Trojan Horses", Recommends Expansion of Trusted Program
- **2007:** Program broadened to entire microelectronics supply chain for ASICs
  - Accreditation process launched
  - CRADA creates need for DD254
  - DSS provides location and personnel review
- **2010:** Trusted Supplier Steering Group is Formed
- **2017:** Multiple efforts to expand Trust to non-ASICs such as FPGAs, PCBs, Standard Products, etc.

Distribution Statement A: Approved for Public Release

78 Trusted Suppliers

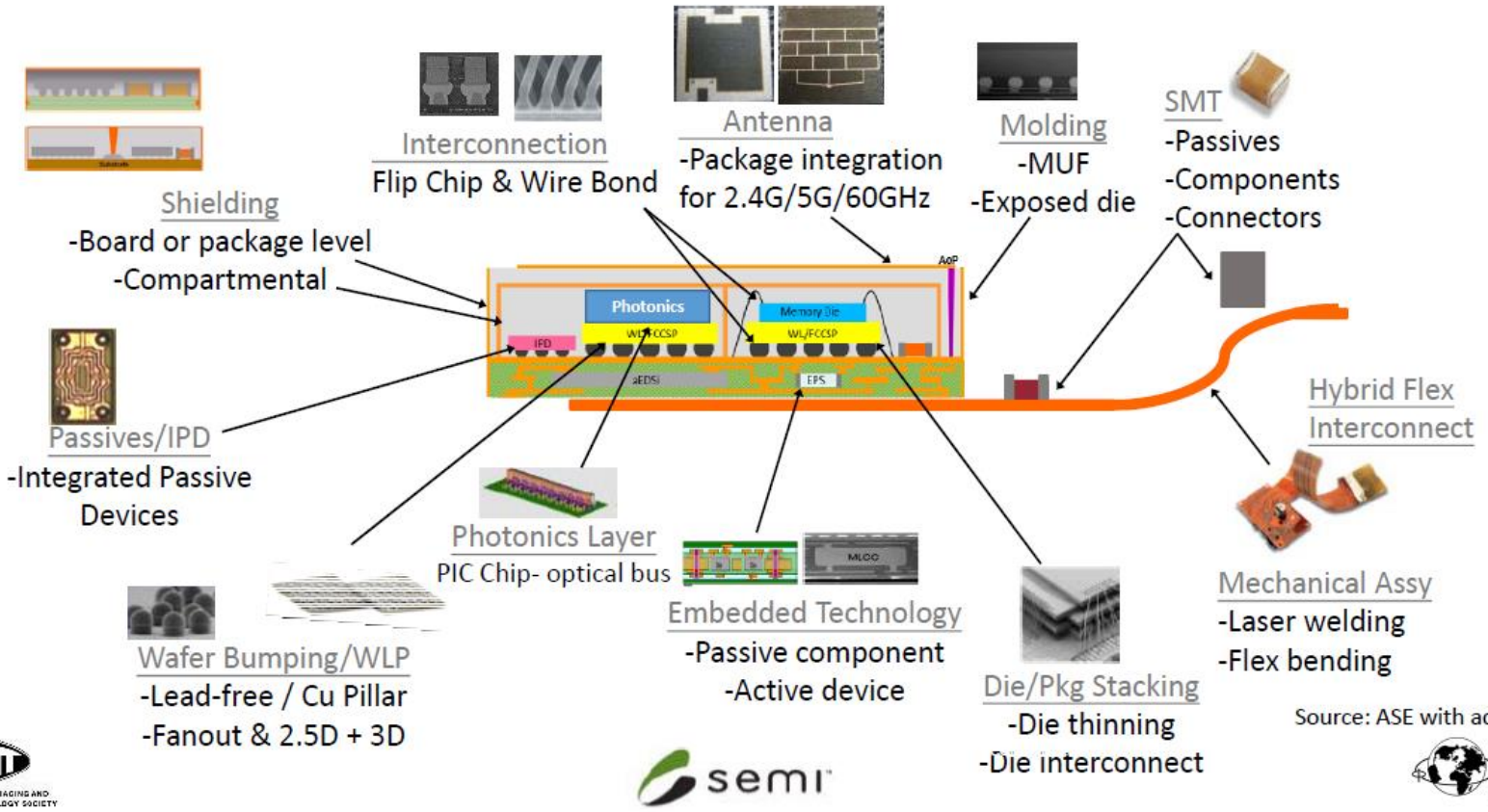


Accreditation Types - Trusted Companies



Distribution Statement A: Approved for Public Release

Future Supply Chains



Heterogeneous Integration is the integration of separately manufactured components into a higher assembly (SiP) that, in the aggregate, provides enhanced functionality and improves operating characteristics

Bill, Chen, " Heterogeneous Integration Roadmap," IEEE CPMC Symposium Japan, Nov 8, 2016

Spectrum of Supply Chain Risks



Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors

The Growing Risk in Electronics

Global Supply Chains and Increased Cyber Insecurity

Each New Product:

- Many Parts from a Vast Network of Suppliers
- Deep Layers of Hardware and Software
- Dozens of Countries Providing Labor/Parts



Dramatic Rise in Cyber Insecurity

- Criminal Tools Rising at Internet Speed
- More User Features = More Openings
- Economic Pressures Drive Insecurity



Types of Threats

Economic/Criminal Drivers:

- Counterfeits
- Selling of Bad Parts
- Theft of Device or Data or Money

Malicious Nation-States

- Terror
- Mission Defeat
- Theft of National Secrets and Industrial Intellectual Property



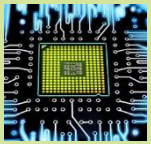
Distribution Statement A: Approved for Public Release

What to PROTECT in Electronics?

Choose the Intersection of Vulnerability and Criticality

Vulnerability

- What is easy to alter?
- What alteration can be hidden?



Criticality

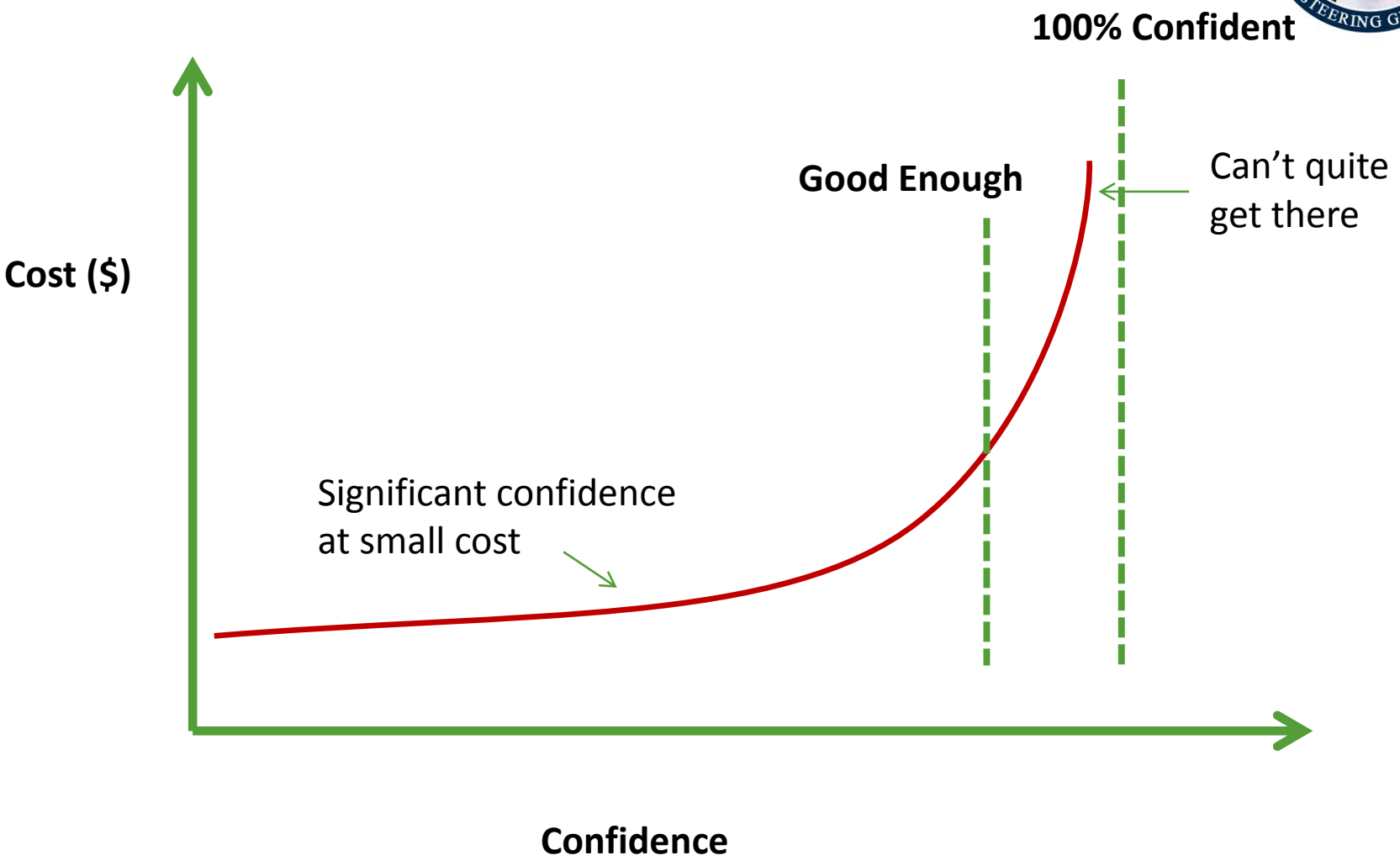
- What is Important to Protect?
- Where is the secret sauce?

Conclusion: Protect the Intellect!

- Custom Chips: The "Intellect" of all Systems
- Compromised Chips can not be detected easily, if at all
- Offshore Design or Manufacture opens the door to alteration (as well as poor cyber-security within US firms)

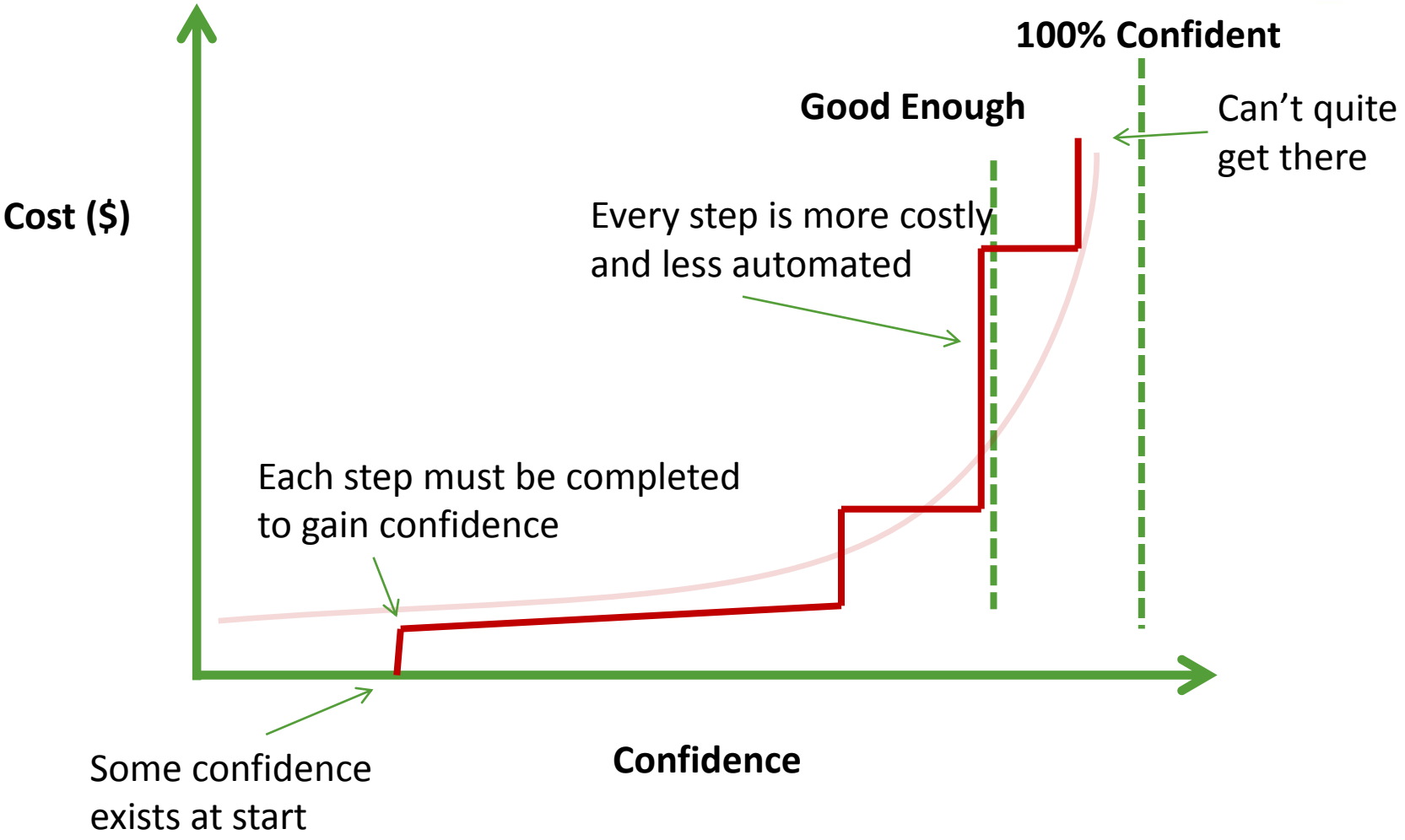
Distribution Statement A: Approved for Public Release

The Cost of Confidence:
An Abstract View



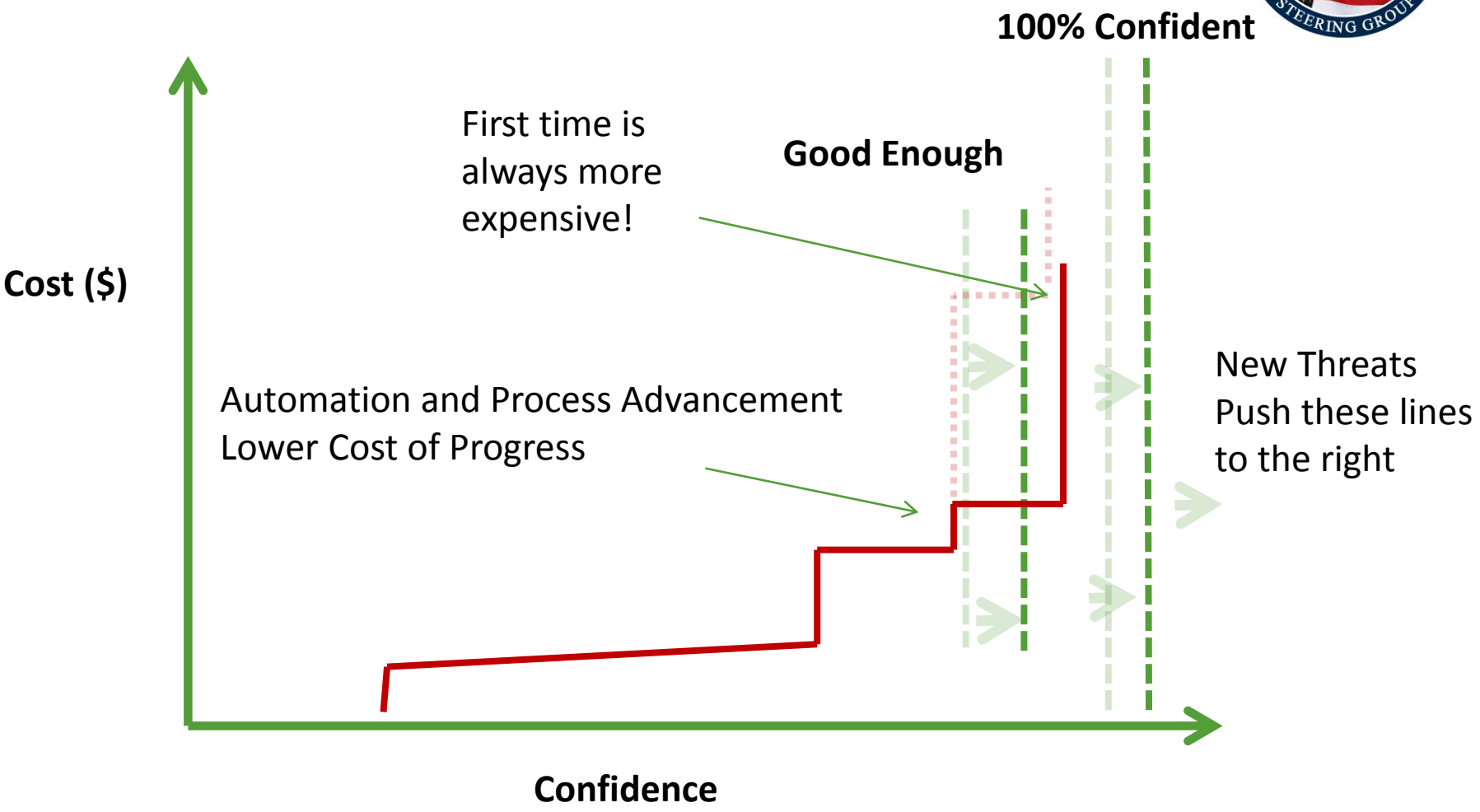
Distribution Statement A: Approved for Public Release

The Cost of Confidence:
Less Abstract View



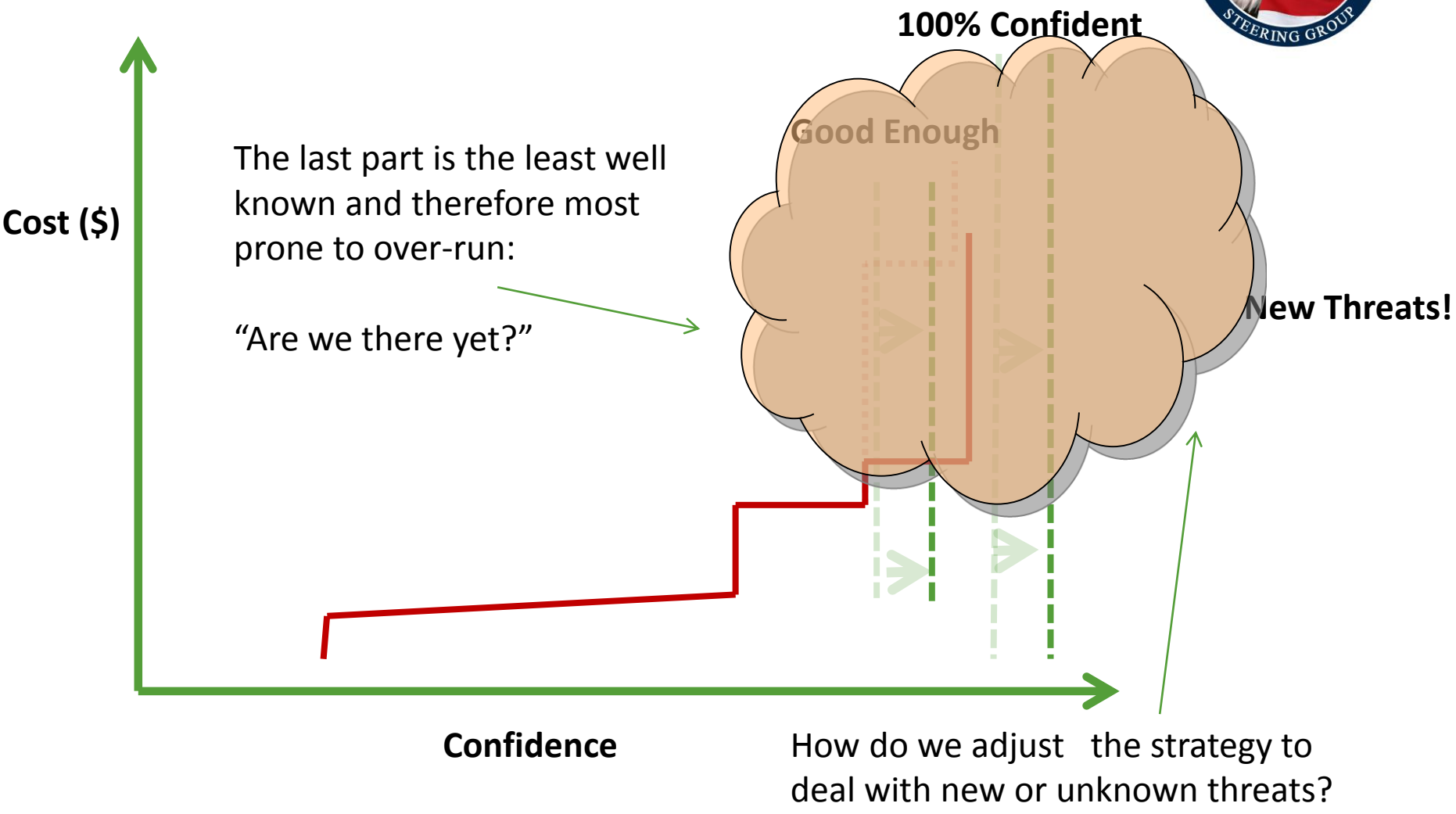
Distribution Statement A: Approved for Public Release

The Cost of Confidence
Effects of Time



Distribution Statement A: Approved for Public Release

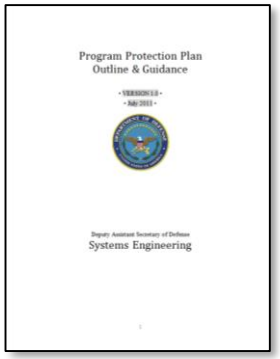
The Cost of Confidence
Clouds of Doubt



Distribution Statement A: Approved for Public Release

Rules and Regulations

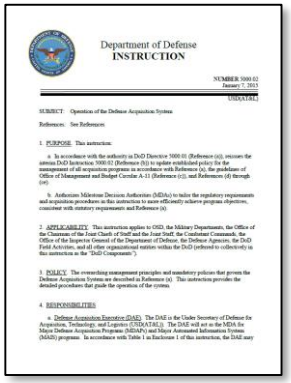
- DoDI 5000.02: **Create Program Protection Plan** (PPP)



- DoDI 5200.39: **Identify Critical Program Information**
  - CPI Includes mission critical functions, PPP covers information security threats and vulnerabilities, supply chain risk management, HW and SW Assurance, Cybersecurity, Anti-Tamper

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

  "In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASICs))."



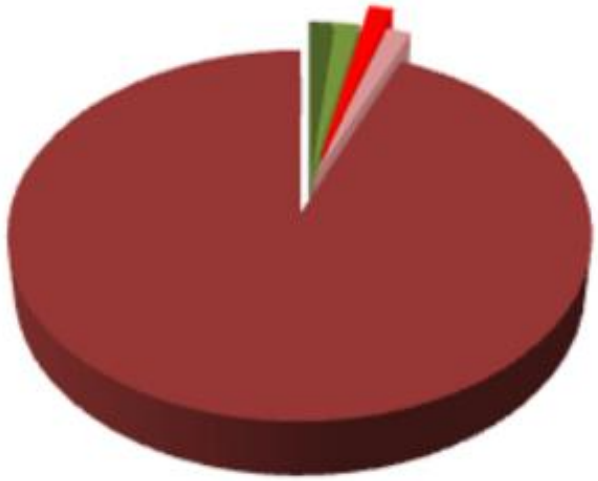
Realities of Using Trusted Flows

- Reality #1: Not All desirable ASICs are Available as Trusted
  - Developers must look closely at options
- Reality #2: Trusted is not always Classified but its often Close!
  - DSS insures ***capability*** of Secret, Developers/Suppliers choose specifics
  - Each Supplier has specific guidance and approach unique to their business
  - Classified Processing using all NISPOM standards is more expensive than commercial
- Reality #3: The MOST important thing is to lower RISK
  - Trusted Suppliers have security infrastructure, process, mindset
  - Developers should identify compliance with NIST 800-171
- Reality #4: SSE Knowledge of Risks outstrips Regulations
  - Technology and Risks change faster than any Government Process
  - Enforcement of Regulations? Systems that are Secure is the Goal!

Distribution Statement A: Approved for Public Release

Most Electronics: Unprotected by DMEA Trust

- Many ASICs and Most SOTA Processes
- FPGAs
- Standard Products
- Most Intellectual Property as ASIC Inputs
- PCBs and Interconnect Technology



Distribution Statement A: Approved for Public Release

Summary and Reasons for Guidebook

- Trusted Suppliers have distinct advantages but only for a subset of the solution space in a large dynamic risk space
- Regulation-based enforcement must trail common sense trade-offs of money vs. risk mitigation
- Standards and Rules are written by lawyers and enacted by lawmakers: **Plain language Advice and Guidance is Critical**
- DoD Stakeholders (Gov't offices, primes, subsystem manufacturers) have been looking for guidance in this form
- Guidebooks can be amended and updated at market speeds

Feedback from SSE Users will be the Lifeblood of This Effort

Distribution Statement A: Approved for Public Release

Trusted Supplier Steering Group

Speaker Contact Info:

Jim Gobes – CEO
Intrinsix Corp.
(508) 658-7658
jgobes@intrinsix.com

NDIA Systems Engineering Conference
Oct. 26, 2017

Distribution Statement A: Approved for Public Release

SYSTEMS ENGINEERING RESEARCH CENTER

Georgia Tech Research Institute

Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems

Mr. Tom McDermott
Dr. Valerie Sitterle
Georgia Tech Research Institute

NDIA 20th Annual Systems Engineering Conference
26 October 2017

Springfield, Virginia

Model-Based System Assurance



- A workshop focused on identifying and prioritizing appropriate research questions related to next generation system assurance, i.e. Model-Based System Assurance (MBSA)
  - relevancy from a practitioners' perspective,
  - and uniqueness and rigor from a research and academic perspective

Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the Cyber Resiliency of Military systems 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

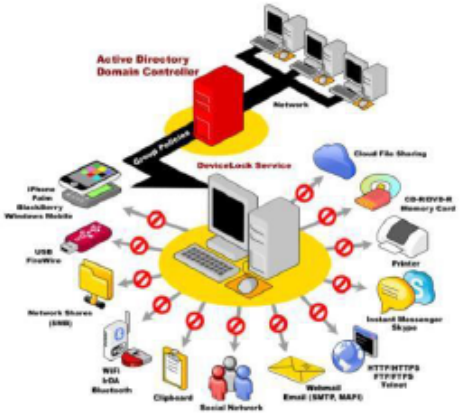
Government control — COTS

Architectures

Diverse — Common

Interfaces

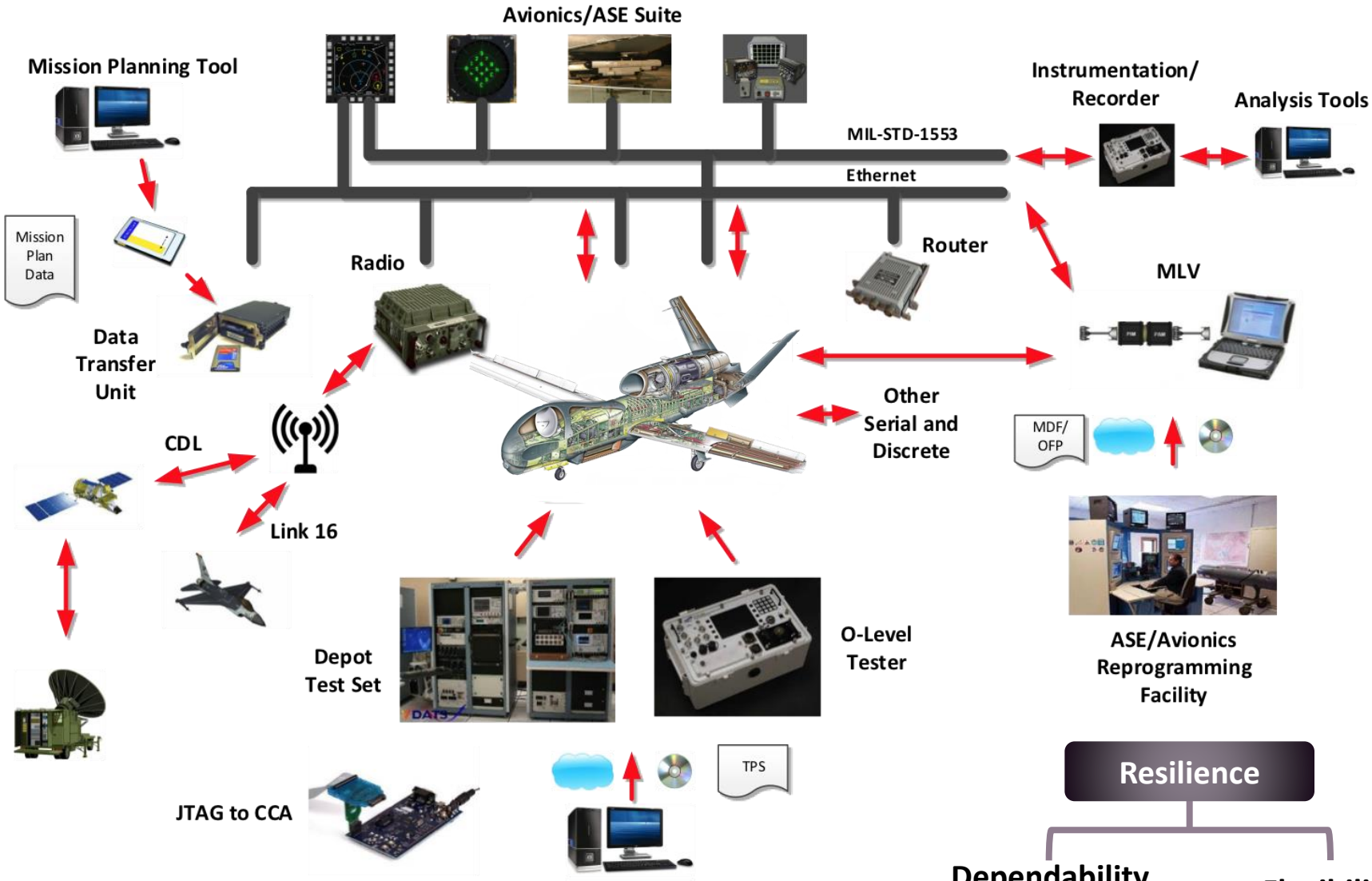
Customized — Standardized



IT Systems

DISTRIBUTION A. Approved for public release: distribution unlimited.

Is My System Cyber-Resilient?



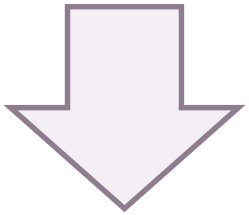
Resilience

- **Dependability and Security**
- **Flexibility**

Security at Design Time

1. To evaluate security for a system with cyber elements, we must holistically evaluate the system, the threat(s), and the protection (i.e., the security design pattern(s)) as a single ecosystem.

2. Resilience is best understood as a non-functional property that emerges from the dynamics across interdependent elements in an ecosystem. A single system perspective or a strictly topological perspective will be insufficient.



Executable, contextual, and analyzable representation of
"Did our 'designing-in' for Resilience
indeed preserve mission-critical functionality in the face of the threat(s)?"

Systems and Future Needs

Systems are increasingly …

Comprised of heterogeneous elements

Cyber-ized



That are interdependent and independent

Logical and spatial in scale

New capabilities



New threats



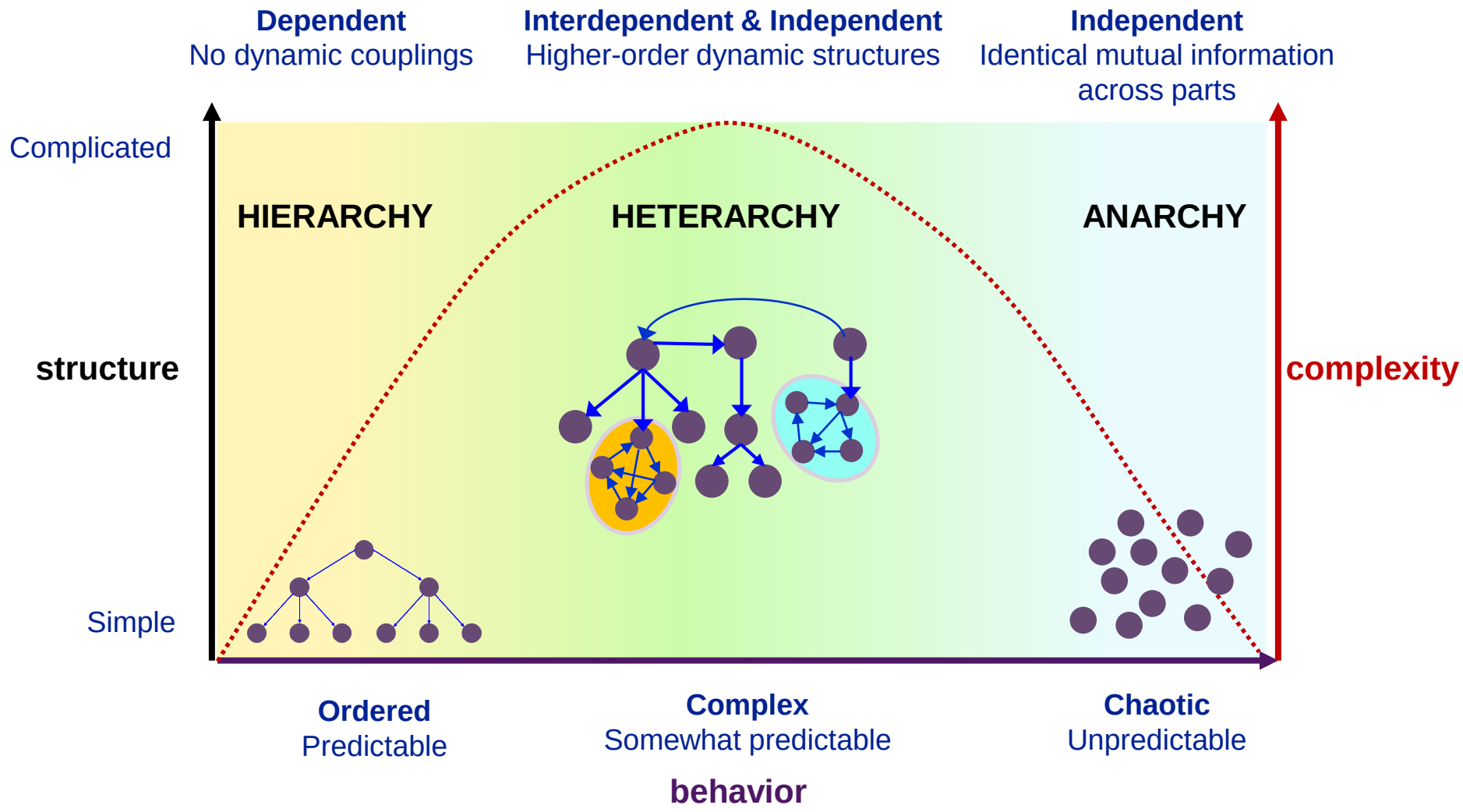
Context

Traditional Systems Engineering (SE) lacks external context inclusion in design selection M&S.

How can we 'design-in' Resilience at an earlier stages in the SE process?

Cyber-Physical systems are a good model.

Order and Form



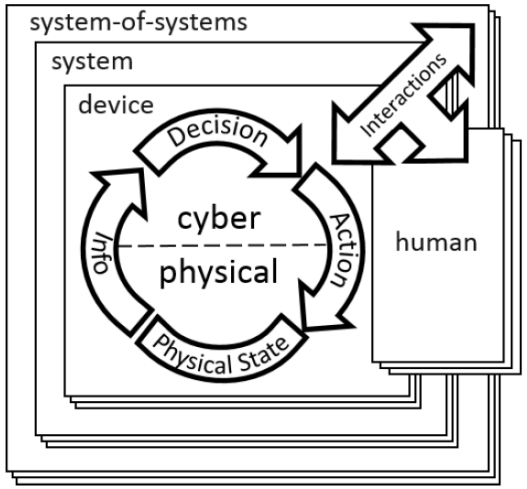
Structure and function are intrinsically linked.

System-Theoretic Accident Model and Processes (STAMP)

Nancy-Leveson_STAMP-Intro-2017.pdf

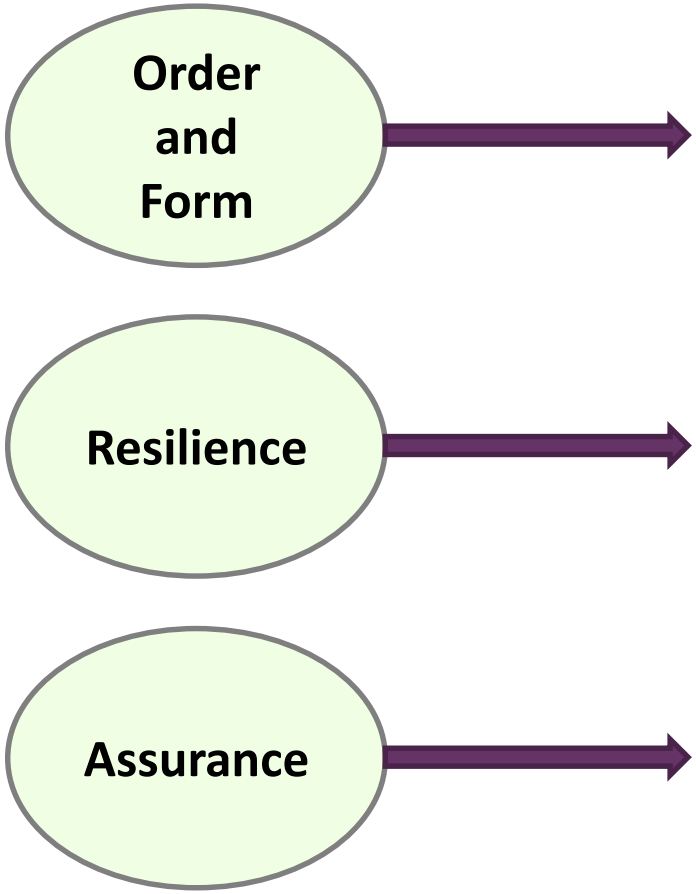
- ***Reductionist View***
  - Divide system into components
  - Assume system faults & failures are caused by component faults & failures
  - Identify chains of directly related physical or logical component failures that can lead to a loss (fault trees, event trees, attack trees,…)
  - Evaluate vulnerability or reliability of components separately and later combine analysis results into a system vulnerability or reliability value

- ***System Theoretic View***
  - Safety and security are emergent properties of the structure, function, and behaviors of a complex system
  - Safety and security are assured by controlling emergent properties (e.g., enforcing constraints) from individual components and interactions
  - View safety and security as a control structure



- ***Goal: Design an effective control structure that eliminates or reduces adverse events***

Where Does This Leave Us?



Defense systems of the future will tend toward 'Ordered Complexity'.

Behavior not fully revealed via decomposition.

Is contextual and emergent.

A System-only view is insufficient to understand and evaluate Resilience.

Cannot be explicitly determined up front.

Is a measure of functional preservation by a control structure.

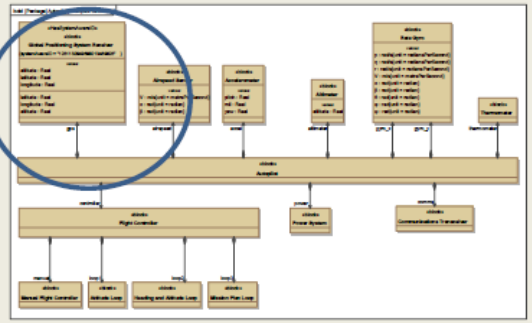
Designing-in Resilience therefore requires both bringing in the context and elucidating structure-function relationships to behavior.

SERC System-Aware Cyber-Security

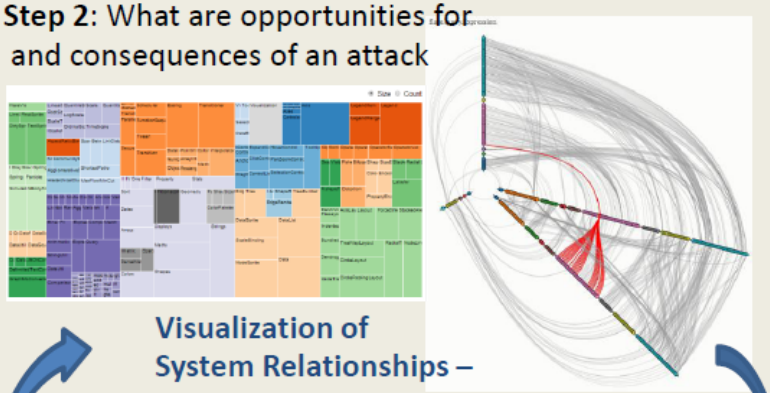
System Aware Cyber Security Framework: V2.0

Step 1: Identify Critical Assets

SysML models of UAV
(High fidelity Model Semantics)



Step 2: What are opportunities for and consequences of an attack

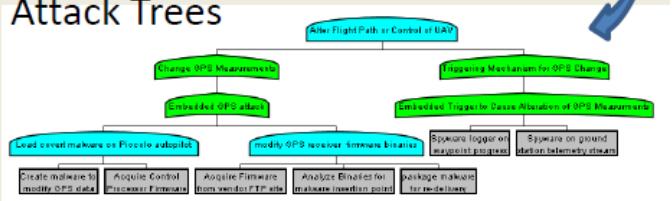


Visualization of System Relationships – Better Coverage of Attack Surfaces

Explicit information exchange- Information from SysML models helps create Attack Trees closer to reality

Step 3: What is exploitable and by whom

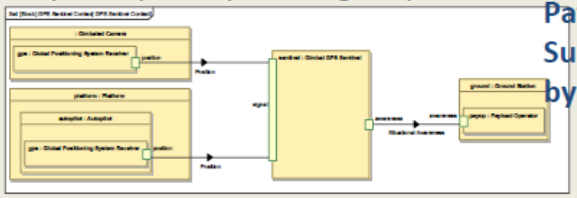
Attack Trees



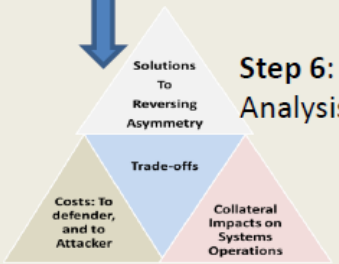
Output:
- Ease of Attack
- Capabilistic Propensity
- Relative Risk

Step 4 and 5: Select/Evaluate Best Design Patterns to effect Adversary's capability to exploit Target System

Evaluation of Design Patterns Now Supported by Functional Models



Step 6: Cost Benefit Analysis



Decision making now aided with Easy to use Data Analysis/Visualization Tools

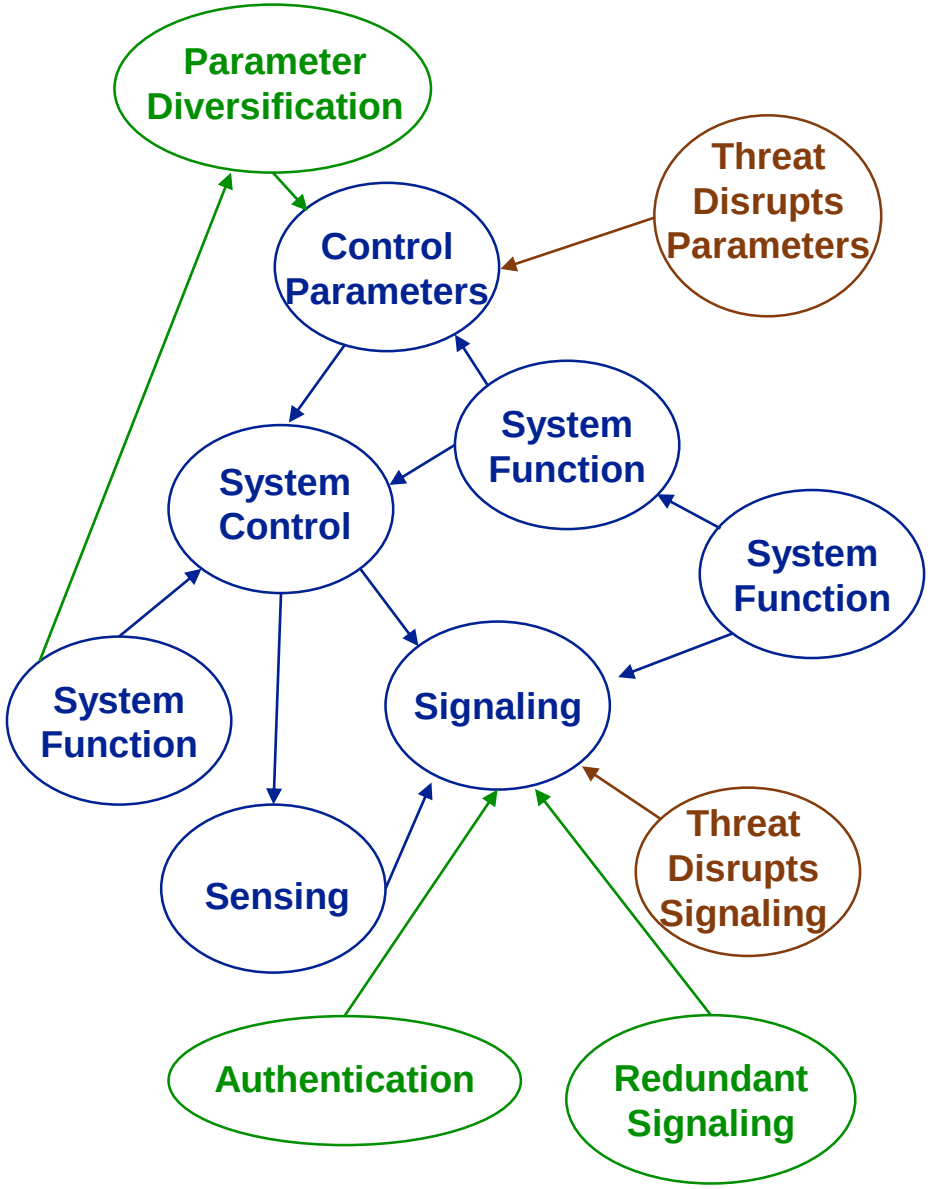
Resources for Attack

Attack Descriptions

Agent Profiles

Where to Start?
– Think executable functional model of the ecosystem

- **Extract system functional information**
  - Directed Acyclic Graph
- **Extract relationships between threat vectors and functional assets**
  - Attack vectors captured in an attack tree
  - Semantic mapping of attack vector descriptors to targeted assets
- **Extract a semantic mapping of Blue design patterns to:**
  - Their functional capabilities
  - Assets they require to achieve capabilities
  - Critical functions/assets they will protect
  - Specific threat capabilities and/or threat assets they are designed to detect or counter through direct connective action

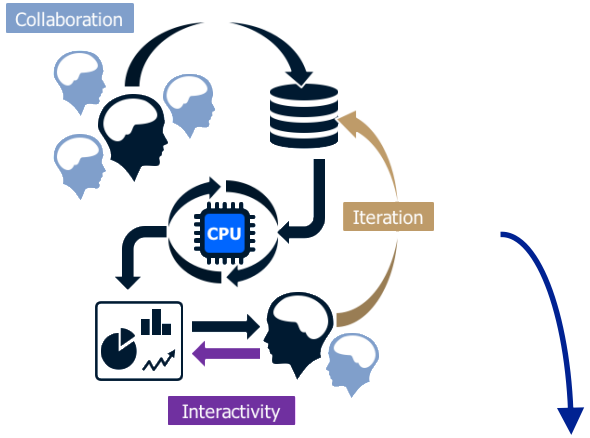


Resilience comes at a Cost

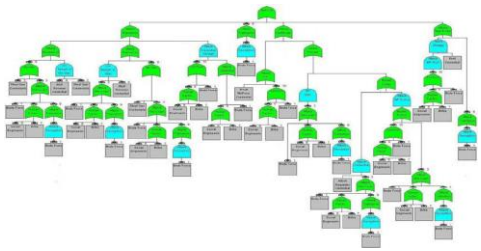
Reduce your space –

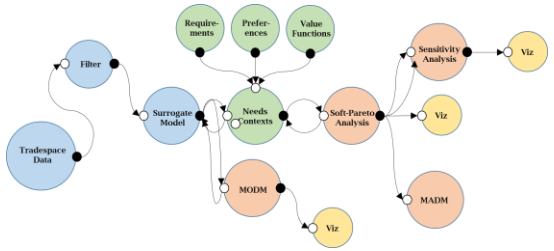
SME-guided analysis of system functions, attack vulnerabilities, and protection methods.

Protection methods serve as defense design patterns.



Create a "library" of security design patterns and associated threats.

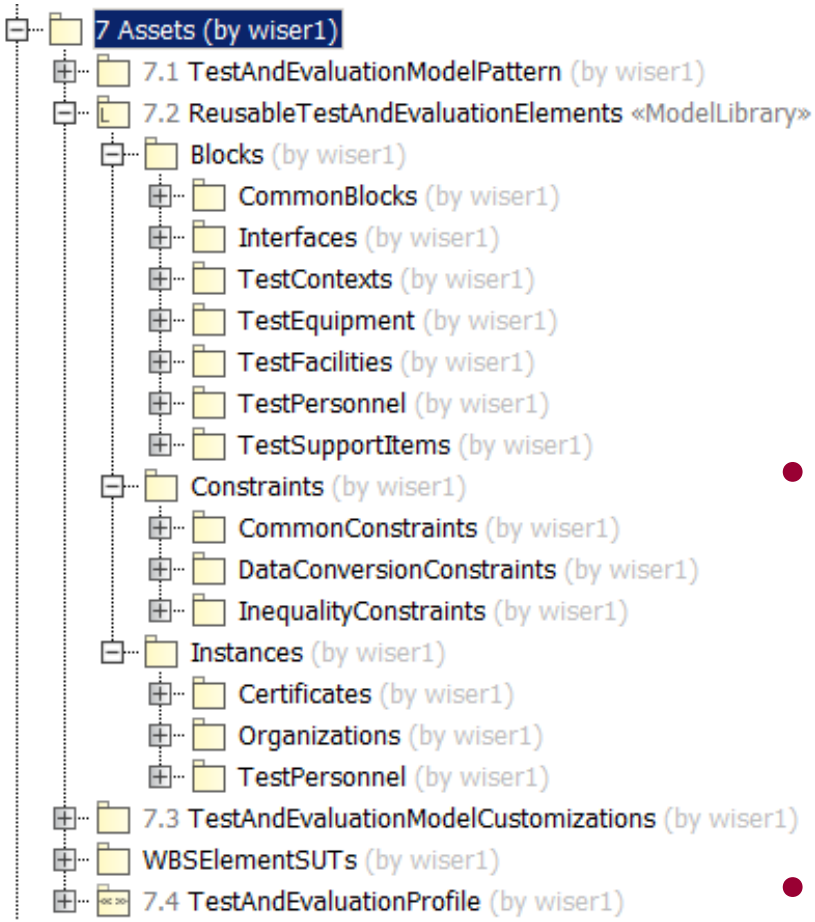




- Prioritize threats and security implementations via decision tool.
- Perform trades on effectiveness, ease, and "cost" parameters.
- Narrow down threat and security implementation spaces.



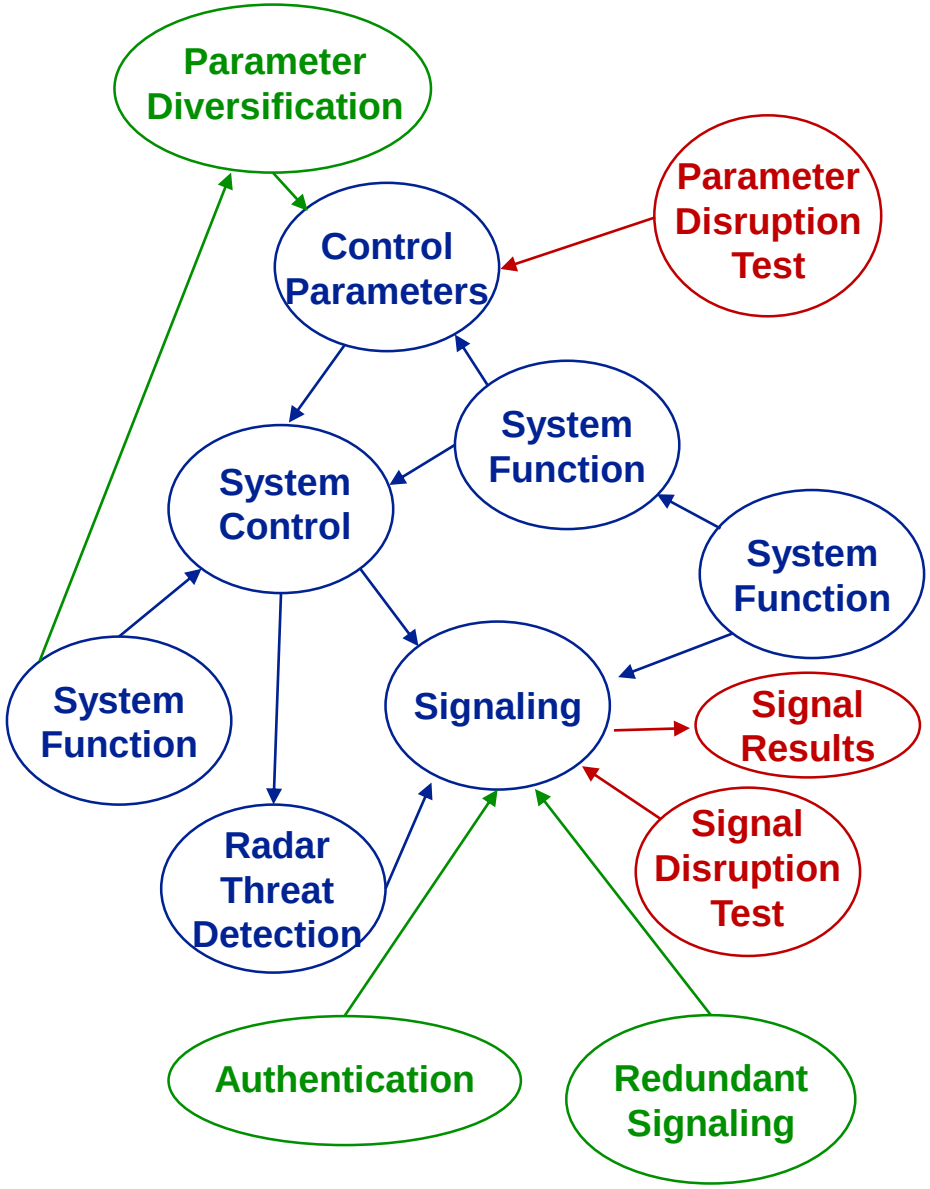
SysML for Test Framework



- Forces Test and SE teams to <u>get specific</u>
  - Captures test knowledge
  - Provides leadership with clear and comprehensive vision of how system will be integrated (and tested),
- It's integrated with the design model
  - The T&E strategy, implementation, and status are integrated with our design model (i.e. our 'source of truth').
- Consistency
  - Assists in the transition process as personnel turnover responsibilities

Where to End?
– Test an executable functional ecosystem model

- **Extract system functional information**
- **Extract relationships between threat vectors and functional assets**
- **Extract a semantic mapping of Blue design patterns**
- **Create assurance test framework and patterns to:**
  - Evaluate system response to threat
  - Maintain explicit knowledge of vulnerabilities and corrective patterns in design model
  - Build standard libraries of test strategies



Motivation for Research

Represent:

(a) impact of a threat, and

(b) impact of a protective implementation, and

(c) How it was evaluated, on

(d) the critical functional capabilities of a CPS.

… but challenges remain.

Structure-Function Relationships

- How do we reveal complex structure-function relationships that may not be visible via the functional decomposition model produced in early-stage design?

Identical number of nodes, links, and degree distribution.

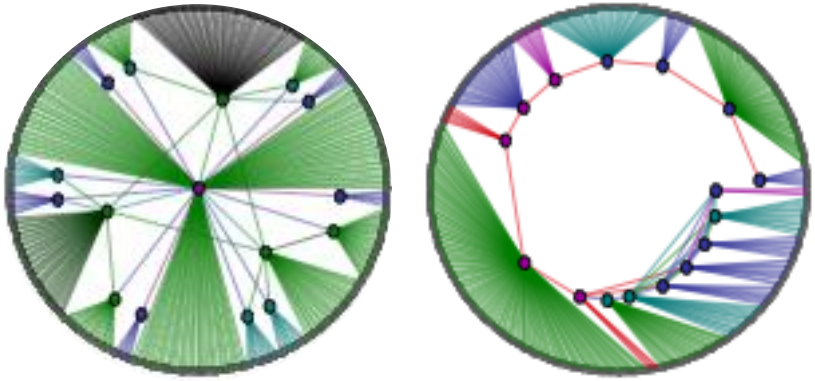


Image from Li (2005)

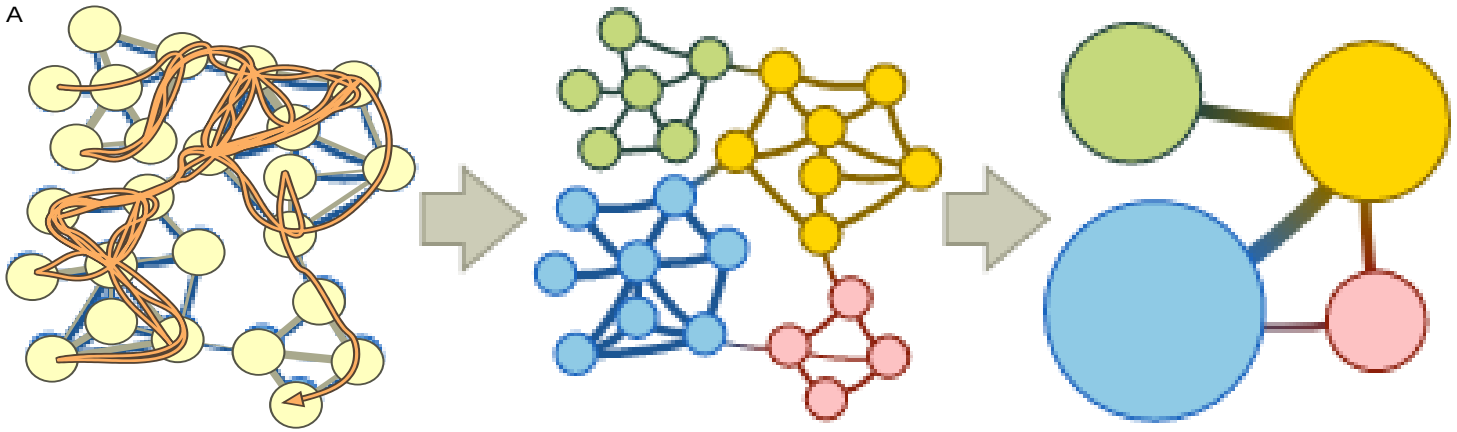
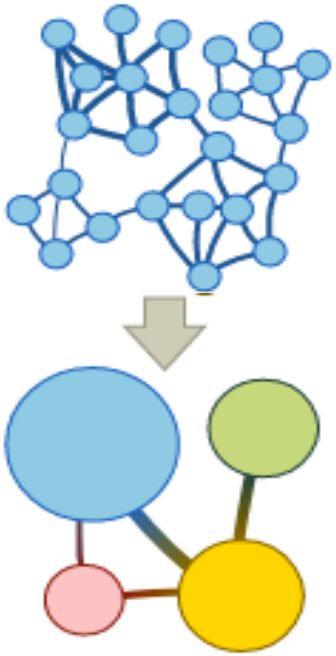


Image from Rosvall, http://www.tp.umu.se/~rosvall/

Elucidate Structure-Function relationships by discovery.

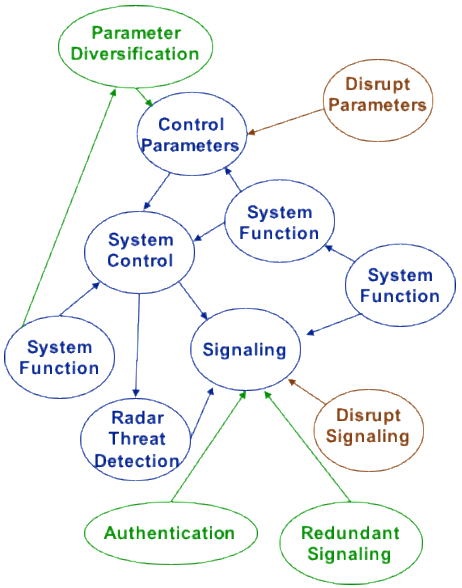
Synergy between Relationship Mapping and Model-Based System Design Processes

Embrace natural complexity of systems, revealing emergent behaviors, economies and diseconomies of scale, and consequences otherwise hidden



Research questions:

- Explain relationship between functional representations
- What does mapping reveal about fault or failure modes not discernible in the original topology?
- Do structural design changes preserve functionality of system?
- Can we use to determine impact of different approaches –
- Did our design decisions preserve functionality for our system?



Model-Based System Assurance

SYSTEMS ENGINEERING RESEARCH CENTER

A U.S. DEPARTMENT OF DEFENSE UNIVERSITY AFFILIATED RESEARCH CENTER



- Please see me to request an invite
- Tom.mcdermott@gtri.gatech.edu

Cybersecurity as an Integral Part of Systems Engineering

October 26, 2017

Bill Decker
Kim Kendall
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35806
kim.kendall@dau.mil
256-922-8143

www.DAU.mil

Approved for Public Release

Ground rules

- This is a discussion, not a lecture
- Your opinions and viewpoints are welcomed
- There are no right/wrong answers

Agenda

- Introduction
- Risk Management
  - Technical Risk
  - Cyber
  - Differences/similarities
- Conclusion

Traditional Risk Management

- Identify potential risks
  - FMEA, team, etc.
- Risk Management
  - Criticality analysis
  - Root cause analysis
  - Potential consequence
  - Document in a risk statement (If-Then)
  - Identify risk reduction efforts (cost – benefit)
  - Track risk mitigation over time
  - Categorize (green, yellow, red) for management

Cyber risk management

- Identify the criticality of the system
- Use to determine which controls are applied
  - Risk reduction?
- Rinse and repeat on a regular basis

Table 6: RMF for DoD IT Activities Throughout the Life Cycle

Life Cycle Event	RMF for DoD IT Activities
ASR	• Categorize the information types • Select security control (SC) baseline • SC trace to the preliminary system performance specification • Incorporate SC requirements into the TMRR system performance specification and SOW
SRR	• Refine derived SC system-level requirements • Incorporate into specifications for the technical solution
SFR	• Tailor the security controls • Allocate tailored SC into system requirements • Ensure the updated tailored SC requirements are included in the system functional baseline • Incorporate CS functional requirements and verification methods into the initial Development RFP
PDR	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
CDR	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing
SVR/FCA, P&D and O&S Phases	• Tailor and Allocate SC requirements to the hardware and software design • Incorporate tailored SC requirements into system performance specification, SOW, and other contract documents for Development RFP • Align the security assessment plan with the T&E master plan to ensure inclusion of CS testing

From Defense Acquisition Guidebook CH 9–3.2.2 Risk Management Framework for DoD IT

How DoD is addressing

- Next few slides are from an August 2017 briefing by Colonel Dean “Data” Clothier, Chief of the Cyberspace Division, Joint Staff/J-6, title:

“New DoD Approaches on the Cyber Survivability of Weapon Systems”

Background

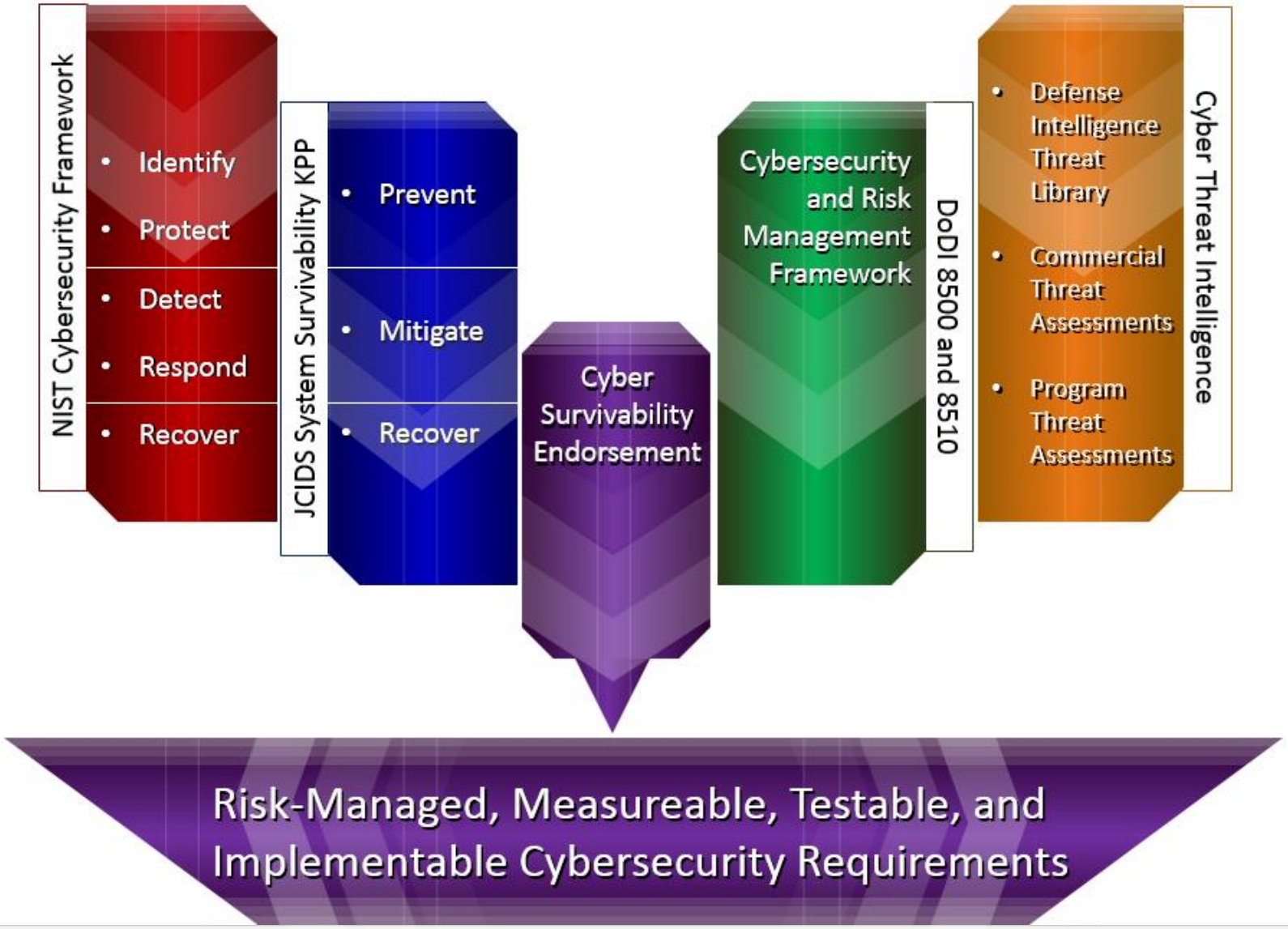
- **DepSecDef (DSD) directed Joint Staff develop Cybersecurity KPP**
  - Initiated when DSD briefed on DOT&E Cybersecurity Report w/ OUSD(AT&L), OUSD(P), DOD-CIO and VCJCS … *Highlighted multiple weapon systems with vulnerabilities that should have been known and fixed prior to DT&E.*
  - Intended to eliminate or sufficiently mitigate known vulnerabilities prior to fielding.
  - Implemented through deliberate design, test and associated DOTmLPF-P in applicable operational environments.

- **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents.

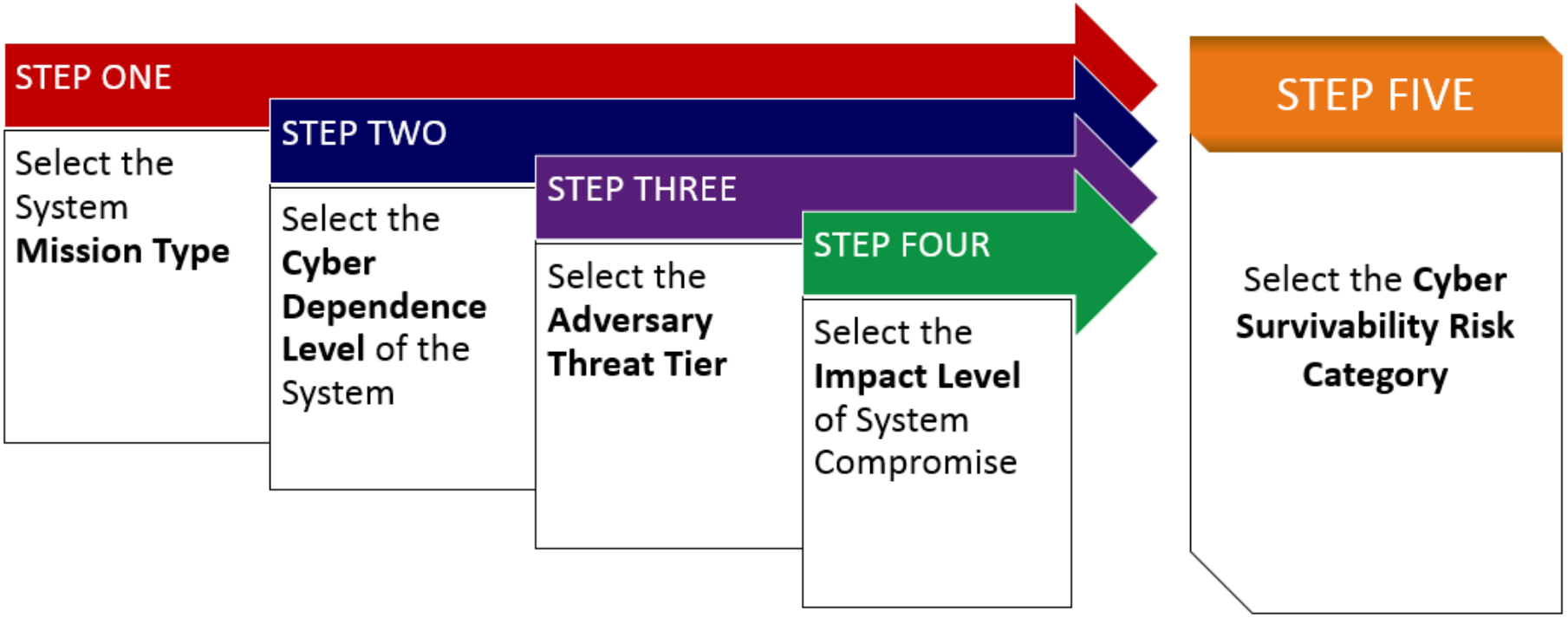
- **Objectives**
  - Drive development of the Joint cyber survivability requirements ... to meet requirements for cyber attack prevention, mitigation and recovery
  - Ensure performance measures are consistent with the threat and consistently applied … during requirements definition, development and testing
  - Ensure cyber survivability and cybersecurity requirements are considered … and included as part of the operational risk trade space

End State: All DoD weapon systems are cyber survivable commensurate with a risk managed approach to countering a capable and determined adversary

Cybersecurity Framework Integration



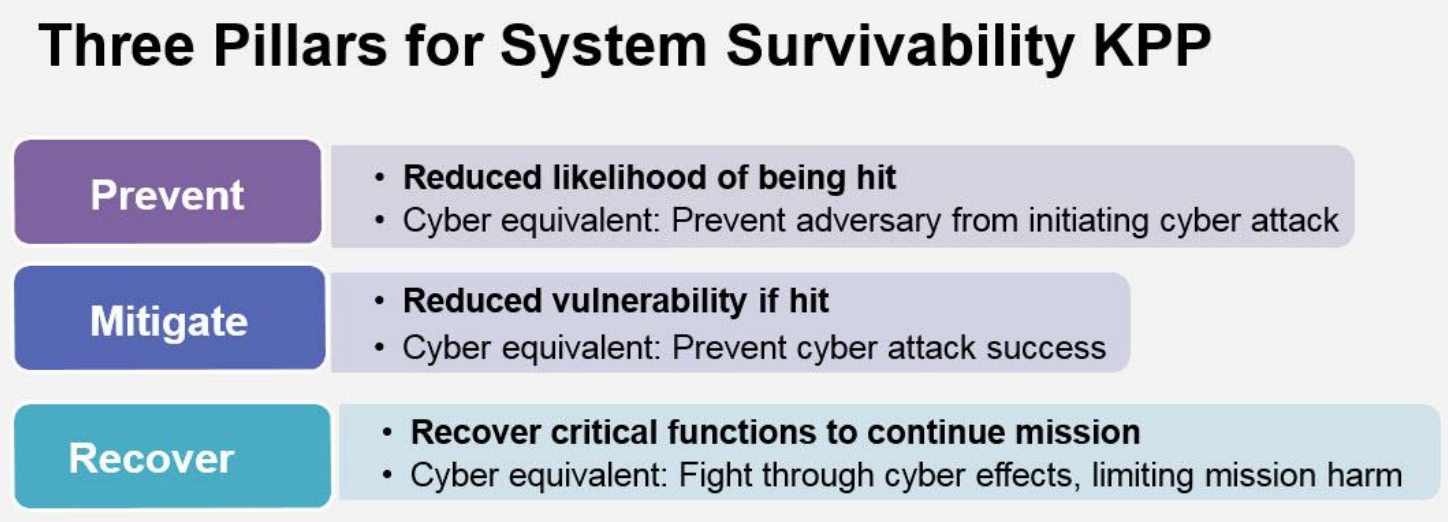
Risk Managed Approach



The CSE 5 step risk managed approach takes into account several variables … the resulting CSRC provides consistency between levels of CS requirements, development and testing

Cyber Survivability Endorsement to the System Survivability KPP

- The Joint Staff and DoD CIO developed Cyber Survivability Endorsement (CSE) criteria to assess requirements for key attributes that increase cyber survivability.



Ref: https://rmfks.osd.mil/rmf/Guidance/RMFRelatedTopics/CybersecurityAndAcquisition/Pages/KeyPerformance.aspx

Cyber Survivability Attributes to Tailor in the CDD/CPD

SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSA) (All are considered, select those applicable)
Prevent	CSA 01 - Control Access
	CSA 02 - Reduce Cyber Detectability
	CSA 03 - Secure Transmissions and Communications
	CSA 04 - Protect Information and Exploitation
	CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels
	CSA 06 - Minimize and Harden Cyber Attack Surfaces
Mitigate	CSA 07 – Baseline & Monitor Systems, and Detect Anomalies
	CSA 08 - Manage System Performance if Degraded by Cyber Events
Recover	CSA 09 - Recover System Capabilities
***All* 3 KPP Pillars**	CSA 10 – Actively Manage System's Configuration to Counter Vulnerabilities

- Prevent – Design requirements that protect weapon system's functions from most likely and greatest risk cyber threats.
- Mitigate – Design requirements that detect and respond to cyber-attacks; enabling weapon systems functions resiliency to complete the mission.
- Recover – Design requirements that ensure minimum cyber capability available to recover from cyber attack and enable weapon system quickly restore full functionality

Fundamental to the CSE construct is enabling sponsor to select and articulate CSA choices to achieve each SS KKP Pillar

Wrap-Up

- **Problem:** System survivability requirements not sufficiently articulated for cyber-attack prevention, mitigation and recovery, within requirements documents

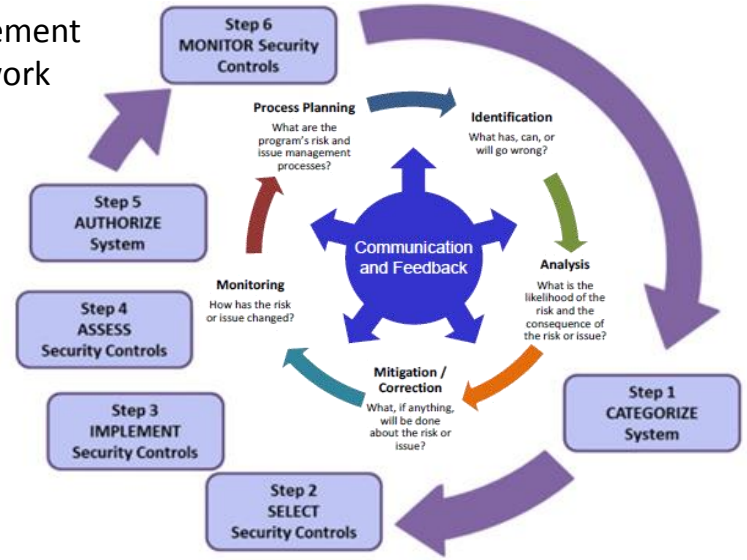
- **CSE Implementation Guide Objectives:** Joint Staff led effort, with active participation from OSD-CIO, OUSD(AT&L), OUSD(I), DOT&E, DIA, and NSA.
  - **Drives development of Joint cyber survivability requirements** … to meet requirements for cyber attack prevention, mitigation and recovery.
  - **Incorporates high level cybersecurity exemplar statements** … prior to the availability of DIA or Service development of system specific threat assessments.
  - **Defines Cyber Survivability Risk Category (CSRC)** … to enable a consistent approach to cybersecurity requirements, development and testing.
  - **Outlines Cyber Survivability Attributes (CSAs)** … to be **considered** by requirement sponsors, which can be **consistently** applied, **implemented** by system security engineers, and **tested** by DT&E/OT&E.
  - **Provides Exemplar Requirements and Scorecard** … support development and assessment and management of requirements.

- Due out shortly (Fall 2017)

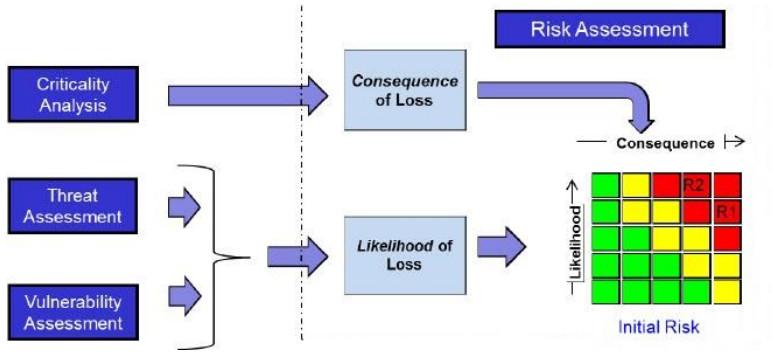
End State: All DoD weapon systems are cyber survivable commensurate with a risk managed approach to countering a capable and determined adversary

Risk Management Integration

Cybersecurity Risk Management Framework (RMF)



Program Protection and Trusted Systems & Networks (TSN)



TSN Analysis

Risk, Issue, and Opportunity Management

Discussion

- Does this help?
- What will be the disconnects?
  - Vocabulary (CSE, controls, etc.)
  - Still delegated to “cyber guy/gal”
- What would be gained (lost) if we used traditional RM processes

Conclusion/recommendations

- Cyber requirements difficult to quantify
- CSE approach will help – guide coming Fall 2017
- Vocabulary/processes still not the same for cyber and other threats
- DoD recognizes the problem
- Challenge is rationalizing the two systems
- Debate on whether to use one approach for both



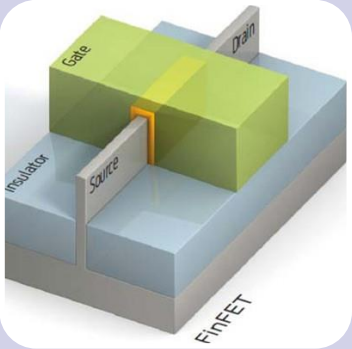
Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs

Jeremy Muldavin, Ph.D.
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

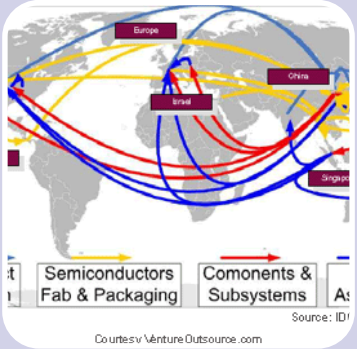
20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Microelectronics Trends









State-of-the-art Devices

- Deeply-Scaled Silicon ICs (10nm)
- 2.5 & 3D ICs
- Heterogeneous System-on-Chip (SoC) ICs
- Flexible and miniature packaging
- Accelerator and SoC architectures

Increasing Cost and Complexity

- $5-15B for a modern fabrication facility
- >$500M for a new commercial smart phone SoC development
- Reliance on third-party Intellectual Property (IP)
- No one can do it alone

Globalization and Commercial Dominance

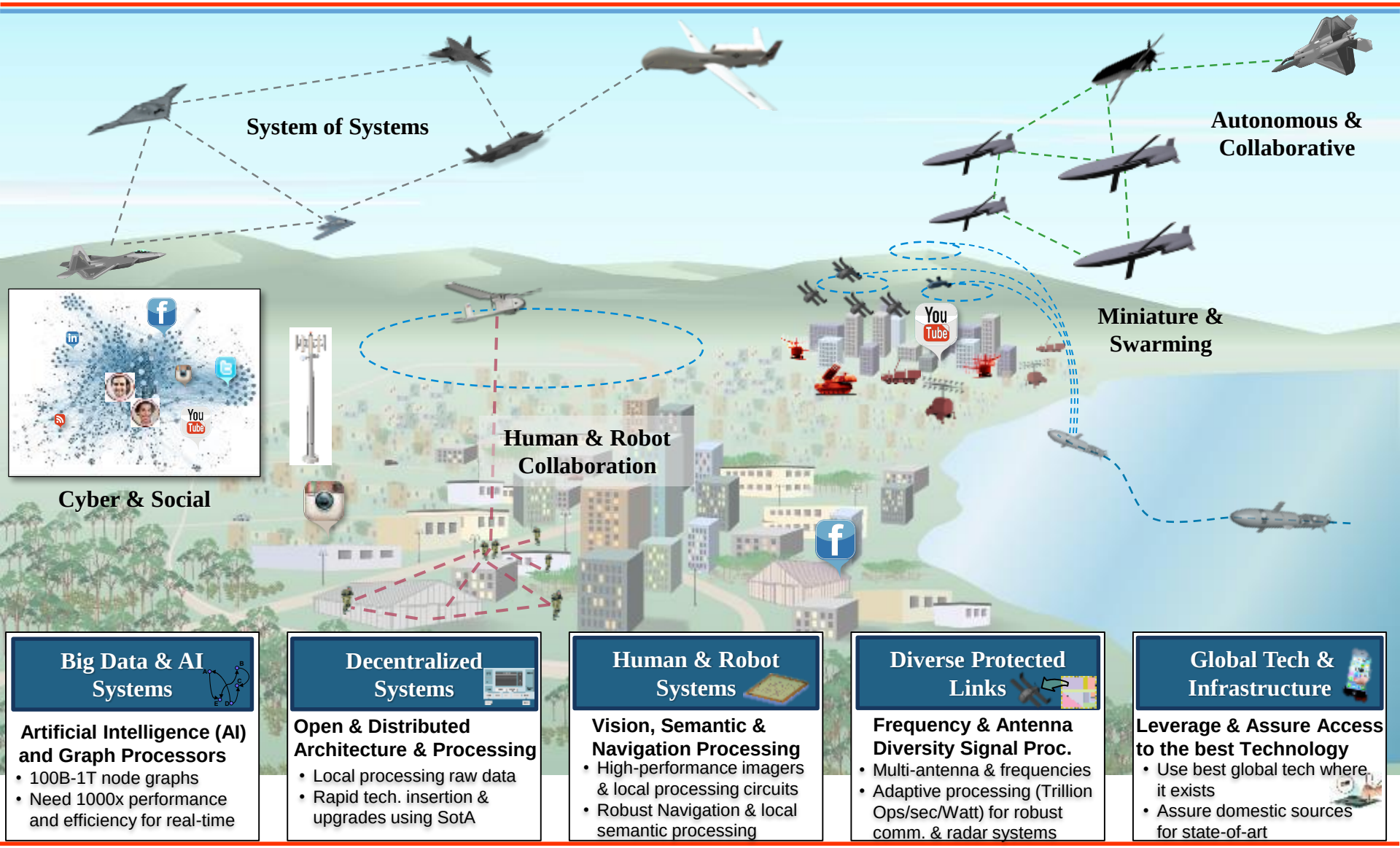
- State-of-the-art fabrication consolidation
- Commercially driven (DoD <1% of market)
- Complex global supply chain
- China ($150B) & Saudi Arabia ($100B) investing heavily

New Applications

- Internet of Things
- Big Data systems
- Autonomous systems
- Spectral and spatial communication agility
- Government & Defense need all of above with higher security & performance

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Future Warfighting Systems
Advanced Microelectronics Needs



Big Data & AI Systems

Artificial Intelligence (AI) and Graph Processors

- 100B-1T node graphs
- Need 1000x performance and efficiency for real-time

Decentralized Systems

Open & Distributed Architecture & Processing

- Local processing raw data
- Rapid tech. insertion & upgrades using SotA

Human & Robot Systems

Vision, Semantic & Navigation Processing

- High-performance imagers & local processing circuits
- Robust Navigation & local semantic processing

Diverse Protected Links

Frequency & Antenna Diversity Signal Proc.

- Multi-antenna & frequencies
- Adaptive processing (Trillion Ops/sec/Watt) for robust comm. & radar systems

Global Tech & Infrastructure

Leverage & Assure Access to the best Technology

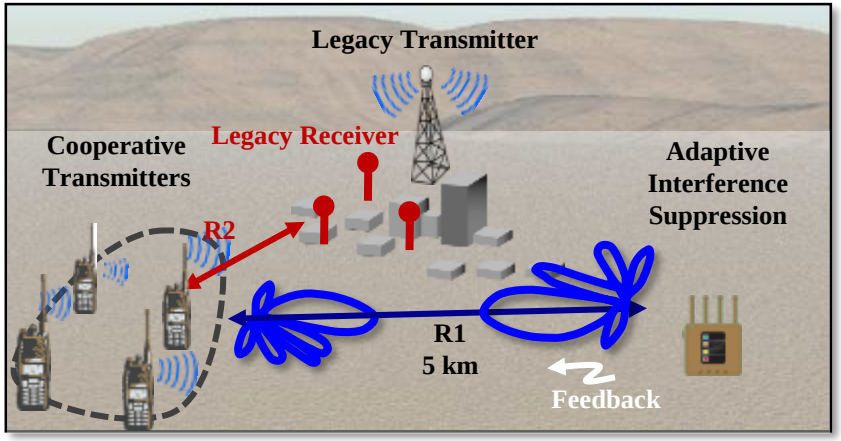
- Use best global tech where it exists
- Assure domestic sources for state-of-art

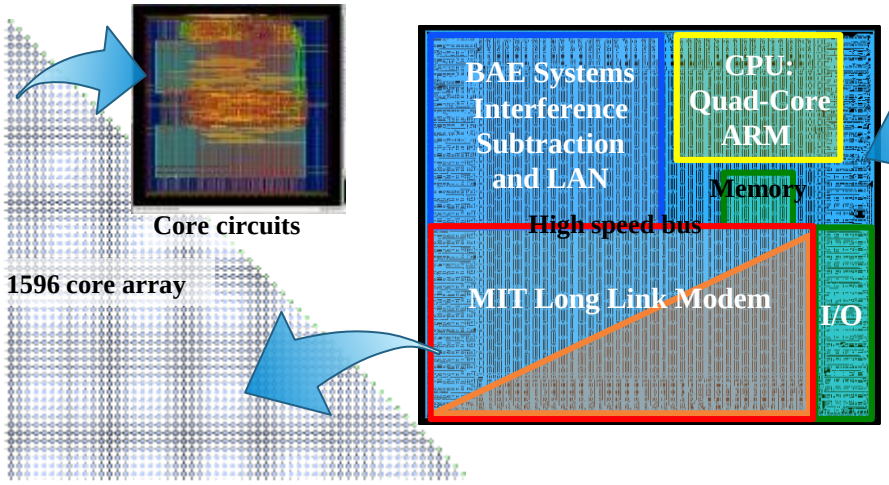
Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

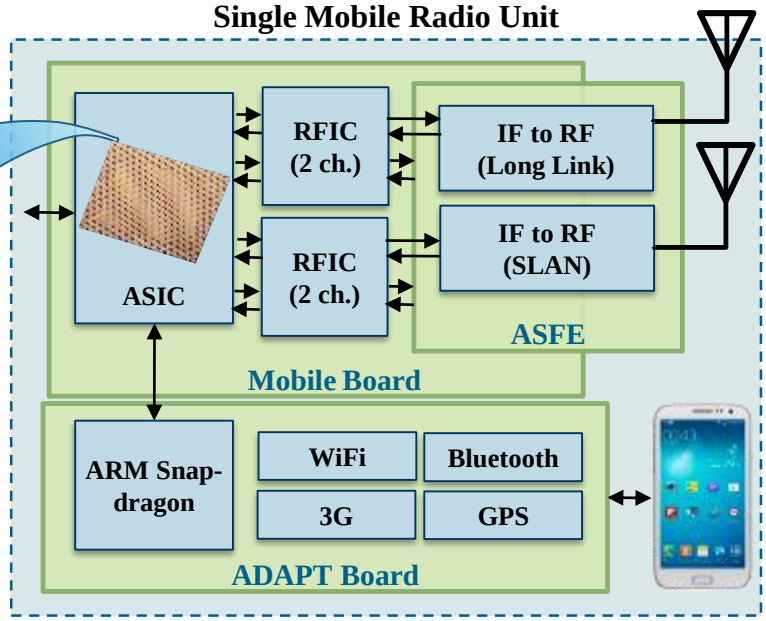
A DoD System on Chip Example

Leverages extreme ASIC computational technologies

- Coherent beam forming, adaptive nulling and interference cancellation:
  - 5-10x range extension or 1000x lower power
  - 10000 interferer to signal ratios
- Mobile radio form factor achieved by ASIC accelerators with 1.7 TOPS/W





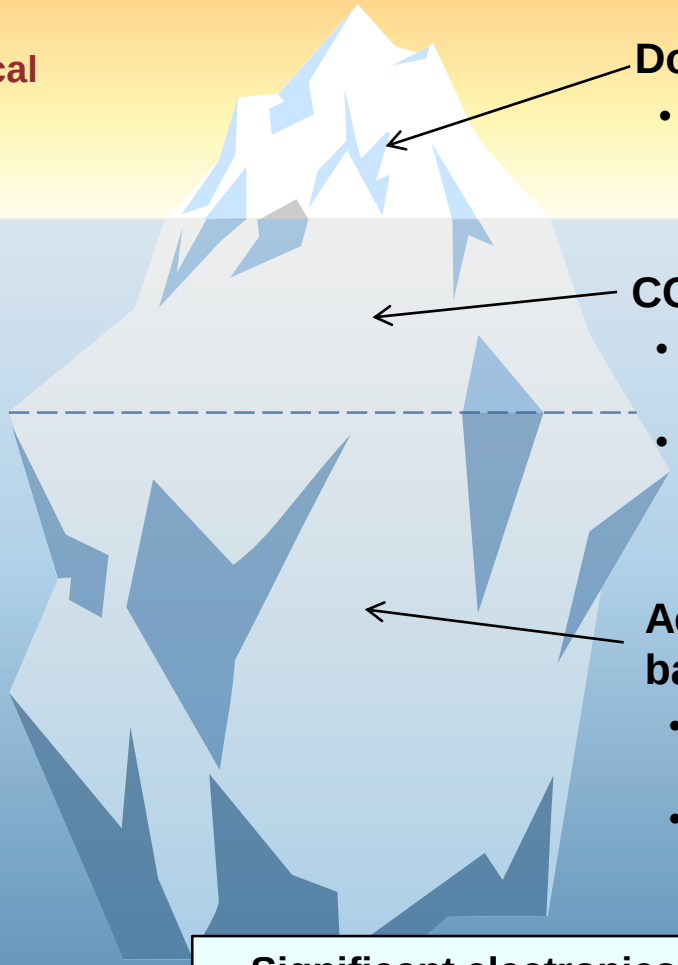


1.7 TOPS/W System on Chip for MIMO Communications Applications

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Electronics as a Strategic Issue

Current Tactical Issue



Larger Strategic Issue

DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-16 Trusted Foundry Program

COTS Electronics Trust (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 17: Trusted & Assured Micro-electronics

Access to Electronics / Electronics based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

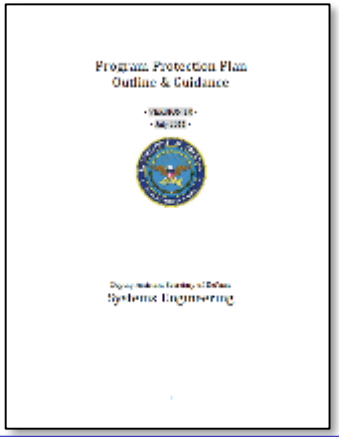
POM 19-23: Micro-electronics Innovation for National Security

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

What We Are Doing



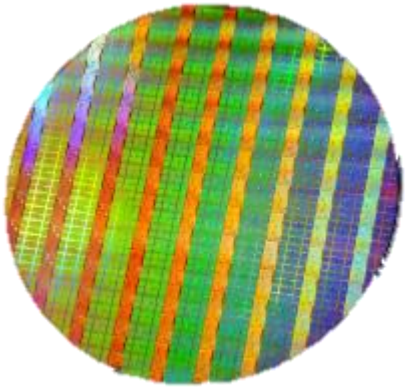
Policy

- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)



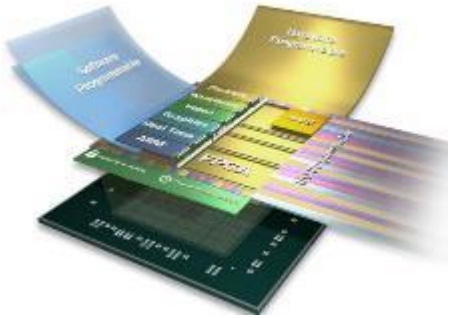
Joint Federated Assurance Center

- Software assurance knowledge & tools
- Hardware assurance knowledge & tools
- Advanced verification & validation capabilities



Trusted & Assured Microelectronics

- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance

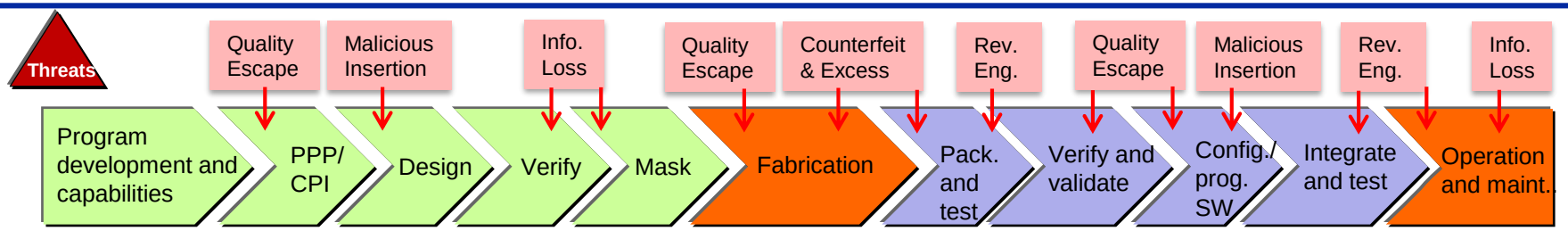


COTS and FPGA

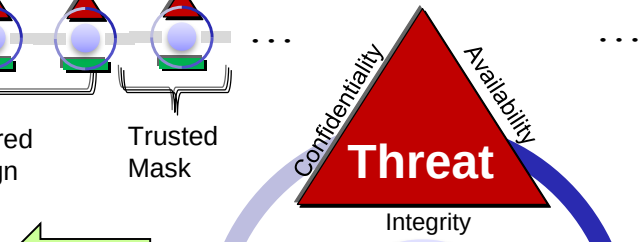
- Supply chain risk management
- FPGA Assurance Study
- Radiation-hardened microelectronics initiative

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Systems Engineering Approach







JFAC & Industry

Efficacy

Impact

Mitigation



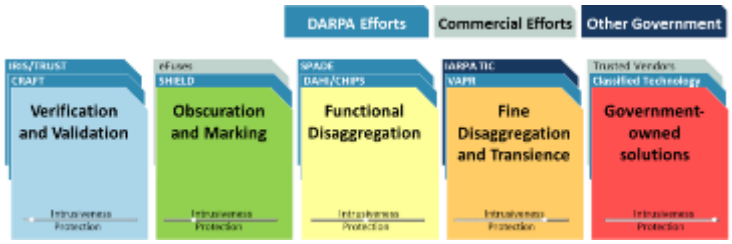
Innovators & Developers

System architects

R&D engineers

Acquisition experts

Manufacturing experts





Adopters & Improvers

System integrators

Test and validation

Operators and maintainers

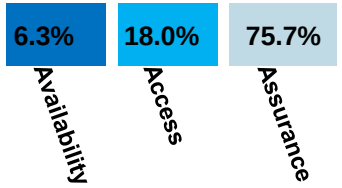
Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

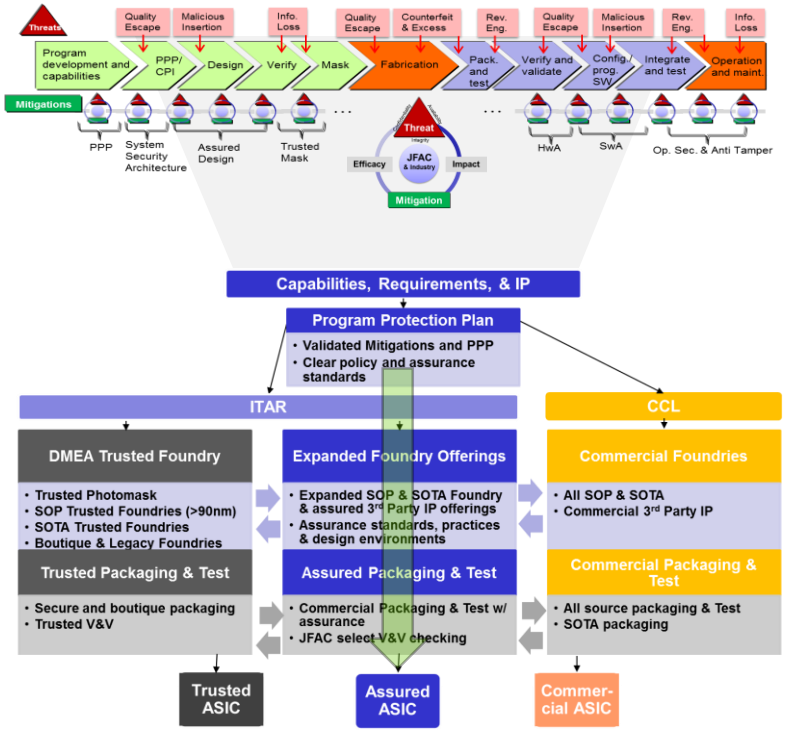
Trusted & Assured Microelectronics FY18 Activities and Investments

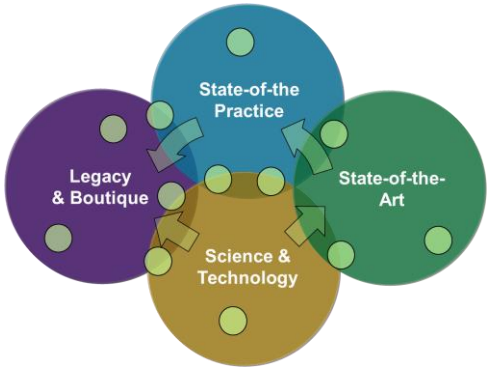
Overall

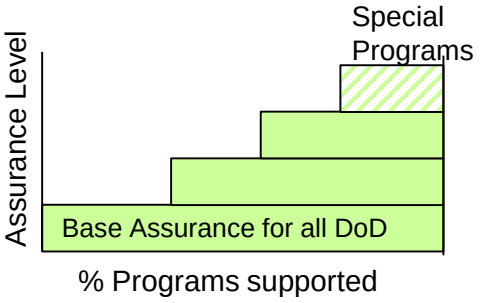
Inputs	Investments & Actions	Deliverables & Outcomes
• DARPA, IARPA, & Commercial Assurance Technologies • JFAC Labs, DMEA, FFRDCs • DoD Programs & Commercial Suppliers	• Develop, Mature and demonstrate Assurance Mitigations • Evaluate Effectiveness of protections of IP and Integrity • Support trusted mask fabrication • Transition to & support programs	• List of Validated mitigations and V&V capabilities • PPP and mitigation guides and best practices • Program demonstration support and trusted mask creation • Special program V&V support

FY18 Funding Distribution





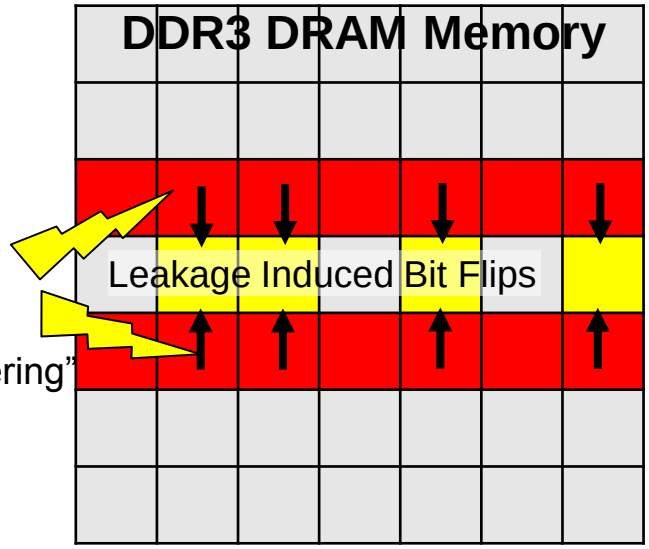




Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Examples of Recent Cyber Attacks on HW Vulnerabilities

- **Rowhammer Attack**
  - Fault in DDR3 DRAM modules
  - High integration density allows leakage current to neighbor rows on readout
  - Rowhammer induces frequent readout to intentionally force bit flips in adjacent transistor rows.
  - **Effects**: Loss of Data, Loss of Reliability, Privilege Escalation



- **Cyber attack on Smart Phones with Adups Firmware (FW)**
  - FW uses HW to perform data exfiltration of texts and personal data, enabling Chinese gov't to monitor citizens
  - Very weak security protections enabled exploitable FW to be loaded on American Smart Phones.
  - **Effects:** Millions of smartphones affected worldwide and devices geographically targeted thru GPS data

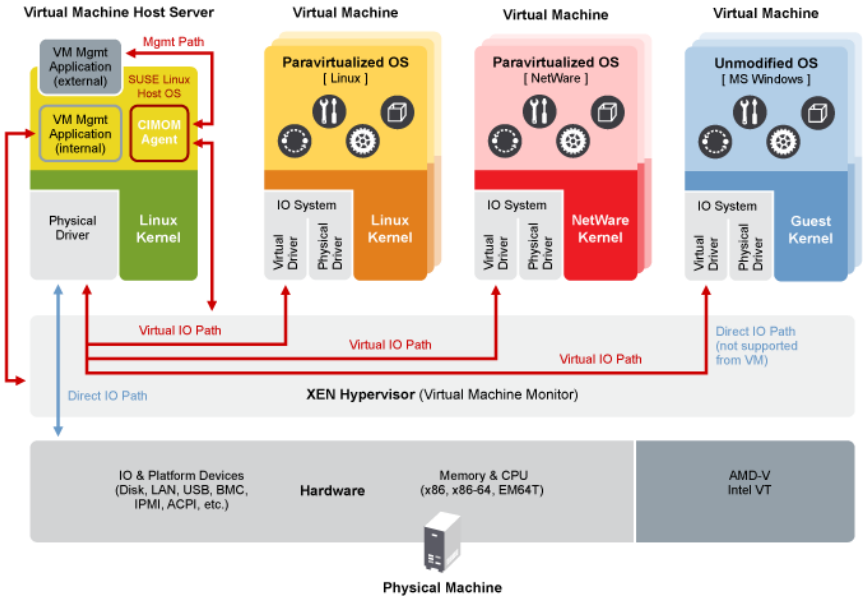
Reference:<https://en.wikipedia.org/wiki/Row_hammer>
Reference:<https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html?_r=2>

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Mitigations to Cyber Exploits of HW Vulnerabilities

- **Root of trust (ROT)**
  - Encryption of data
  - Monitoring for unauthorized operations
  - Detection of attempts to root a device
  - Memory security partition management
  - Digital rights management
- **Embedded Hypervisor Enforces Security Rules from ROT**
  - Requires only signed SW and FW can be loaded onto HW
  - Controls authentication and setup of initial system state to restrict unauthorized access to HW
- **Monitoring Software**
  - Software that observes execution of the system
  - Alerts to any unauthorized behavior

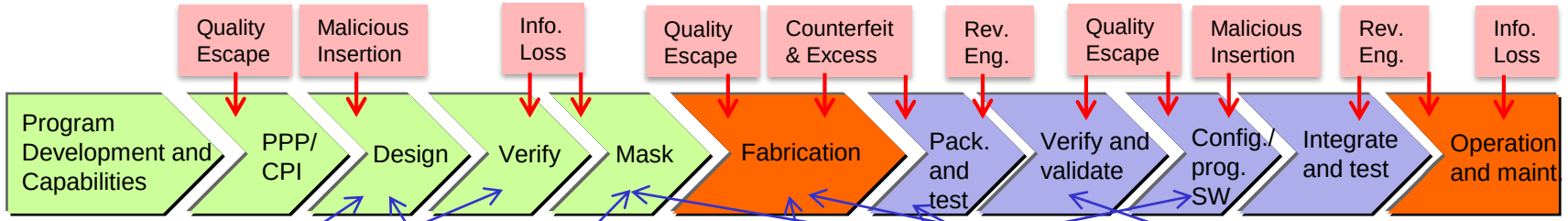
XEN Hypervisor Implementation



Reference:<http://www.novell.com/documentation/vmserver/virtualization_basics/data/ba0khrq.html>

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

New Trust and Assurance Approaches

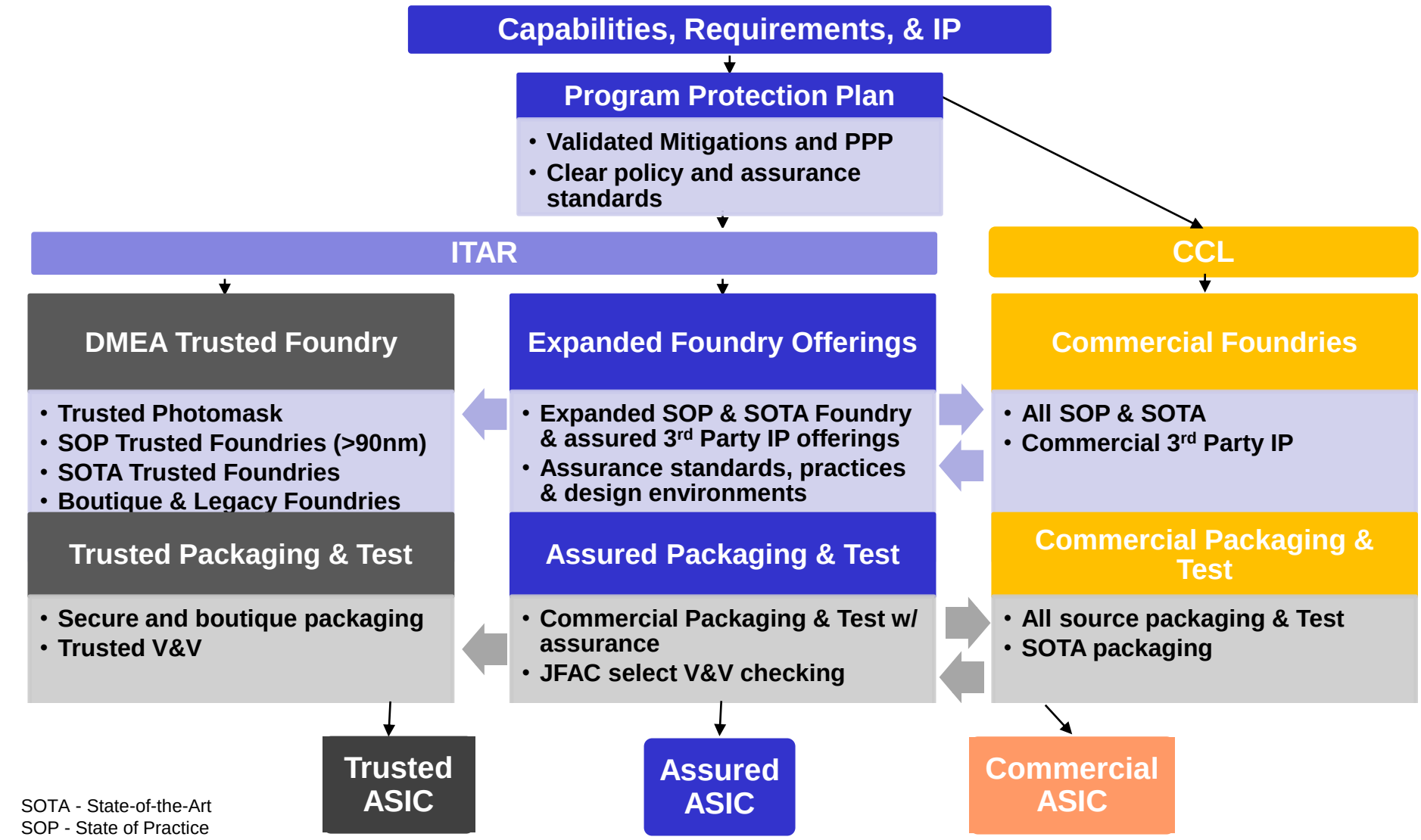


Design for trust	IP protection	Low-volume/high-mix production	Electronic component markers	Imaging technologies and forensics
• Designing techniques to limit full use/functionality to trusted operation	• Preventing exploitation, including control of use, concealment, reconfiguring, partitioning, or employment	• Innovative methods to permit cost-effective, Trusted and assured low volume manufacturing of state-of-the-art ICs	• Tagging/marking ICs and subassemblies to authenticate and track supply chain movements	• Advanced capabilities to efficiently evaluate dense, state-of-the-art commercial components

Implement and demonstrate assurance capability with transition partners

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Potential Paths to ASIC Production for DoD



SOTA - State-of-the-Art
SOP - State of Practice

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

T&AM Focus Areas

Verification & Validation

- Improves microelectronics test and verification methodologies in support of verifying the trust and assurance of parts

Design Assurance

- Assured and immediate access to domestic production of advanced microelectronics and disruptive research and development investments to surpass the impending limitations of Moore's Law on silicon microelectronics

FPGA Assurance

- Demonstrate innovative design, manufacturing, imaging, tagging, control and assessment approaches for protecting DoD's microelectronics supply chain and intellectual property

Enhanced Manufacturing

- Development of advanced node microelectronics fabrication and packaging capabilities at existing SOTP foundries with a focus on high-mix, low-volume alternatives

Radiation Hardened Microelectronics

- Demonstrate innovative design, manufacturing, and assessment approaches for trusted, strategic radiation-hardened electronics in advanced technology nodes for next-generation strategic systems

Outreach & Standards

- Develop standards and practices to foster commercial development of secure, trusted and assured parts.
- Document and promulgate security-enhancing design practices across government, industry, and academia

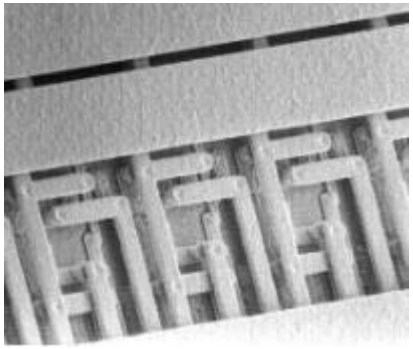
Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

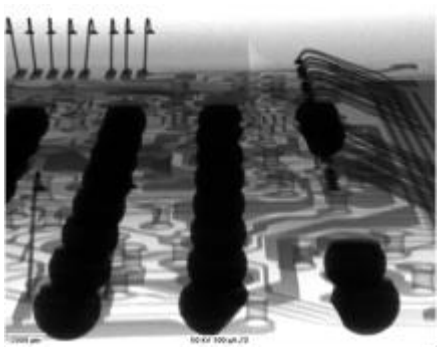
Microelectronics Trust Verification Technologies

- **Verification needed when Trusted Foundry not available**
  - DoD formed JFAC to provide this service
  - Long-term challenge to analyze leading-edge ICs and scale up capacity

Design Verification	Physical Verification	Functional Verification
• Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.	• Destructive analysis of ICs and Printed Circuit Boards	• Non-destructive screening and verification of select ICs







DoD, Intelligence Community, and DoE enhancing capability to meet future demand

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Verification & Validation: Survey Status and Initial Results

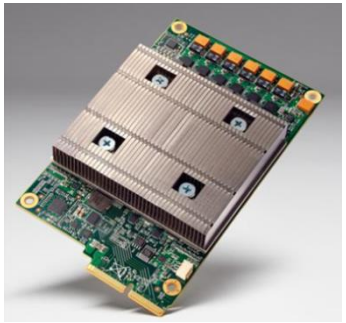
Data obtained from:

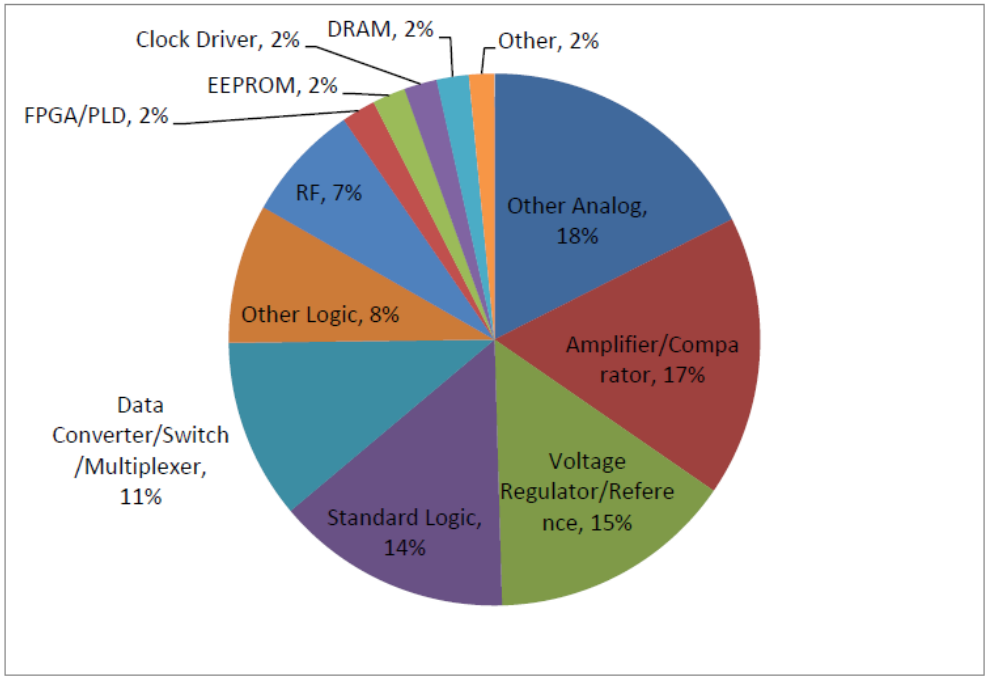
- Programs (early production and pre-production) based on BOMs
- Commercial Assemblies bases on BOMs
- Programs that have completed prioritized usage survey
- Companies that have completed prioritized usage survey
- S&T Programs that have completed prioritized usage survey



NVIDIA Tesla GPUs
15.3 Billion transistors IC

Google's Tensor Processing Unit could advance Moore's Law 7 years into the future





Above chart curtesy IDA report, *Examination of DoD's Use of Microelectronics in Weapon Systems*, 2013

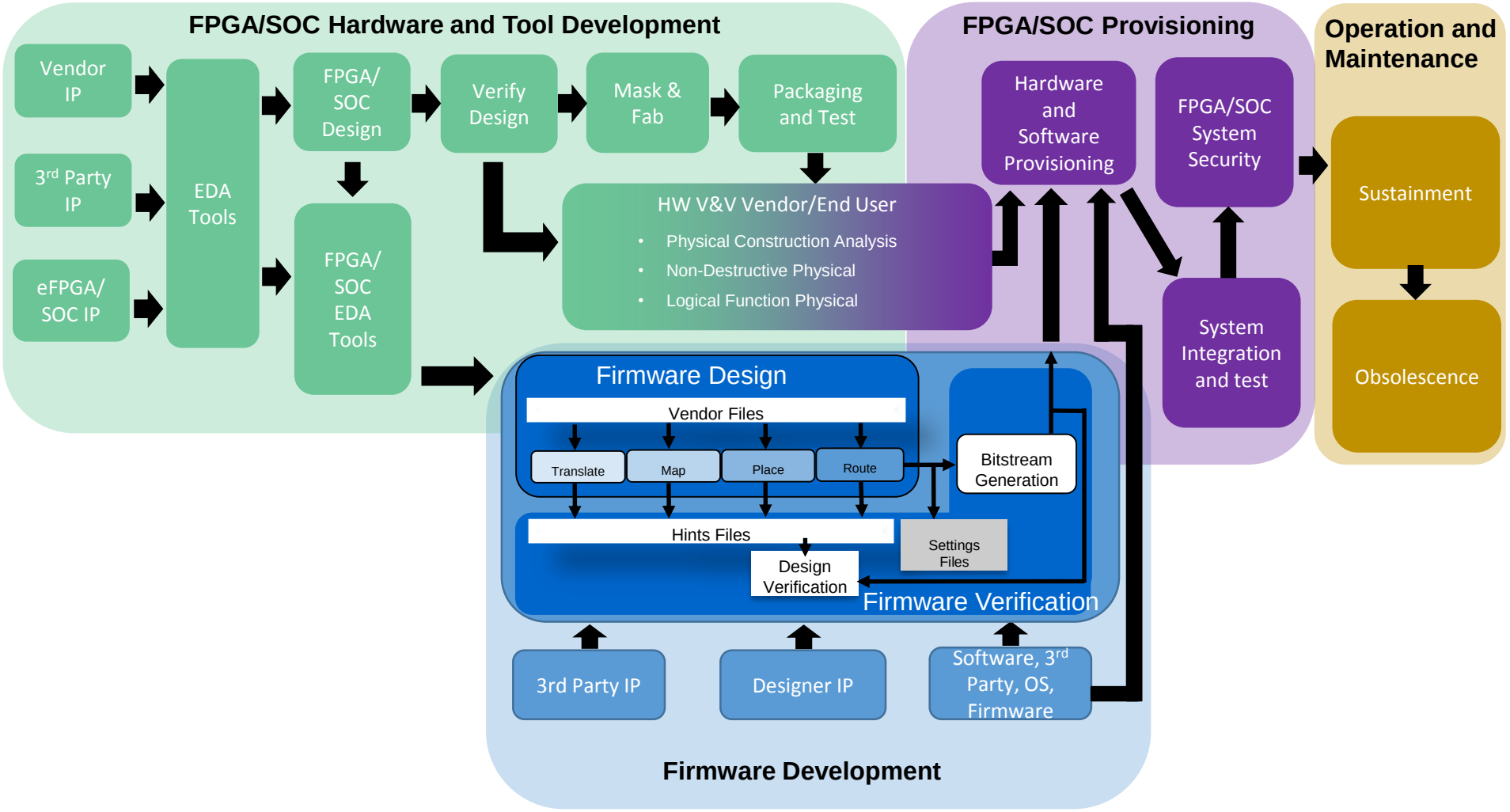
Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Outreach and Industry Standards

- **JFAC Standards and Best Practices Sub Group**
  - Establish a charter to be reviewed and approved by JFAC, T&AM and Service/Agency communities
- **Evaluate COTS methods and realistic/practical alternatives for attaining trustworthiness**
  - Extension and application of the Trustworthy Supplier Framework
- **Develop and expand the NDIA Collaboration**
  - Work towards the establishment of the “Electronics Division”
    - Shared government liaison – DASD(SE), DMEA, DASD(MIBP) and NRL on behalf of the MEC MWG
  - Continue building community, workshops and meetings – build the NDIA Electronics as a central focus for industrial dialog with the government
- **Collaboration and Information Sharing**
  - Pilot with FPGA Assurance and the JFAC Standards Group - Collaboration models, Information sharing
  - IntelDocs on Intelink for FOUO/Unclass (NIPR)
  - Pilot Standards Information Sharing on IntelDocs
  - IDA Sharepoint for Unclass/US citizen (TM JWG and Trust Models)
- **Outreach – Education, Training and Awareness**
  - Develop a long-term plan and near term FY18 goals
  - Build outreach materials for awareness of the FJAC and HwA
  - Coordinate T&AM efforts for outreach
- **Coordination**
  - Coordinate government wide HwA and T&AM activities
  - A single POC for common announcements, questions and interfaces with government, industry and academia
  - Active coordination and collaboration of T&AM related Conferences and Meetings
    - GOMACTech, HOST, MIM, FICS, etc.

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

FPGA/SOC Lifecycle Map



Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

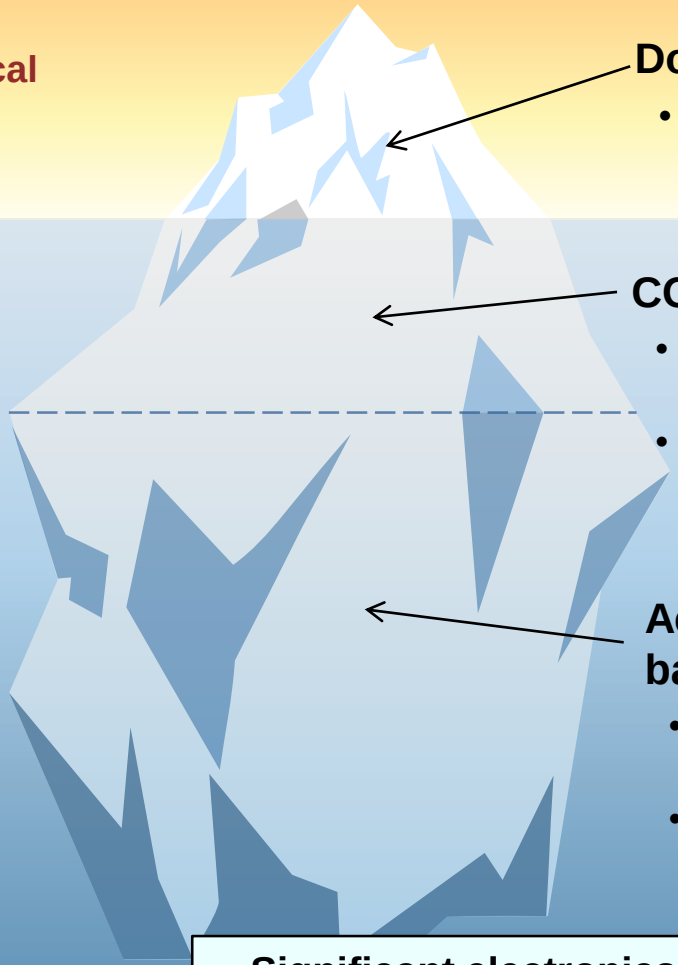
Pursuing Multiple Focus Areas Across the FPGA Lifecycle

	FPGA/SoC Hardware Development	FPGA/ Firmware Development	FPGA/SoC Provisioning	Operation & Maintenance
Policy	Adopt policy to promote best practices across acquisition programs			
Independent Verification And Validation	Expand IV&V capability and capacity for Physical, Functional and Design Verification To be offered to the			
New Technology	Development of new techniques to verify and validate protect IP Confidentiality, deliver advanced supply chain tracking technology and			
Supply Chain Threat	Enhanced interaction with the Intelligence Community to provide more specific threat information to better enable risk analysis and Risk Analysis			
Industry Engagement	Manufacturers' relations are critical: • IV&V requires timely and detailed design related information, • Design tool distribution and usage • Design verification features in the design or enabled by the design tools			
Leverage Related Efforts	Coordinate with Major Efforts across DOD and IC Communities: • Title III Trusted FPGA • Trust in FPGA Study • Aerospace TOR Guidance			

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Electronics as a Strategic Issue

Current Tactical Issue



DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-16 Trusted Foundry Program

COTS Electronics Trust (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 17: Trusted & Assured Micro-electronics

Larger Strategic Issue

Access to Electronics / Electronics based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

POM 19-23: Micro-electronics Innovation for National Security

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

NDAA Strategy Request

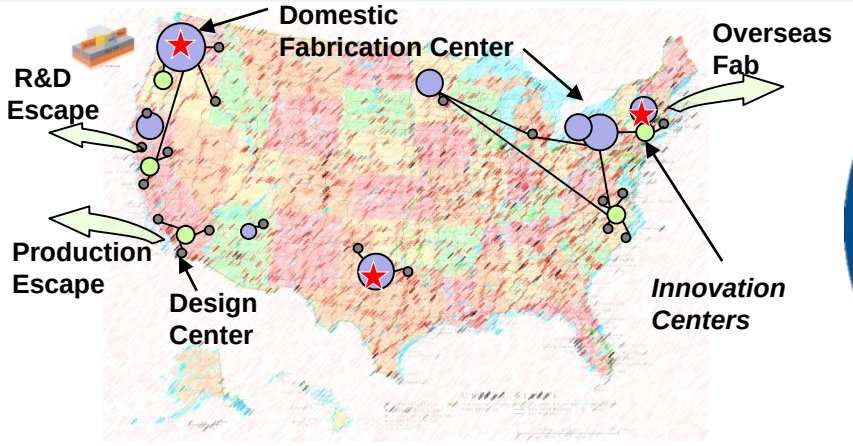
1. Define the various levels of trust required by DoD systems
2. Identify means of classifying DoD systems based on the required level of trust for microelectronics within the system
3. Identify means by which trust in microelectronics can be assured
4. Identify a means to increase the supplier base for assured microelectronics to ensure multiple supply pathways
5. Provide an assessment of the microelectronics needs of the DoD in future years, including the need for trusted, radiation-hardened microelectronics
6. Provide an assessment of the microelectronics needs of the DoD that may not be fulfilled by entities outside the DoD
7. Identify the resources required to assure access to trusted microelectronics, including infrastructure workforce, and investments in science and technology
8. Develop a research and development strategy to ensure that the DoD can, to the maximum extent practicable, use state of the art commercial microelectronics capabilities or their equivalent, while satisfying the needs for trust
9. Develop recommendations for changes in authorities, regulations, and practices, including acquisition policies, financial management, public-private partnership policies, or in any other relevant areas, that would support the achievement of goals of the strategy

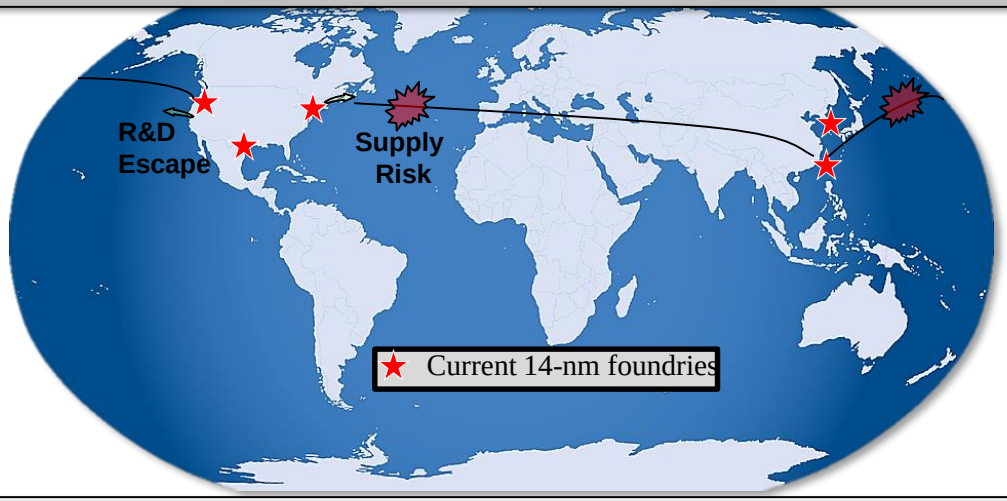
Source: National Defense Authorization Act for Fiscal Year 2017, Section 231

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

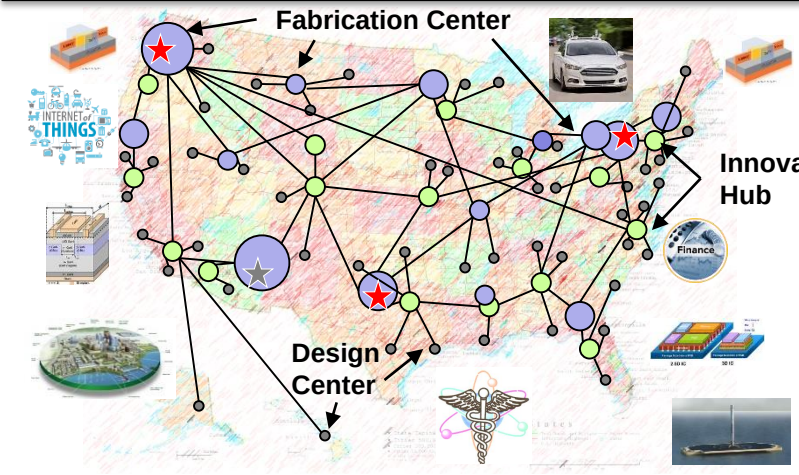
Leverage and Dominate Microelectronics for US Interests

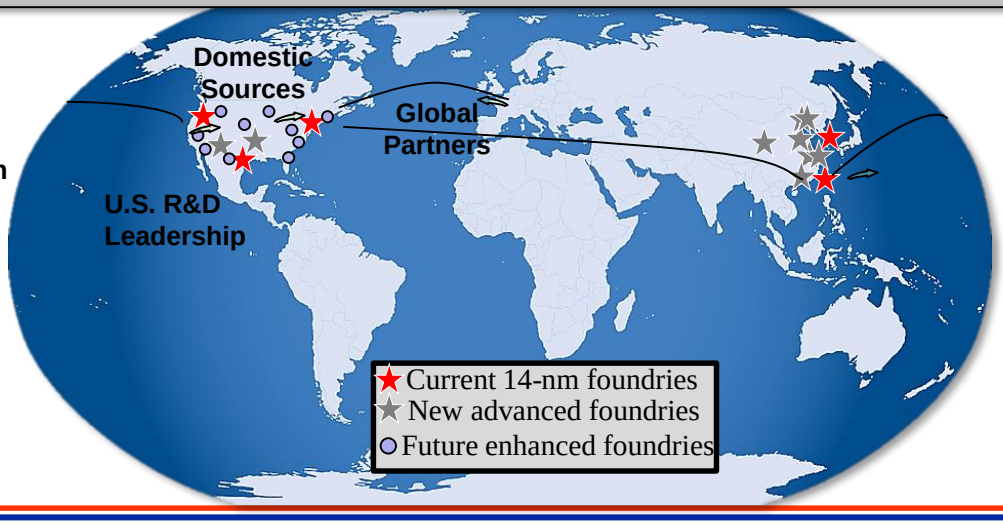
Current Global Microelectronics Leadership





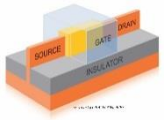
Possible Future Global Microelectronics Leadership



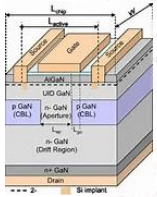


Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Create Microelectronics Innovation Throughout the United States





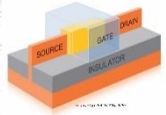




Fabrication Center

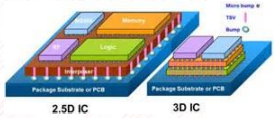


Innovation Hub





Design Center







Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Rebuilding US Microelectronics Leadership and Dominance

Strategic National Security Applications







Secure IoT



Financial & Data Analytics


Autonomous Systems + AI


Robust + Agile Communicators

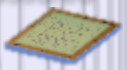

Commercial Space


Biomedical

Strategic National Economic Competitiveness Applications

Proactive Awareness & Security
- Supply Chain track
- Proactive Authorities
- Intelligence & CI

Access & Assurance
- Secure Design
- IP, EDA, experts
- Foundry assured Access
- Prototype Demonstrations



Enabling Manufacturing
- SoP Back-end parity with SotA
- SotA on 200mm tools at SoP
- Mini fabrication for high-mix low vol.

Incentives & Market Growth
- Acquisition reform & incentives
- Tax, policy, regulation reform
- R&D and domestic fab incentives

Strategic Alliances
- Cooperative R&D
- Trade & FMS
- Americas
- Europe
- Asia partners

Disruptive Research & Development

Materials, devices, circuits | Architectures | Design tools for Complexity

Experts, Infrastructure, Venture Capital | Science & Technology, R&D

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Microelectronics Strategy Challenges & Investments

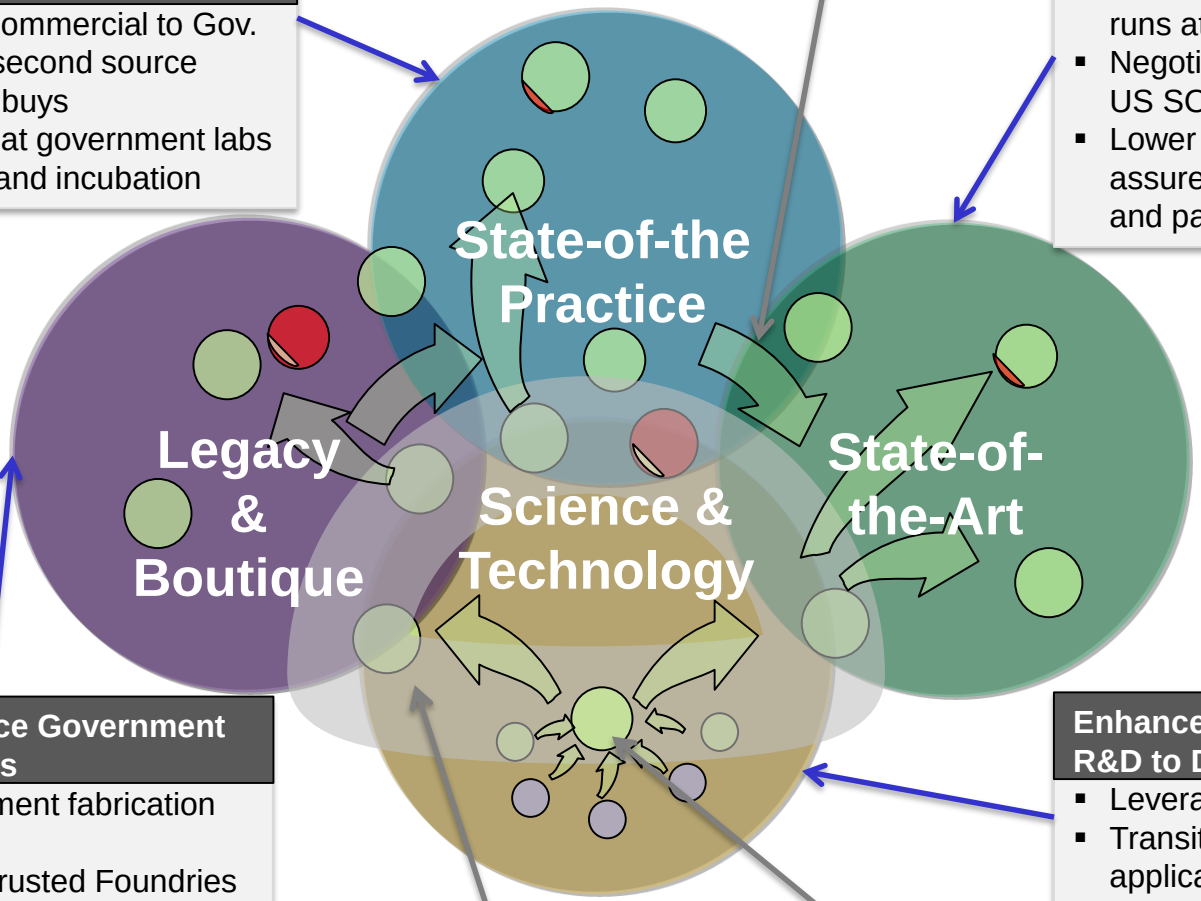
Preserving US Government Involvement in SoP

- IP transfer from commercial to Gov. and commercial second source
- Execute Lifetime buys
- Dual use-access at government labs for R&D capture and incubation

Enabling Manufacturing

Access to Assured SOTA in US

- Contract for access and shuttle runs at SOTA foundries
- Negotiate dedicated line(s) in a US SOTA foundry
- Lower barriers to innovation assured design, IP, fabrication and packaging



- **Commercial Access**
- **Commercial & Assured Gov. Line**
- **Government dual use**
- **R&D facilities**

Preserve & Enhance Government Unique Capabilities

- Enhance government fabrication capabilities
- Cooperate with Trusted Foundries for strategic radiation-hard
- Invest in development of disruptive fabrication tools for low-volume

Enhance and Bridge Disruptive R&D to Domestic Production

- Leverage and focus R&D
- Transition R&D capabilities to applications & production
- Invest in advanced materials, device, circuits, and complex systems design tools

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Demonstrating Innovation for National Security and Interests



Innovators & Developers

Small Business, Individuals, defense and commercial R&D, FFRDCs, University researchers, etc.

Private | Gov.

Competitive Selection

Contest

Autonomy, IoT, Space, Bio, etc.

Judges

Gov. & Private Investors

Prototype Co-Development

A | **6.3-4**

Design Team, IP, Business Model, Demo Plan

$$ + services

Production & Adoption

B

Innovative Demo + Business Model + Customers

$$$

C

Market Tested Part + Business Model + Market

$$$$

Acquisitions

Risk Reduction + Side-car demo

$$$$

Maintenance

Refresh & Upgrade Ideas

$$$



Adopters & Improvers

Contractors, Acquisition, private users, operators, and consumers

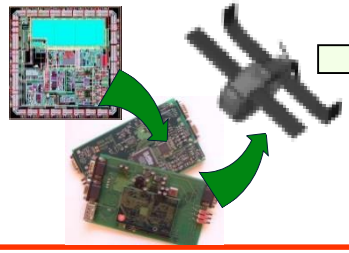
Private | Gov.

Communities, Infrastructure, & Investments

Designers, Innovators, VC, R&D, Gov. & Private	Secure EDA, 3rd & Gov. IP, V&V, Software, Simulators	Foundry Access, Packaging, Testing, etc.	Sponsors, Venture Capitol, Acquisition











Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Disrupting Innovation for National Security and Interests

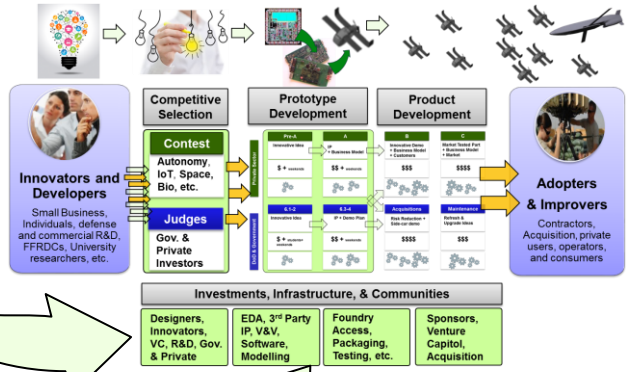
Enabling Ubiquitous Low-cost Manufacturing

90nm to 65nm & Copper
- Bring Gov. & merchant SoP to 65nm feature size with wet 193 litho
- Copper back end parity with SotA

SotA at SoP & Ebeam litho
- Multi-beam e-beam direct write litho for low-volume
- 200mm tools for SotA at SoP foundries

SotA Mini Fabs
- Plethora of miniature fabs for high-mix low-volume production
- Market for fab recipes & low-cost mini-fabs

Prototype Demonstrations



Disruptive Research and Development



Science & Technology R&D

Defense and commercial R&D, FFRDCs, University researchers, etc.

Materials & Devices
- Novel materials systems for next generation logic, memory, and interconnects
- Integrate novel devices with advanced SOTA microelectronics
- Demonstrate new circuits applications

Architectures
- Combine memory and processing on a single part
- Stackable, 3-D logic and memory
- Combine non-silicon and silicon components
- Calculations with new type of logic devices

Complex Design
- Robust Software Development tools
- EDA tools to design complex systems with small agile teams



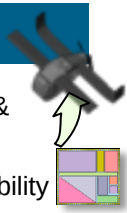
Innovators and Prototype Developers

Small Business, Individuals, defense and commercial R&D, FFRDCs, University researchers, etc.

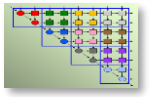
Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Microelectronics Innovation for National Security

	Problem	Actions & Investments	Outcomes
Access & Assure Ecosystem	• **Few domestic SotA foundries** & packaging, dominated by commercial forces, **$$ to access**, growth in Asia • **Development complexity, costs**, and lack of expertise and security are stifling innovation in SoC ASIC hardware • DoD influence is limited & national **security needs not being met**	• Provide **Assured access** to SotA, SoP, and Gov. foundries & packaging • Provide **Assured development community** (IP, EDA, experts, secure computing, Gov. IP) for innovation • Support **Innovative co-development of 10-1000x capabilities** for USG and strategic growth application areas	• Strong **domestic assured source** for Gov. & private innovative microelectronics products • Significantly **reduced barriers** to rapid capability development with assurance for Gov. and cooperative emerging industries • Immediate **demonstration of 10-1000x** perf. for USG & industry in autonomous systems, IoT, financial, commercial space, etc.
Enabling Domestic Manufacturing	• Many domestic SoP foundries are at 200mm and >65nm nodes and **aren't being updated** • Advanced-node flexible, scalable manufacturing is **not available in U.S.** • **Innovative R&D going to foreign sources** to scale and integrate new device and circuits architectures	• **Enhance SoP foundries** to 65nm & copper back end & E-Beam litho now • Co-develop **advanced fabrication** (5-65nm) tools for existing 200mm • Develop mini-fab to **transform and distribute SotA** disruptive technology development for high-mix low-volume production	• Immediate **performance improvement** and close parity to SotA processes for USG purposes • Create **manifold sources** for SotA in the installed US SoP foundries to remain competitive • **Rapid low-cost development** of materials, device, and process for low cost high-mix and low-volume production to **capture innovation & manufacturing** throughout the U.S.
Dominate & Disrupt R&D	• USG investment in disruptive R&D for next- generation microelectronics has **significantly diminished** • **Research is stagnant** when an inflection point in the electronics industry marked by changes in Moore's Law is about to occur • The country that exploits this inflection point will maintain or obtain **economic and security superiority**	• Leverage DARPA JUMP program and industry collaboration to **develop disruptive materials & electronics** • Lead the development of **new circuit architectures** for next-generation computing and strategic applications • Develop tools and technologies that allow **rapid redesign of complex systems**	• Develop the onshore manufacturing and design capacity to **own the next generation** of microelectronics technology • Maintain **U.S. leadership** in the semiconductor industry with healthy **U.S. R&D community** • Highly **productive designers** able to develop **complex systems with assurance**, at a rapid pace and **low cost** to keep ahead of our global competitors







Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

For Additional Information

Dr. Jeremy Muldavin

ODASD, Systems Engineering

571-372-6690

jeremy.b.muldavin.civ@mail.mil

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Backup

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Commercial Computing Trends



Mobile Computing



Internet of Things & SDR

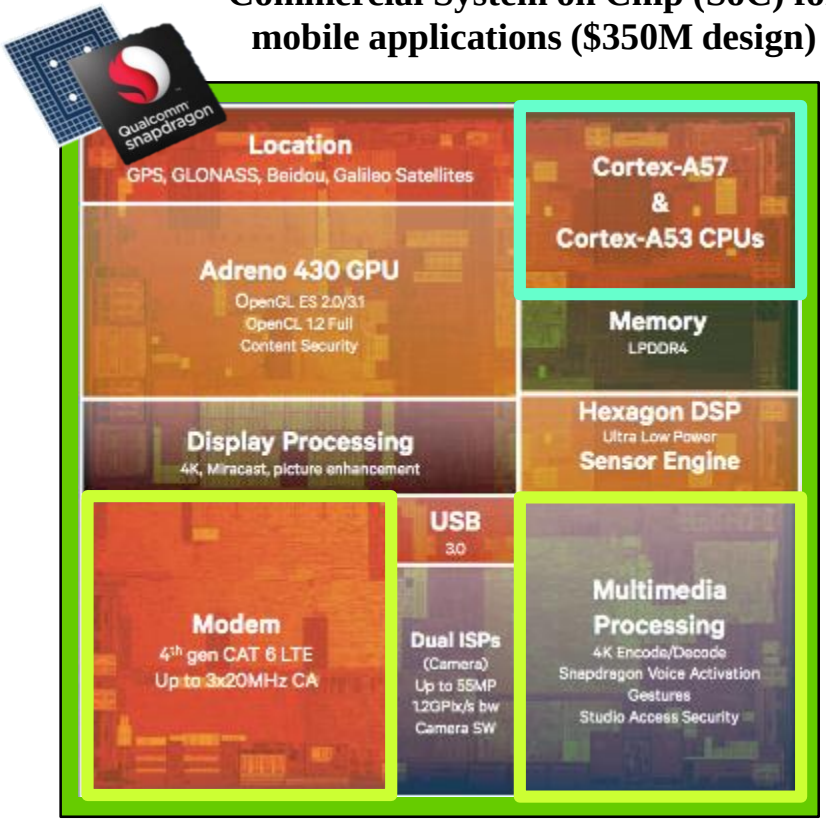


Powerful Test & Measurement



Cloud Computing & Infrastructure

Commercial System on Chip (SoC) for mobile applications ($350M design)



Global mobile computing & infrastructure brings powerful capabilities to EVERYONE

Accelerators enable 10-1000x capabilities in SoC and server architectures

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Long-Term Strategy Time Line

DoD Trusted Foundry Program Consolidation - Defense Microelectronics Activity (DMEA)

Transition

Newly Established Trusted Foundry Contract

Sustained Network of Trusted Certified Suppliers

Trusted and Assured Microelectronics Program:

Alternate Source for Trusted Photomasks

Preparation activities

Capability Development

Deploy new capability

Verification and Validation (V&V) Capabilities and Standards for Trust

Preparation activities

Improve capabilities and capacity, and provide support to program needs, for analysis of microelectronics trust

Identify and develop standards, practices, and partnerships to improve availability of trust from commercial providers

Advanced Technology and Alternative Techniques for Microelectronics Hardware Trust

Preparation activities

Capability development and demonstration

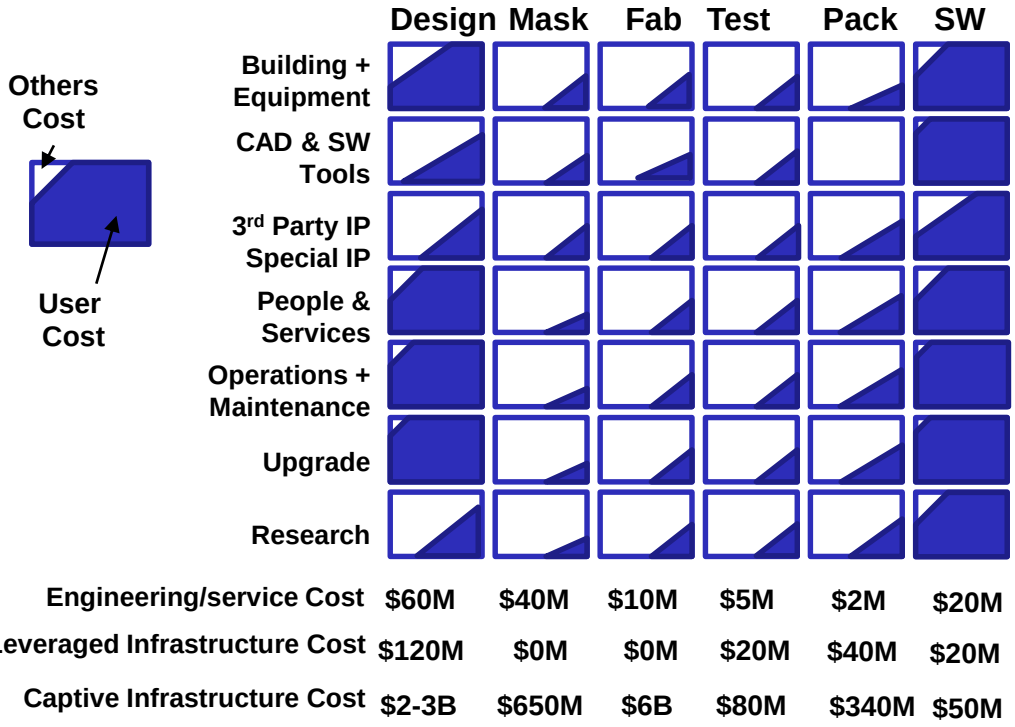
Deploy new capabilities

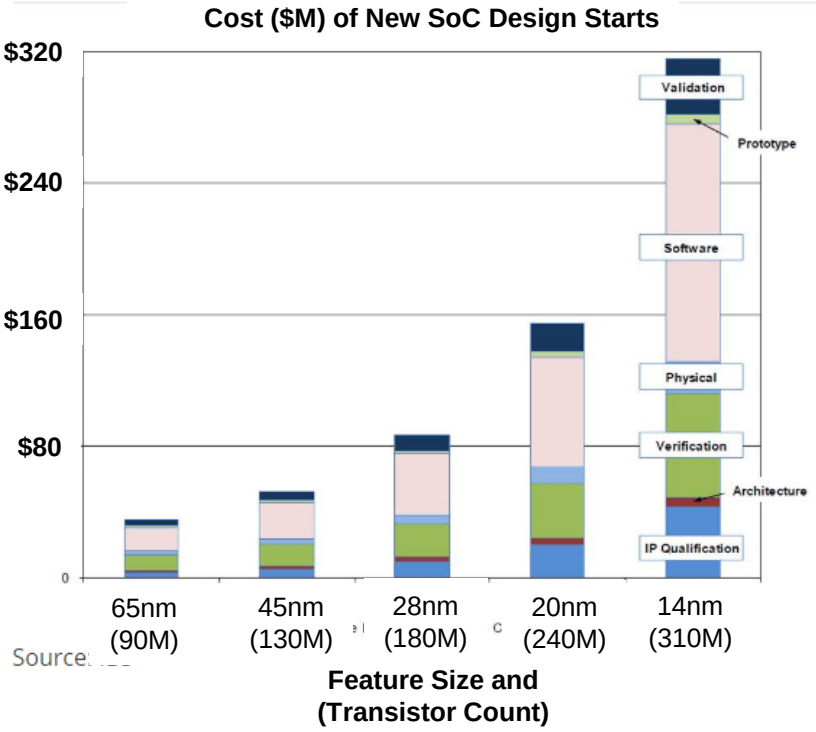
2015 2016 2017 2018 2019 2020 2021 2020 2023 2024

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Barriers to Innovation Using (28nm) System on Chip





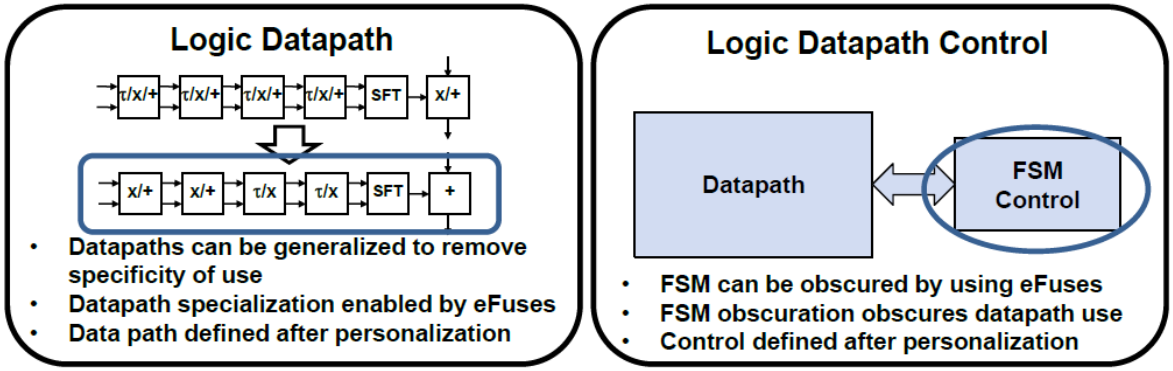


http://semiengineering.com/how-much-will-that-chip-cost/

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.

Mitigations to Cyber Exploits of HW Vulnerabilities

- **Address Space Layout Randomization (ASLR)**
  - Randomly assigns memory layout to increase complexity of attack on specific memory locations
  - Using this method at runtime increases level of security
- **Obfuscation**
  - Multiple variants of HW to obfuscate circuit functionality against attacks
  - Data-path generalization to remove specificity of use



Reference:<http://www.darpa.mil/attachments/NDIA2.3.pdf>

Reference:<http://www.cs.vu.nl/~herbertb/download/papers/anc_ndss17.pdf>

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0066 applies. Distribution is unlimited.



Field Programmable Gate Array (FPGA) Assurance

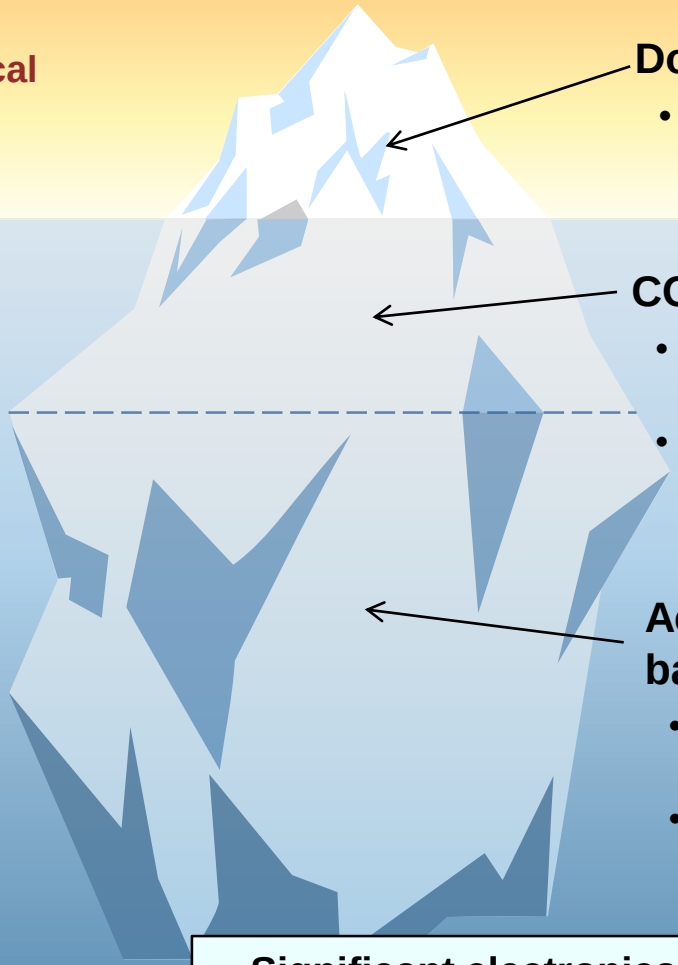
Raymond C. Shanahan
Deputy Director, Anti-Tamper/Hardware Assurance
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

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

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0073 applies. Distribution is unlimited.

Electronics as a Strategic Issue

Current Tactical Issue



DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-present: DoD Trusted Foundry Program

COTS Electronics Assurance (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 2017: Trusted & Assured Micro-electronics

Larger Strategic Issue

Access to Electronics / Electronics-based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore's Law potential carries economic impacts**

PB 2018/ POM 19: Microelectronics Innovation for National Security and Economic Competitiveness

Significant electronics challenges represent a strategic level national issue

† **Including the broader national security community, banking, critical infrastructure, commercial industry, etc.**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Need for Assured FPGA Functionality

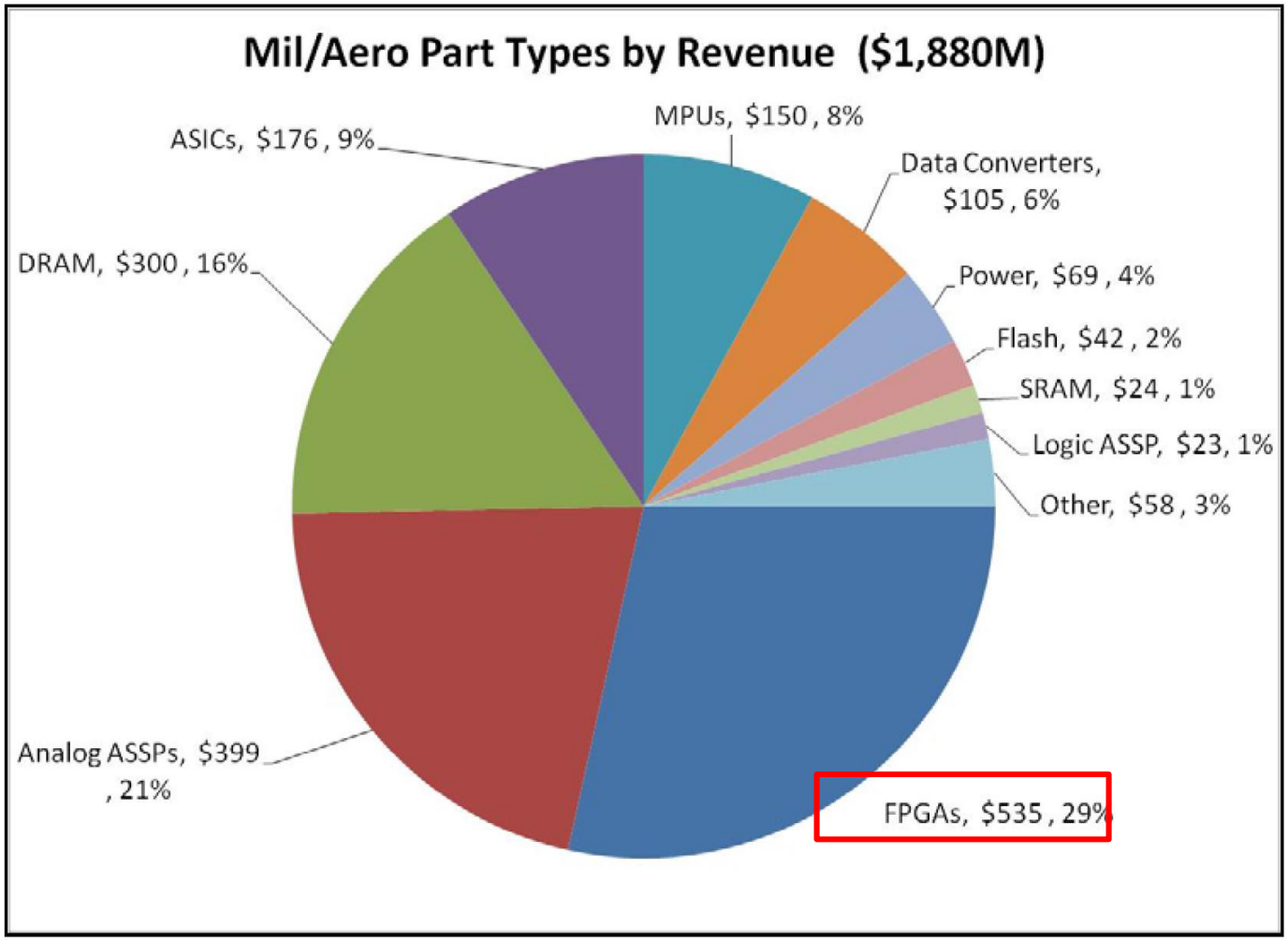
- **Commercial FPGAs are in widespread use across National Security Systems (NSSs) in embedded, special purpose applications**
  - Programmable nature of FPGAs and System on Chips (SOCs) make them vulnerable to cyber malware and malicious insertion
- **While Application-Specific Integrated Circuits (ASICs) have performance of ten to a thousand times that of FPGAs, FPGAs are seen as achieving custom hardware performance without the high manufacturing cost of custom ASICs**

FPGA applications:

- Communication systems
- UAVs
- Tactical robotics
- Radar systems
- Missile control
- Satellites
- Ships
- Vehicle control systems
- Other

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Usage by Revenue in Military/Aerospace Sector



Source: IDA report, Examination of DoD's Use of Microelectronics in Weapon Systems, 2013

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Policy Requirement for Trust vs. Assurance

- **There is no policy requirement in DoDI 5200.44 for a Trusted FPGA or other COTS product; only ASICs as follows:**
  - "In applicable systems, integrated-circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC))."
- **However, there are policy requirements for assurance in DoDI 5200.44, to include the following of particular relevance to FPGAs:**
  - "Mission critical functions and critical components within applicable systems shall be provided with assurance consistent with criticality of the system, and within their role within the system."
  - "Control the … security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use."
  - "Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions in accordance with DoDI 4140.67"
  - "Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing"

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Definitions of Trust and Hardware Assurance

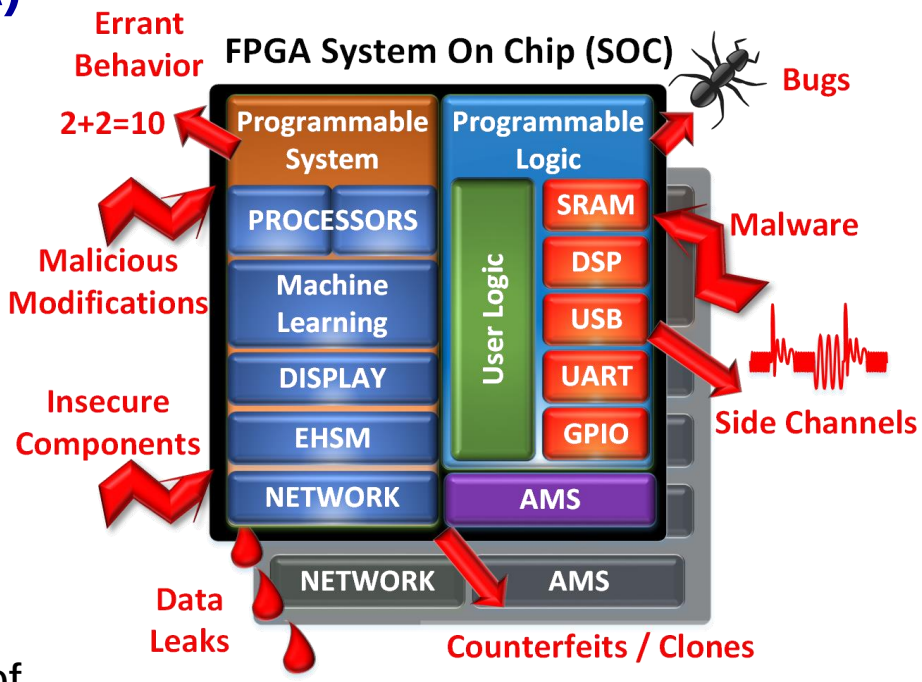
- **The NDAA FY2017 Sec. 231 trust definition below reflects DASD(SE)'s working definition of the term, "hardware assurance (HwA)"**
  - The other trust definition below is used by the DoD Trusted Foundry Program
- **Planned update of DoD Instruction (DoDI) 5200.44 needs to add, clarify, and harmonize the definition(s) of HwA and/or trust**
  - Needed to eliminate existing confusion in the community between what constitutes trust versus HwA; sometimes referred to as "big T" versus "little T" trust or assurance
  - These definitions do not compete with one another, but can be complementary if integrated and harmonized into an internally consistent definition or set of definitions within DoDI 5200.

2004 AT&L Memorandum	NDAA FY2017 Sec. 231
trust: "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components"	**trust:** "with respect to microelectronics, to the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its lifecycle"

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

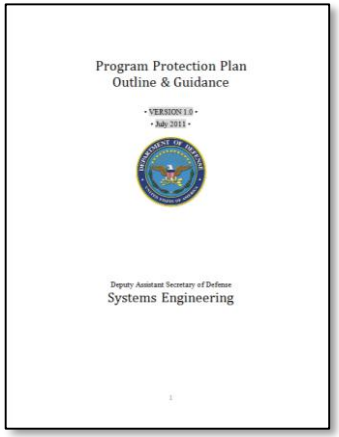
FPGA/SOC Assurance Risks

- **Commercial FPGA/SOC security, third party intellectual property (3PIP), and Electronic Design Automation (EDA) tools are largely unverified**
- **Industry unlikely to invest unless encouraged**
- **Some Military/Aerospace and specialty needs are not being met**
- **DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist**
  - Potential for compromise of IP confidentiality and/or integrity, or EDA tool integrity, from design through deployment
  - Inconsistencies and uncertainty/lack of clarity in methods, policy, and enforcement
  - Supply chain threat and vulnerability awareness is poor

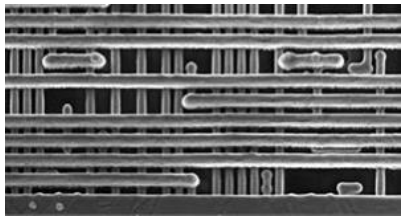


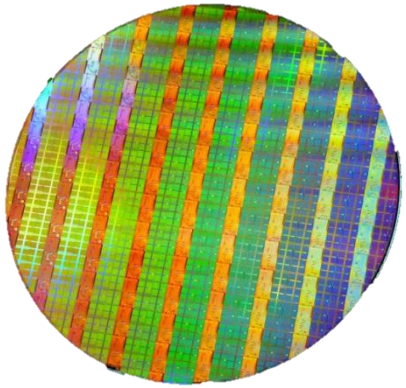
Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

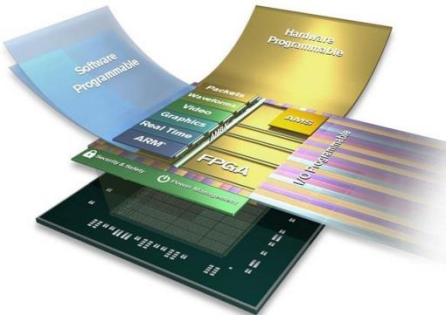
Advancing Hardware Assurance











Policy

- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)

Joint Federated Assurance Center

- Software assurance Know-how & tools
- Hardware assurance Know how & tools
- Advanced V & V capabilities
- Firmware Assurance planning

Trusted & Assured Microelectronics

- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance
- Implement & Demo

COTS and FGPA

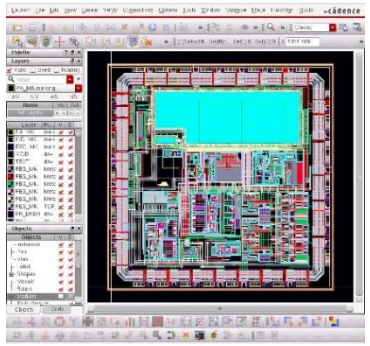
- Supply chain risk management
- FPGA Assurance Strategy
- Radiation hardened microelectronics initiative

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0073 applies. Distribution is unlimited.

Microelectronics Trust Verification Technologies

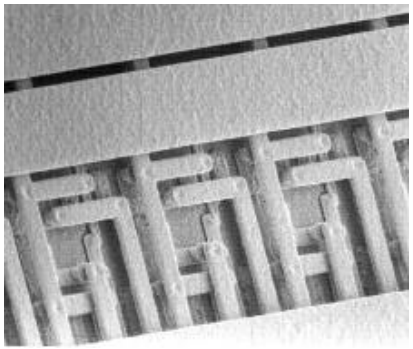
Design Verification

- Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.



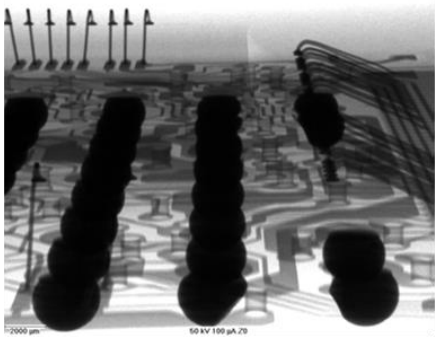
Physical Verification

- Destructive analysis of ICs and Printed Circuit Boards



Functional Verification

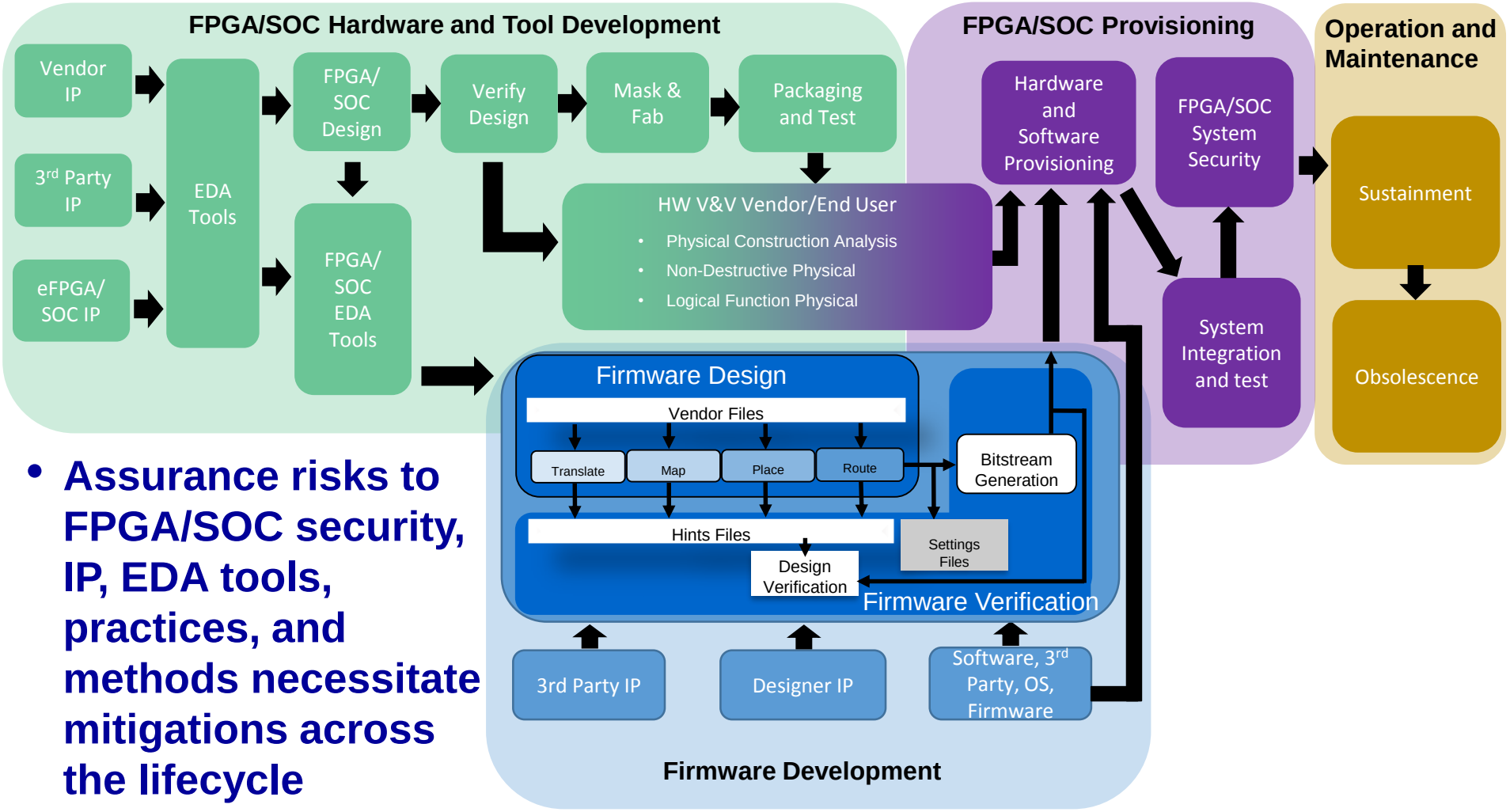
- Non-destructive screening and verification of select ICs



DoD, Intelligence Community, and DoE enhancing capability to meet future demand

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0073 applies. Distribution is unlimited.

FPGA/SOC Lifecycle Map

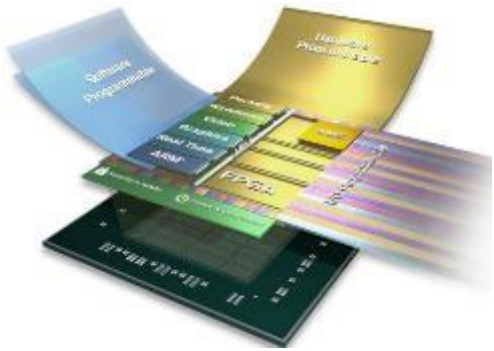


- **Assurance risks to FPGA/SOC security, IP, EDA tools, practices, and methods necessitate mitigations across the lifecycle**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Assurance Strategy Overview

- **DASD(SE) continues to refine the strategy to address FPGA assurance risks in coordination with the Joint Federated Assurance Center (JFAC) HwA Technical Working Group (TWG) and the Trusted and Assured Microelectronics (T&AM) program**
  - Leverage existing USG and industry efforts to the maximum extent possible
  - Promote community awareness of related USG efforts via a series of workshops and conference
  - As a community, continuing to identify and refine the portfolio of assurance efforts to focus on with the goal of synchronizing and eliminating stove-pipes and separate, single-point solutions when possible
  - Identify gaps and/or activities requiring investment and elevate relevant needs to the JFAC Steering Committee for prioritization and direction regarding resourcing
  - In particular, align with, and inform, the execution plan for the T&AM program



Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Assurance Strategy has multiple FPGA Assurance Focus Areas across the FPGA Lifecycle

		FPGA/SoC Hardware Development	FPGA/ Firmware Development	FPGA/SoC Provisioning	Operation & Maintenance
AVAILABILITY	**DoD Specific Needs**	Increase availability for DoD specific needs in Military/Aerospace, e.g., Strategic Radiation-Hardened (SRH) technologies, and other domestic manufacturing needs			
	Leverage Related Efforts	Coordinate with other major efforts across the DoD, Intelligence Community (IC), the broader United States Government (USG), industry, and academia. For example: • Defense Production Act (DPA) Title III Trusted FPGA • Trust in FPGA Studies • Aerospace Terms of Reference (TOR) related to assured FPGA and ASIC development			
ACCESS	**Supply Chain Threat**	Enhanced interaction with the IC to provide more specific threat information to enable enhanced threat assessment and vulnerability analysis			
	Industry Engagement	Engage FPGA manufacturers, EDA, 3PIP, and other vendors to facilitate: • USG IV&V access to timely/detailed supply chain information, e,g., design, chain of custody, etc. • Design tool and 3PIP distribution and enterprise usage • Verification features in the design or that are enabled by the design tools • Commercial verified and validated security features, EDA tools, 3PIP or other supply chain tools			
	Policy and Guidance (P&G) and Standards	Develop, contribute to, and/or adopt P&G and standards that promote best practices across DoD and other USG acquisition programs as well as industry to the extent possible • Facilitate use of commercially viable/supportable tools, IP, and best practices where possible			
ASSURANCE	**Independent Verification And Validation (IV&V)**	Expand JFAC IV&V capability and capacity for physical, functional and design V&V to be offered to clear contractors and USG acquisition programs, leverage co-development, data access, design for assurance, and other best practices to enable better V&V			
	New HwA Techniques and Tools	Develop and facilitate the transition of new HwA techniques and tools to verify and validate, protect the confidentiality and integrity of, and gain insight into the chain of custody of, IP, EDA tools, and the FPGAs/SOCs themselves			

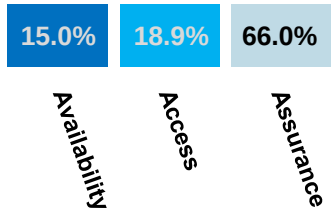
Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

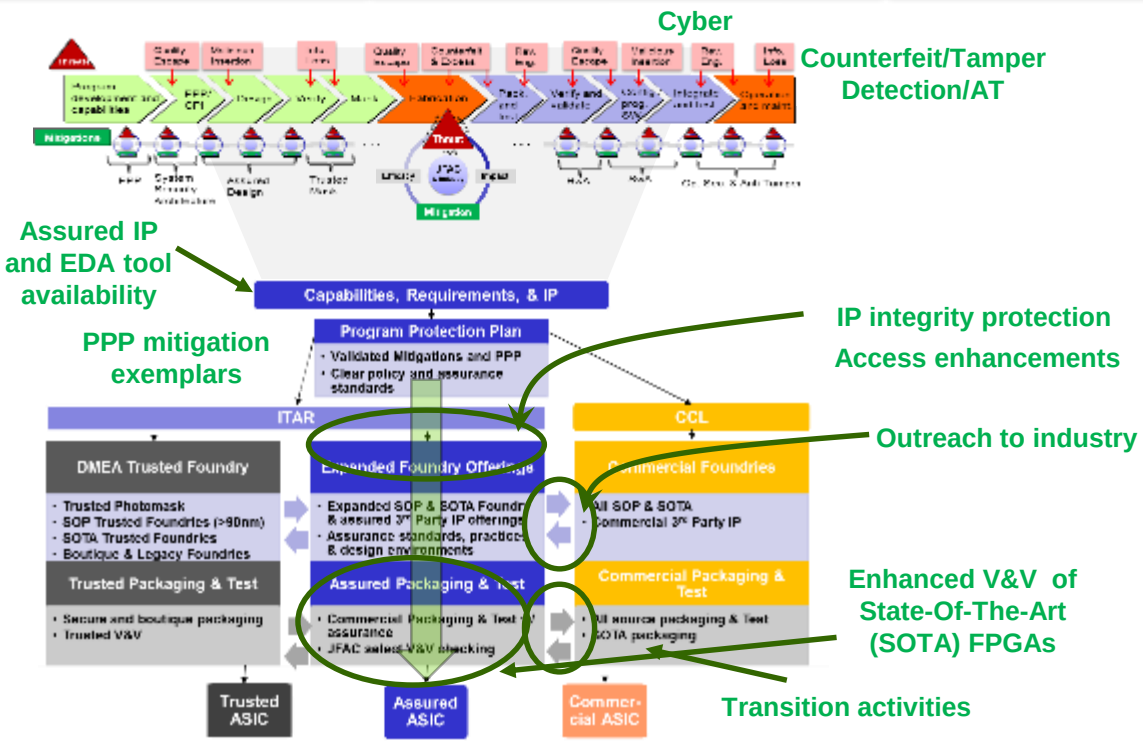
FPGA Activities and Investments

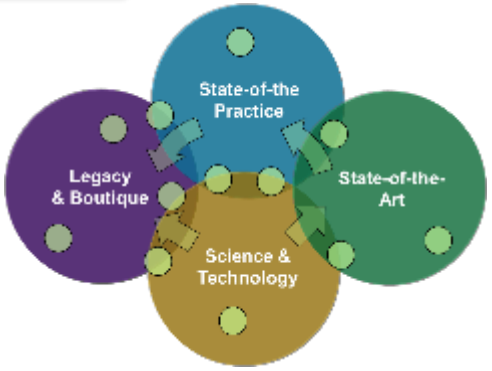
Overall

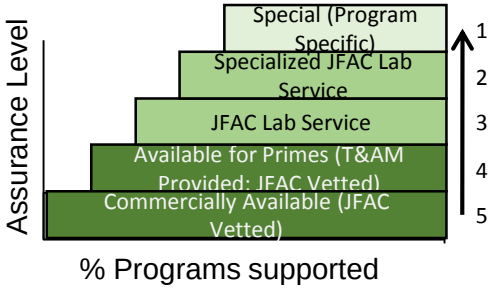
Inputs	Investments & Actions	Outcomes
• Established relationships and programs with FPGA and other vendors • JFAC labs, FFRDCs, expertise • Other USG partners and commercial suppliers • Programs and COTS parts	• EDA tool and 3PIP V&V development • Physical V&V tool and capability development • Security and assurance architecture development • Radiation testing and validation	• USG and third party EDA and 3PIP V&V tools • JFAC-assessed FPGA list, IV&V tools, vulnerability assessments • Counterfeit and SCRM tools • P&G, standards, and best practices, PPP • SRH assessments

Investment Breakout



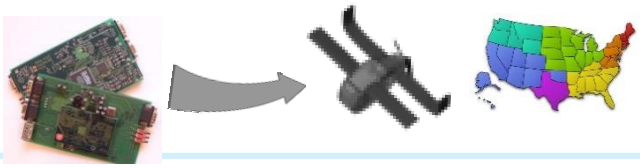
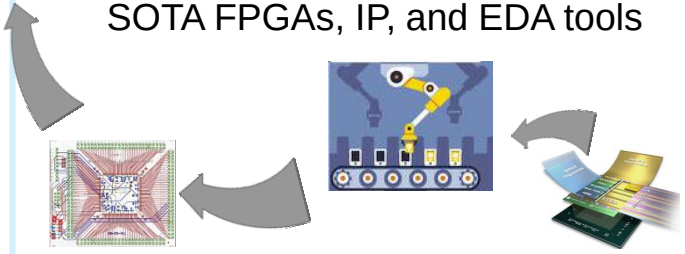
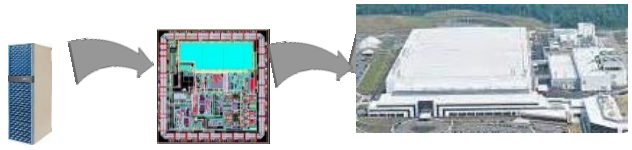






Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Strategy Outcomes

	Problem	Actions & Investments	Outcomes
Availability	• DoD influence is limited and national security needs not satisfactory for required production and volume	• Support domestic, manufacturing of SOTA FPGAs and industrial engagement for USG and strategic growth application areas, including radiation-hardening, high voltage, etc.	• Availability of assured SOTA FPGAs, tools, and IP for USG acquisition programs 
Access	• Potential for compromise to confidentiality and integrity through design access, COTS insertion, and deployment of commercial FPGA creates risk when USG accesses SOTA FPGA	• Evaluate and adopt best practices, and specialized tools and services to assure integrity and confidentiality of IP	• Enhanced USG access to assured SOTA FPGAs, IP, and EDA tools 
Assurance	• DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist	• Provide USG HwA community with access to, or knowledge of, assured USG IP, 3PIP, EDA tools, experts, secure computing, techniques, etc. for innovation 	• Assurance throughout the FPGA/ SOC lifecycle through secure design environments, best practices, V&V and supply chain tools, and specialized services 

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Leverage Related Efforts

- **Trust in FPGA Studies**
- **JFAC HwA TWG efforts**
- **Defense Production Act (DPA) Title III Trusted FPGA Projects**
  - In FY17, DPA Title III Phase 1 worked with FPGA vendors to develop product strategies to allow USG to assure FPGAs
  - In FY18, Phase 2, planned start of implementation of those product strategies
- **Defense Microelectronics Activity (DMEA) Trusted FPGA Study**
  - Congressional Add to engage major vendors
- **Anti-Tamper Executive Agent-related technology development**
- **Printed Circuit Board and Interconnect Technology Executive Agent technology development**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Leverage Related Efforts (cont'd)

- **NSA/R2-sponsored FPGA Trust & Integrity Research**
  - Aerospace documenting this research. Final product in FY17
- **Mission Assurance Improvement Workshop (MAIW) and Aerospace Terms of Reference (TOR)**
  - FPGA assurance-related TORs for design, Trust Assurance, and SME training in development
  - Other FPGA and ASIC related TORs already completed
- **National Defense Industrial Association FPGA Assurance Workshops**
- **Intelligence Advanced Research Projects Activity Trusted Integrated Circuit (TIC) Phase 3**
  - FPGA developed using split fabrication
- **Defense Advanced Research Projects Agency programs**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security and assurance in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers and develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
  - Co-development of next generation COTS with DoD capabilities and assurance considered
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics, to include FPGAs/SOCs, that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0073 applies. Distribution is unlimited.

For Additional Information

Raymond C. Shanahan

Deputy Director, Anti-Tamper/ Hardware Assurance

ODASD, Systems Engineering

571-372-6558

raymond.c.shanahan.civ@mail.mil

E-mail – osd.pentagon.ousd-atl.mbx.fpga-assurance@mail.mil

JFAC Portal -- https://jfac.army.mil

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0073 applies. Distribution is unlimited.

DoD Joint Federated Assurance Center (JFAC) 2017 Update

Thomas Hurt

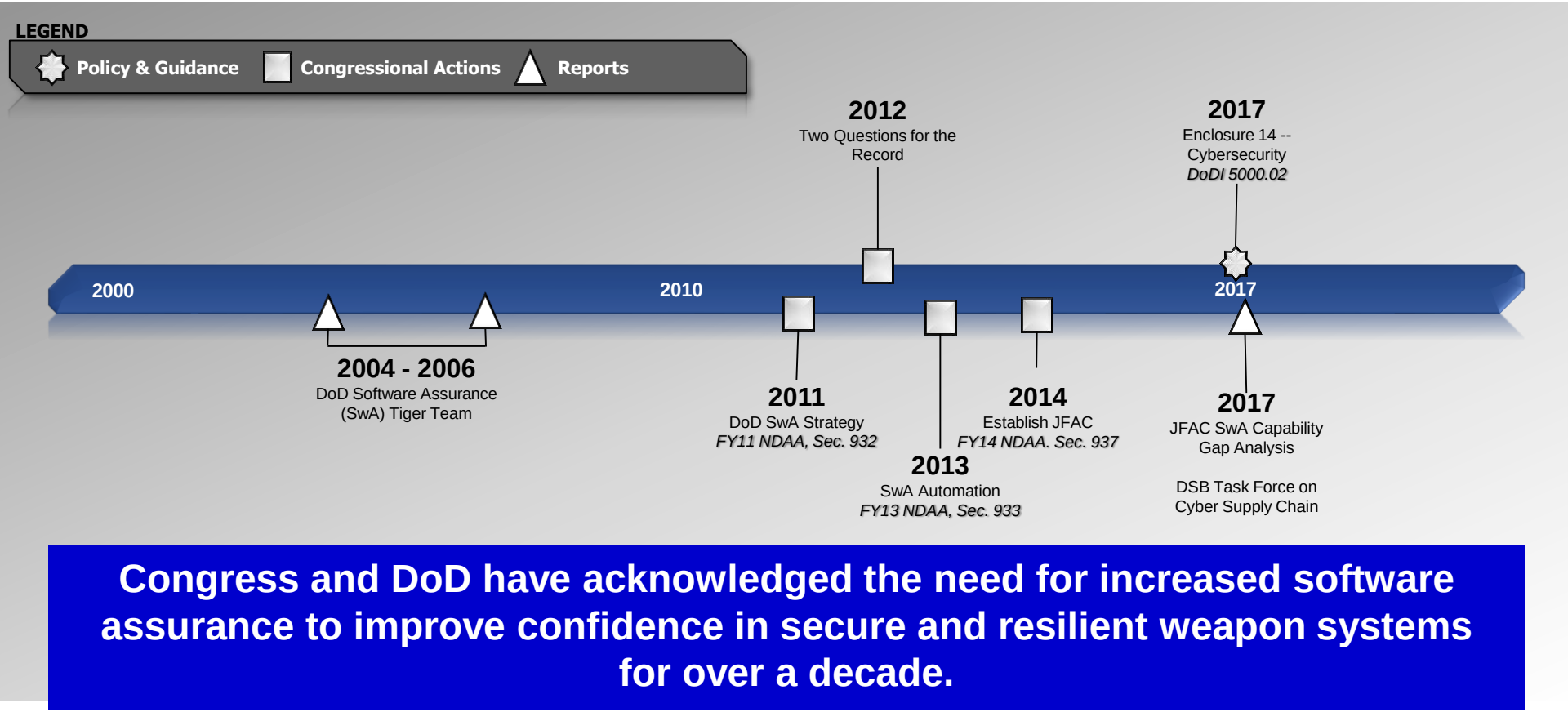
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 26, 2017

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

How Did We Get Here?



Congress and DoD have acknowledged the need for increased software assurance to improve confidence in secure and resilient weapon systems for over a decade.

JFAC: Joint Federated Assurance Center

Distribution A Statement. Approved for public release by DOPSR. Case # 17-S-2487. Distribution is unlimited.

Joint Federated Assurance Center (JFAC)

FY14 NDAA Section 937—Joint Federated Assurance Center (JFAC)

Key provisions:

- "provide for the establishment of a **joint federation of capabilities** to support the trusted defense system needs…to ensure security in the **software** and **hardware** developed, acquired, maintained, and used by the Department"
- "consider whether capabilities can be met by existing centers"
- **"[if gaps] shall devise a strategy [for] resources [to fill such gaps]"**
- "[NLT 180 days, SECDEF shall] issue a **charter**…"
- "submit to congressional defense committees…a **report** on funding and management"

Charter elements:

- Role of federation in supporting program offices
- SwA and HwA expertise and capabilities of the Federation, including policies, standards, requirements, best practices contracting, training and testing
- R&D program to improve code vulnerability analysis and testing tools
- Requirements to procure manage, and distribute enterprise licenses for analysis tools

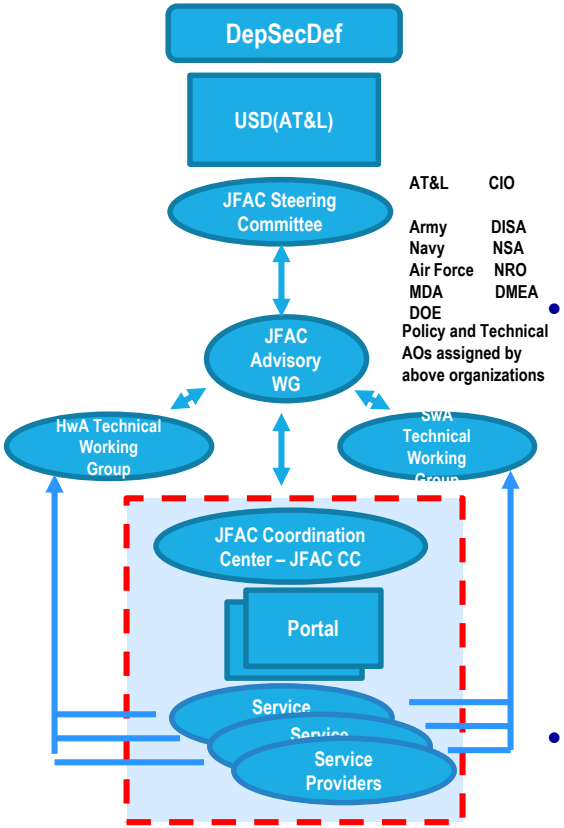
Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

What Has DoD Done?

- **Development of Concept of Operations (CONOPs) and Charter**
- **Establishment of JFAC Coordination Center (JFAC-CC), Steering Committees, Working Groups (WGs)**
- **Piloting Software Assurance (SwA) license distribution and management**
- **Conduct SwA and Hardware Assurance (HwA) Capability Gap Analysis**

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

JFAC Operational Structure



- **SwA and HwA Working Groups**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Recommend policy and guidance
  - Provide community forum for "hard problem" analysis and question/answer
- **JFAC Coordination Center**
  - Coordination of **Service Providers**
  - Supports programs with situational awareness, information/best practices, coordination
  - SwA analysis tool license distribution
  - **Portal:** https://jfac.army.mil
  - Assessment Knowledge Base (future)
- **JFAC Action Officer (AO) WG**
  - AOs for JFAC Steering Committee
  - Maintain enterprise and strategy cognizance
  - Reporting and ROI status

Distribution A Statement. Approved for public release by DOPSR. Case # 17-S-2487. Distribution is unlimited.

What's Going On Now?

- **JFAC Web portal and SwA tool license distribution**
- **Security Classification Guide**
- **Field Programmable Gate Array (FPGA) Strategy**
- **Resourcing**

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

What's Next?

- **Develop JFAC Full Operational Capability (FOC) strategy**
  - Improve DoD SwA throughout Lifecycle Planning, Execution and Sustainment
  - Invest in Technology and Resources
  - Upgraded Infrastructure for Federated DoD-wide Coordination of Software Assurance
  - Linking Sustainment to Early Program Development

- **JFAC website on SIPR, JWICS**
  - One-stop shop for SwA tools and best practices
  - New S&T and Assessment Knowledge Base portals
  - https://jfac.army.mil

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

Conclusion

- **The JFAC's goal is to provide DoD programs a one-stop shop to request, evaluate, and obtain resources to improve their software assurance practice.**
  - SwA analysis tool license distribution and management
  - Service providers for programs' SwA work; SMEs focused on hard problems
  - SwA best practices

- **JFAC is addressing key software assurance gaps.**
  - Developing FOC strategy to execute as resourcing becomes available
  - Publishing best practices at JFAC web portal (https://jfac.army.mil)

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

For Additional Information

Mr. Thomas Hurt

ODASD, Systems Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0071. Distribution is unlimited.

Achieving DoD Software Assurance (SwA)

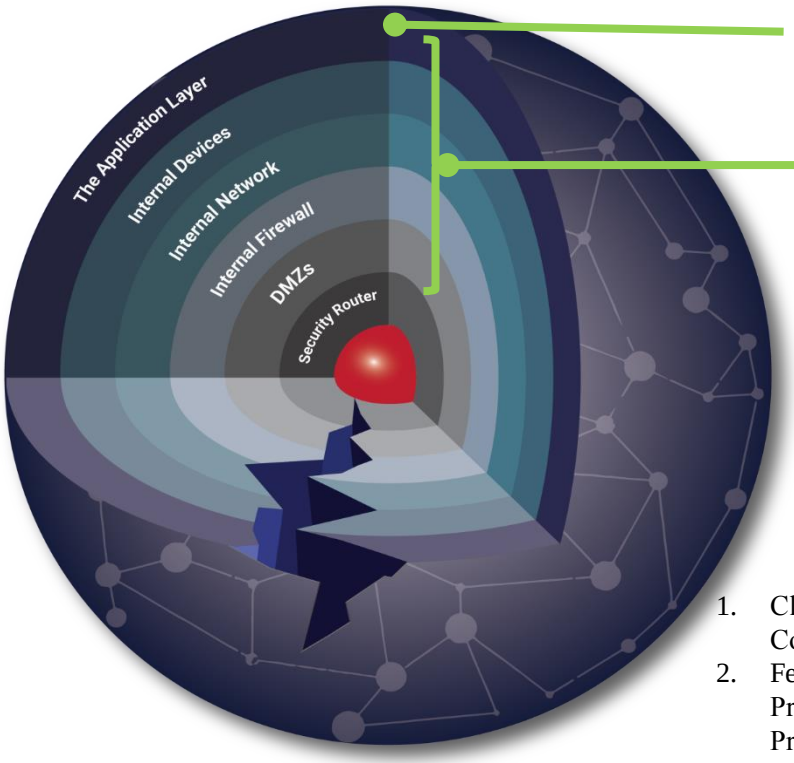
Thomas Hurt
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

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

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

First Line of Defense in Software Assurance Is the Application (Software) Layer

Software assurance (SwA) provides the required level of confidence that software functions as intended (and only as intended) and is free of (known) vulnerabilities, either intentionally or unintentionally designed or inserted in software, throughout the life cycle.



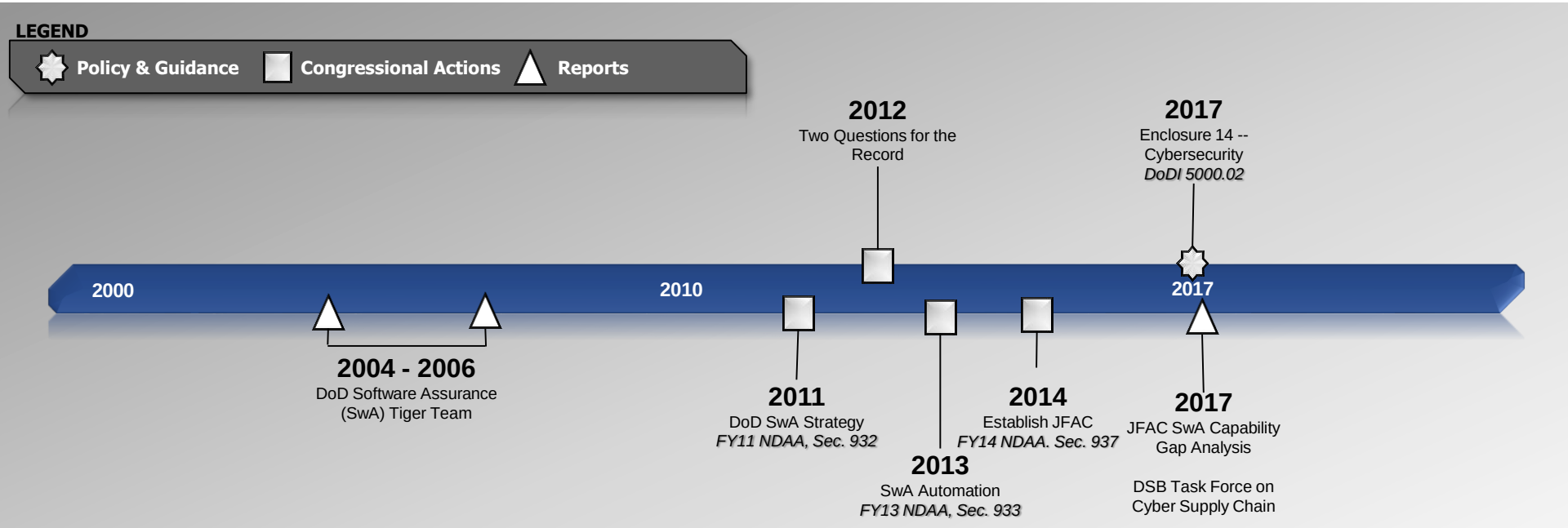
84% of breaches exploit vulnerabilities in the application[1]

Yet funding for IT defense vs. software assurance is 23 to 1[2]

1. Clark, Tim, "Most Cyber Attacks Occur from This Common Vulnerability," *Forbes*, 03-10-2015
2. Feiman, Joseph, "Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves," *Gartner*, 09-25-2014. G00269825

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

How Did We Get Here?



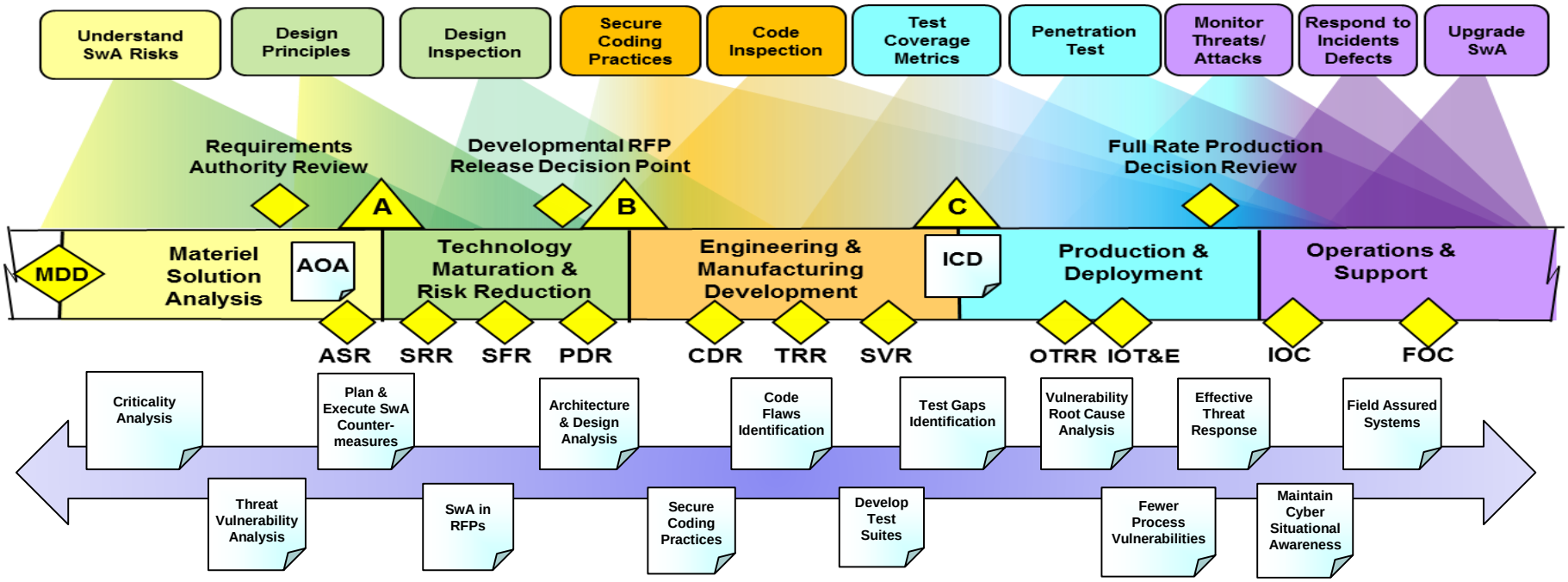
Congress and DoD have acknowledged the need for increased software assurance to improve confidence in secure and resilient weapon systems for over a decade.

JFAC: Joint Federated Assurance Center

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

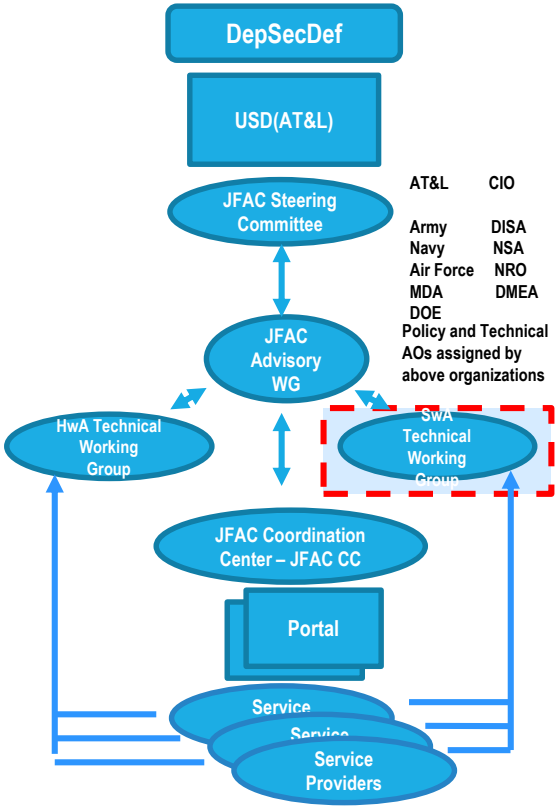
How to Engineer Software Assurance Across the DoD Acquisition Life Cycle

Software Assurance best practices, as a part of Systems Engineering, focus on increasing the level of confidence of software functioning as intended.



Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

SwA within DoD



- **JFAC SwA Working Group**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Recommend SwA policy and guidance
  - Provide community forum for "hard problem" analysis and question/answer
- **DoD SwA Community of Practice**
  - Tri-leads; meets quarterly with various DoD stakeholders' participation
  - Sponsors research and pilots into hard SwA problems

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

What's Going on Now? (1 of 3)

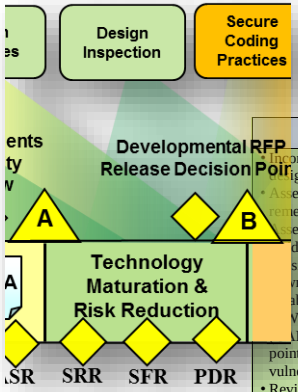
- **DoD Software Assurance Community of Practice**
  - Past products include: Contract language for integrating SwA; State-of-the-Art Resource (SOAR) for SW Vulnerability Detection, Test, and Evaluation; SwA metrics
  - Recent Topics and Ongoing Activities
    - SwA Risk Assessment process
    - Malware discovery in binary code
    - SwA analysis of mobile software
- **The Journal of Cyber Security and Information Systems: Design & Development Process for Assured Software–Vol 1***
  - Software Assurance in the Agile Software Development Lifecycle
  - Is Our Software REALLY Secure?
  - Development and Transition of the SEI Software Assurance Curriculum
  - Keys to Successful DoD Software Project Execution
  - Hacker 101 & Secure Coding: A Grassroots Movement toward Software Assurance



* https://www.csiac.org/journal-issue/design-and-development-process-for-assured-software-volume-1/

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

What's Going on Now? (2 of 3)



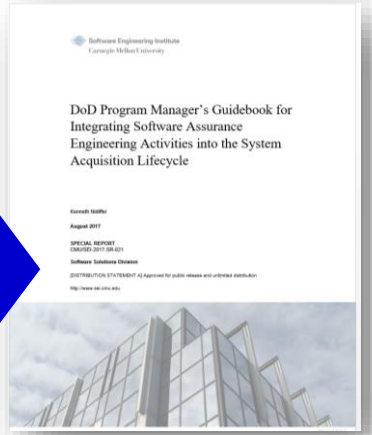
Acquisition Phase Considerations

SOFTWARE ASSURANCE CONSIDERATIONS (TMRR Phase)
• Incorporate SwA requirements, tool use, metrics, and assurance thresholds into solicitations. Architectures, designs, and code developed for prototyping are frequently reused later in development. • Assess system functional requirements and verification methods for inclusion of SwA tools remediation across the development life cycle. ssess requirements for SwA are correct and complete regarding assurance. Consider mea ders and adversaries using malicious inserts; system characteristics; interoperability wi sion threads; and other factors. Assure that mapping and traceability are maintained as wnstream assessments. ablish baseline architecture and review for weaknesses (e.g., use of Common Weakness VE)) and susceptibility to attack (e.g., use of Common Attack Pattern Enumeration and APEC)), and likelihood of attack success considering each detected weakness; identify points and mission impacts. Consider which families of automated SwA engineering tools vulnerability or weakness detection. • Review architecture and design for adherence to secure design principles and assess sound decisions considering likely means of attack; programming language choices; development frameworks; and use of open source software, etc. • Identify and mitigate technical risks through competitive prototyping while engineering in prototypes may be physical or math models and simulations that emulate expected perform concepts may require scaled models to reduce uncertainty too difficult to resolve purely by emulation. SW prototypes that reflect the results of key trade-off analyses should be demo TMRR phase. These demonstrations will provide SW performance data (e.g., latency, secu integration of legacy services, graceful function degradation and re-initiation, and scalabili decisions as to maturity; further, EMD estimates (schedule and life cycle cost) often depen components developed in TMRR; therefore to prevent technical debt, SwA considerations must have been taken into account. • Develop a comprehensive system-level architecture, then design (address function integrity, assurance of the functional breakout, function interoperation, and separation of function) that covers the full scope of the system in order to maintain capabilities across multiple releases and provide the fundamental basis to fight through cyberattack. The program focused on a given SW build/release/increment may only produce artifacts for that

Systems Engineering Technical Review Success Criteria

Objective	SwA Success Criteria
Preliminary Design Review (PDR)	
Recommendation that allocated baseline fully satisfies user requirements and developer ready to begin detailed design with acceptable risk. Allocated baseline is established such that the design provides sufficient confidence that the program demonstrates a high likelihood of accomplishing its intended mission, including in a cyber-contested environment. Preliminary design and basic system architecture support capability need and affordability target achievement.	• Determine that baseline fully satisfies user requirements, with assurance engineered in. • Determine that likely means of attack through software have been assessed and used in architecture and design implementation. • Review architecture and design against secure design principles; including system element isolation, least common mechanism, least privilege, fault isolation, input checking and validation. Consult JFAC planning tools, best practices in architecture and design, and guidance. • Determine if initial SwA Reviews and Inspections from prior SETR activities capture planning and requirements appropriately, including assurance. • Confirm that SwA requirements that were previously mapped from tactical use threads, mission threads, system requirements, and system interoperability requirements, are mapped to module test cases and to the final acceptance test cases. • Establish automated regression testing procedures and tools as a core process, and assure regression testing is conducted for remediated vulnerabilities, defects, and weaknesses.

PM's Guidebook for SwA Activities



To be published by SEI.

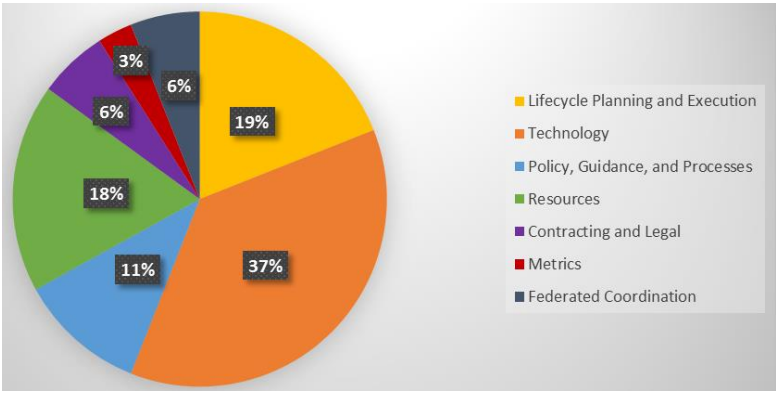
Upcoming Journal of Cyber Security and Information Systems article:
"Engineering SwA into Weapon Systems during the DoD Acquisition Life Cycle"

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

What's Going on Now? (3 of 3)

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:

Gap Examples:
2.2.2 - SwA requirements lacking in system requirements
5.2.1 - Lack of SwA training for Program Managers
6.1 - Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible



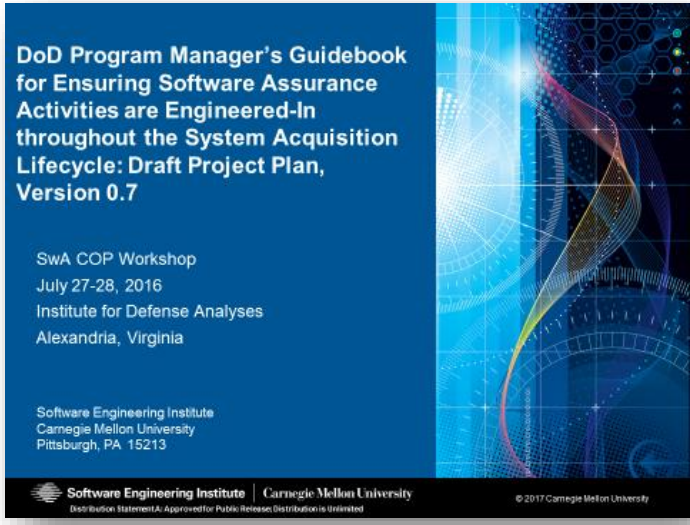
As chair of the JFAC Steering Committee, Ms. Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), approved the analysis* and directed the Technical Working Group to **develop a strategy to address the identified gaps**. DASD(SE)'s JFAC lead, Mr. Tom Hurt, supported the **NDIA-sponsored joint industry-government workshop**.

*Distribution C, available upon request.

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

What's Next?

- **DoD Program Manager's Guidebook for Integrating Software Assurance Engineering Activities into the System Acquisition Life Cycle**
  - To be written and published by SEI in collaboration with JFAC SwA Technical WG
  - Partner Document: Software Developers Guidebook
- **DASD(SE) Activities**
  - FY18 Business Case Analysis for SwA Tools
- **JFAC website on SIPR, JWICS**
  - One-stop shop for SwA tools and best practices
  - New S&T and Assessment Knowledge Base portals
  - https://jfac.army.mil
- **Develop JFAC Full Operational Capability (FOC) strategy**
  - Improve DoD SwA throughout Lifecycle Planning, Execution and Sustainment
  - Linking Sustainment to Early Program Development



Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

Conclusion

- **DoD has been focused on software assurance for over a dozen years.**
  - DASD(SE) leads the development and implementation of the supporting best practices, guidance, tools, and workforce competencies to ensure PMs have the means to mitigate SwA vulnerabilities and risk.

- **The JFAC's goal is to provide DoD programs a one-stop shop to request, evaluate, and obtain resources to improve their software assurance practice.**
  - SwA analysis tool license distribution and management
  - Service providers for programs' SwA work; SMEs focused on hard problems
  - SwA best practices

- **JFAC and DoD SwA COP is addressing key software assurance gaps.**
  - Developing FOC strategy to execute as resourcing becomes available

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

For Additional Information

Mr. Thomas Hurt

ODASD, Systems Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

Distribution A Statement. Approved for public release by DOPSR. Case # 18-S-0072. Distribution is unlimited.

Reducing Software Vulnerabilities
The "Vital Few" Product and Process Metrics

NDIA

20th Annual Systems Engineering Conference

Girish Seshagiri

19735

CMMIDEV /5 SM
Exp. 2017-03-07 / Appraisal #21757

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Topics

- Why We Are Here
- Ubiquitous Software Defects, “Patch and Pray”, What is at Stake
- Unique Point in Time
- State of the Practice – Software Development
- Managing Secure Software Development
- “Vital Few” Metrics
- Case Study

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Main Points

- **Defective software** is insecure
  - "If you have a quality problem, you have a security problem"
- Cannot **rely on testing alone** to find and remove software defects
  - Common misconception – "if it passes test, it must be OK"
  - Root cause of "Deliver now, Fix later" culture, technical debt, increase in total ownership cost in many agile projects
- Move from reactive to proactive – **threat detection to threat prevention**
- **Reducing vulnerabilities** - number one goal for every agile software team
  - Manage software by managing software quality
- Need **transformation** – organization, team, individual
  - Combine high maturity CMMI Maturity Level 5 with agile team process to create secure software by self-managed teams and empowered developers with certifications

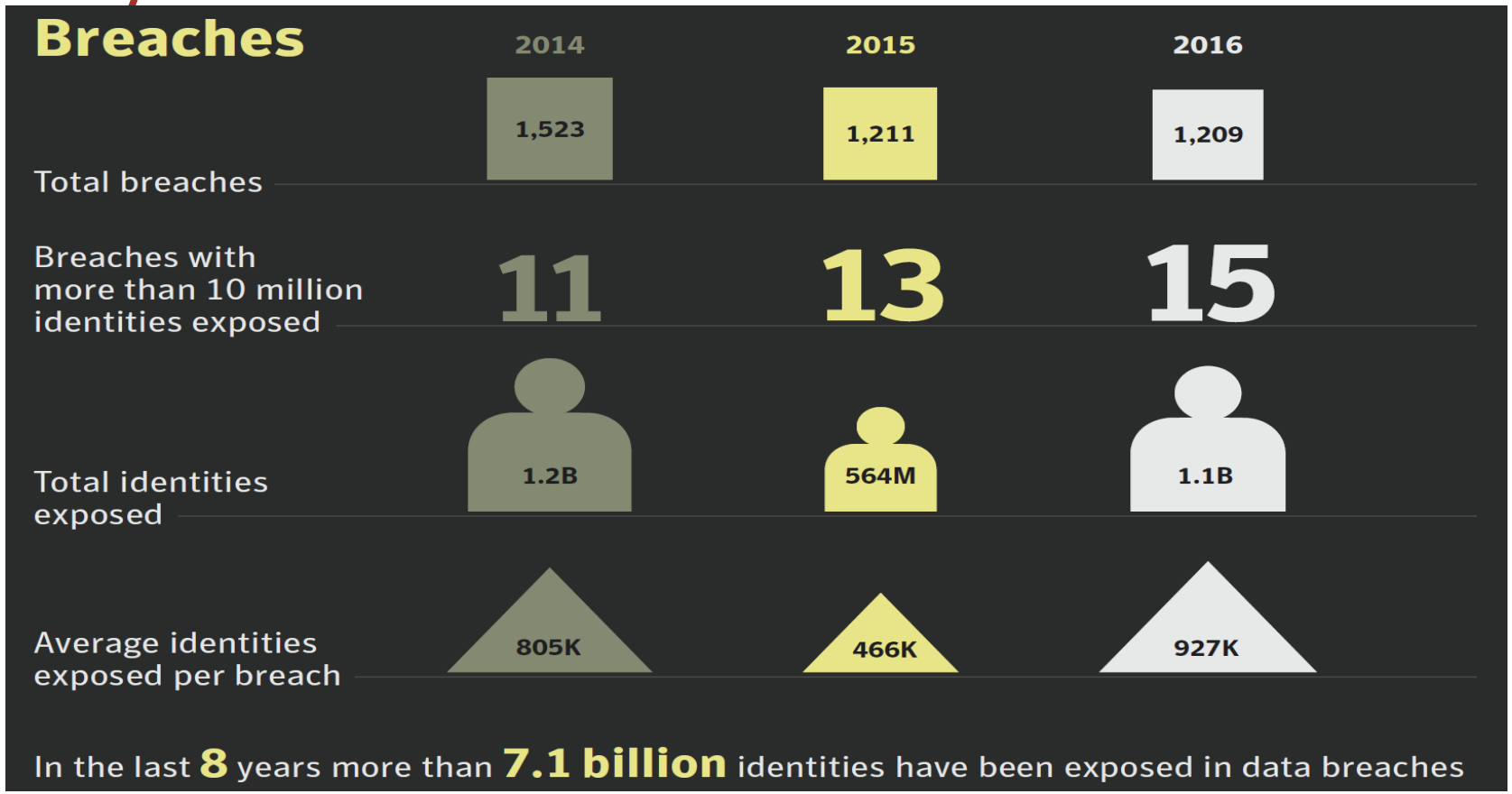
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Why We Are Here

- Increasing number of cyber attacks against critical infrastructure
- Current cybersecurity measures are reactive
- 90% of attacks are successful by exploiting defects in software
- Software developers not trained to deliver software with fewer vulnerabilities
- 1.5 million cybersecurity jobs currently unfilled

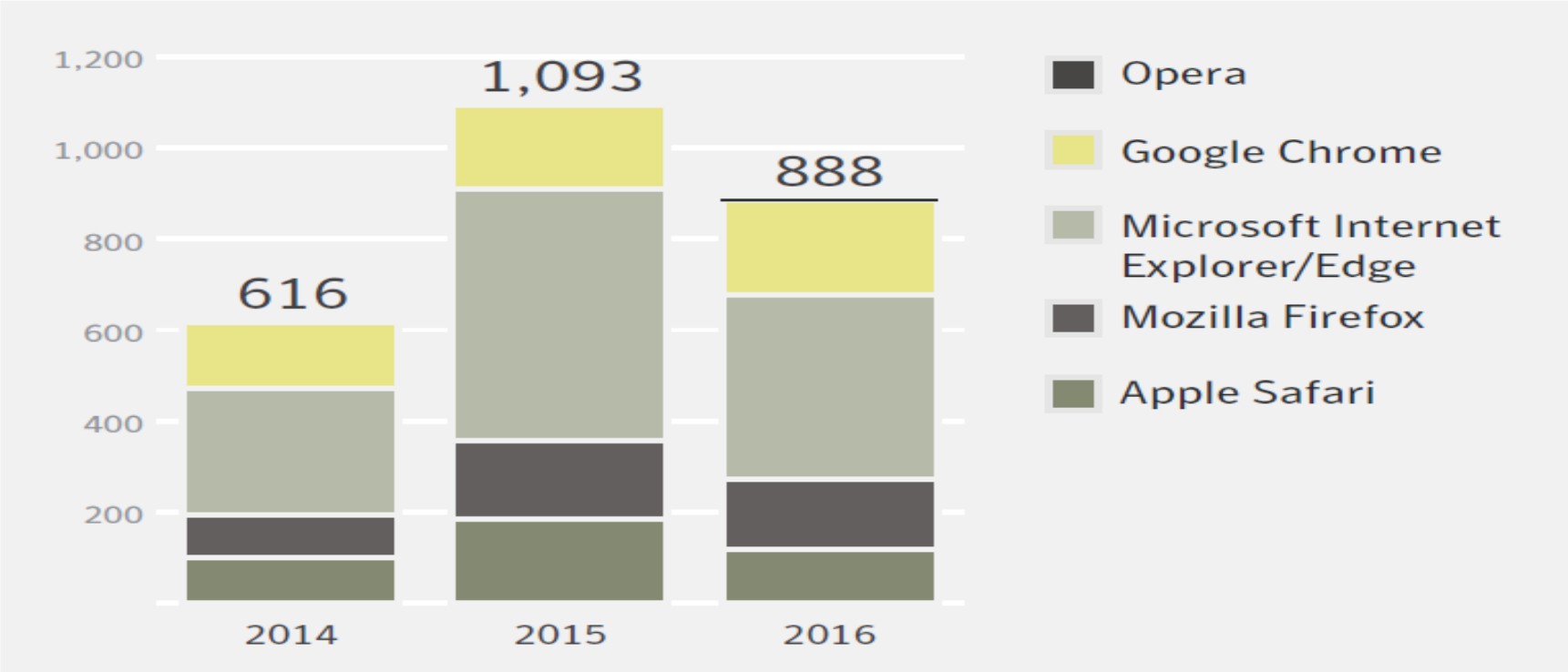
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Why We Are Here
Personal Identity Breaches



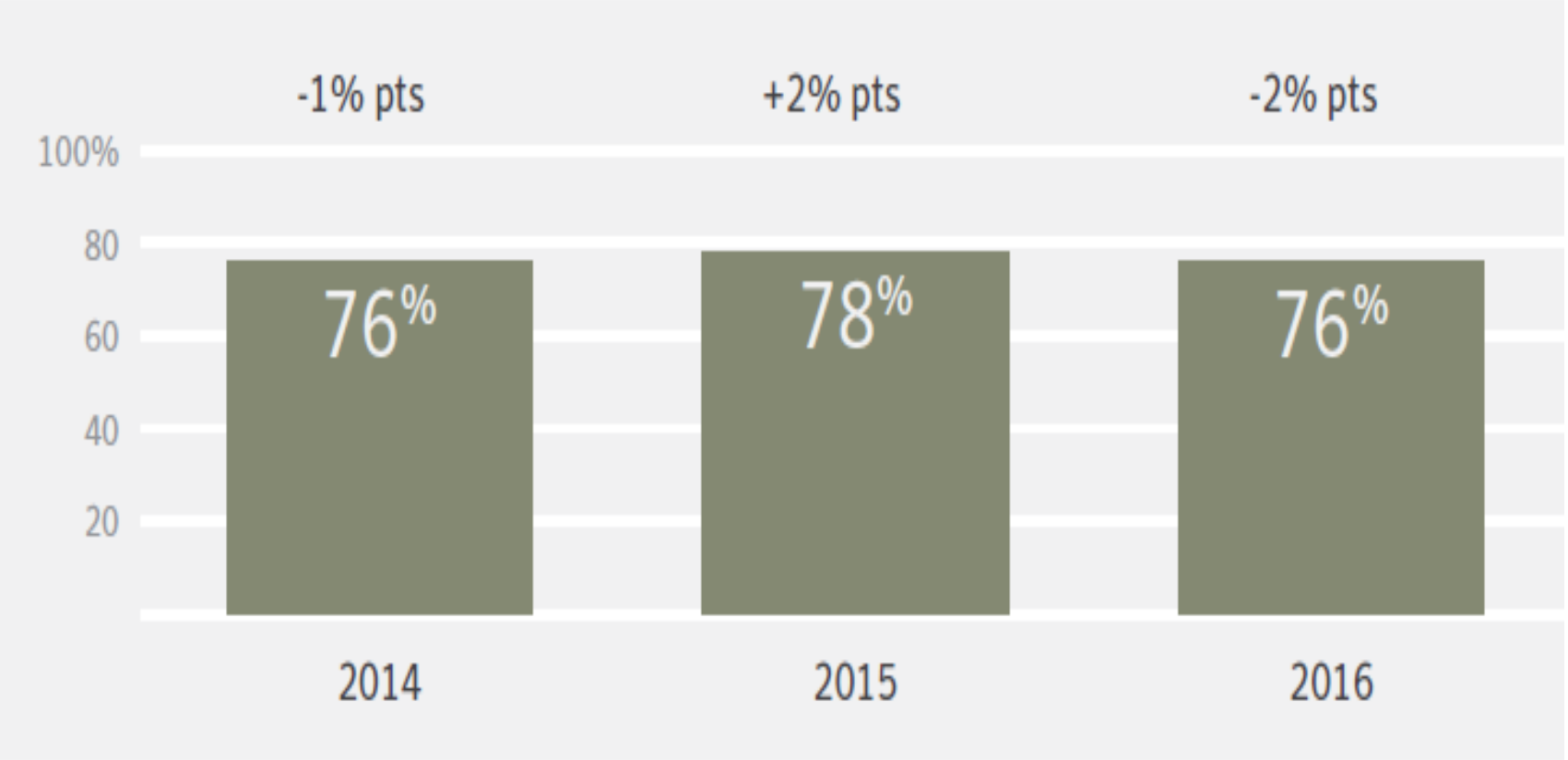
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Why We Are Here
Browser Vulnerabilities



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Why We Are Here
Websites with Vulnerabilities



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 1

Microsoft Patch Tuesday

On Tuesday, September 12, Microsoft released fixes for more than 80 security issues in multiple products, including Windows, Office, Microsoft .NET Framework, Flash, Internet Explorer, and Edge.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 2

Apache Struts Vulnerability Exploited in Equifax Breach

Equifax has acknowledged that the massive breach that exposed personal information of as many as 143 million people was due to a failure to apply a patch for a vulnerability in Apache Struts. A patch for the flaw was released on March 6, 2017. The Equifax breach occurred in "mid-May" 2017.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 3

Adobe Security Updates

Adobe has released updates to address security issues in Flash Player, ColdFusion, and RoboHelp for Windows. The Flash updates, available for Windows, Mac, Linux, and Chrome OS, address two critical memory corruption flaws. The ColdFusion update includes fixes for four flaws, and the RoboHelp update fixes two flaws

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Patch and Pray - 4

Patches dominate the Top of the News this week.

Bill Murray speaks for many when he writes: "The cost to tolerate or remediate a design, recording, or coding error goes up exponentially with the time to its discovery. **There is something fundamentally wrong with an industry in which the toleration, indeed the institutionalization, of late discovery and remediation of error is as it is in ours."**

And John Pescatore offers a path toward fixing that fundamental flaw in the software industry, describing a future where larger buyers of software (government, for example, along with the Business Roundtable) set a much higher bar for application security testing at multiple stages of the development life cycle, both for custom software they develop and for every package they buy, with **substantial contractual penalties for vendors who fail**.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake - 1

Some US States Are Going Back to Paper Ballots

In the wake of rising concerns about the security of electronic voting systems, several US states are returning to the use of paper ballots for their elections. Georgia will pilot a paper-ballot system in elections this fall.

FDA Approves Pacemaker Patch, Announces Recall of Abbott/St. Jude Medical Devices

The US Food and Drug Administration (FDA) has announced a recall of more than 450,000 pacemakers because they require a firmware update to address several security issues. The recall applies to several models of pacemakers manufactured by Abbott, formerly known as St. Jude Medical. Patients must visit their doctor's office where the update can be installed while the device is in backup mode. The flaws could be exploited to gain unauthorized access to vulnerable devices and issue commands to modify the pacemaker's settings and functionality.

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake - 2

Car Safety Vulnerability Lies in the Way CAN Handles Error Messages

A vulnerability in the Controller Area Network (CAN) that exists in most new automobiles could be exploited to shut down components of the car, including safety systems. Any component connected to the car's CAN bus could be affected. The issue is not one that can simply be patched because it lies in the CAN bus messaging protocol standard. Components that send too many error messages are disconnected from the CAN, so if attackers can spoof error messages to appear to be coming from a targeted component, that component could be shut off from the CAN.

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

What is at Stake -3

National Infrastructure Advisory Council Report - A Pre 9-11 Moment

"There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack, [for the nation] to organize effectively and take bold action," said the US National Infrastructure Advisory Council report. The report lists 11 recommendations, including "establish separate, secure communications networks specifically designated for the most critical cyber networks; ... identify best-in-class scanning tools and assessment practices; ... [and] establish clear protocols to rapidly declassify cyber threat information."

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Unique Point in Time – 1

- Software is the most important technology contributing to global high standards of living
- Cyber-attacks are increasing; 90% of attacks result from exploiting defects in software
- The cybersecurity spend estimated to grow to $170 billion by 2020
- 50 billion devices coming online during the next 5 years (IOT)
- Government is dependent on legacy code which is insecure

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Unique Point in Time – 2

- GAO has added the Management of Information Technology (IT) Acquisitions and Operations to high risk list
- Many agencies are convinced that agile/Scrum is the silver bullet solution
- Majority of the government's IT spend is for operations & maintenance; majority of the maintenance spend is for corrective maintenance
- There is no evidence that software project management capability has improved during the past 50 years

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Software Engineering's Persistent Problems – 1

- Exponential rise in cybersecurity vulnerabilities due to defective software
- Unacceptable cost, schedule, and quality performance of Enterprise Resource Planning (ERP) and legacy systems modernization projects
- The number one cost driver in software projects – cost of finding and fixing bugs (i.e. scrap and rework)
- Arbitrary and unrealistic schedules leading to a culture of "deliver now, fix later"

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Software Engineering's Persistent Problems – 2

- Inability to scale software engineering methods even for medium size systems
- Lack of understanding of the impact of variation in individual productivity
- Absence of work place democracy and joy in work

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Managing for Secure Software Development – 1

- Staff the projects with team members who are formally trained in estimating, planning and tracking, and measuring and managing quality
- Start each project right with a jelled team capable of making disciplined commitments that the team knows it can meet
- Ensure team members are trained to conduct personal and peer reviews of all design and code artifacts in order to put the highest-quality code components into test, striving for 90 – 100% defect-free components with zero cybersecurity vulnerabilities

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Managing for Secure Software Development – 2

- Ensure the review checklists incorporate specific checks for the types of vulnerabilities identified within “The OWASP Top Ten and CWE/SANS Top 25 Most Dangerous Programming Errors”
- Support the teams in collecting, analyzing, and reporting product and process data—size, effort, schedule, and quality
- Require teams to report status weekly
  - Precise and accurate data on planned versus actual size, effort, schedule, earned value and defects injected and removed

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CISQ Quality Characteristic Measures

CISQ What Attributes Should Be Measured ?

CISQ Quality Characteristic Measures		Business outcomes
Security	Ability to prevent unauthorized intrusions and data theft	Damages, customer confidence
Reliability	Ability to avoid outages and to recover operations quickly	Damages, lost revenue, customer loss
Performance Efficiency	Ability to avoid response degradation, resource overuse	Lost customers, operating cost
Maintainability	Ability to understand and modify software quickly	Cost of ownership, time to market

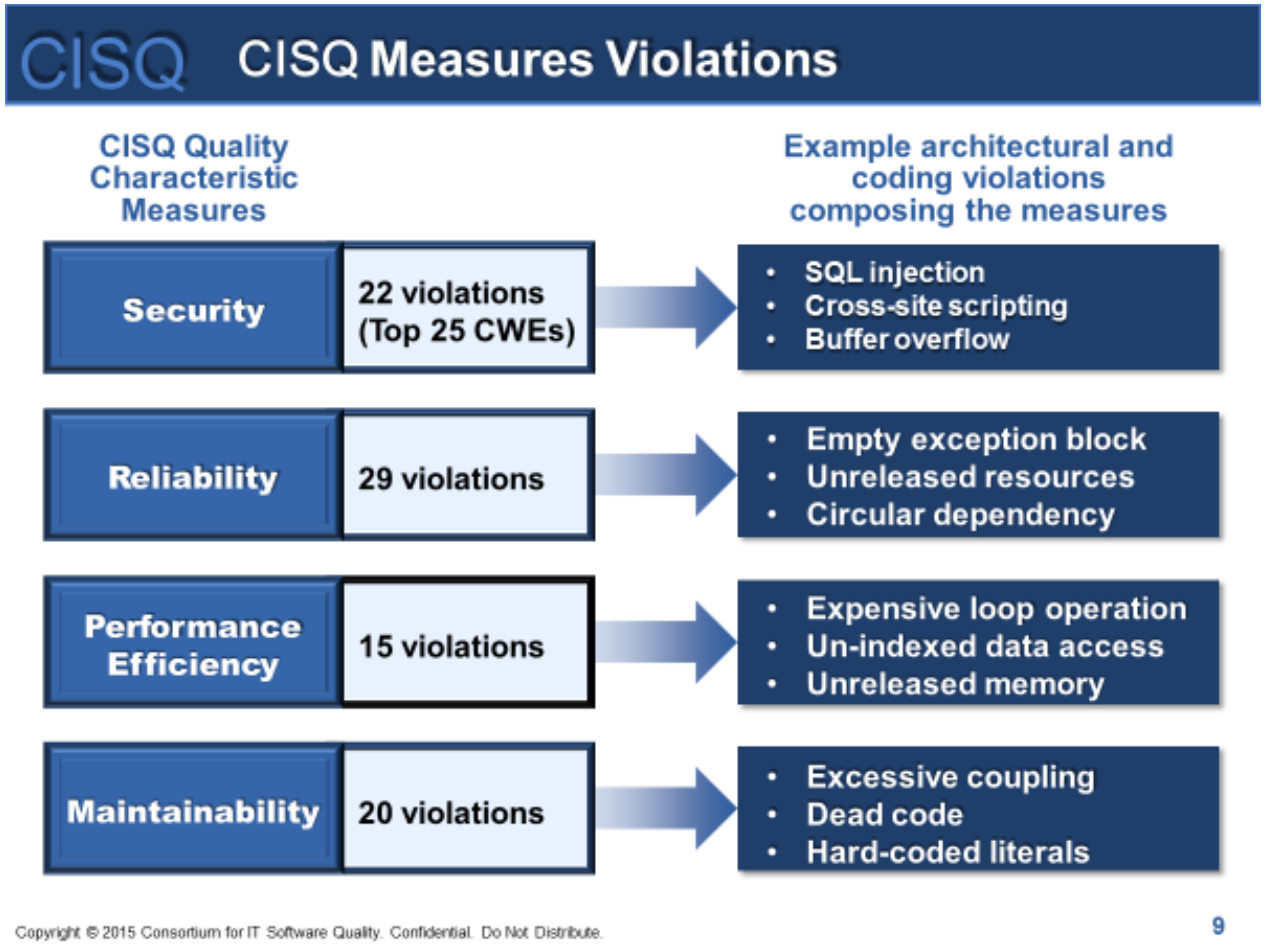
http://it-cisq.org/standards/automated-quality-characteristic-measures

Copyright © 2015 Consortium for IT Software Quality. Confidential. Do Not Distribute.

5

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

CISQ Quality Characteristic Violations



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Principles for Successful Metrics Program

- Metrics derived from business and team goals
  - What do we need to know to make sure we are achieving the goals?
- Software teams must be focused on the “vital few” metrics and not the “trivial many”
- Size metric is essential to normalize data
- Operational definitions, precision, and accuracy of data are of utmost importance
- Unless data is collected and used by trained team members, it won’t be useful
- Never use defect data for performance appraisal

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Operational Definitions

Term	Definition
% schedule deviation	Actual schedule divided by planned schedule (by months) times 100 minus 100
Acceptance test defect	Defect found during the acceptance test of the product. This defect may be identified by the customer as well as the ISHPI team. Acceptance test period starts after the completion of system test of the product and ends when the code is deployed to production.
Cost of Quality (COQ)	COQ = (effort in appraisal tasks + effort in prevention tasks + effort in failure tasks) x 100 Total effort towards the commitment (including project management) • Appraisal tasks: Personal reviews, peer reviews, and first-time test execution • Prevention tasks: Training, postmortems, and causal analysis • Failure tasks: Analyzing and fixing defects found in reviews and testing
Defect density	The number of defects identified in a product divided by the size of the product component, expressed in standard measurement terms for that product (e.g., 1000 lines of new and changed code)
Earned value	Percentage of effort for tasks completed divided by total effort of the tasks
First Time Right (in acceptance test)	Deployed software changes, accepted by the customer the first time, with no further rework
Peer review yield	The percentage of the total defects that are found and removed in peer review
Personal review yield	The percentage of the total defects that are found and removed in personal review

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Recommended Team Base Measures

Measure	Unit
Size	Lines of code
Task time	Minutes
Defects	Number
Task Completion	Yes/No

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

"Vital Few" Metrics to Reduce Vulnerabilities

Performance Metrics	Leading Indicator?	Lagging Indicator?	Organization	Project	Increment	Component
Planned vs. actual size	Y		✓	✓	✓	✓
Planned vs. actual effort	Y		✓	✓	✓	✓
Planned vs. actual schedule	Y		✓	✓	✓	✓
Planned vs. actual earned value	Y				✓	
Planned vs. actual defect profile	Y	Y	✓	✓	✓	✓
Total Cost of Quality (COQ)	Y	Y	✓	✓	✓	
First Time Right in acceptance test		Y	✓	✓	✓	
Acceptance test defect density in delivered code		Y	✓	✓	✓	

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Decision Process to Reduce Vulnerabilities

- Size, effort, schedule deviation
  - Review process adherence and test and rework due to poor quality
- Earned value deviation
  - Review hours worked against plan, task dependencies
  - "What if" scenario using process performance model
- Planned versus actual defect profile
  - Review personal and peer review yields – design, code
  - Estimate defect counts and defect densities for downstream steps using quality projection model

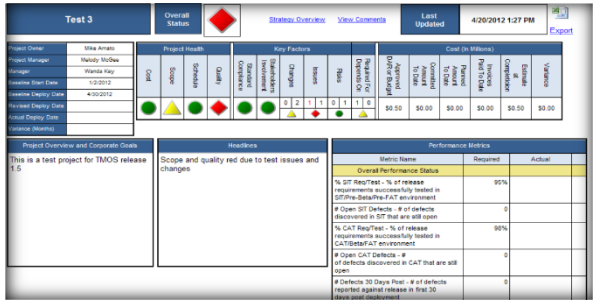
(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Project Management

advanced technology • native know-how

Inc. 5000 HONOR ROLL SIX-TIME HONOREE

Metrics SW



Agile Milestone Tracking

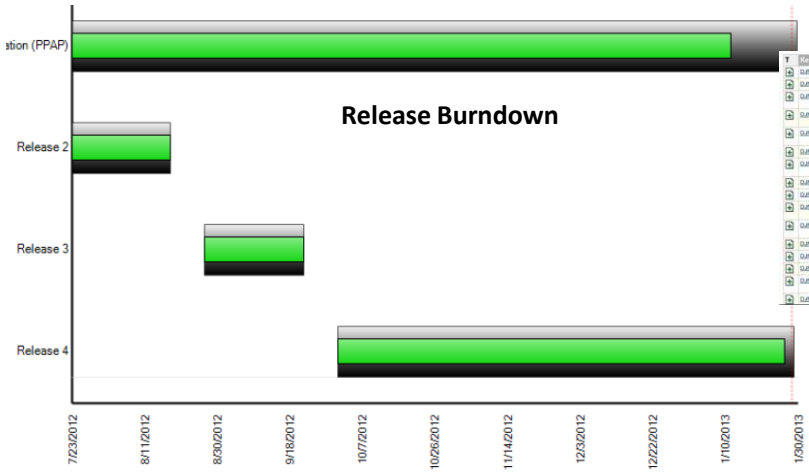
Scorecard Indicator	WBS	Task Name
	1	Sample Agile Project Plan Template
Initiate and Plan	1.1	Initiate and Plan
Sprint 0	1.2	Sprint 0 - Analysis and Design
Development Sprints	1.3	Development - Sprint 1 through n
SIT	1.4	Systems Integration Test
CAT	1.5	Customer Acceptance Test
Governance	1.6	Governance
Release	1.7	Release

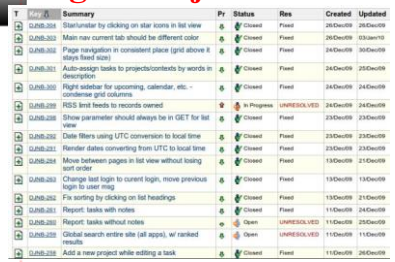
Detail Project Planning

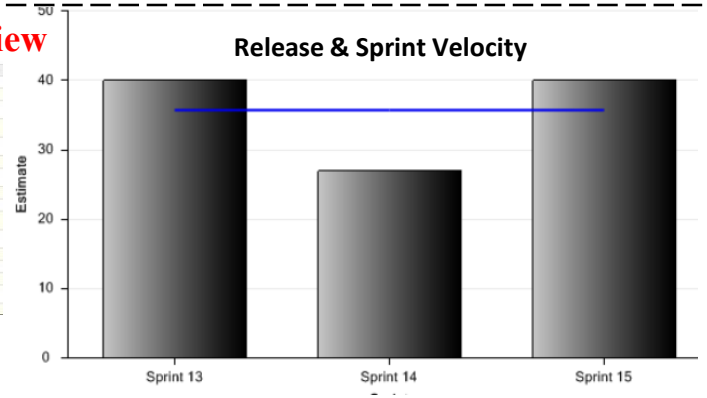


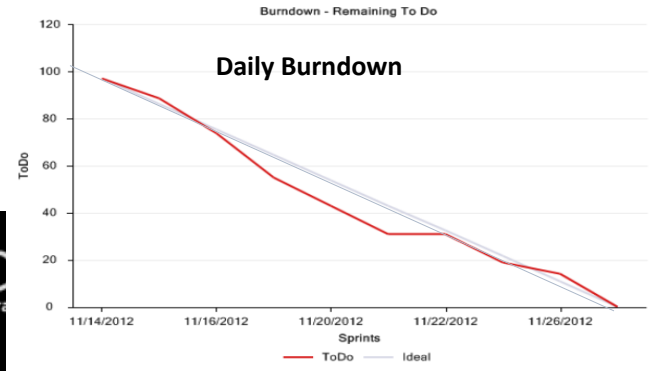
Senior Management View

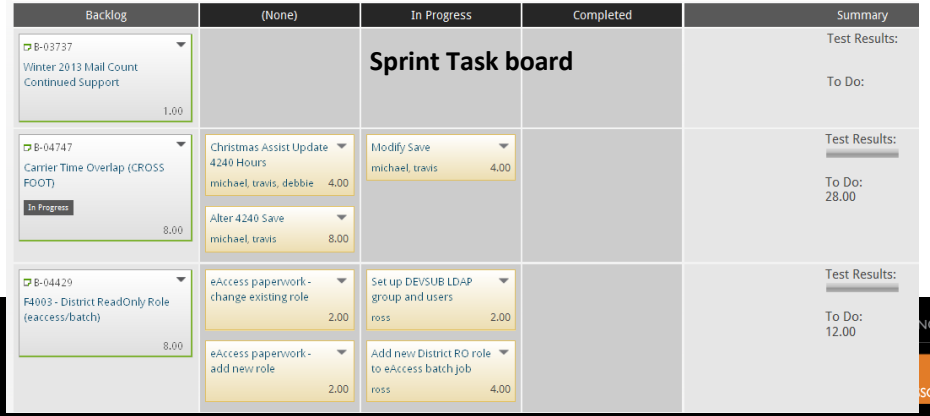
Agile Project Team View











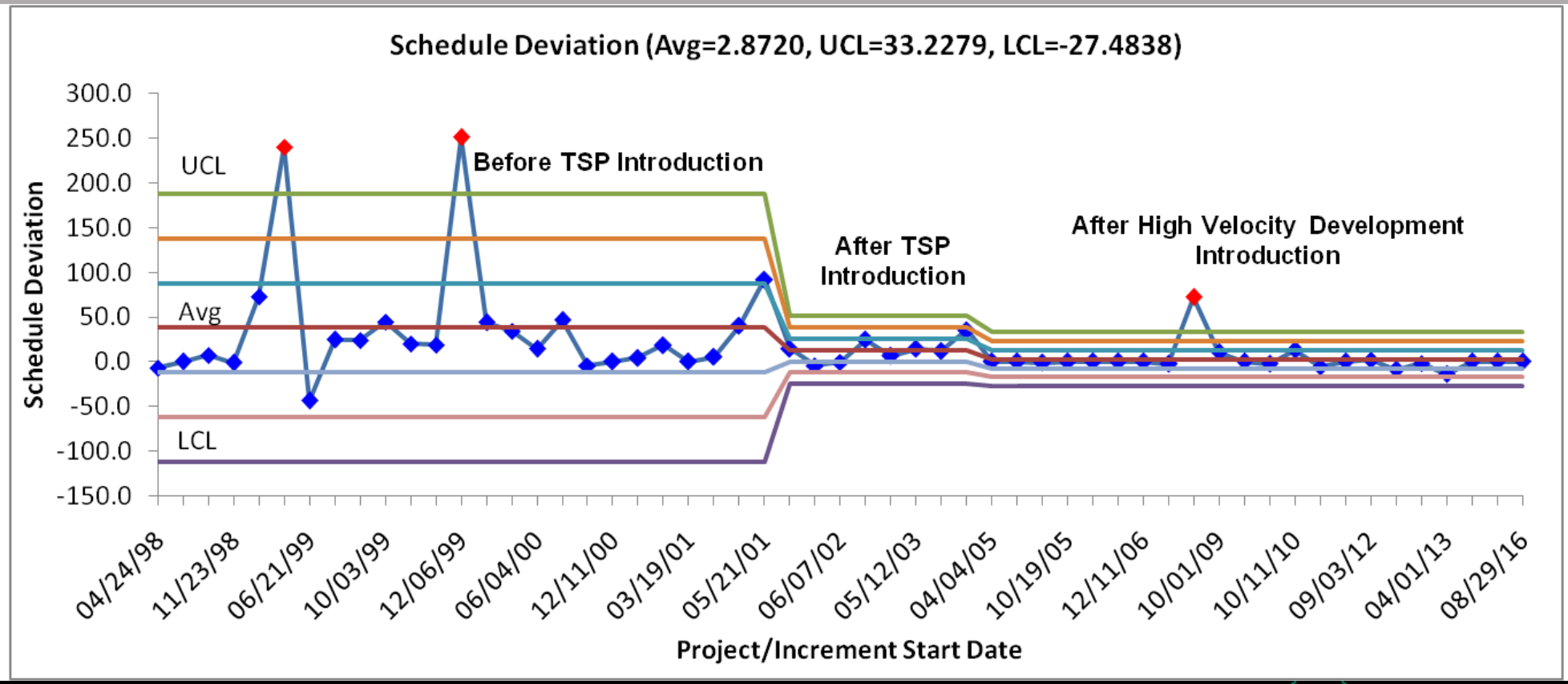
ation Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

NG A SAFE AND SECURE CYBER WORLD.

SCP CAP CSSLP CCFP HCISPP CCSP

Organization Capabilities – 1

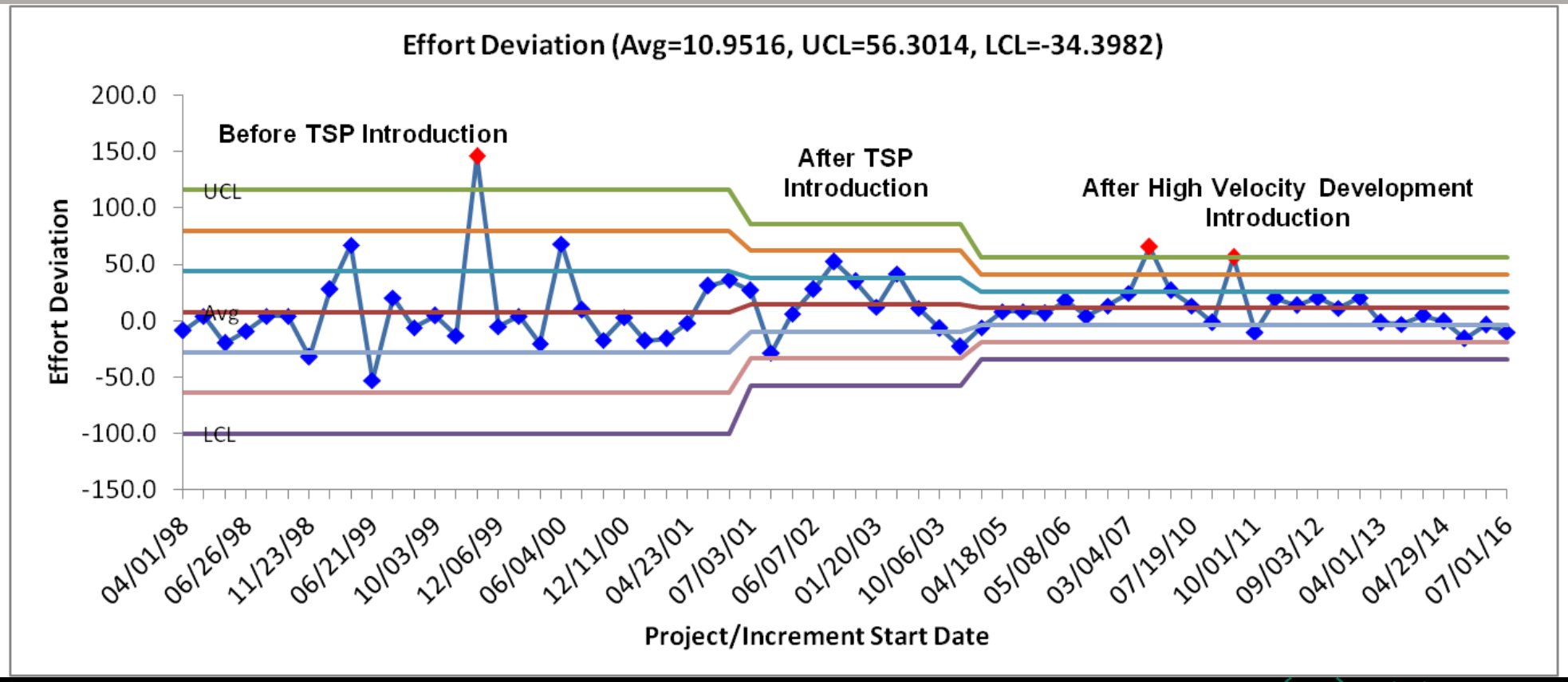
Schedule Deviation – Development Phases



(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Organization Capabilities – 2

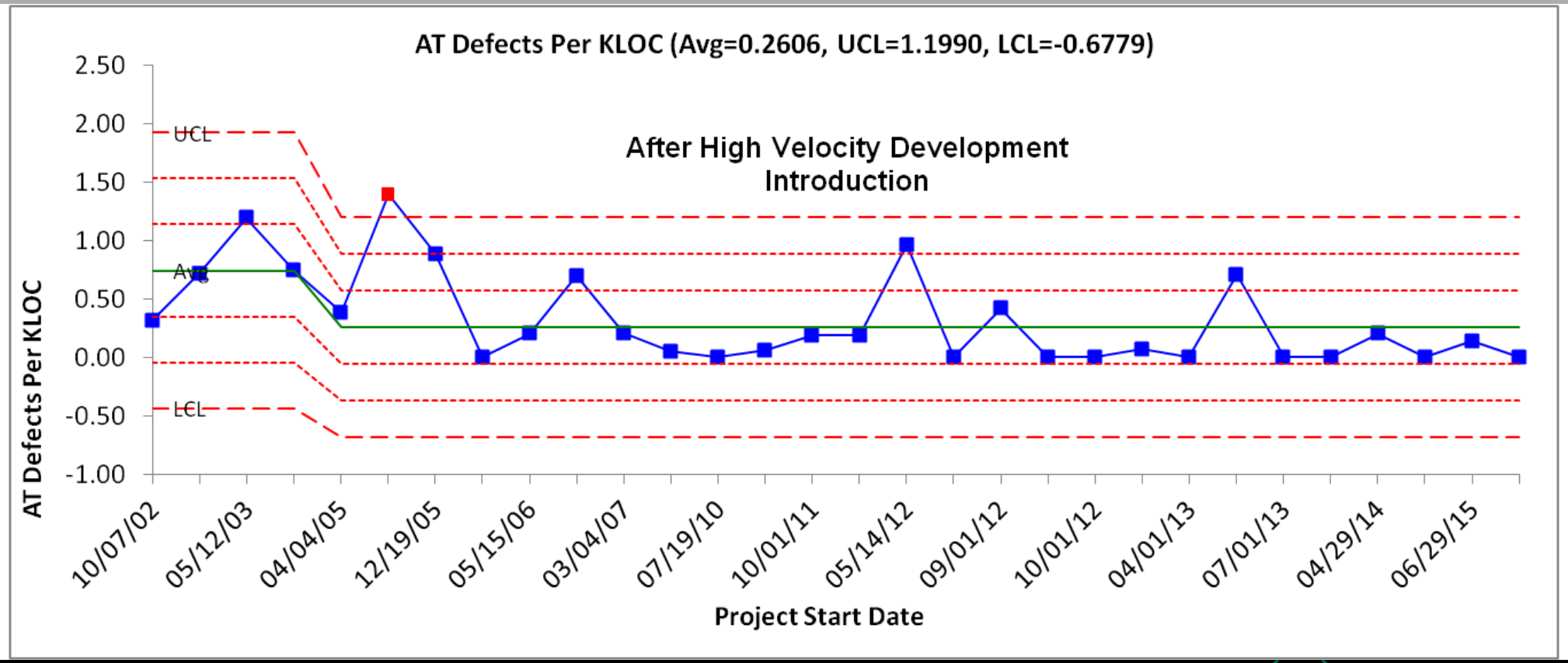
Effort Deviation – Development Phases



(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Organization Capabilities – 3

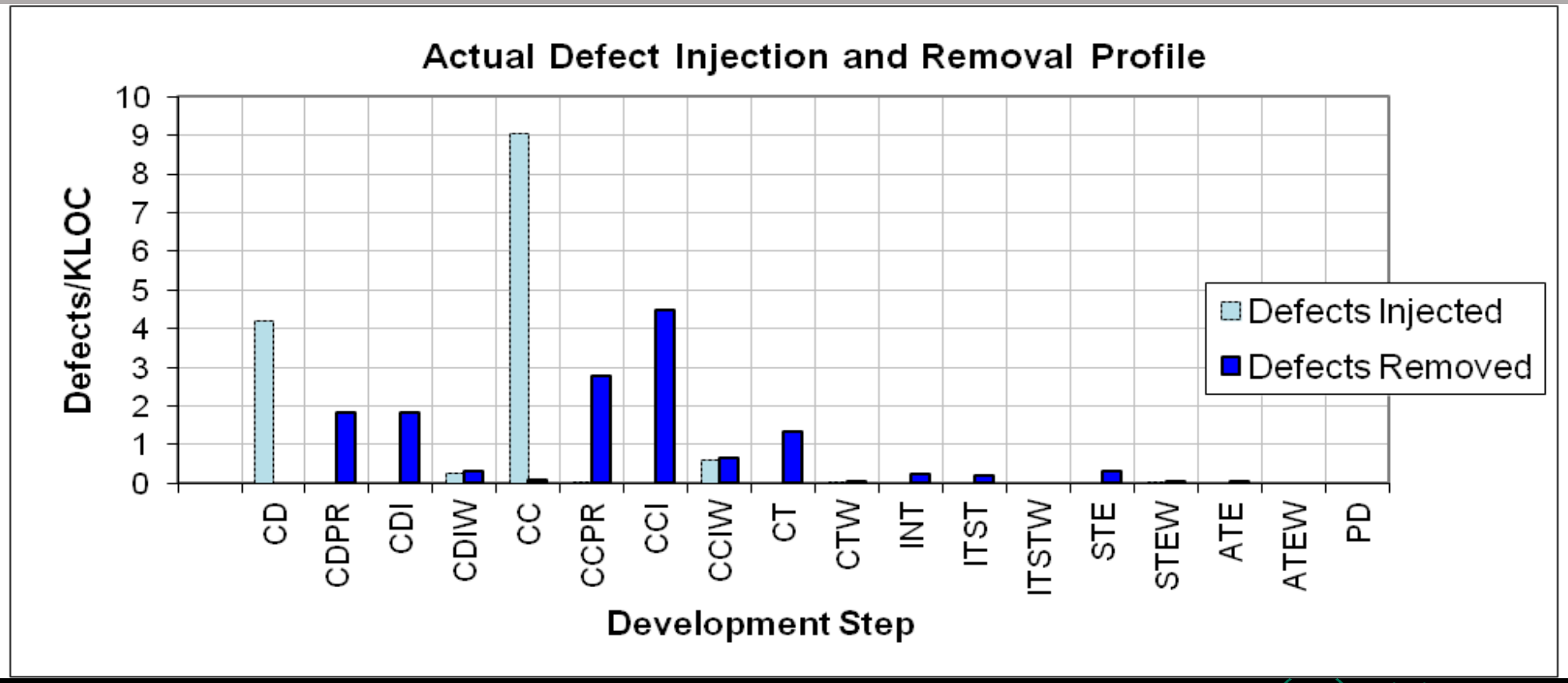
Acceptance Test Defect Density – Maintenance/Enhancement



© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Organization Capabilities – 4

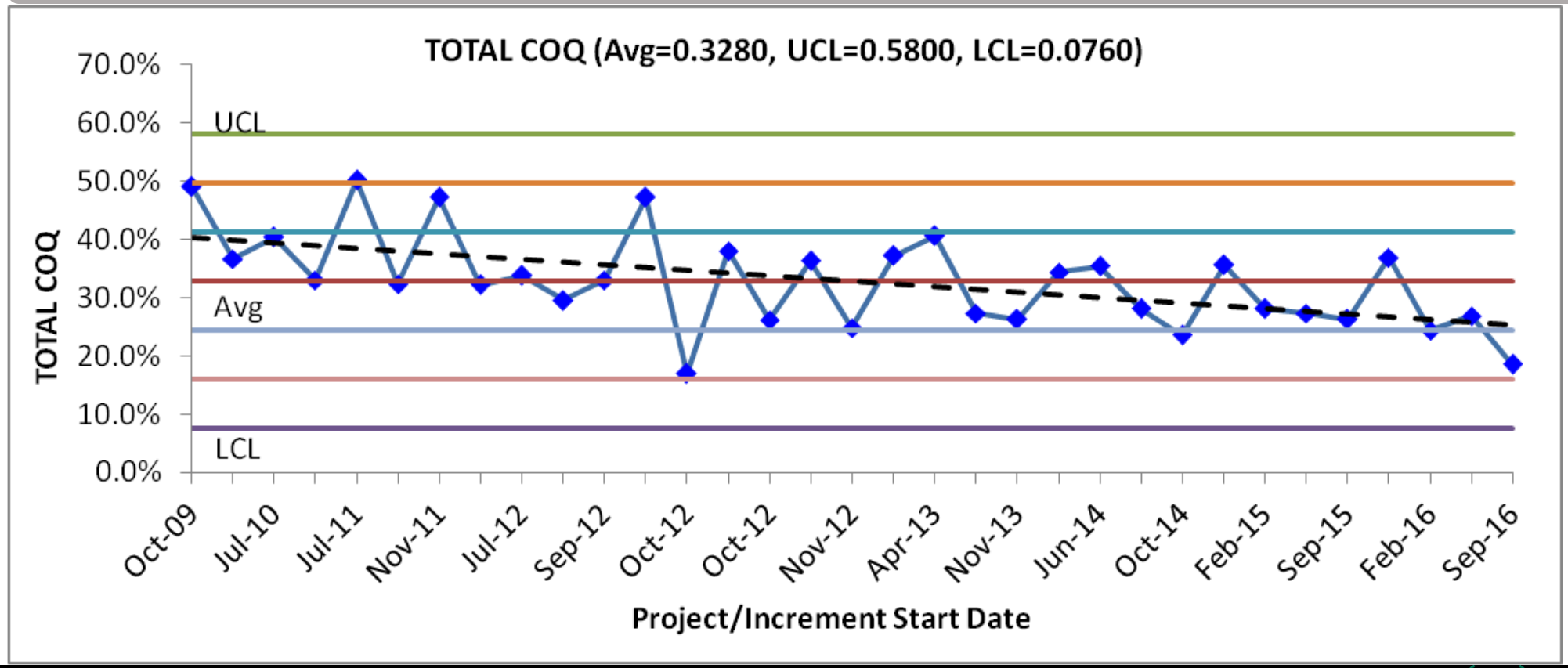
Defect Injection and Removal Profile



(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Organization Capabilities – 5

Total Cost of Quality



Appraisal
+ Failure
+ Prevention
= COQ

Appraisal
- Personal reviews
- Peer reviews
- All levels of first-time test execution

Failure
- Rework from reviews
- Rework from tests
- Regression testing

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Organization Capabilities Summary

Industry, Best in Class, Organization

Performance Metrics	Industry Average	Best in Class Average	Org. Average
Schedule deviation	> 50%	6%	< 3%
Acceptance test defects in delivered product (100,000 Source Lines of Code)	> 100	55	< 27
% of design and code inspected	< 100%	100%	100%
Customer's time to accept 100,000 LOC product	> 4 months	3.4 weeks	< 5 weeks
% of defects removed prior to system test	< 60%	70 – 95%	> 85%
% of development time in rework fixing system test defects	> 33%	2.7 – 10%	< 10%
Cost of quality	> 50%	29%	< 33%

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Customer Benefits of Optimizing Process and Agile Development

- Frequent incremental deliveries that meet customer business goals
- Dramatically reduces and practically eliminates cyber security incidents attributable to poor quality software code
- Reduces software operations & maintenance (O&M) costs by more than half
- Fewer bugs to fix in production software making available a larger percentage of O&M spend for new features and enhancements
- Enables lifetime warranty

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP
© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Main Points

- **Defective software** is insecure
  - "If you have a quality problem, you have a security problem"
- Cannot **rely on testing alone** to find and remove software defects
  - Common misconception – "if it passes test, it must be OK"
  - Root cause of "Deliver now, Fix later" culture, technical debt, increase in total ownership cost in many agile projects
- Move from reactive to proactive – **threat detection to threat prevention**
- **Reducing vulnerabilities** - number one goal for every agile software team
  - Manage software by managing software quality
- Need **transformation** – organization, team, individual
  - Combine high maturity CMMI Maturity Level 5 with agile team process to create secure software by self-managed teams and empowered developers with certifications

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Takeaways/"ASKs"

- Act with a **sense of urgency** to move from reactive "patch and pray" to proactive secure software development
- Begin **transformation** of organization, teams, and individuals to consistently deliver software which is secure from cyber attacks
- Manage secure software development by **managing software quality**
- Focus on the **"vital few"** metrics and not the "trivial many"
- Support teams in **reducing vulnerabilities** as the number one project goal
- Develop industry/government/academic coalition led by industry to address cybersecurity **"skills gap"** and talent pipeline

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

References

NIST Publication NISTIR 8151

http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf

Dramatically Reducing Software Vulnerabilities

Report to the White House Office of Science and Technology Policy

ISHIPI Technical Report, 22 July 2016

Barti Perini, Stephen Shook and Girish Seshagiri

Reducing Software Vulnerabilities – The Number One Goal for Every Software Development Organization, Team, and Individual

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

Contact

Girish Seshagiri

girish.seshagiri@ishpi.net

(703) 426-2790

(ISC)² OFFICIAL TRAINING PROVIDER
(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.
CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP

© Ishpi Information Technologies, Inc. (DBA *ISHPI*). All Rights Reserved

NDIA Workshop Report: DoD and Defense Industry Analysis of DoD Software Assurance (SwA) Capability Gaps

June 22-23 2017

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

Dr. Kenneth E. Nidiffer
Director of Strategic Plans for Government Programs
Carnegie Mellon University
Software Engineering Institute
Email (SEI): nidiffer@sei.cmu.edu
Email (OSD): kenneth.e.nidiffer.ctr@mail.mil

NDIA* Workshop Sponsors

This event was a jointly sponsored workshop by **NDIA SED, NDIA SSE & SwA Committees** with the DoD's **Joint Federated Assurance Center (JFAC) SwA Community of Practice (CoP),** hosted by **MITRE,** with analysis provided by **Engility Corporation**.

*NDIA – National Defense Industrial Association

Overview

- **Workshop Purpose & Participants**
- **Background**
- **Workshop Activities**
- **Analysis and Observations**

Workshop Purpose

- The government conducted a DoD Software Assurance (SwA) Capability Gap Analysis and afforded the defense industry an opportunity to review and provide their perspective.

- The workshop participants – from industry and gov't – provided a diverse set of background experiences, and allowed for a better consideration of different perspectives.

- This workshop provided insight into what industry believes are SwA gaps and priorities that affect U.S. technical capability advantage.

Workshop Participants

33 participants from industry and government

- **CACI**
- **Engility Corp**
- **General Dynamics**
- **IDA**
- **Lockheed Martin**
- **MITRE**
- **Northrup Grumman**
- **Raytheon**
- **SEI**
- **DASD(SE)**
- **DoD CIO**
- **DOE**
- **Army**
- **Navy**
- **Air Force**

Report developed by Dr. Scott Brown and Ms. Madison Rudy (Engility Corporation) in coordination with NDIA leads and Mr. Tom Hurt, DASD(SE).

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
7) Federated Coordination

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

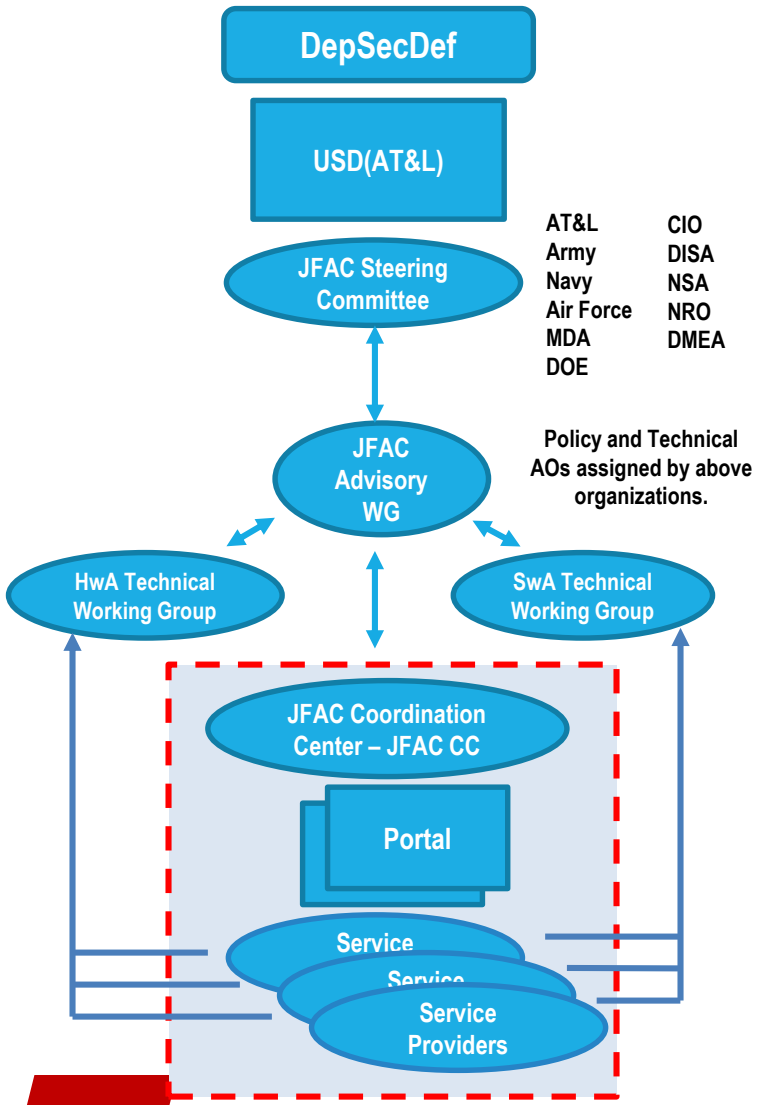
DASD(SE)'s JFAC lead, Mr. Tom Hurt, agreed to support an **NDIA-sponsored joint industry-government workshop**.

Background – FY14 NDAA Section 937

- **Key provisions:**
  - "provide for the establishment of a **joint federation of capabilities** to support the trusted defense system needs…to ensure security in the **software** and **hardware** developed, acquired, maintained, and used by the Department"
  - "consider whether capabilities can be met by existing centers"
  - **"[if gaps] shall devise a strategy [for] resources [to fill such gaps]"**
  - "[NLT 180 days, SECDEF shall] issue a **charter**…"
  - "submit to congressional defense committees…a **report** on funding and management"
- **Charter elements:**
  - Role of federation in supporting program offices
  - SwA and HwA expertise and capabilities of the Federation, including policies, standards, requirements, best practices contracting, training and testing
  - R&D program to improve code vulnerability analysis and testing tools
  - Requirements to procure manage, and distribute enterprise licenses for analysis tools

DoD established the Joint Federated Assurance Center in 2014; JFAC reached IOC in 2016.

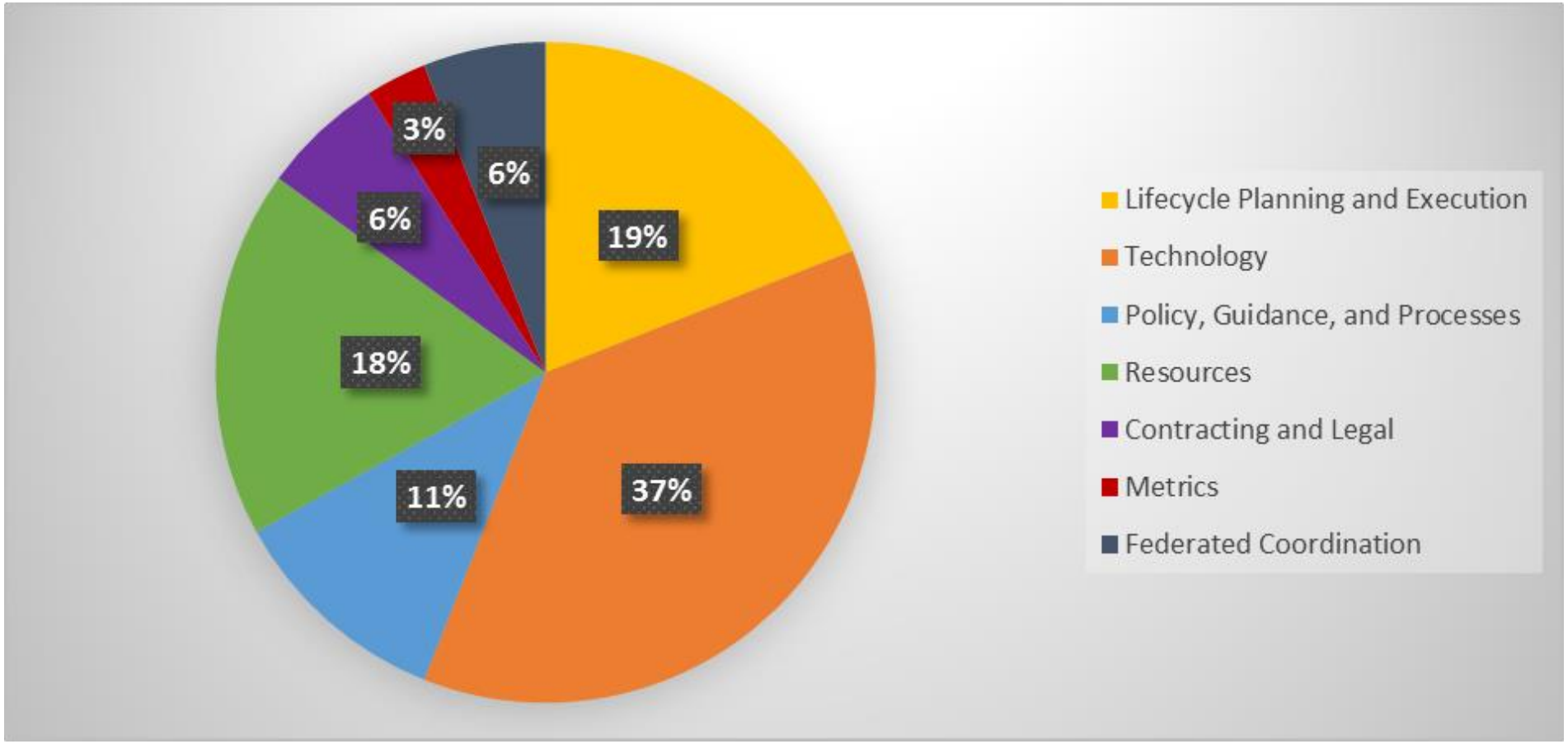
Background – JFAC Operational Structure



- **JFAC Action Officer (AO) WG**
  - AOs for SES-level JFAC Steering Committee
  - Maintain enterprise and strategy cognizance
  - Reporting and ROI status
- **SwA and HwA Working Groups**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Provide policy guidance
  - Provide community focal point for “hard problem” analysis and question/answer
- **JFAC Coordination Center**
  - Coordination of **Service Providers**
  - Supports programs with situational awareness, information/best practices, coordination
  - SwA analysis tool license distribution
  - **Portal:** https://jfac.army.mil
  - Assessment Knowledge Base (future)

Background – JFAC SwA Technical Working Group Capability Gap Analysis

Gaps (63 total) were categorized into seven areas*



*This graphic is from the JFAC SwA Technical Working Group Capability Gap Analysis Report (Distribution C, available from DASD(SE)).

Six Sigma Voice of the Customer (VOC)

- The “voice of the customer” is a process used to **capture the requirements/feedback from the customer (internal or external)** to provide the customers with the best in class service/product quality. This process is all about being **proactive and constantly innovative to capture the changing requirements of the customers** with time.
- The “voice of the customer” is the term used to describe the **stated and unstated needs or requirements of the customer.** The voice of the customer can be captured in a variety of ways: Direct discussion or interviews, surveys, focus groups, customer specifications, observation, warranty data, field reports, complaint logs, etc.
- This data is used to **identify the quality attributes needed** for a service provider to incorporate in the process or product.

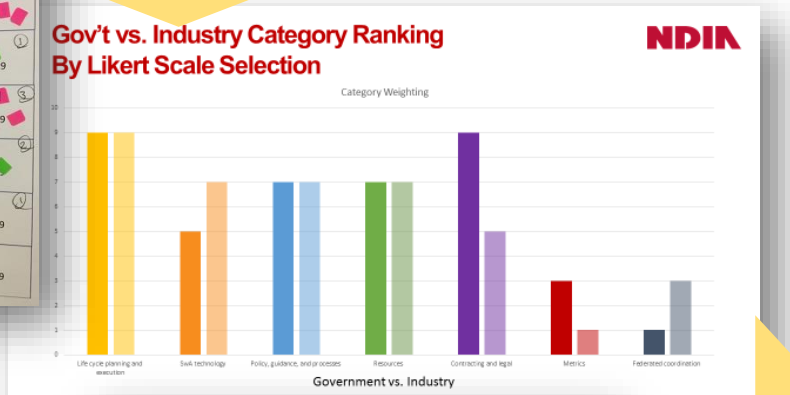
Workshop Activities

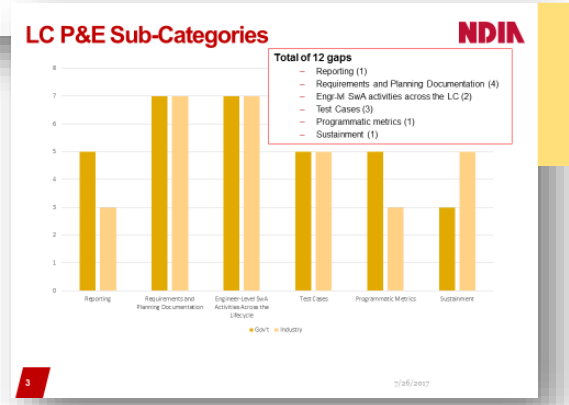
JFAC SwA Capability Gap Analysis

Government	Industry

Prioritized Gap Categories & Sub-categories

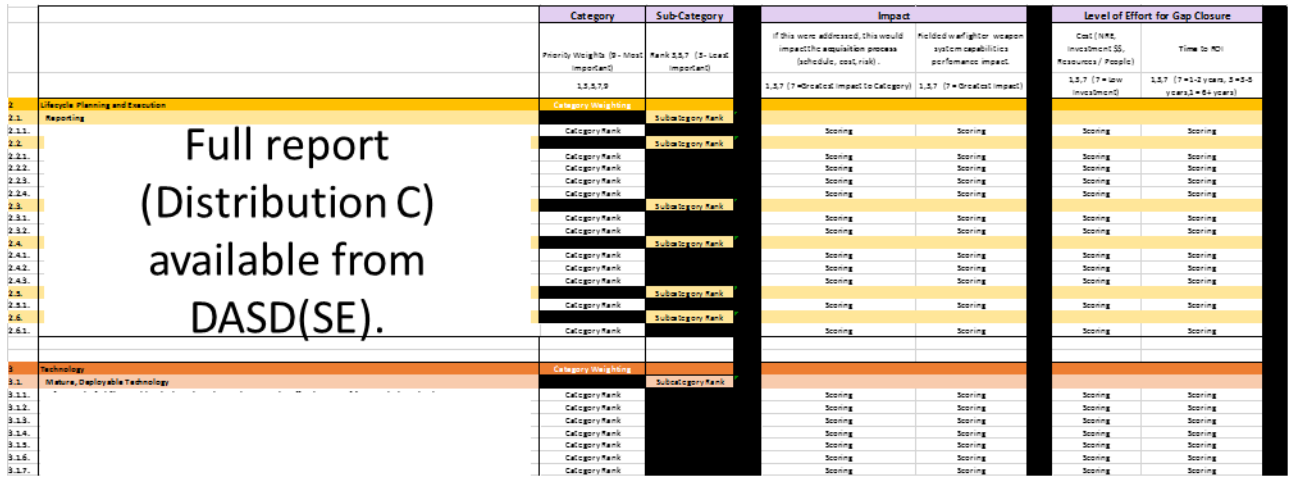






Voice of the Customer (VOC) Assessment

Government	Industry



Facilitated Break-out Sessions (Combined gov't/industry)	Assess (Individually)
1. Lifecycle planning & execution 2. SwA technology 3. Policy, guidance, process and Federated Communication 4. Resource 5. Contracts, Legal and SwA metrics	<u>Influence</u> • Acquisition (cost, schedule, risk) • Weapon system capability <u>Level of effort</u> to close gap • Cost • Time to ROI

SwA Capability Gap Analysis
"Voice of the Customer" Worksheet

63 SwA Gaps

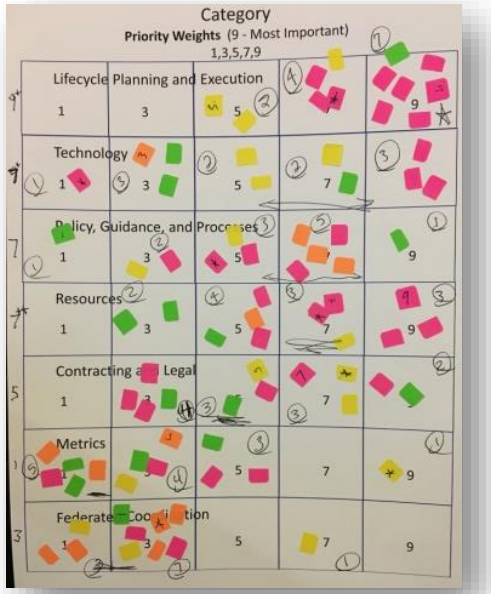
Prioritize Categories

Assess Influence/Level of Effort

		Category	Sub-Category	Influence		Level of Effort for Gap Closure	
		Priority Weights (9 - Most Important)	Rank 3,5,7 (3 - Least Important)	If this were addressed, this would impact the **acquisition process** (schedule, cost, risk) .	Fielded warfighter weapon system capabilities perfomance impact.	Cost (NRE, Investment $$, Resources / People)	**Time** to ROI
		1,3,5,7,9		3,5,7 (7=Greatest influence)	3,5,7	3,5,7 (7=lowest cost)	3,5,7 (7=1-2 yrs, 5=3-5 yrs, 3=5+ yrs)
2	Lifecycle Planning and Execution	Category Weighting					
2.1.	Reporting		Subcategory Rank				
2.1.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.			Subcategory Rank				
2.2.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.4.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.3.			Subcategory Rank				
2.3.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.3.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.			Subcategory Rank				
2.4.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.5.			Subcategory Rank				
2.5.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.6.			Subcategory Rank				
2.6.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
3	Technology	Category Weighting					
3.1.	Mature, Deployable Technology		Subcategory Rank				
3.1.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.4.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.5.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.6.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.7.		Category Rank		Scoring	Scoring	Scoring	Scoring

Full report (Distribution C) available from DASD(SE).

Group Sessions – Category / Sub-category Analysis



- **During a facilitated session, participants were divided by Government and Industry affiliation to score the seven gap categories and their respective sub-categories.**

- **Each participant was provided voting 'chits' – one for each gap and sub-category – and was asked to score each category / sub-category using a Likert scale (1-9, where 9 = highest priority):**

- **The two groups discussed their voting to seek understanding of individual scores and an agreed to rank.**
  - A groups' averaged score based on individual votes was calculated to compare / contrast between Government and Industry.

Gap Category Ranking By Likert Score & Mean Value

The table below provides the ranked categories by each groups' averaged Likert scores and rank.

Rank	Category (Government Likert average & rank)	Category (Industry Likert average & rank)
1	Contracting and Legal (7.18 / 9)	Lifecycle Planning and Execution (7.77 / 9)
2	Lifecycle Planning and Execution (7 / 9)	Resources (6.17 / 7)
3	Policy, Guidance and Processes (5.89 / 7)	Technology (5.55 / 7)
4	Resources (5.45 / 7)	Policy, Guidance and Processes (5.5 / 7)
5	Technology (5.18 / 5)	Contracting and Legal (5.5 / 5)
6	Metrics (3.91 / 3)	Metrics (3.15 / 1)
7	Federated Coordination (2.6 / 1)	Federated Coordination (2.82 / 3)

* Where two categories received the same average value, rank numbers are interchangeable.

Observations – Gap Categories and Sub-categories

- **Lower ranking does not denote lack of importance of the category / sub-category or the associated gaps.**
  - Participants were required to use all Likert scale values – something had to be a 1.
  - Each and every one of the 63 gaps has one or more Government organization 'sponsors'.
- **Contracting and Legal category had largest difference in Likert rank and score.**
  - Government felt strongly that without explicit contractual direction, contractors' SwA activities would not be sufficient; Industry recognized the priority and importance of contract language, but as engineers participating in the workshop, they focused on engineering-focused categories.
  - Individual gap scores in this category did rank in the top quartile (see slide 17)
- **The only sub-category with more than 1 Likert rank difference was Policy.**
- **Metrics and Federated Coordination were ranked lowest because participants felt the Government had started to address the associated gaps.**
  - Industry gave the lowest Likert score to Metrics although the actual votes averaged 3.15, higher than Federated Coordination (score: 2.82).
  - JFAC has produced some (initial) metrics for JFAC web portal and SwA tool use.
  - JFAC has a several working groups and communities of practice in addition to a web portal that allows for coordination. Biggest need: ability to include industry in coordination / collaboration

Breakout Session – Gap Analysis

- **During facilitated break-out sessions for each of the gap categories, groups consisting of both Government and Industry participants discussed the gaps in their assigned category.**
- **After discussion, each individual participant was asked to score each category gap using a Likert scale (3-5-7) in the VOC worksheet, assuming the gap could be closed:**
  - Influence: how would gap closure positively influence acquisition cost/schedule/risk (e.g., lower acquisition cost) and warfighter capability (e.g., 7 = highest influence of capability)
  - Level of Effort: how much cost (e.g., 7 = lowest cost to close gap in terms of funds or resources) and how long before time to Return of Investment for gap closure (e.g., 3 = 6 or more years)
- **VOC worksheets were collected and analyzed after the workshop concluded.**
  - Weighted scores were calculated with and without category/sub-category scores.

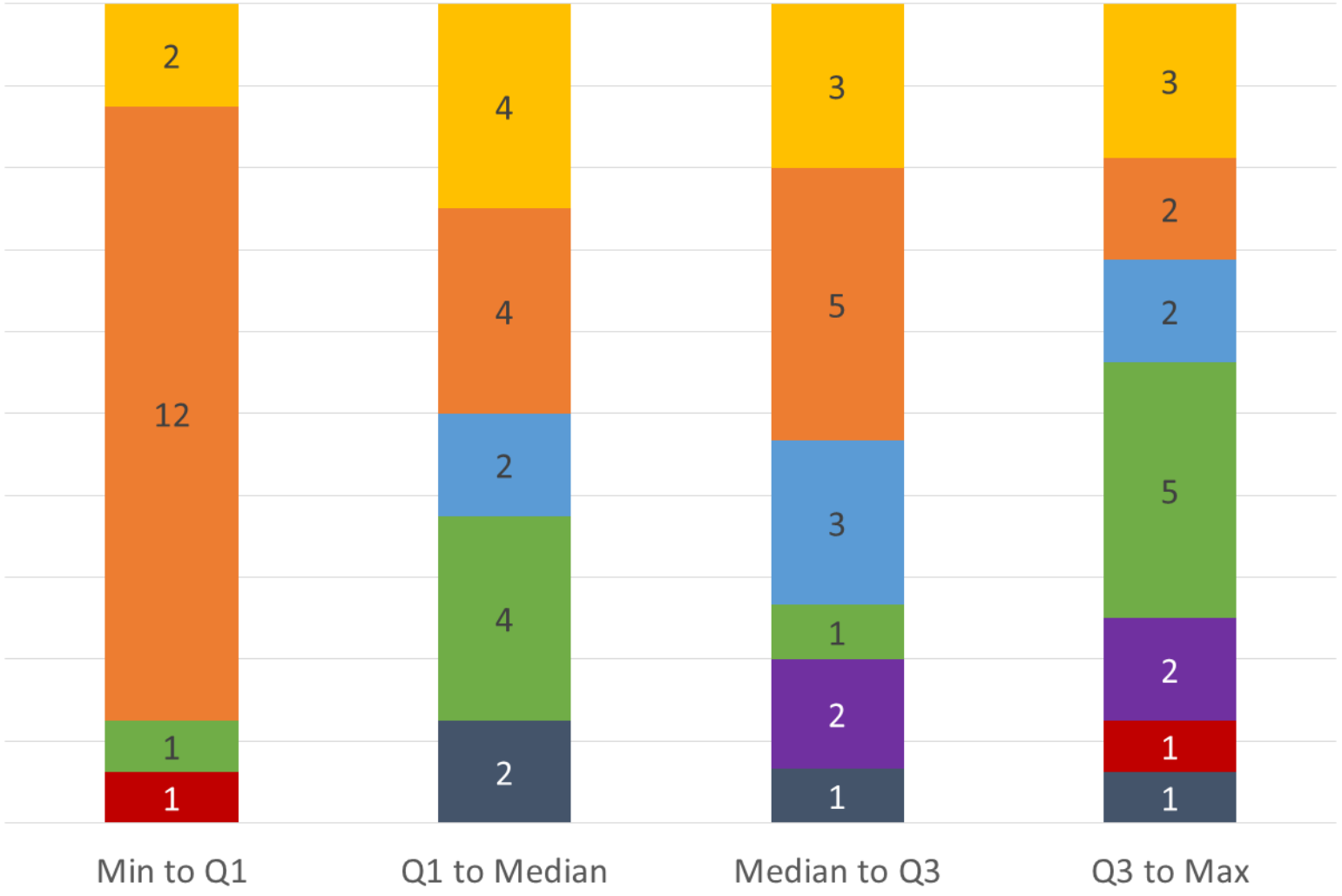
VOC Gap Analysis – Gaps in Top Quartile by Weighted Score

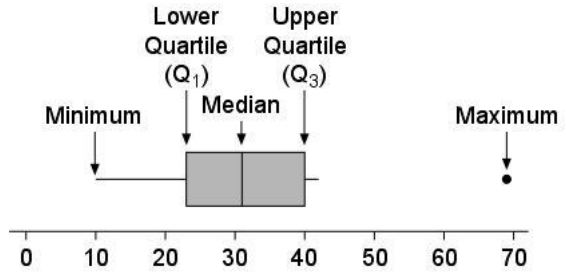
Weighted Gap Score = Influence(acquisition process) * Influence score(warfighter capability) * LOE(cost) * LOE(time to ROI)

1	Contracting and Legal	6.1 - Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible
2	Resources	5.2.1 - Lack of SwA training for Program Managers
3	Resources	Tools
4	Metrics	7.1 - Lack of agreed-upon metric set that will be collected and analyzed
5	Policy, Guidance and Processes	Policy
6	Federated Coordination	8.4 - Lack of enterprise-wide approval for tool use on networks
7	Technology	3.1.4 - Lack of use of defense technology
8	Lifecycle Planning & Execution	2.2.2 - SwA requirements lacking in system requirements
9	Resources	Training
10	Technology	Deployable Technology
11	Resources	Tools
12	Resources	Tools
13	Policy, Guidance and Processes	Process
14	Lifecycle Planning & Execution	SwA Activities
15	Contracting and Legal	6.2 - Lack of strategy for SwA of COTS and NDI
16	Lifecycle Planning & Execution	2.1.1 - No clear reporting requirement on software assurance planning, activities, and status

Full report (Distribution C) available from DASD(SE).

Number of Gaps by Category per Quartile based on Weighted Gap Scores





Observations – VOC analysis

- **All categories have 1 or more gaps in the highest quartile based on Influence/Level of Effort scores**
  - This analysis validates the keynotes, group and break-out discussions at the workshop – even if a gap was in a low ranked category (e.g., Metrics), the associated gaps may have high “pay-off” (i.e., ability to reduce program cost/schedule/risk and improve warfighter capabilities, low cost/resources to implement and quick time to ROI)
- **Each category, except Technology, has at least half of its gaps in the top 50%; Contracting & Legal has all its gaps in top 50%.**
  - Technology gaps, composing the largest number of gaps (37%), had some of the lowest Time to ROI scores
  - The highest scored gap was in Contracting & Legal – “Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible”

Observations – "Missing" Gaps

- **Life Cycle Planning and Execution**
  - SwA needs to flow into industry documents as well (SW Dev Plan) (Gaps 2.2.1 & 2.2.2)
  - Lack of operator's perspective in life cycle (Gap 2.3)
- **Technology**
  - Lack of integrated build environment with Software Assurance tools
  - Lack of ability to select appropriate technologies based on program characteristics
- **Policy & Guidance / Federated Coordination**
  - Unification – relationship mapping and coordination of statute, policies and guidance. U.S. Code; DFARS; DoDI 5000.02, 8500; NIST, …. They are pointing to each other.
  - Coverage – Policy & Guidance needs to cover whole life cycle, all technologies, all systems regardless of ACAT level or type (e.g., weapon system vs. IT)
  - Industry access to JFAC & associated capabilities (e.g., Assessment Knowledge Base)

Observations – "Missing" Gaps

- **Resources**
  - Industry expertise is also a gap.
  - Specialized SwA workforce is NOT the answer. System and SW engineers need to understand SwA.
  - SwA training is not available across DoD career fields or restricted to certain career fields
  - Software Engineering Body of Knowledge has not been adopted across the DoD in terms of minimum skill sets (such as the IEEE SWEBOK)
- **Contracts / Metrics**
  - Need consistency between all security related areas in what is put in contract language
  - Legality of doing analysis of the COTS software before you buy it
  - Legality of publishing results of doing analysis of the COTS software (make the DeWitt clause illegal)
  - Providing incentives for robust vendor software assurance program
  - Research into improved metrics – for projects

Conclusion and Way Forward

- **This workshop served to provided insight into what industry believes are SwA gaps and priorities that affect U.S. technical capability advantage.**

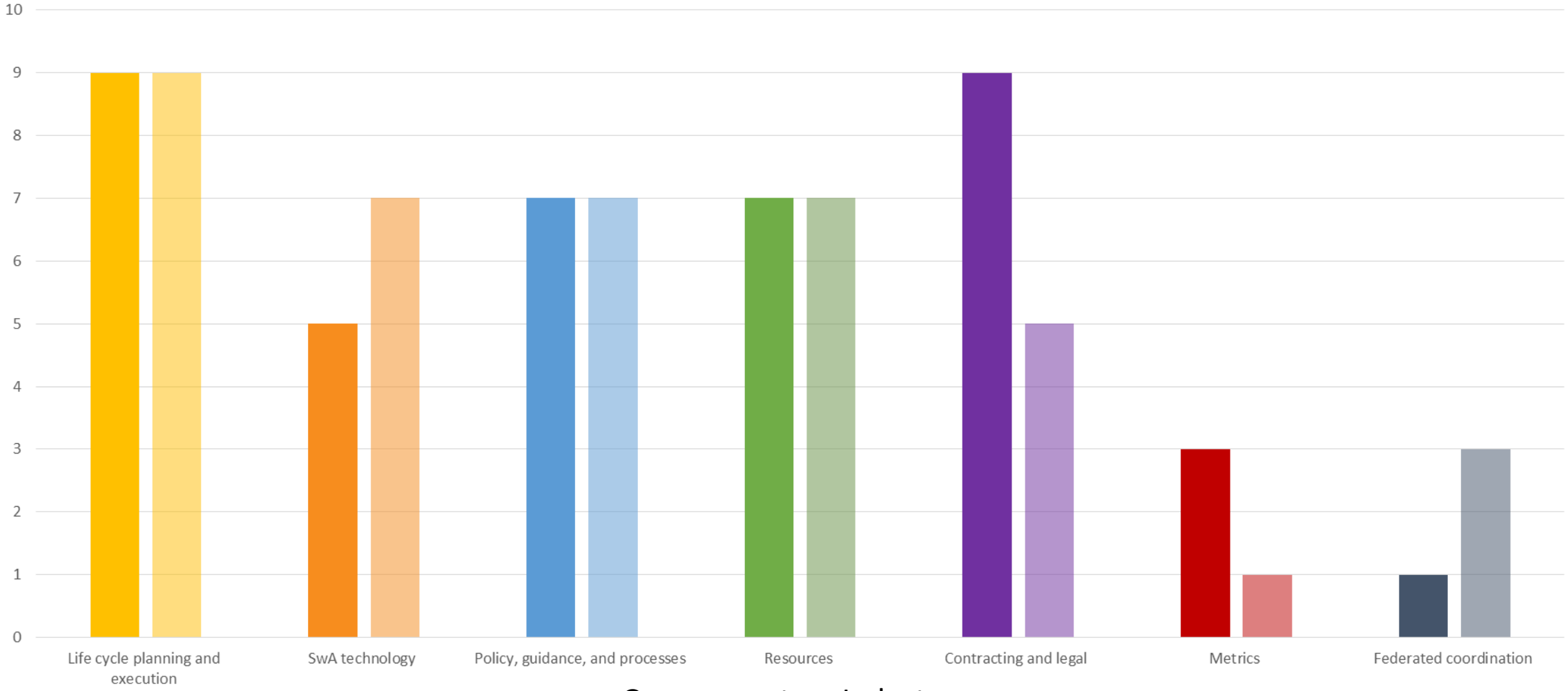
- **The analysis quantifies and validates ongoing discussion in JFAC working groups and other DoD and NDIA venues (e.g., Cyber Resilient Weapon System workshops) – there is high payoff expected if we address Software Assurance gaps.**

- **Analysis will be presented at various forums.**
  - NDIA SE Fall Conference: Holly Dunlap & Tom Hurt

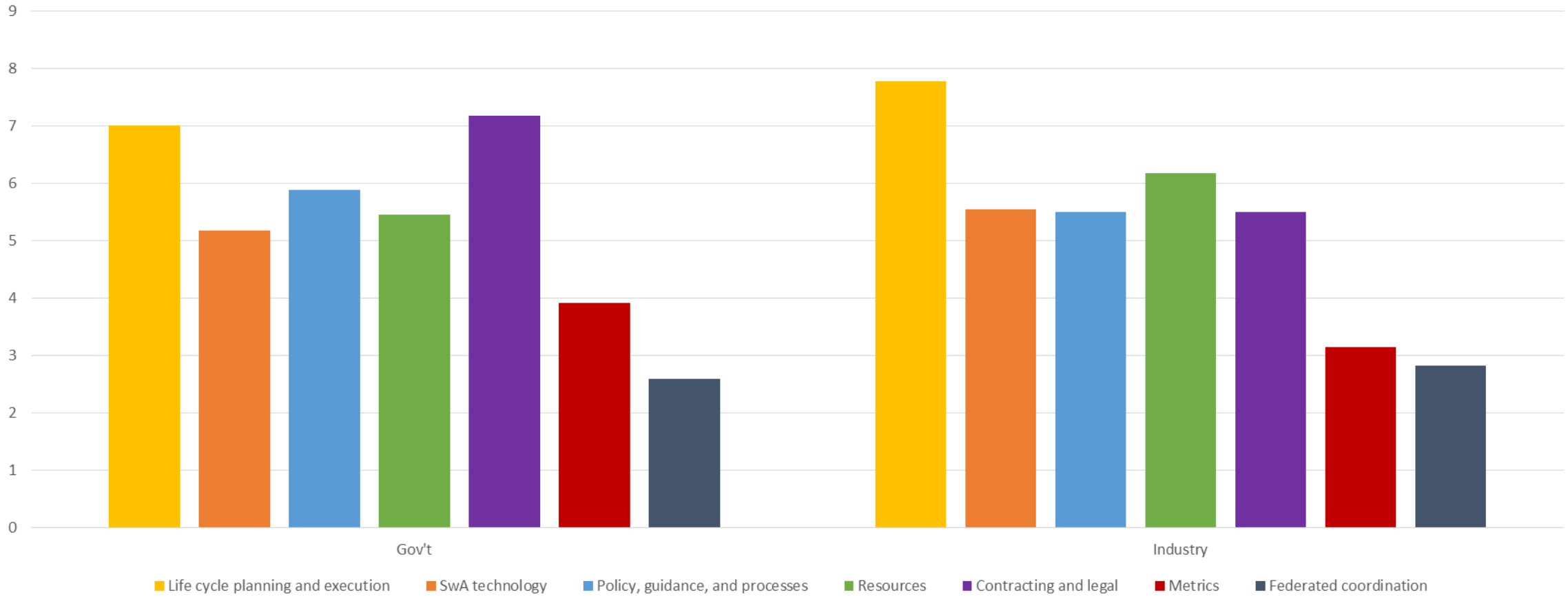
- **“High payoff” initiatives will be considered for funding based on analysis.**

Supporting Material

Gov’t vs. Industry Category Ranking By Likert Scale Selection



Gov’t vs. Industry Groups’ Averaged Likert Score



Government vs. Industry

Category Ranking By Likert Scale Selection

- **The following table provides the group selected category ranking grouped by Government and Industry.**
- **Where two categories are given the same Likert scale value, rank numbers for that group are interchangeable.**

Rank	Government Category	Industry Category
1	Lifecycle Planning and Execution (9)	Lifecycle Planning and Execution (9)
2	Contracting and Legal (9)	Technology (7)
3	Policy, Guidance, and Processes (7)	Policy, Guidance, and Processes (7)
4	Resources (7)	Resources (7)
5	Technology (5)	Contracting and Legal (5)
6	Metrics (3)	Federated Coordination (3)
7	Federated Coordination (1)	Metrics (1)

Dynamics of Integrating Software Assurance Engineering Activities into the System Acquisition Life Cycle

Dr. Kenneth E. Nidiffer

20th Annual Systems Engineering Conference
Waterford Conference Center
Springfield, VA
October 23–26 2017

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Distribution Statement A: Approved for Public Release; Distribution is Unlimited

© 2017 Carnegie Mellon University

Dynamics of Integrating Software Assurance Engineering Activities into the System Acquisition Life Cycle

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY 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. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0799

Software-Enabled Systems Are Today's Strategic Resource



Dr. Bill Scherlis*

"Software is the building material for modern society"

Manual Labor



Water



Steam



Oil



Software





Increasing Globalization, Productivity, and Complexity

Source: SEI

© 2017 Carnegie Mellon University

Context: Increasingly Software Assurance Is a Moving Target

- **Definition:** Software assurance provides the required level of confidence that software functions as intended (and no more) and is free of vulnerabilities, either intentionally or unintentionally designed or inserted in software, throughout the life cycle*
- **Perspective:** The changing and expanding role that software plays in cyberspace means that the development of software-intensive systems must continue to evolve while we pursue software assurance



*** NDAA 2013, Section 933**

Source: SEI

© 2017 Carnegie Mellon University

Challenges: Integrating Software Assurance Engineering Activities into the System Acquisition Life Cycle

1. Increasing complexity of software-intensive systems
2. Satisfying unique operational mission and business needs
3. Solving the vulnerability identification chasm
4. Addressing system sustainment as a strategic initiative
5. Handling the expanding code base
6. Understanding attack patterns, vulnerabilities, and weaknesses
7. Increasing vulnerabilities
8. Designing-in software quality throughout the life cycle
9. Reducing technical debt
10. Working in the infancy of the software engineering discipline

Distribution Statement A: Approved for Public Release; Distribution is Unlimited
© 2017 Carnegie Mellon University

Context: Software Assurance/Cyber Imperative

- Software is a foundation of the DoD's military power and the building material for modern society
  - *Software assurance is a moving target*
- The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) updated DoDI 5000.02 to include a new Enclosure 14 - 2017. The policy states, in part,
  - *Program managers, assisted by supporting organizations to the acquisition community, are responsible for the cybersecurity of their programs, systems, and information…"*
- Direct link between cybersecurity engineering and systems and software assurance engineering*

**Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*, Carol Woody and Nancy Mead, 2017

© 2017 Carnegie Mellon University

Context: Dynamics of Software

- Software is ubiquitous and growing in importance
- Codebases are increasing
- Vulnerabilities (defects, flaws) are increasing
- Software represents increasingly more system functionality and cost
- Research is needed to address emerging software challenges
- Software-reliant systems are becoming more complex and intertwined



- There is national and global dependence on software
- We need to improve the management of software-intensive systems
- Software assurance is increasingly important, and achieving it is a moving target

Distribution Statement A: Approved for Public Release: Distribution is Unlimited
© 2017 Carnegie Mellon University

Context: DoD Stakeholders and Different Perspectives on Software Assurance



Source: DAU

© 2017 Carnegie Mellon University

Context: The Fabric of Computing Is Changing, and Achievement of Software Assurance Is More Challenging



Networks are becoming software defined

- Generic network nodes can adapt function to usage and demand

Field-Programmable Gate Arrays (FPGAs) are proliferating

- Now even the processor's function is determined by software and malleable after fielding

Emergence of Artificial Intelligence and Machine Learning

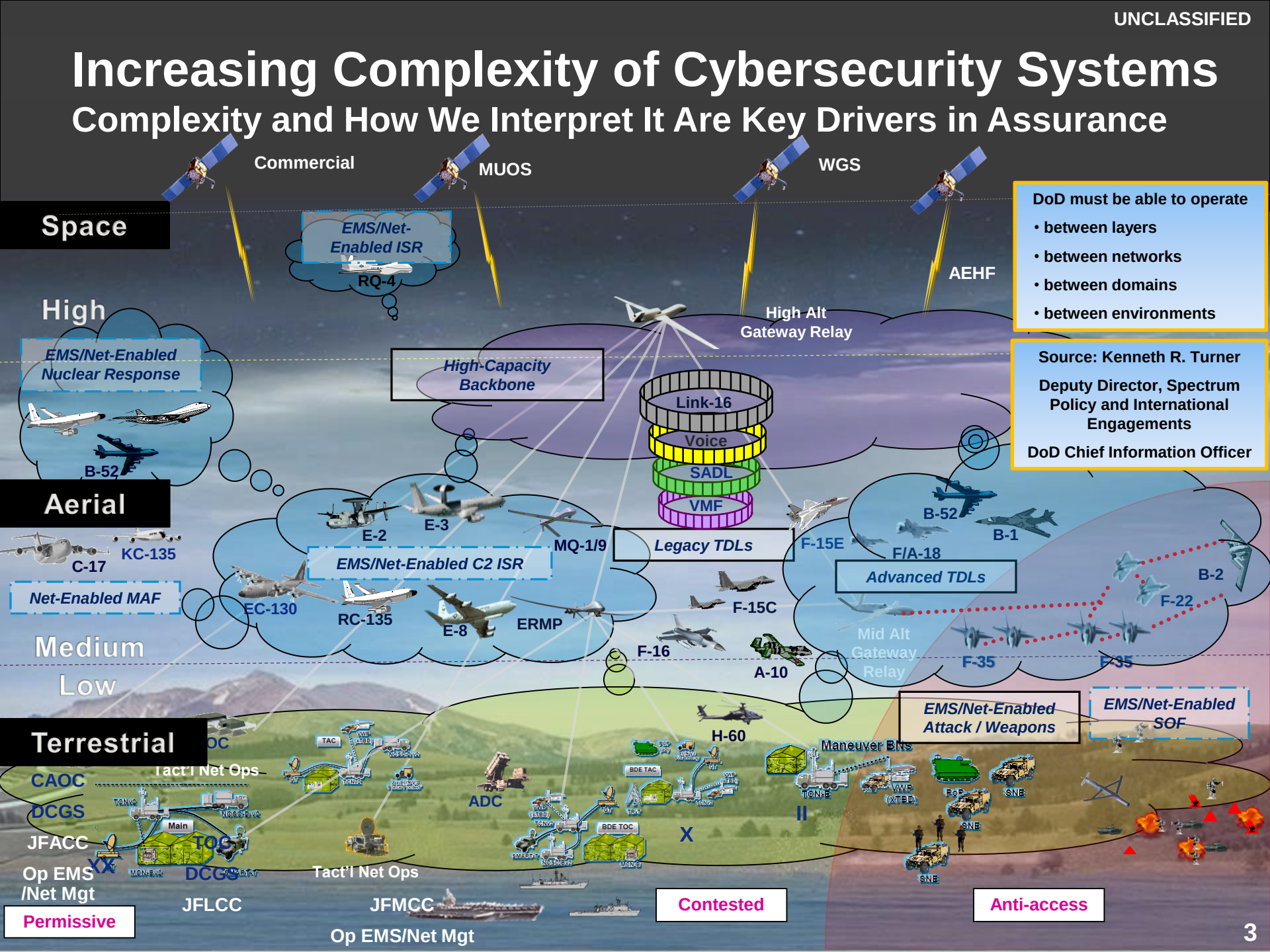
- Tasks change from direct programming to data curation and feature discovery

Source: SEI

© 2017 Carnegie Mellon University

Increasing Complexity of Cybersecurity Systems

Complexity and How We Interpret It Are Key Drivers in Assurance



DoD must be able to operate

- between layers
- between networks
- between domains
- between environments

Source: Kenneth R. Turner

Deputy Director, Spectrum Policy and International Engagements

DoD Chief Information Officer

Satisfying Unique Operational Mission and Business Needs as Commercial Products Are Integrated into Military Systems





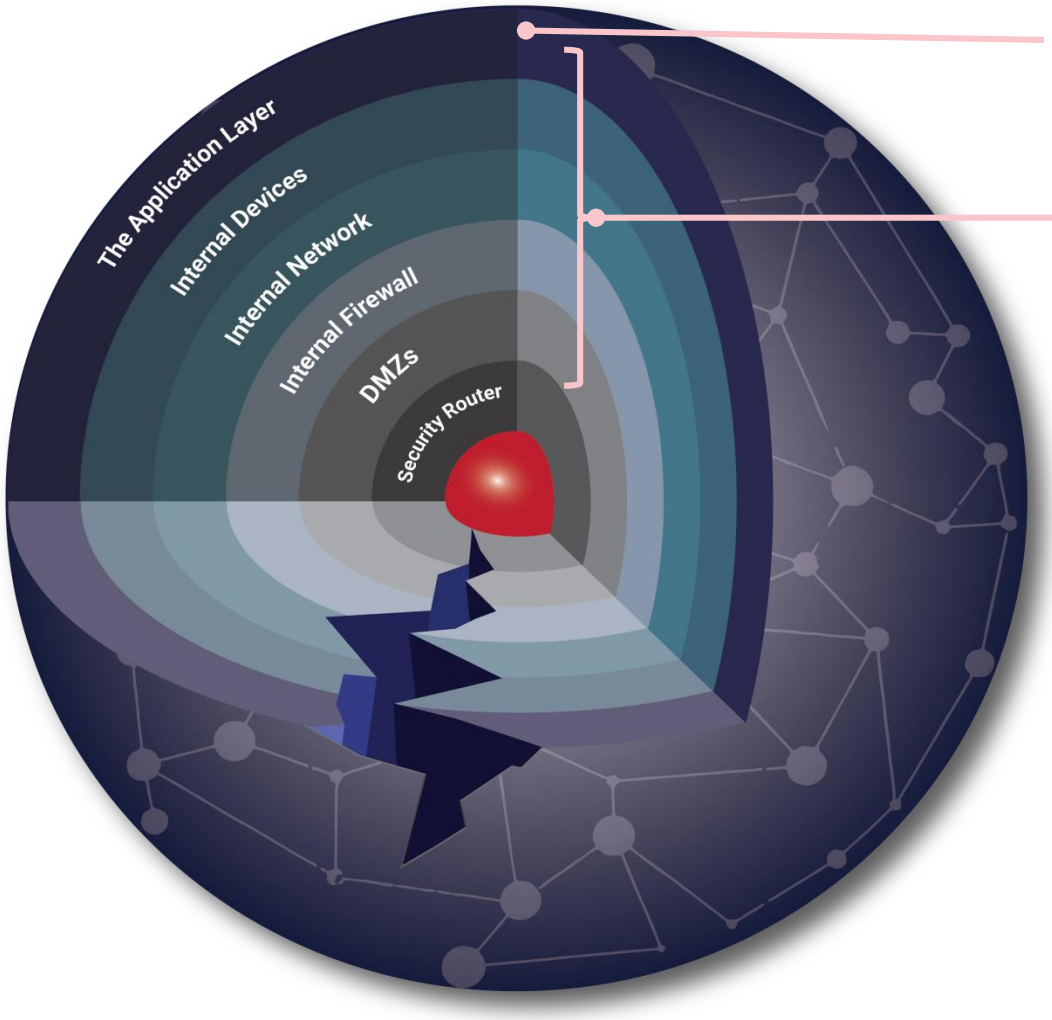


Source: SEI

© 2017 Carnegie Mellon University

Solving the Vulnerability Identification Chasm

First line of defense in software assurance is the application (software) layer



84% of breaches exploit vulnerabilities in the application[1]

Yet funding for IT defense vs. software assurance is 23 to 1[2]

1. Clark, Tim, "Most Cyber Attacks Occur from This Common Vulnerability," *Forbes*, 03-10-2015
2. Feiman, Joseph, "Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves," *Gartner*, 09-25-2014

© 2017 Carnegie Mellon University

Addressing System Sustainment

Strategic Trends Impacting Software Sustainment

- The future is software-centric…dependent…
- Advanced DoD capabilities manifested in algorithms/software
  - Autonomy, machine learning, collaborative systems, competitive networking, system resiliency, IoT, hybrid cloud computing, human-computer interaction, digital security, analytics for decision making…
  - Anticipating/adapting to new dynamic threats and requirements
- Warfighter needs coupled with technology innovation dynamics drive need for strategic enterprise focus on evolving a DoD enterprise life-cycle software strategy to be aligned with this changing environment
  - Policies
  - Current and future infrastructure capabilities
  - Business models
  - Investment strategies





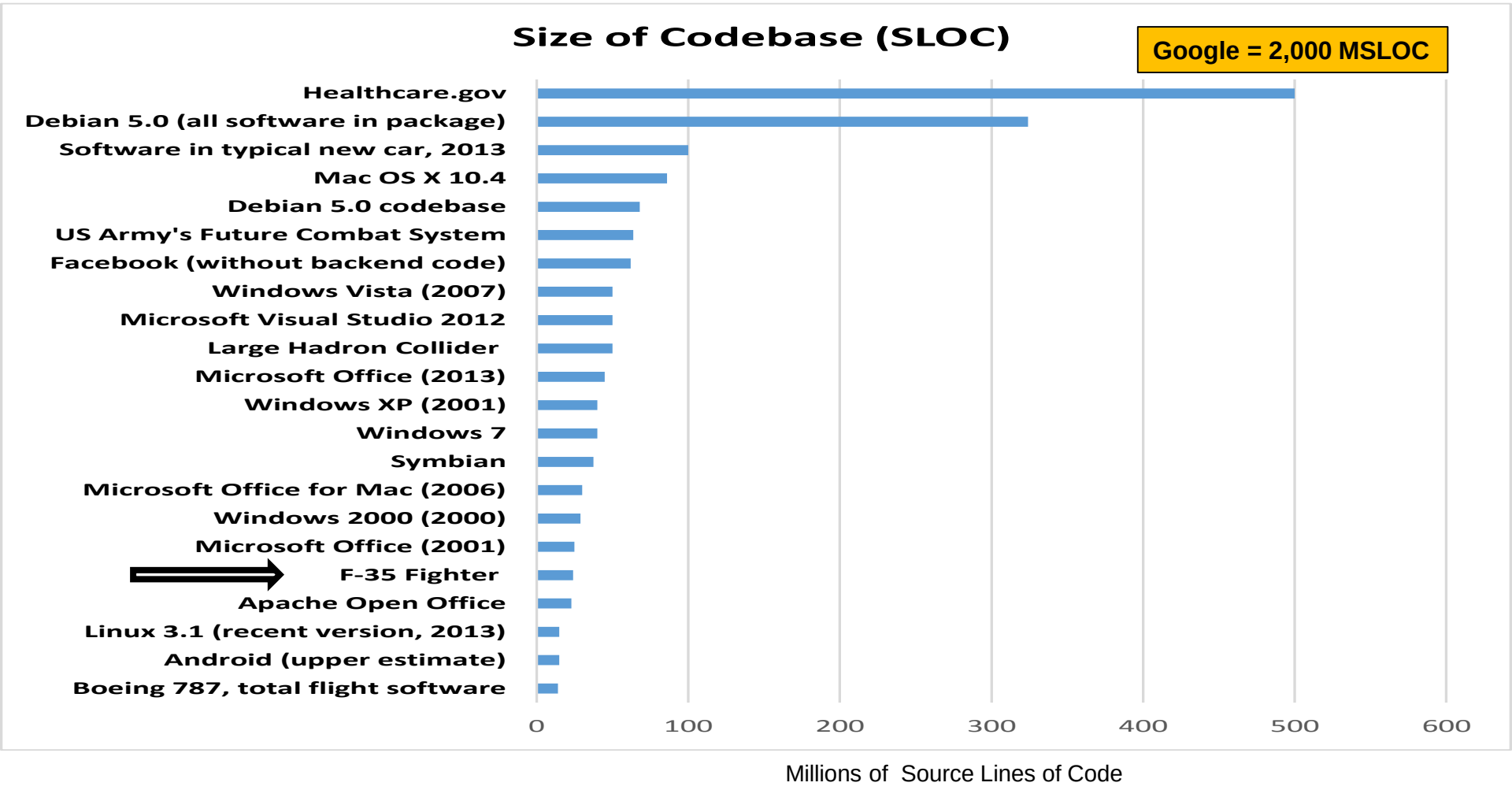




© 2017 Carnegie Mellon University

Handling the Expanding Code Base

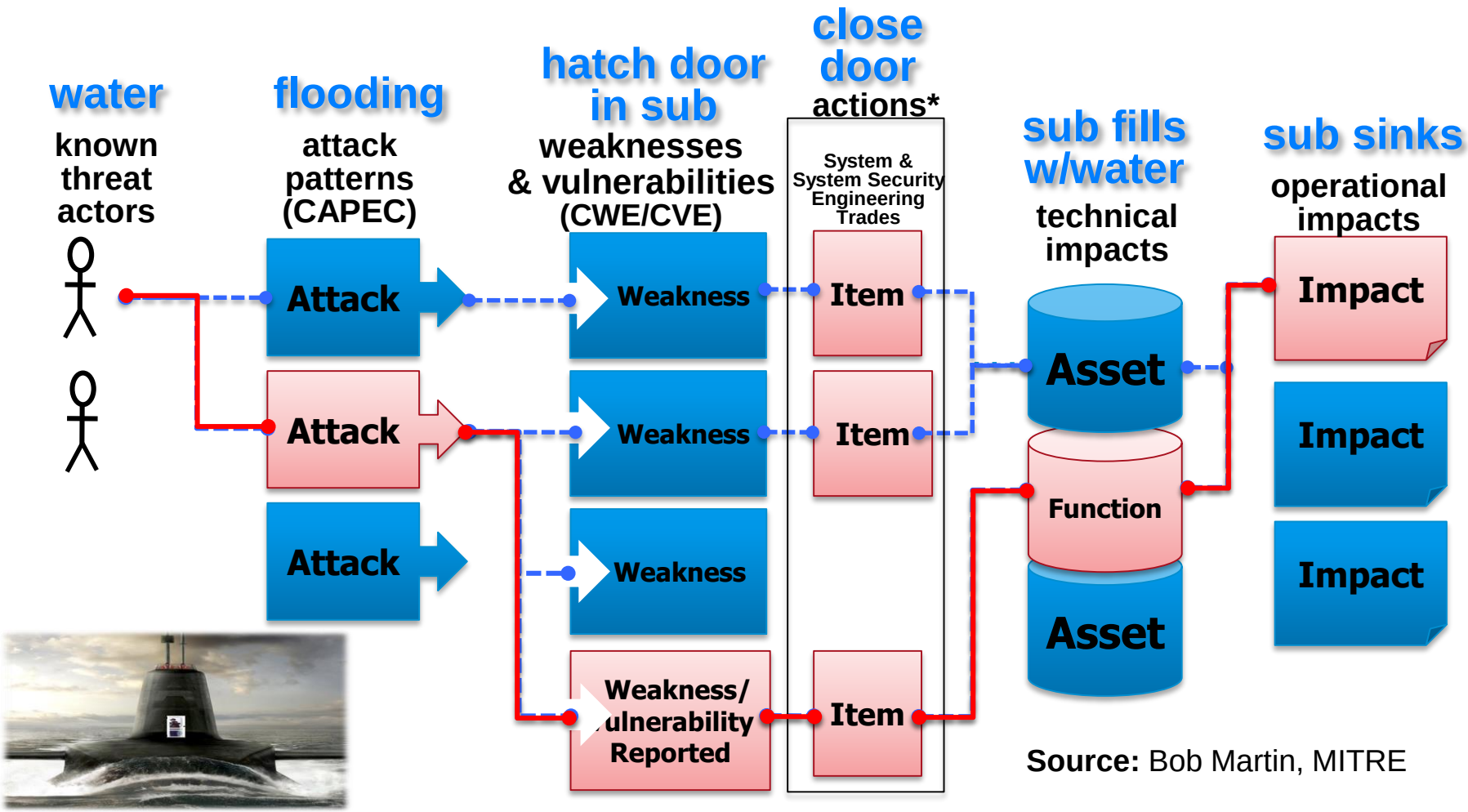
Software is dramatically expanding with limited natural governance



Source: David McCandless, “Information is Beautiful,” 21 September 2016, web retrieval

Distribution Statement A: Approved for Public Release: Distribution is Unlimited
© 2017 Carnegie Mellon University

Understanding Attack Patterns, Vulnerabilities, and Weaknesses
Defining software assurance attributes to satisfy information needs

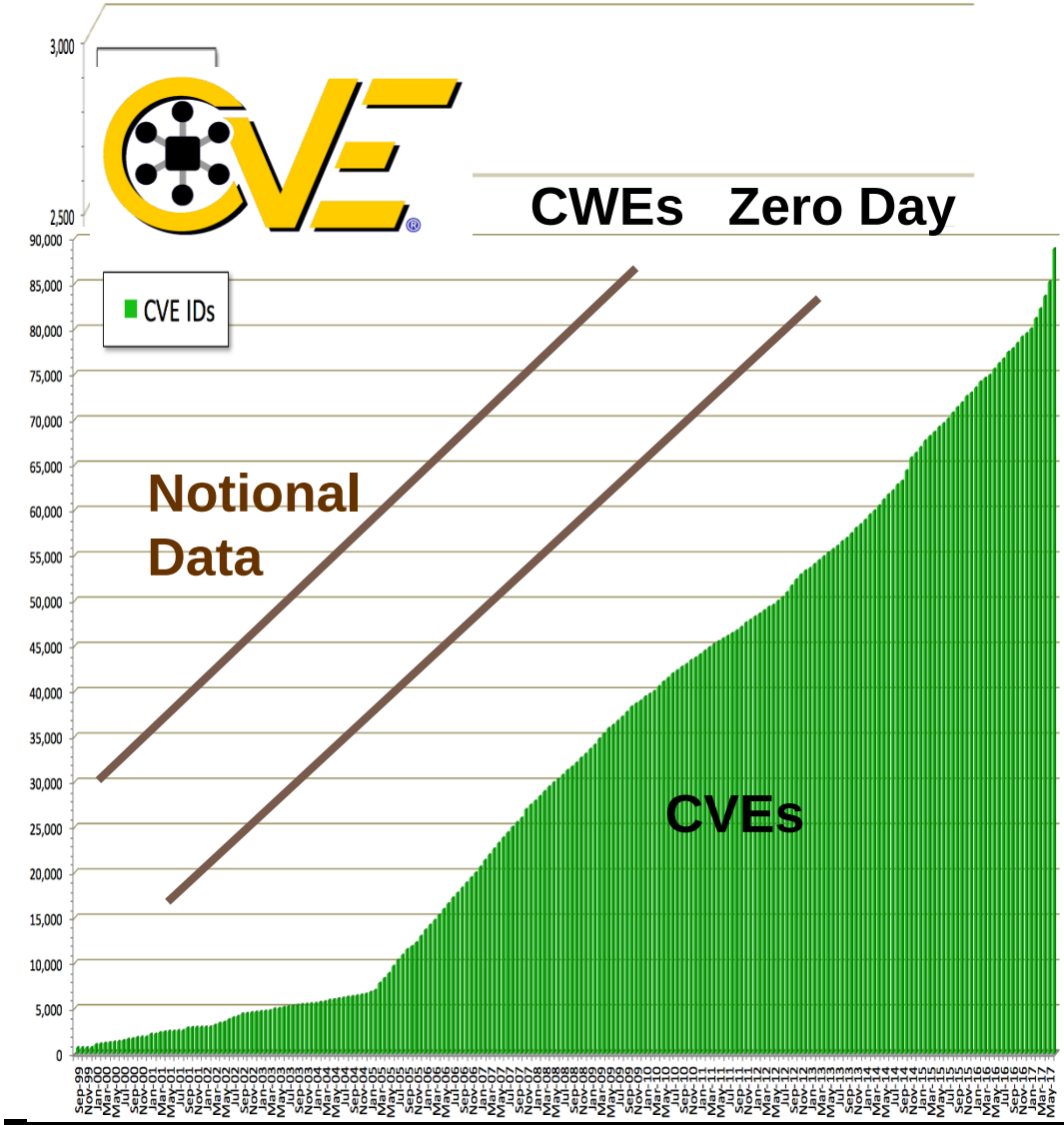


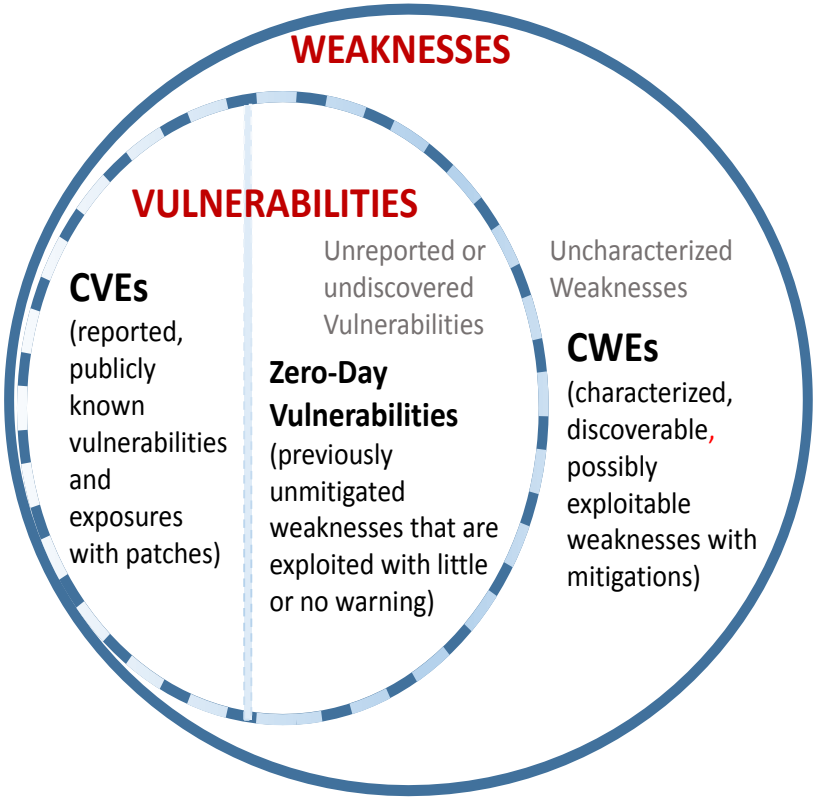
Source: Bob Martin, MITRE

- **Actions** include architecture choices; design choices; added security functions, activities, and processes; physical decomposition choices; static and dynamic code assessments; design reviews; dynamic testing; and pen testing.
- **Vulnerability** is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Distribution Statement A: Approved for Public Release; Distribution is Unlimited
© 2017 Carnegie Mellon University

Increasing Vulnerabilities: CVE 1999 to 2017, Reported Common Vulnerabilities and Exposures (CVE)

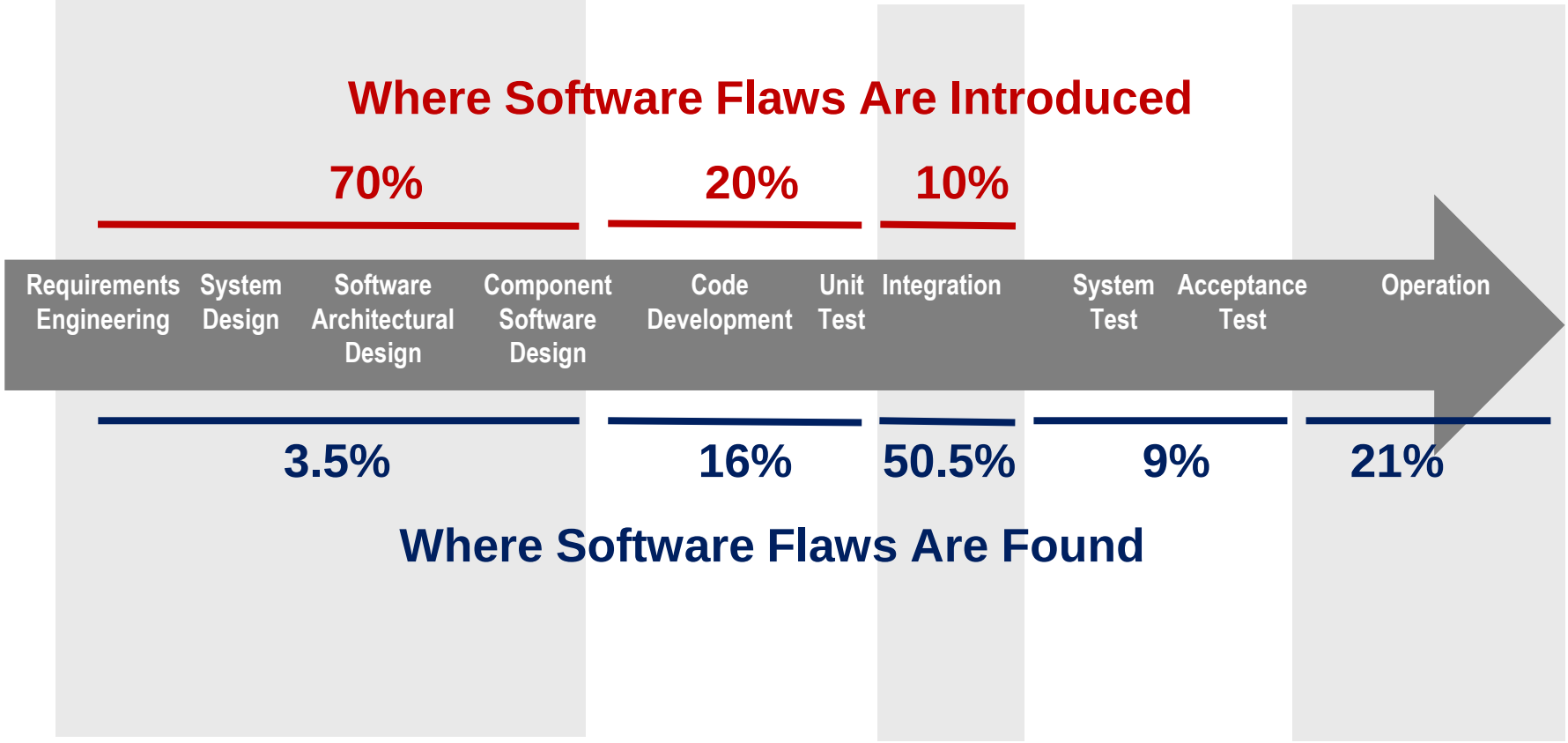




Source: Dr. Robert A. Martin, MITRE Corporation, May 2017

© 2017 Carnegie Mellon University

Designing-in Software Assurance Throughout the System Life Cycle

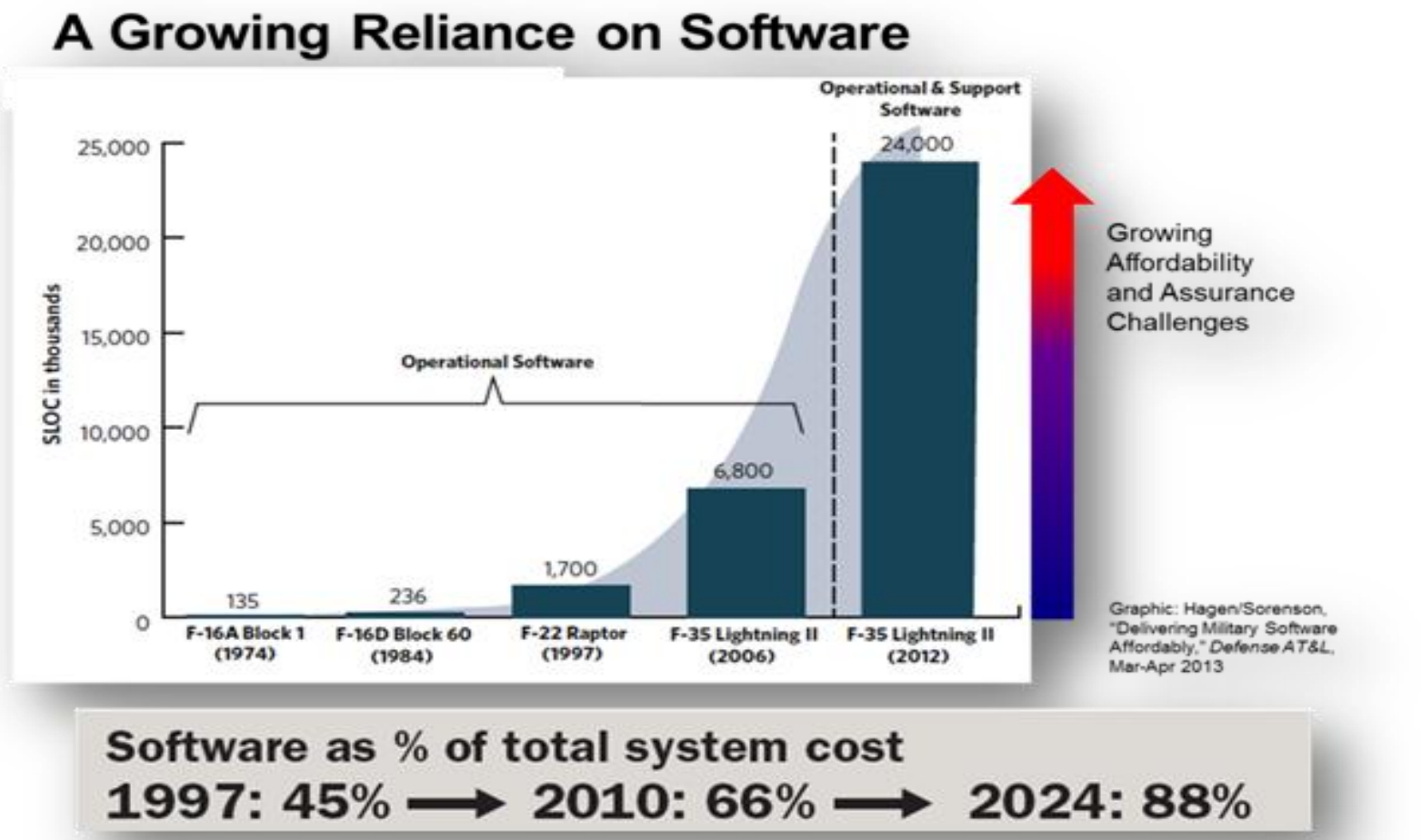


Special emphasis needed up-front in the system life cycle

Sources: *Critical Code*, NIST, NASA, INCOSE, and Aircraft Industry Studies

© 2017 Carnegie Mellon University

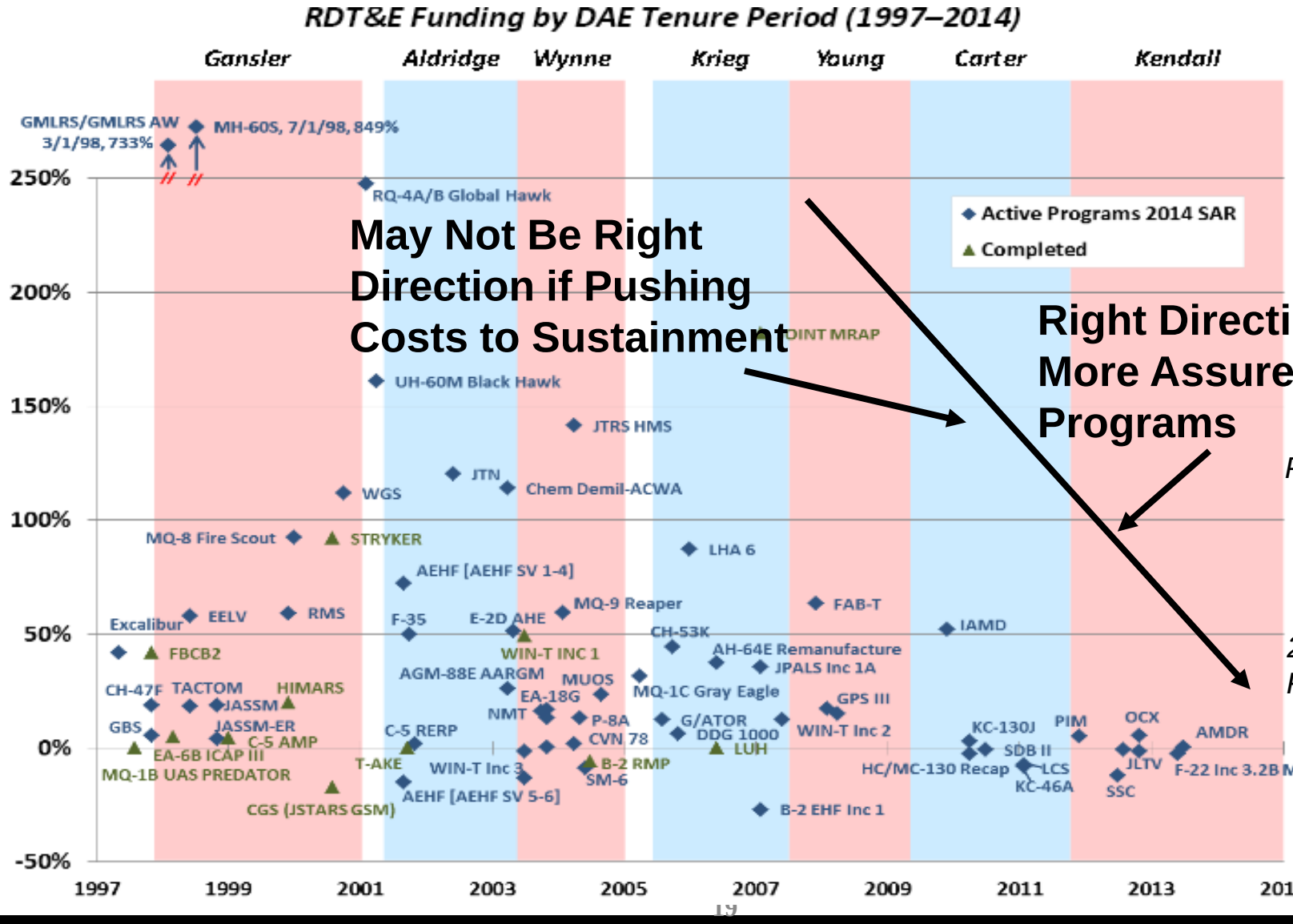
Reducing Technical Debt Over the System Life Cycle



Source: U.S. Air Force Scientific Advisory Board. *Sustaining Air Force Aging Aircraft into the 21st Century* (SAB-TR-11-01). U.S. Air Force, 2011.

© 2017 Carnegie Mellon University

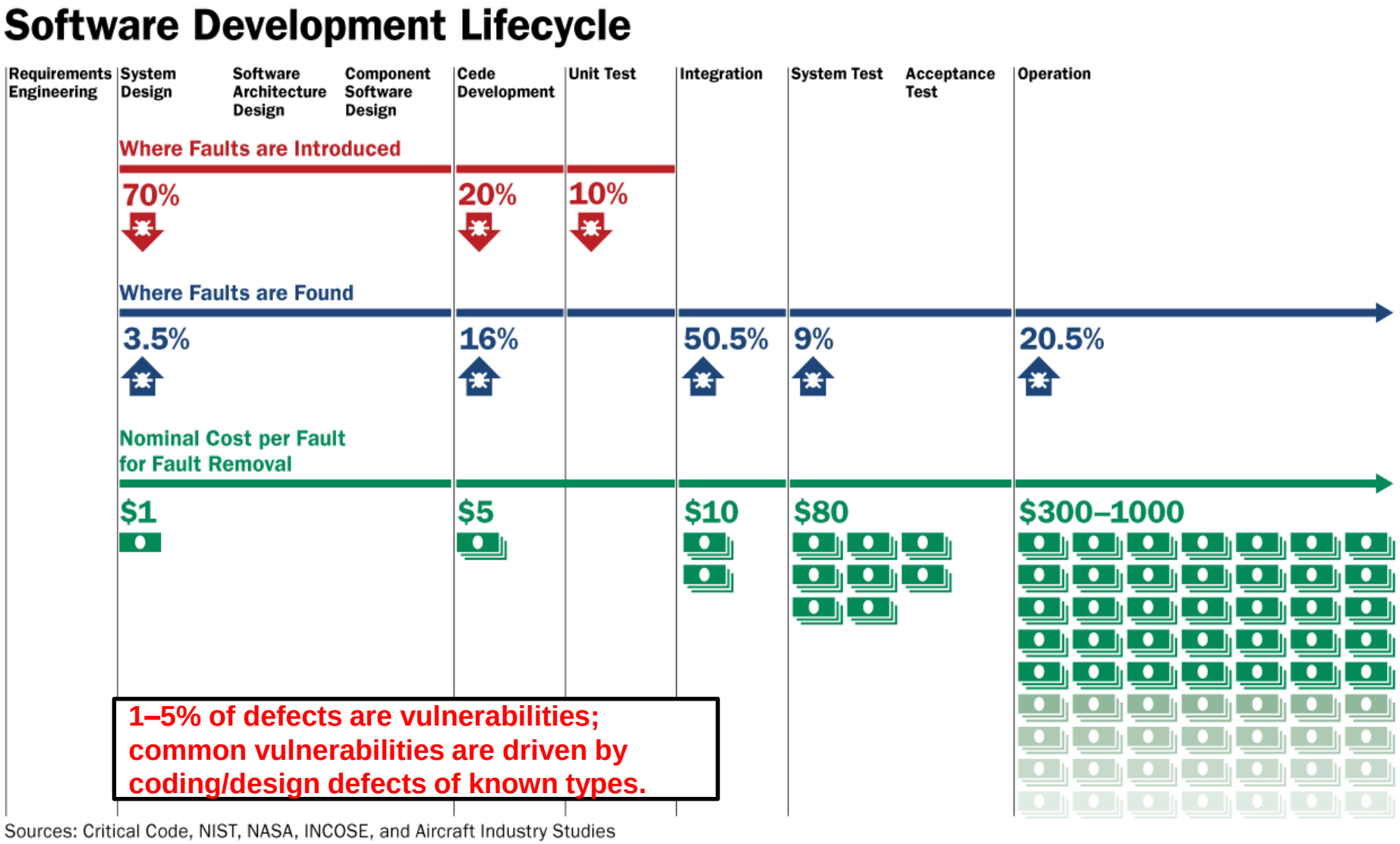
Reducing Technical Debt



Source: *Performance of the Defense Acquisition System 2015 Annual Report*, Sep. 16, 2015

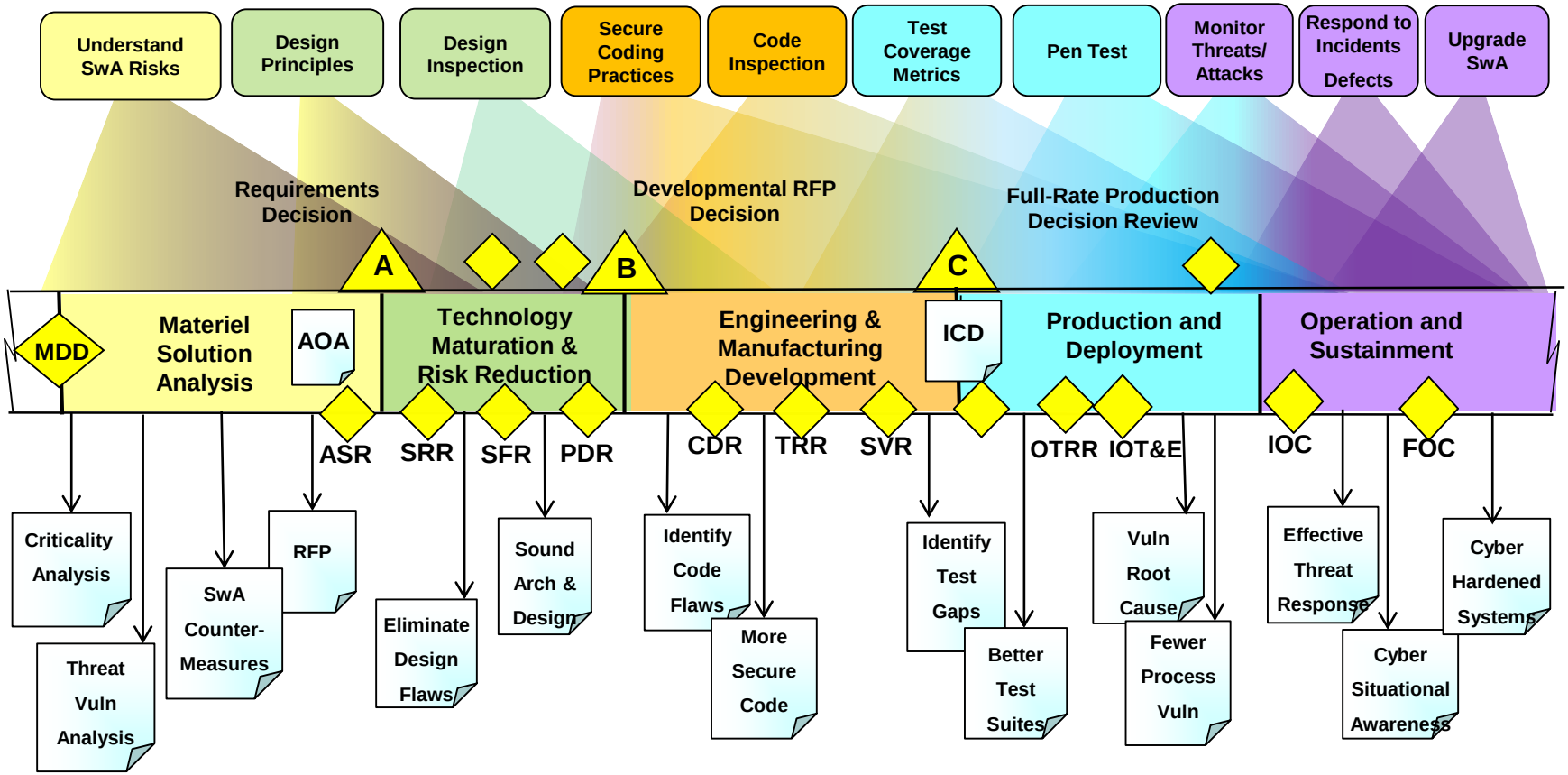
© 2017 Carnegie Mellon University

Reducing Technical Debt



© 2017 Carnegie Mellon University

Reducing Technical Debt: Engineering-in Software Assurance Activities Across the Life Cycle



DoD PM's Guidebook for Integrating Software Assurance Engineering Activities into the Systems Acquisition Lifecycle (Being Developed)

Distribution Statement A: Approved for Public Release; Distribution is Unlimited
© 2017 Carnegie Mellon University

Working in the Infancy of the Software Engineering Discipline

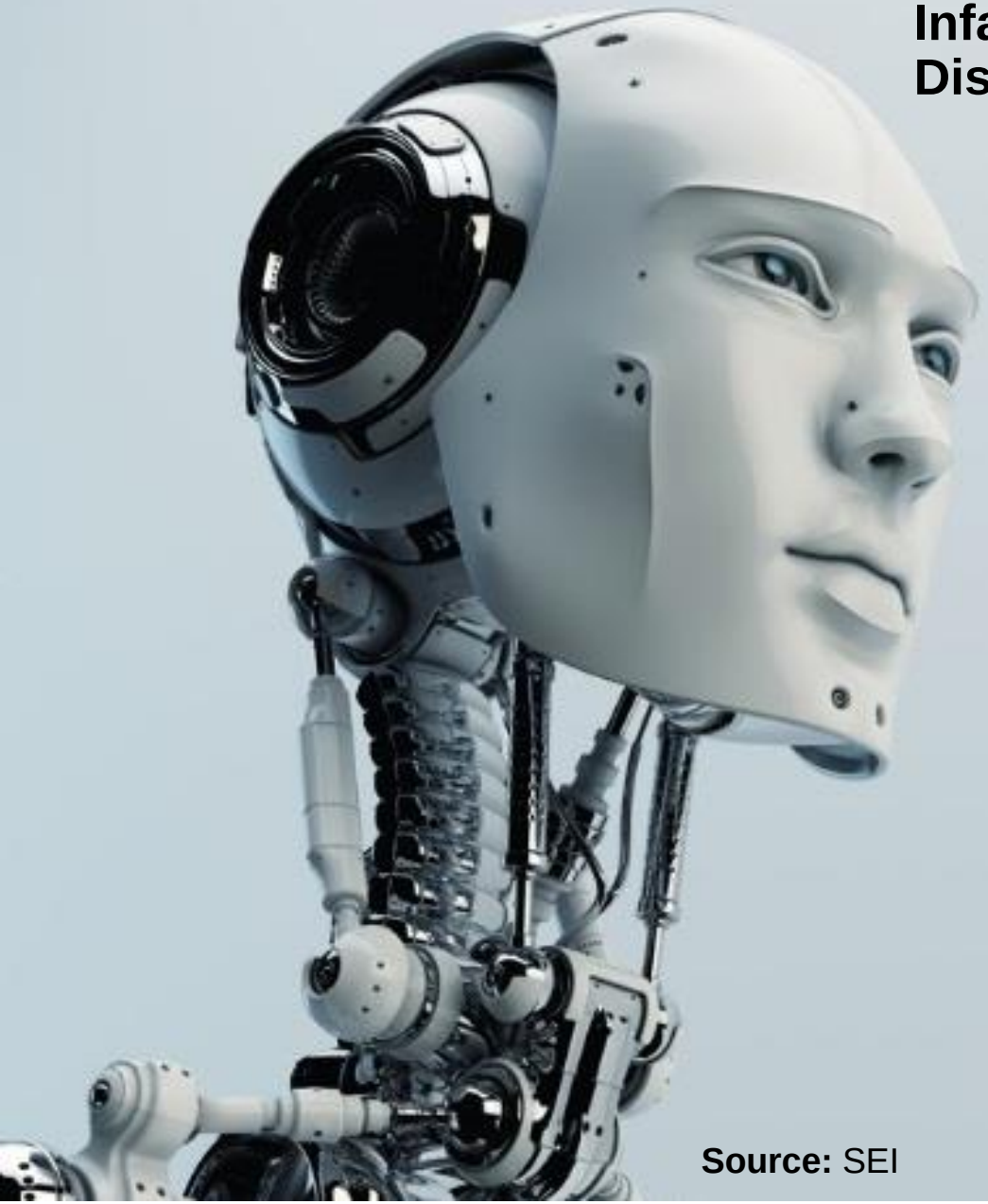
Improving the workforce by developing software core competencies and a DoD career field in software engineering

	Physical Science	Bioscience	Computer/Software/Cyber Science
Origins/History	Begun in antiquity	Begun in antiquity	Mid-20th century
Enduring Laws	Laws are foundational to furthering exploration in the science	Laws are foundational to furthering exploration in the science	Only mathematical laws have proven foundational to computation
Framework of Scientific Study	Four main areas: astronomy, physics, chemistry, and earth sciences	Science of dealing with health maintenance and disease prevention and treatment	• Several areas of study: computer science, software/systems engineering, IT, HCI, social dynamics, AI • All nodes are attached to and rely on a netted system
R&D and Launch Cycle	10–20 years	10–20 years	Significantly compressed; solution time to market must happen very quickly

HCI: human–computer interaction; AI: artificial intelligence

Source: SEI

© 2017 Carnegie Mellon University



Source: SEI

Infancy of Software Engineering Discipline: Human-Machine Teaming

In the real world, autonomy is usually granted within some context—explicit or implicit

- parents and children
- soldiers, sailors, marines, and airmen

How do we do this for machines?

- Explicit may be easy, but implicit is hard for machines
- Commander's intent
- Mission orders

Related to need for explainability and predictability

© 2017 Carnegie Mellon University

So Where Does This Lead Us?

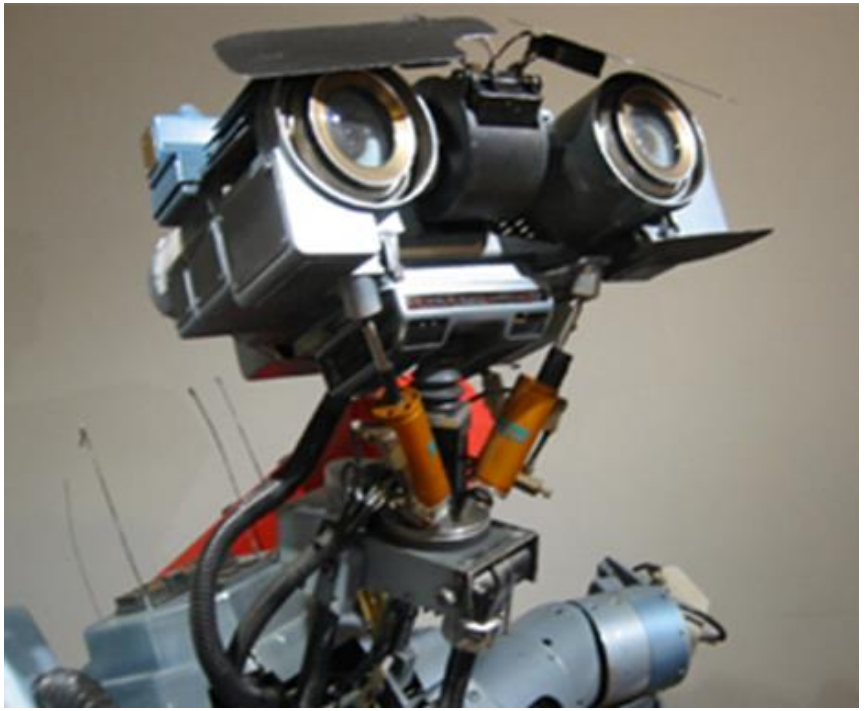
- A more robust software assurance approach will be needed…
- Decision makers will need insight and understanding about how to achieve software assurance
- As software-dominated system projects become larger in scope/complexity, capitalizing on opportunities for making better decisions will become more important
  - Critical to shift from asking “what happened?” which is a question of information based on sparse data
  - To seeking insight by asking “what happened, why, how do we solve the problem, and can we evaluate that it has been solved?”
- Enabling an engineering-based approach that seeks to design-in software assurance is becoming more important
- DoD workforce needs a software engineering career field that includes software assurance core competencies

Distribution Statement A: Approved for Public Release; Distribution is Unlimited
© 2017 Carnegie Mellon University

Final Thought: Advanced Software Engineering with Operational Participation

Will determine if we create C-3PO and Johnny 5 . . .





Source: SEI

© 2017 Carnegie Mellon University

…or the Borg



Source: SEI

© 2017 Carnegie Mellon University

Contact Information



Dr. Kenneth E. Nidiffer, Director of Strategic Plans for Government Programs

Software Engineering Institute

Carnegie Mellon University

Office: + 1 703-247-1387

Fax: + 1 703-908-9235

Email: Nidiffer@sei.cmu.edu



Distribution Statement A: Approved for Public Release: Distribution is Unlimited

© 2017 Carnegie Mellon University

SYSTEMS ENGINEERING RESEARCH CENTER

Georgia Tech Research Institute

Introducing Cyber Resiliency Concerns Into Engineering Education

Mr. Tom McDermott
Georgia Tech Research Institute

Mr. Barry Horowitz
University of Virginia

NDIA 20th Annual Systems Engineering Conference
26 October 2017

Springfield, Virginia

SERC RT 175: Human Capital Development – Resilient Cyber-Physical Systems

- Principal Investigators: Tom McDermott (GT) and Barry Horowitz (UVA)
  01 March – 30 September 2017

- Scope
  - Characterize the existing undergraduate and graduate engineering and computer science education programs in the U.S. as related to emerging needs of large scale cyber-physical systems
  - Develop a taxonomy of related attributes for dependable and secure computing, and
  - conduct a survey of related undergraduate and graduate education programs and lab facilities in the fields of information security, computer science, computer engineering, and electrical engineering
  - identify the challenges for:
    - Developing a body of knowledge for resilient cyber-physical systems,
    - Developing a reference curriculum for SE of resilient cyber-physical systems and resilient computing systems, and
    - Needs and opportunities for developing potential lab facilities.

SYSTEMS ENGINEERING RESEARCH CENTER

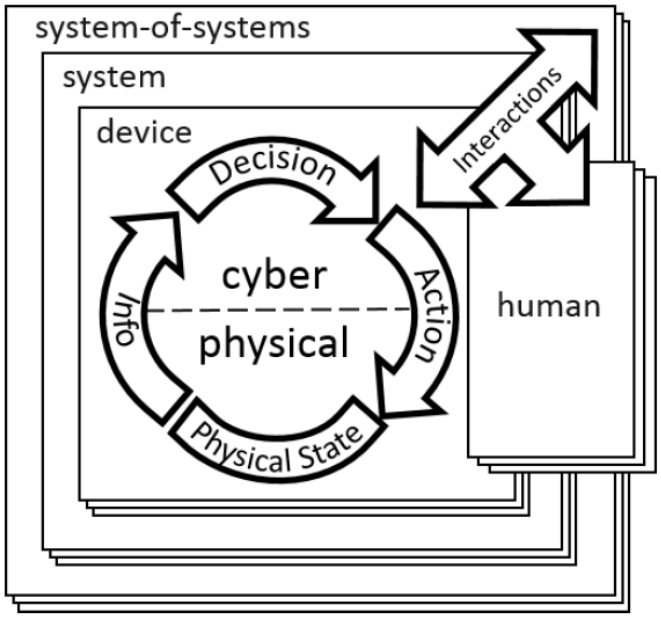
RT 175: Human Capital Development – Resilient Cyber-Physical Systems

- Within the context of military cyber operations and threats, CPS resilience can be interpreted as "the ability of a system to maintain its operational mission effectiveness while under adversary offensive cyber operations, and to manage the risk of adversary exploitation of the system for intelligence purposes." (Holtzman, 2017)

- "…considering large, networked, evolving, systems either fixed or mobile, with demanding requirements driven by their domain of application...these emerging systems suffer from a significant drop in dependability and security in comparison with the former systems" (EU-ReSIST project)

- "Core CPS knowledge involves not only an understanding of the basics of physical engineering and cyber design and implementation, but understanding how the physical and cyber aspects influence and affect each other…Because CPS engineering centers on the interaction of physical and cyber aspects of systems, it will often not be sufficient to create CPS curricula by simply combining material from existing courses." (NAP 2016)

What is a CPS?



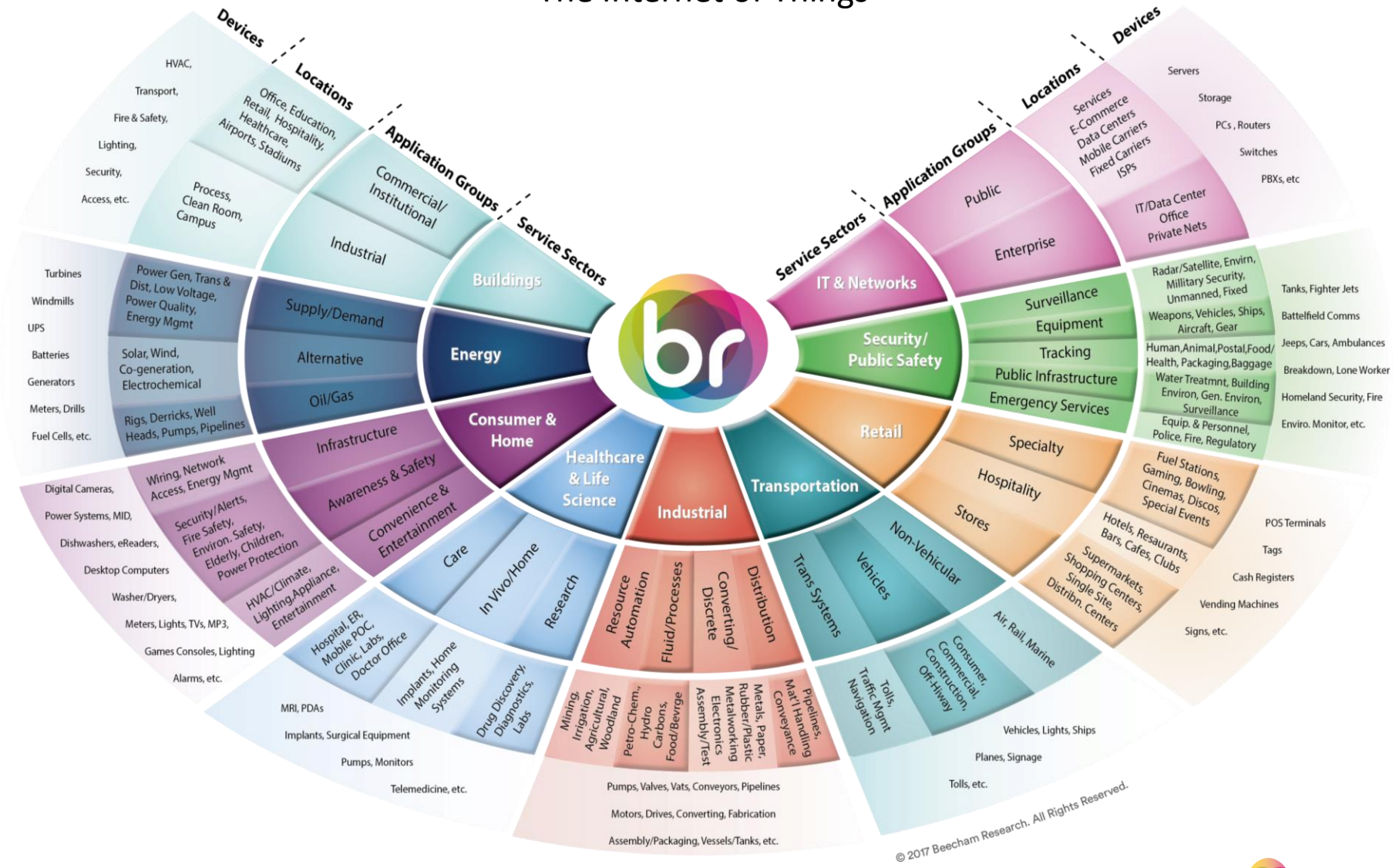
NIST CPS Conceptual Model

- "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components" (NSF)
- "computers and networks which control physical processes, using feedback loops that affect computations and vice versa" (UC Berkeley)

NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview Version 1.0

M2M World of Connected Services

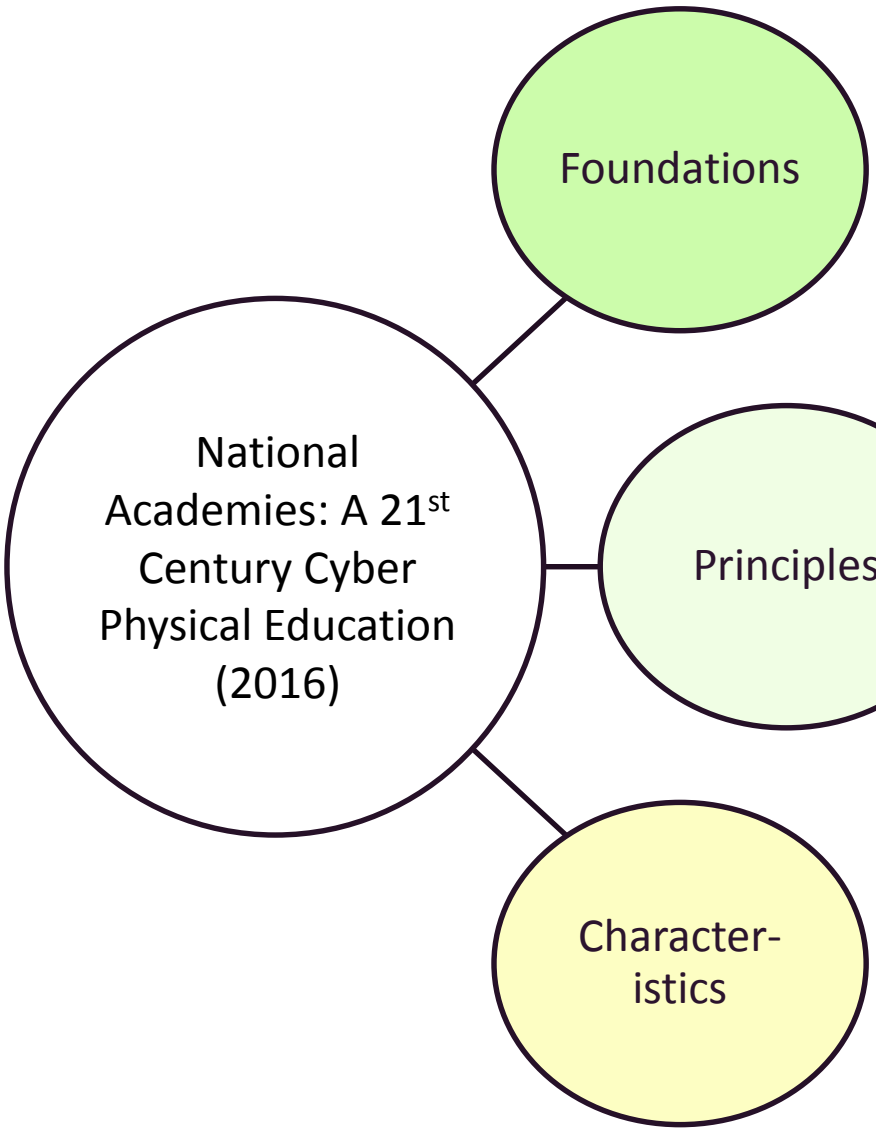
The Internet of Things



http://www.beechamresearch.com/

beecham research

Taxonomy of CPS Competencies

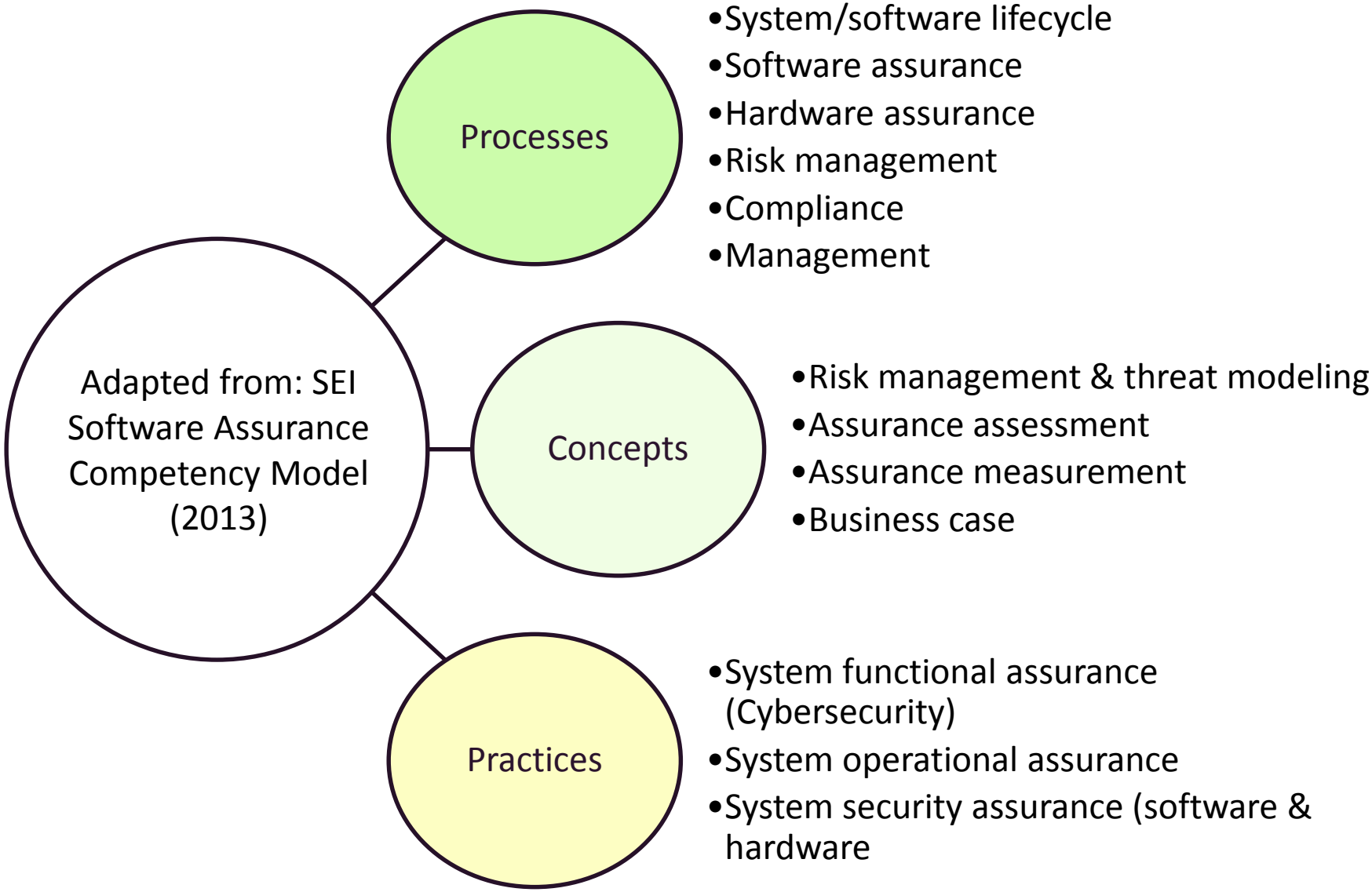


- Basic computing concepts
- Physical world computing properties & constraints
- Cross-cutting applications
- Modeling Dynamic Control processes
- System lifecycle development

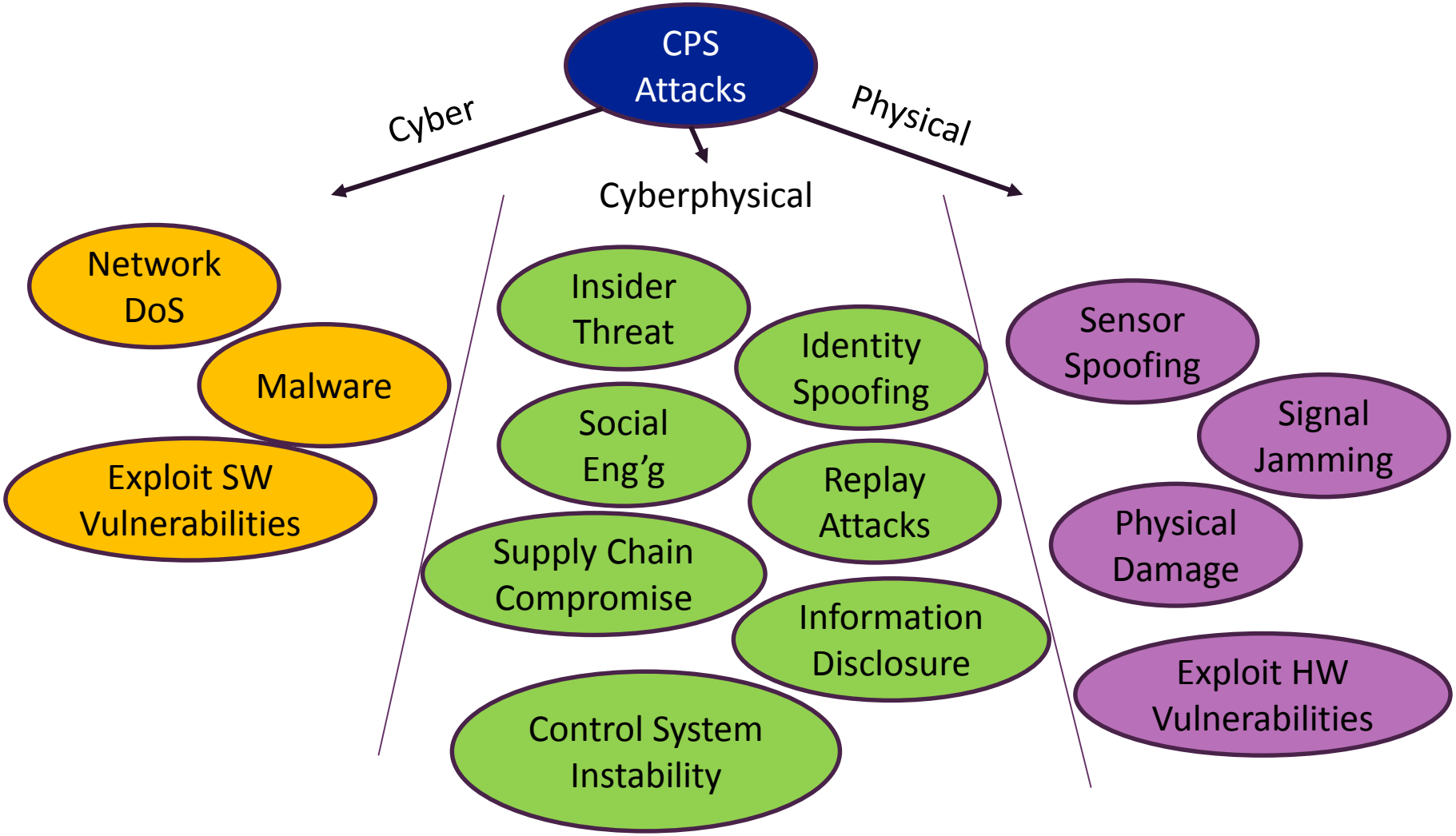
- Communications and networking
- Real-time operation
- Distributed & embedded systems
- Physical properties
- Human interaction

- Dependability
- Security and privacy
- Power and energy
- Safety
- Stability and performance
- Human factors and usability

Taxonomy of Assurance Competencies

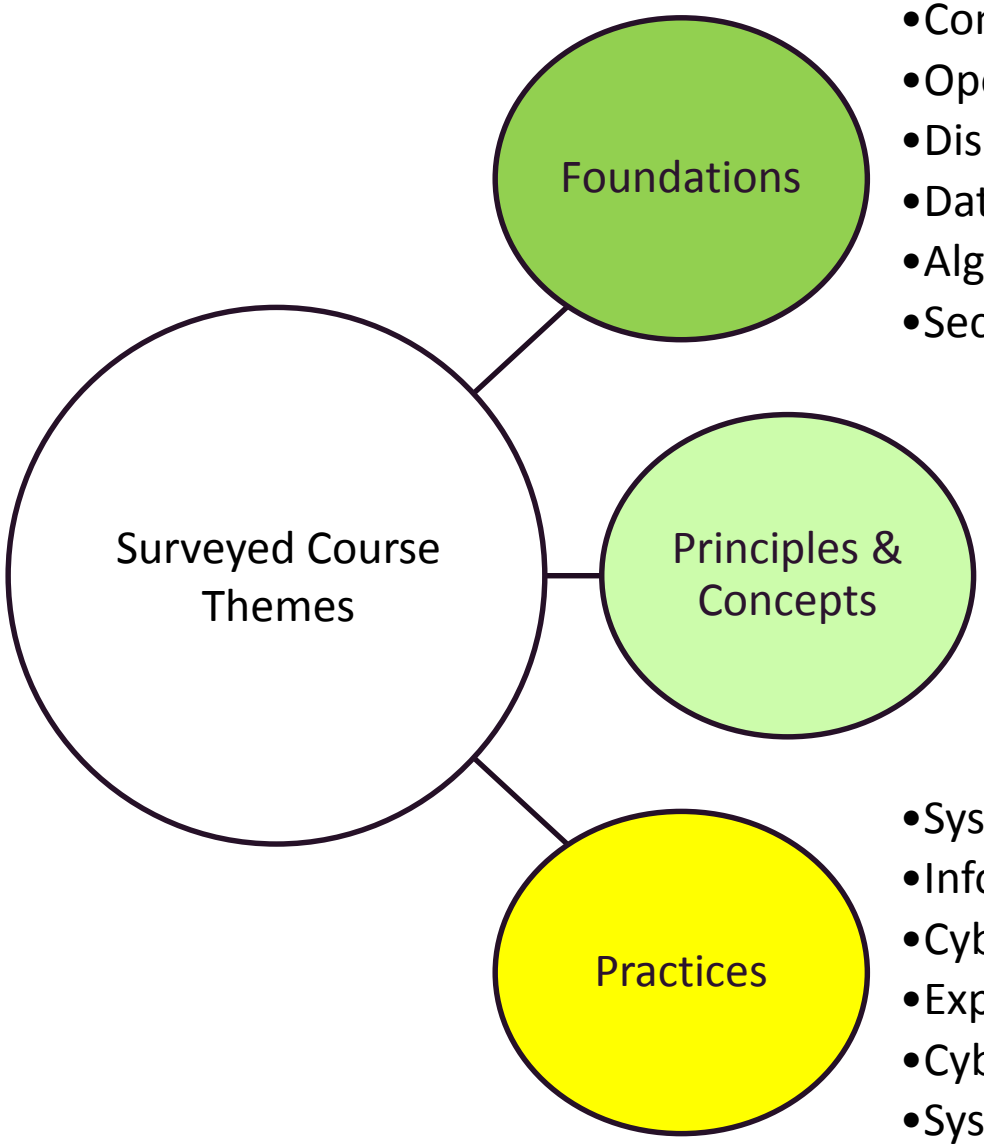


CPS Attack Taxonomy



Because cyber-physical systems consist of both cyber and physical systems, the attack surface, when compared, to either cyber or physical systems solely, is much larger

Derived CPS Security Education Themes

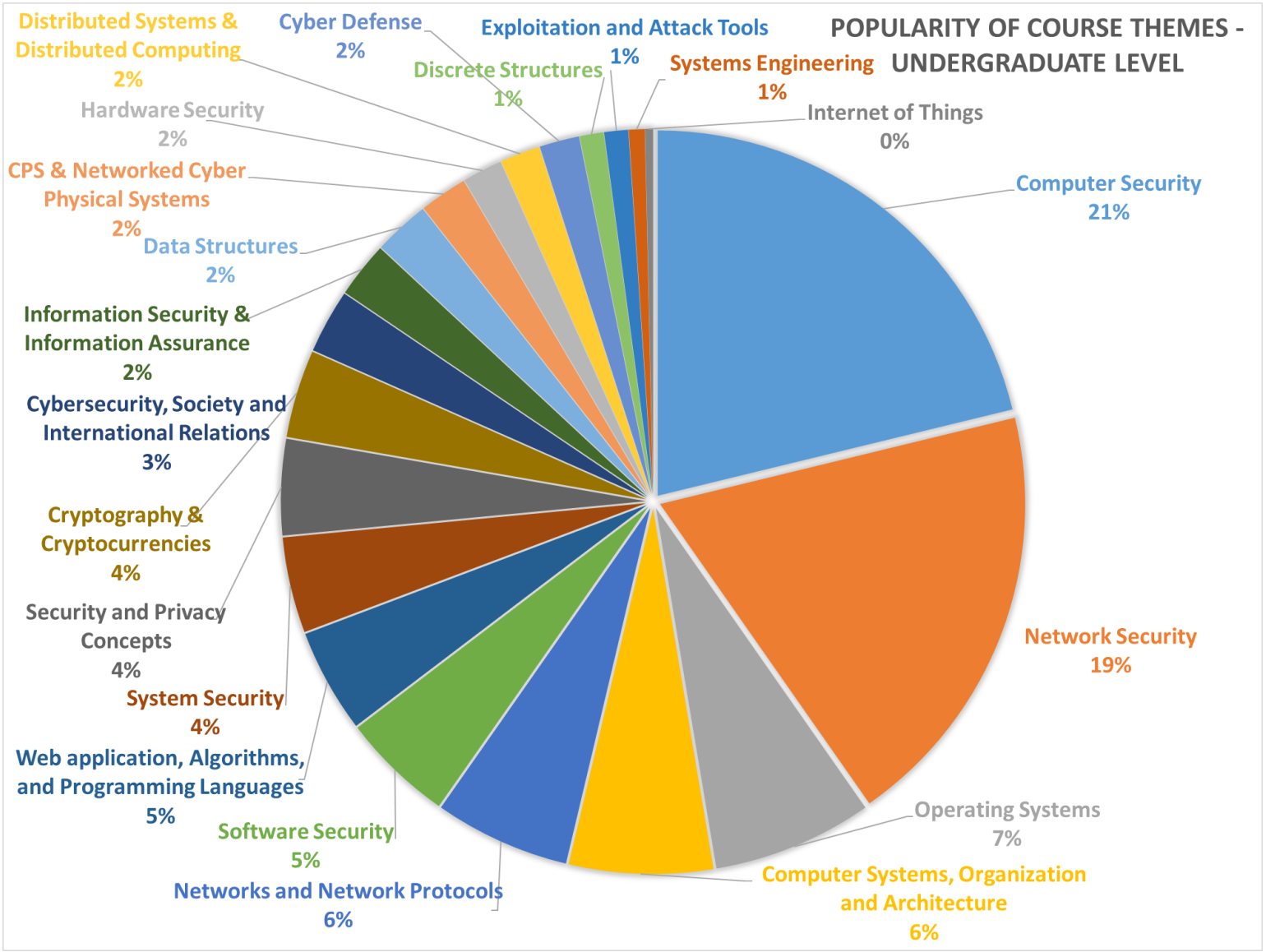


- Computer Architecture
- Operating Systems
- Discrete Structures
- Data structures
- Algorithms & Programming
- Security & Privacy Concepts

- Computer Security
- Network Security
- Networks & Network Protocols
- Cryptography
- Distributed Systems & Computing
- Cyberphysical Systems

- System, HW & SW Security
- Information Security & Assurance
- Cybersecurity & Society
- Exploitation & Attack Tools
- Cyber Defense
- Systems Engineering

Survey of 104 Universities by Course Themes



SYSTEMS ENGINEERING RESEARCH CENTER

Degree & Certificate Programs with Security Themes



Across 104 U.S. Universities

- 3 undergraduate
- 17 graduate
- 11 certificate

A Prototype Professional Education Course

- Underlying concepts for applying resilience-based solutions to cyber security defense
- System-Aware Cybersecurity & Experiments with Technology Prototypes
- Fault Tolerant Systems Design Principles
- Attack Trees
- Attack Taxonomy
- Cybersecurity-related Human Factors Issues
- Project Plan - Hands-on laboratory exercise
- Hands-on attack laboratory activity
- Hands-on decision support tool laboratory activity
- Presentations of Individual Team Exercise Results and Class Evaluation of Results
- Summary and Discussion

Inspiration for a Sharable CPS Security Laboratory



- CPS platforms remotely interfaced and accessible via web browsers or a cloud-based environment
- a software simulator to run first operations in a virtual environment and then transition to hardware experiments
- A framework to overwrite any unsafe situation and reset the system needs to be in place

Recommendations

- The future CPS workforce needs to include a combination of
  - —engineers trained in foundational fields (such as electrical and computing engineering, mechanical engineering, systems engineering, and computer science),
  - —engineers trained in specific applied engineering fields (such as aerospace and civil engineering),
  - —and CPS engineers, who focus on the knowledge and skills spanning cyber technology and physical systems that operate in the physical world
- Consider establishing one or two new cyber physical system resilience education efforts that build upon the study outcomes
- Model-based engineering techniques combined with physical labs would provide students with a greater understanding of the engineering efforts required to both derive and evaluate possible CPS security solutions

Recommendations

- Additional funding and attention must be delegated to research and projects in CPS
  - More research into CPS security and dependability must occur in university lab environments
  - Appropriate use cases for new educational-focused laboratories will need to be developed
- Due to issues associated with DoD information security sensitivities and industry proprietary solution sensitivities, appropriate use cases for new educational-focused laboratories will need to be developed
- A network of CPS Labs accessible to all is a worthy model

Shaping the Department of Defense Engineering Workforce

Ms. Aileen Sedmak

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 26, 2017

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Organic Engineering Workforce Importance

A competent organic engineering workforce across the Defense ecosystem is needed:

- **To retain United States' technological superiority over our adversaries**
- **To identify and mitigate program risks**
- **To efficiently and effectively engineer and deliver complex, flexible systems to our warfighters that adapt and are resilient to evolving missions and threats**

DoD and Industry collaboration is crucial to proactively manage organic engineering capability and competence

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

DoD R&E Ecosystem

Engaging with all partners to ensure technological superiority



Win today's fight



Design and acquire for the next fight

R&E Ecosystem

Global Partners

Academia and Industry Partners

FFRDCs and UARCs

DoD Laboratories, Engineering and Warfare Centers



Force acceleration of science and engineering – driving ideas to capability

FFRDC Federally Funded R&D Center
UARC University Affiliated Research Center

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Our Common Challenge

"Right now…there is a sufficiency of engineers, but one of our greatest industrial organizations, after careful study, predicts the entire absorption of this group by the end of 1936, with a probable shortage of available engineers at that time."

— Collins P. Bliss, dean of New York University's College of Engineering, **1934**

"With mounting demands for scientists both for teaching and for research, we will enter the postwar period with a serious deficit in our trained scientific personnel."

— Vannevar Bush, director of the U.S. Office of Scientific Research and Development, **1945**

"Our national welfare, our defense, our standard of living could all be jeopardized by the mismanagement of this supply and demand problem in the field of trained creative intelligence."

— James Killian, president of MIT, **1954**

"From 1972 through 1975, the expected demand for engineers will exceed not only the supply coming from American engineering schools, but also the combined supply from the United States and foreign countries, according to the [Engineering Manpower Commission] estimates."

— John W. Graham Jr., president of Clarkson College of Technology, **1970**

"The electronics and information technology industries will be short more than 100,000 electrical and computer science engineers over the next five years."

— American Electronics Association, **1983**

"Already spot shortages exist in some science fields in the United States, and unless dramatic changes are made in the way we educate all of our students, including our most talented, the shortages will increase."

— U.S. Office of Educational Research and Improvement, **1993**

"U.S. companies face a severe shortfall of scientists and engineers with expertise to develop the next generation of breakthroughs."

— Bill Gates, chairman of Microsoft, **2008**

"There is a skills gap in this country—for every unemployed person in the United States, there are two STEM job postings. The gap will only widen if we don't engage now to address STEM education at the elementary and high school levels."

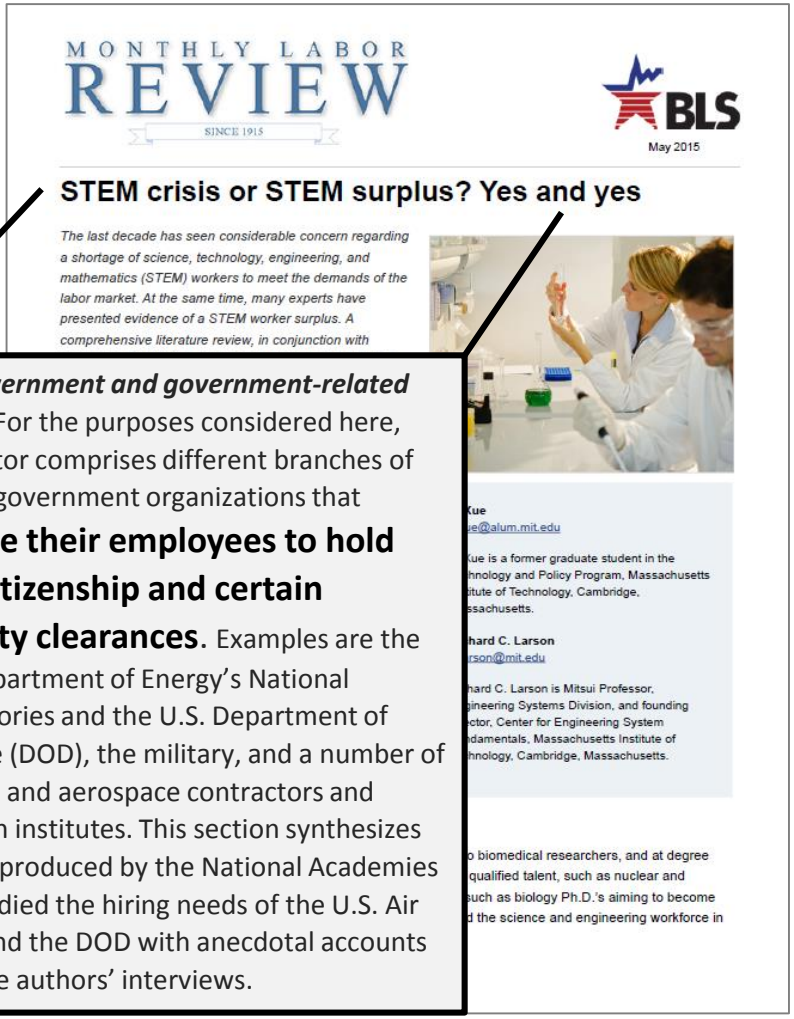
— Richard K. Templeton, chairman, president, and CEO of Texas Instruments, **2013**

Our STEM workforce challenge isn't a recent phenomenon, but can be traced back decades

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Our Common Challenge

In the May 2015 *Bureau of Labor Statistics (BLS)* study "STEM crisis or STEM surplus? Yes and yes," the government and government-related sector were grouped together because of their common need for "employees to hold U.S. citizenship and certain security clearances."


MONTHLY LABOR REVIEW
SINCE 1915
BLS
May 2015
STEM crisis or STEM surplus? Yes and yes
The last decade has seen considerable concern regarding a shortage of science, technology, engineering, and mathematics (STEM) workers to meet the demands of the labor market. At the same time, many experts have presented evidence of a STEM worker surplus. A comprehensive literature review, in conjunction with

The government and government-related sector. For the purposes considered here, this sector comprises different branches of civilian government organizations that **require their employees to hold U.S. citizenship and certain security clearances**. Examples are the U.S. Department of Energy's National Laboratories and the U.S. Department of Defense (DOD), the military, and a number of defense and aerospace contractors and research institutes. This section synthesizes reports produced by the National Academies that studied the hiring needs of the U.S. Air Force and the DOD with anecdotal accounts from the authors' interviews.

Our "different" workforces come from the same pool of clearable talent

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

BLS Identified STEM Shortages

- **Shortages realized in specific areas within the Government and Government-related sector**
  - Systems Engineering
  - Cybersecurity
  - Material Science
  - Nuclear Engineering
- **Deficits observed for clearable candidates due to**
  - U.S. citizenship requirement
  - Early legal infractions making potential candidates un-clearable

We are working to mitigate gaps but can do a lot more with your partnership

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-#### applies. Distribution is unlimited.

DoD Organic Engineering Talent Management

- **DASD(SE) promotes organic engineering talent management discussions on current workforce challenges and cross-cutting initiatives**
  - First meeting held 29 November 2016, where Services identified the following common skill / competency gaps:
    - Systems Engineering
    - Cybersecurity
    - Digital Engineering
- **Services continue to assess their needs / gaps; Progress to date will be reported at next meeting in November 2017**

OSD can advocate/support mitigations at the enterprise level

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Technical Edge Project

Technical Edge



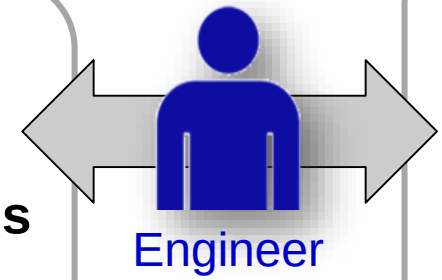
New or Emerging Technologies



Advanced Techniques



Novel Approaches



DoD systems to maintain technological superiority and military advantage

- Identify emerging technologies, techniques, approaches
- Determine engineering skills and competence needed to implement the "Technical Edge"
- Assess whether DoD has appropriate expertise
- Identify how to educate/train our engineers to fill expertise needs and avoid gaps

One of our challenges is keeping the workforce fluent in the latest advances

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Emerging Technologies

Top Technologies Identified Through Tech Edge Project
Autonomy – human machine interface
Robotics
Cybersecurity – system security
Cybersecurity – assessment
Alternative Fuels / Energy Storage
Directed Energy Weapons
Trusted Circuits
Model-Based Systems Engineering
Inertial Navigation Systems
Lightweight Materials

How do we ensure our workforce has competence in these technical areas?

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-#### applies. Distribution is unlimited.

Our Common Future

- **Opportunity exists to investigate and address shared workforce challenges**
- **Currently engaging with Aerospace Industries Association (AIA) in a Workforce Roundtable and would benefit from National Defense Industrial Association (NDIA) participation**
- **Through a broader collaboration base, we can identify common key talent gaps and devise solutions that benefit the overall Defense ecosystem**

Take advantage of the opportunity to improve talent management

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

For Additional Information

Ms. Aileen Sedmak

ODASD, Systems Engineering

703-695-6364

aileen.g.sedmak.civ@mail.mil

Distribution Statement A – Approved for public release by DOPSR. Case # 18-S-0013 applies. Distribution is unlimited.

How Can We Use Verification and Validation (V&V) Techniques in Early Systems Engineering?

STEVEN H. DAM, PH.D., ESEP
CHRIS RITTER
SPEC INNOVATIONS
STEVEN.DAM@SPECINNOVATIONS.COM



Outline

1. V&V in the Early Stages of the Lifecycle?
2. Ontology for V&V
3. What's a Verifiable Requirement?
4. Developing a V&V Plan Using MBSE

1. V&V IN THE EARLY STAGES OF THE LIFECYCLE?



What Is Verification?

- Verification: “the process of establishing the truth, accuracy, or validity of something” [Google definition]
- Meets specification-level requirements
- Proves that the solution-dependent requirements are satisfied
- Proves that solution was or is being built according to agreed requirements

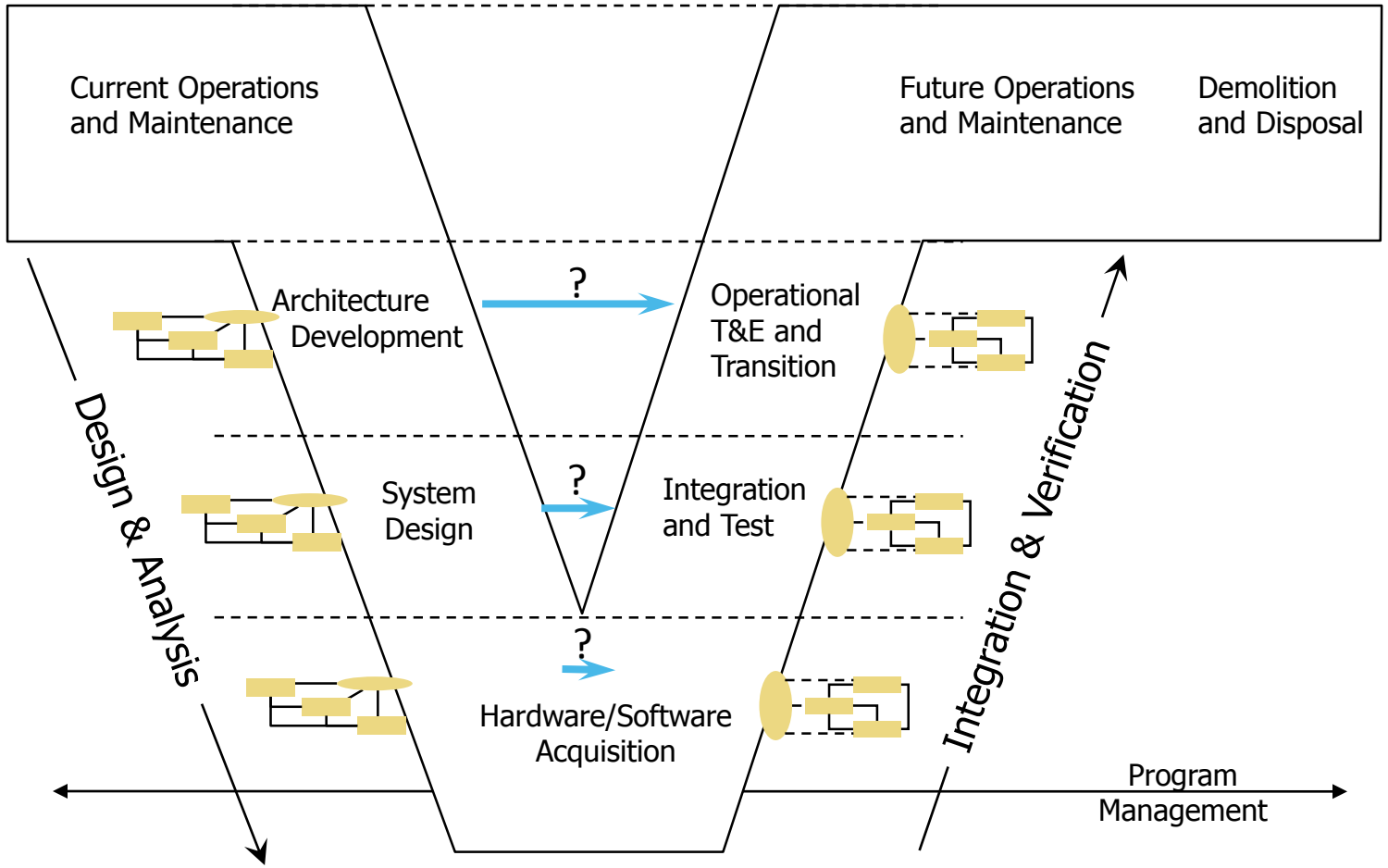
Frequently the terms “Unit Test” and “Developmental Test and Evaluation” apply to verification

What Is Validation?

- Validation: “the action of checking or proving the validity or accuracy of something” [Google definition]
- Relates to customer and other stakeholder satisfaction
- Proves solution-independent requirements are being satisfied
- Usually performed at the enterprise and/or system level
- In process, validation helps ensure system will ultimately be part of the accepted solution in the target environment

Frequently the term “Operational Test and Evaluation” applies to validation

What Do We Need to Do Early?



What Do We Need Early?

- Ontology that includes V&V information
- Verifiable Requirements
- V&V Plan

To do any of these things you need to understand how to prepare for V&V, conduct V&V activities, and report V&V results, so make sure an expert in these areas are part of the early phase

2. ONTOLOGY FOR V&V



Lifecycle Modeling Language's Primary Classes

- Action
- Artifact
- Asset
  - Resource
- Characteristic
  - Measure
- Connection
  - Conduit
  - Logical
- Cost
- Decision
- Input/Output
- Location
  - Physical, Orbital, Virtual
- Risk
- Statement
  - Requirement
- Time

See www.lifecyclemodeling.org for LML specification

Supports capturing information throughout the lifecycle

V&V Extension to LML

- In developing Innoslate's new Test Center capability, we discovered the need to add a subclass to Action: Test Case
- We used the Schema Editor to make these changes, but also we had to add views and reports
- You may discover that you want to add other classes, attributes, and relationships, as well and develop special reports and data entry screens using the SDK

Test Case (Subclass of Action)

- A Test Case entity represents a set of conditions utilized to determine whether a system works as intended

- Properties (Attributes)

Name	Type	Description
Status	ENUMERATION	Status represents the current state of this Test Case.
Actual Result	BIG_TEXT	Actual Results represents the results that are captured after executing a Test Case.
Expected Result	BIG_TEXT	Expected Result represents the result expected when executing this Test Case.
Set Up	BIG_TEXT	Set Up represents the prerequisites that must be fulfilled before executing this Test Case.

3. WHAT'S A VERIFIABLE REQUIREMENT?



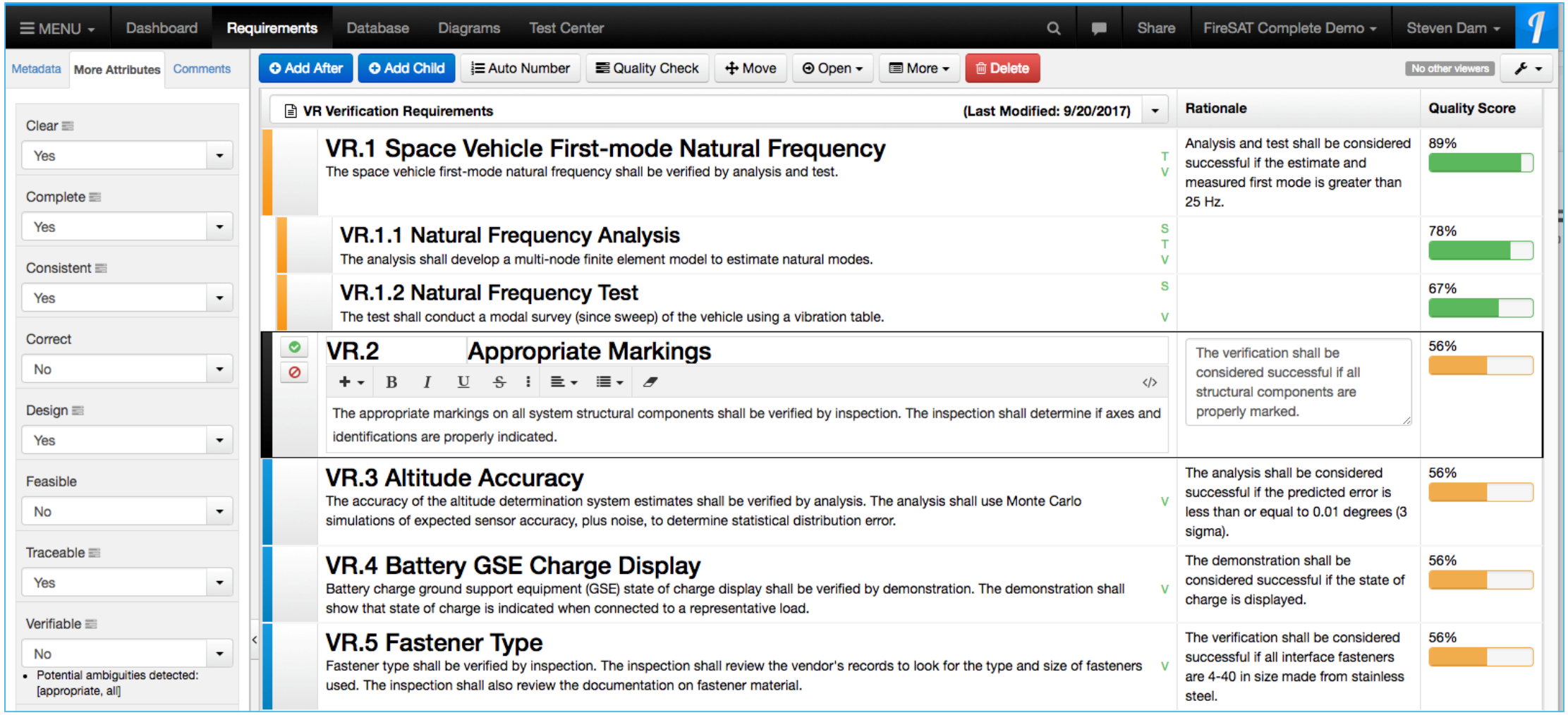
Characteristics of Good Requirements

- Each individual requirement should be:
  - Correct: Describes the user's true intent and is legally possible
  - Complete: Express a whole idea
  - Clear: Unambiguous and not confusing
  - Consistent: Not in conflict with other requirements
  - ***Verifiable: Provable (within realistic cost and schedule) that the system meets the requirement***
  - Traceable: Uniquely identified, and able to be tracked to predecessor and successor lifecycle items/objects
  - Feasible: Able to be implemented with existing technology, and within cost and schedule
  - Modular: Can be changed without excessive impact on other requirements
  - Design: Does not impose a specific solution on design; says "what", Independent not "how"

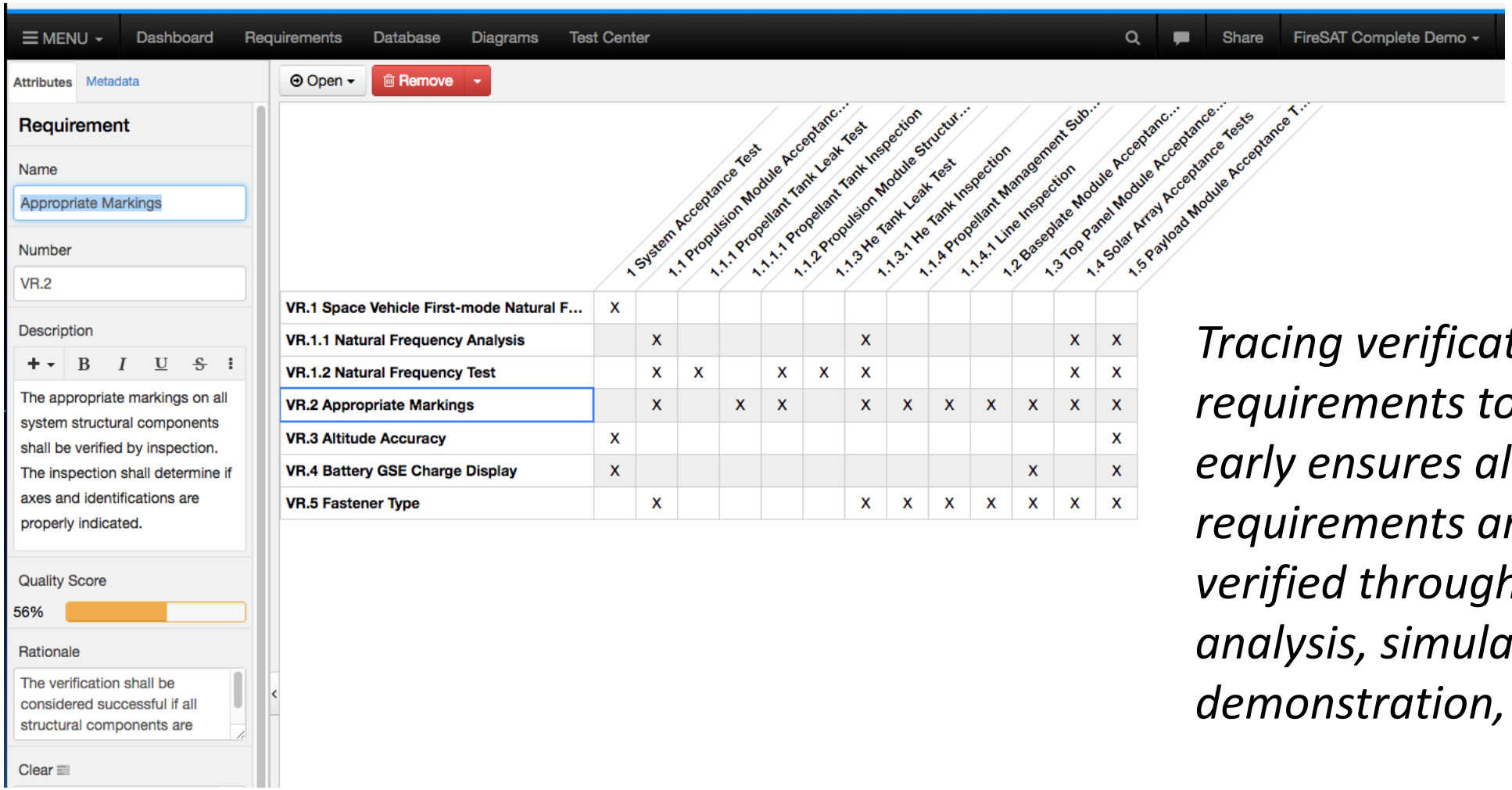
What Makes a Requirement Verifiable?

- You need to answer the following questions:
  - Can the requirement be met?
    - By analysis, demonstration, inspection, modeling & simulation, or test?
  - Will the user accept the results?
- Avoid words such as “excessive,” “sufficient,” “resistant,” etc.
  - Make the requirement quantifiable
- Even “suitability” can be quantified

Example Verification Requirements

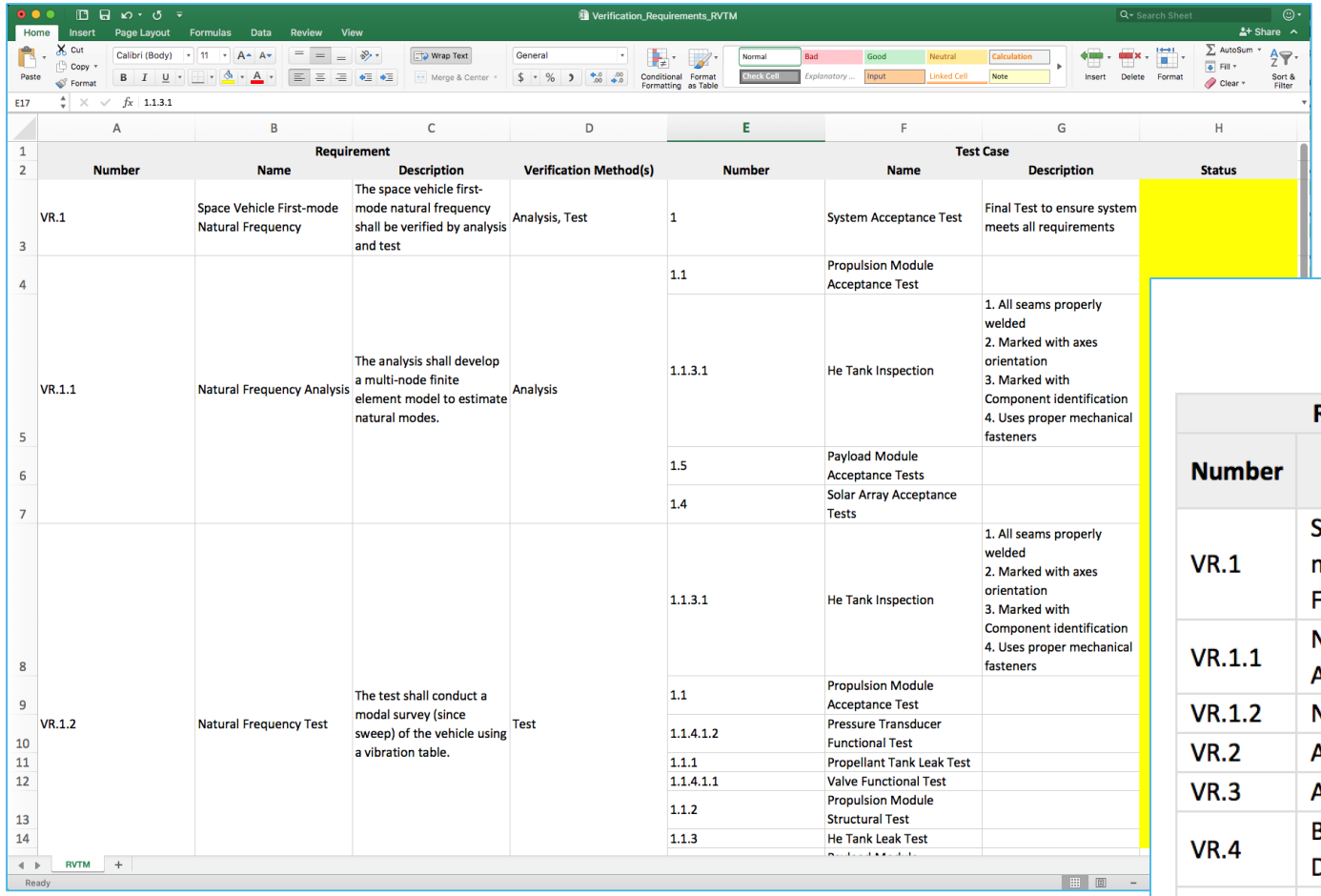


Trace VRs to Test Cases



Tracing verification requirements to test cases early ensures all requirements are properly verified through inspection, analysis, simulation, demonstration, and/or test

Produce Key Reports and Archive Them



Requirement				Test Case			
Number	Name	Description	Verification Method(s)	Number	Name	Description	Status
VR.1	Space Vehicle First-mode Natural Frequency	The space vehicle first-mode natural frequency shall be verified by analysis and test	Analysis, Test	1	System Acceptance Test	Final Test to ensure system meets all requirements	
VR.1.1	Natural Frequency Analysis	The analysis shall develop a multi-node finite element model to estimate natural modes.	Analysis	1.1	Propulsion Module Acceptance Test		
				1.1.3.1	He Tank Inspection	1. All seams properly welded 2. Marked with axes orientation 3. Marked with Component identification 4. Uses proper mechanical fasteners	
				1.5	Payload Module Acceptance Tests		
				1.4	Solar Array Acceptance Tests		
VR.1.2	Natural Frequency Test	The test shall conduct a modal survey (since sweep) of the vehicle using a vibration table.	Test	1.1.3.1	He Tank Inspection	1. All seams properly welded 2. Marked with axes orientation 3. Marked with Component identification 4. Uses proper mechanical fasteners	
				1.1	Propulsion Module Acceptance Test		
				1.1.4.1.2	Pressure Transducer Functional Test		
				1.1.1	Propellant Tank Leak Test		
				1.1.4.1.1	Valve Functional Test		
				1.1.2	Propulsion Module Structural Test		
				1.1.3	He Tank Leak Test		

Add actual results and status as V&V occurs

Verification Cross-Reference Matrix

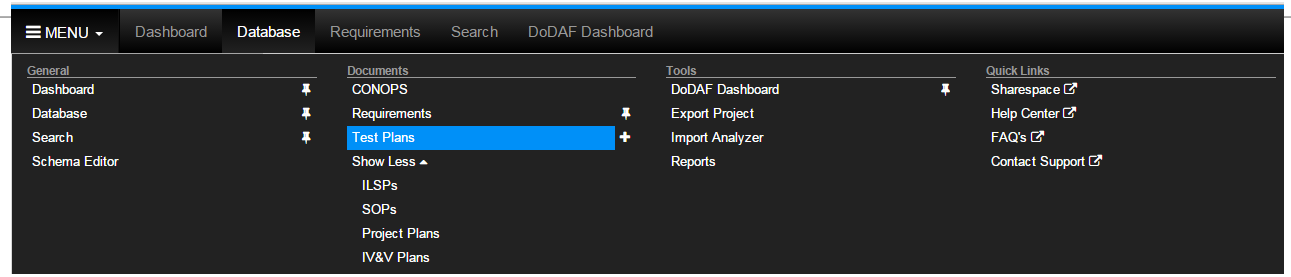
Requirement		Verification Method(s)				
Number	Name	Analysis	Demonstration	Inspection	Modeling & Simulation	Test
VR.1	Space Vehicle First-mode Natural Frequency	X				X
VR.1.1	Natural Frequency Analysis	X				
VR.1.2	Natural Frequency Test					X
VR.2	Appropriate Markings			X		
VR.3	Altitude Accuracy	X				
VR.4	Battery GSE Charge Display		X			
VR.5	Fastener Type			X		

4. DEVELOPING A V&V PLAN USING MBSE



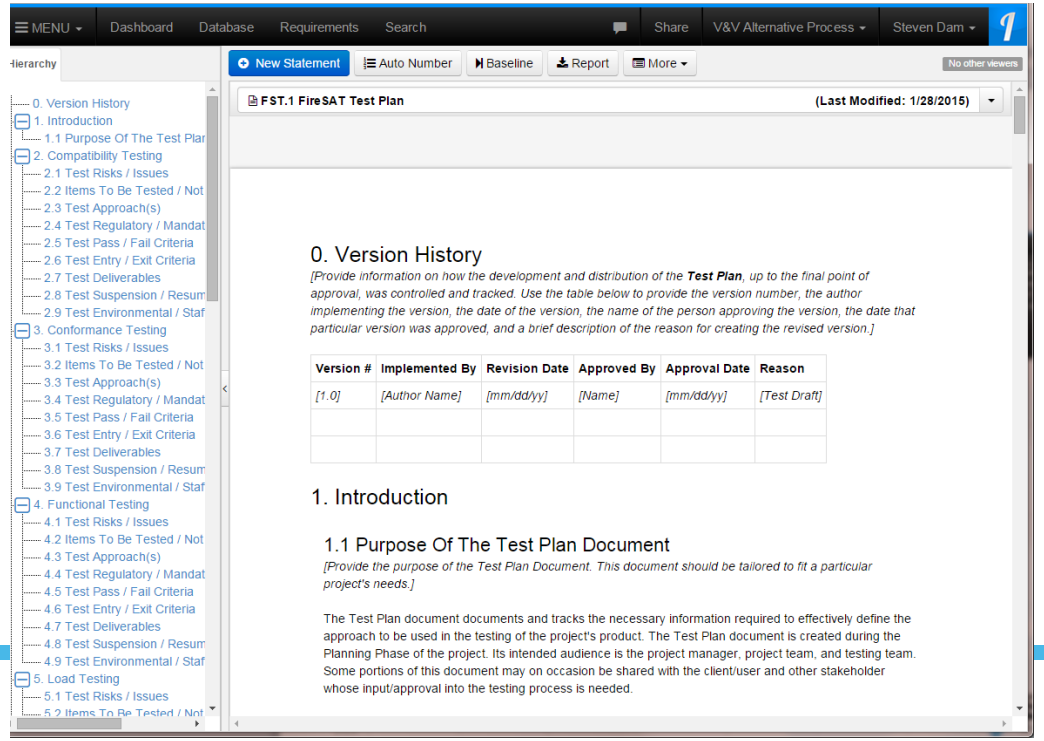
Create a Test Plan

1. Select Test Plans from Menu



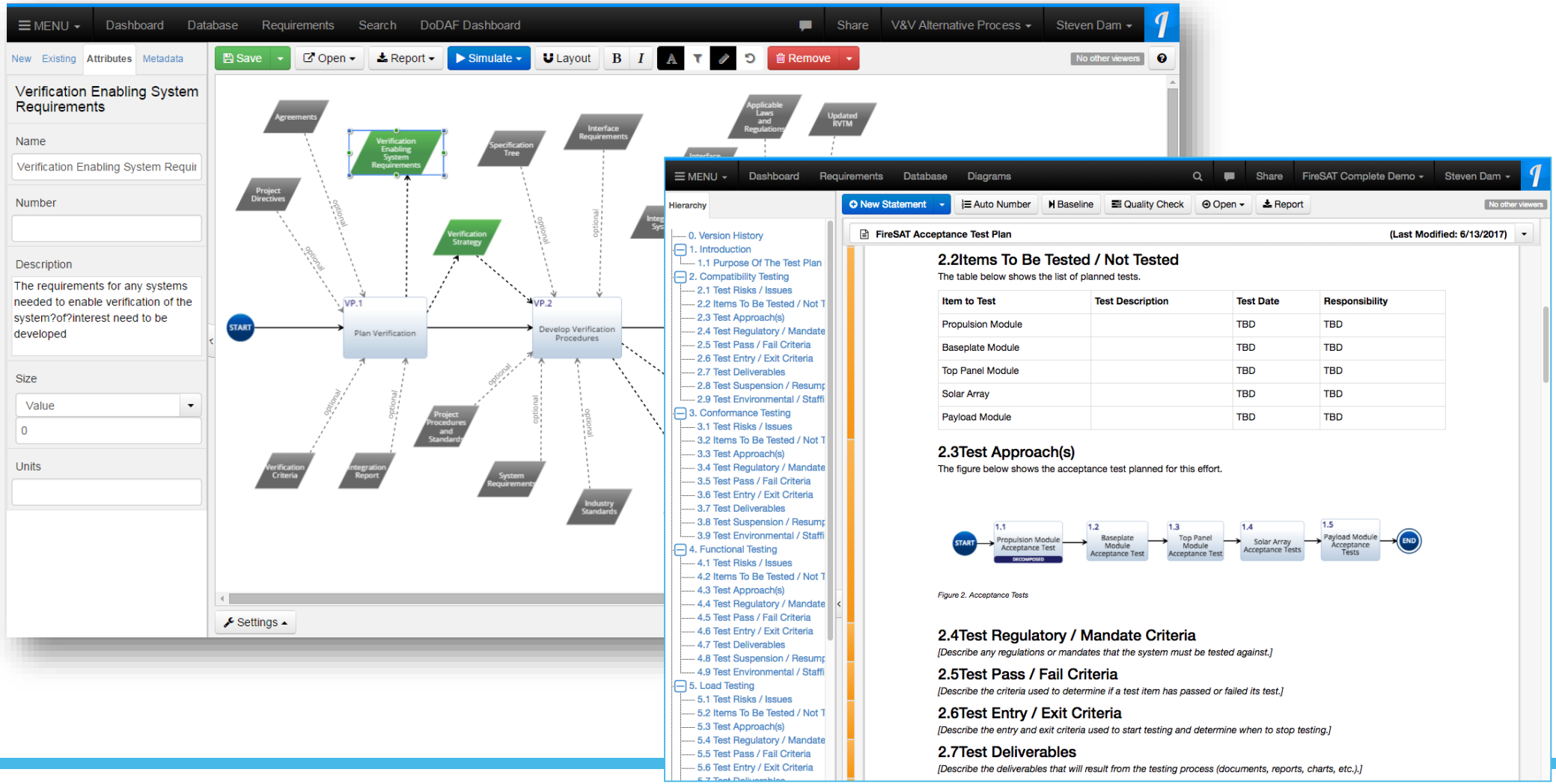
2. Answer questions (use our template or create your own)

3. Fill-in resulting template

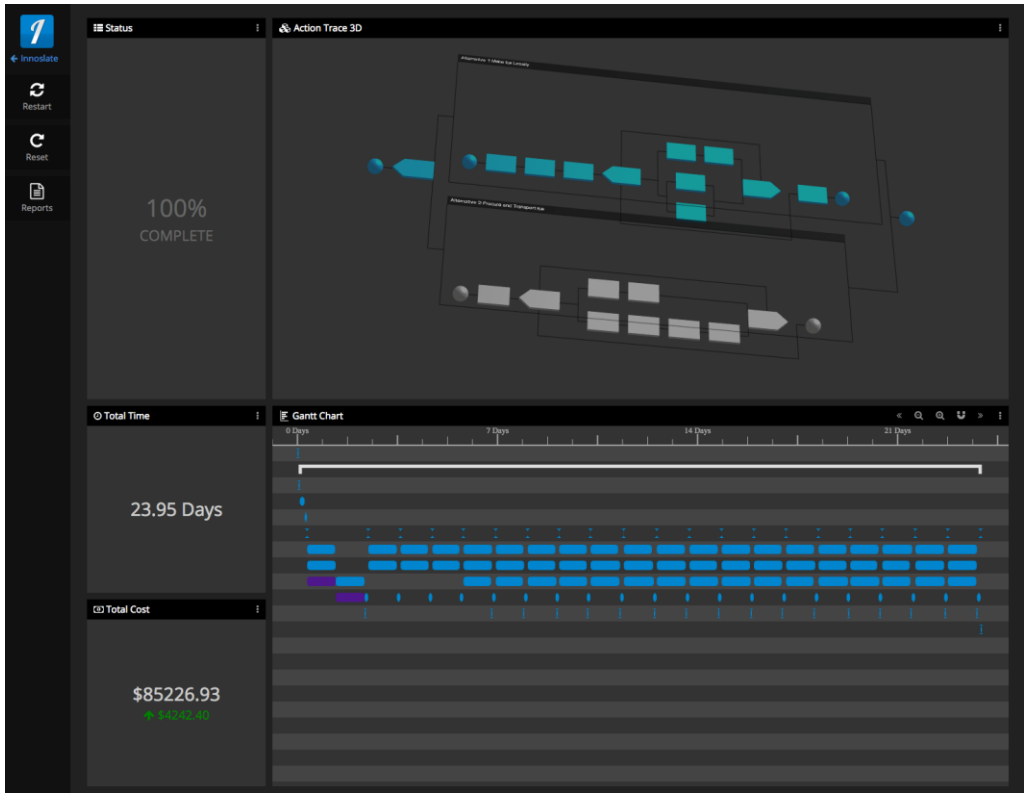


Create Test Processes (Test Cases)

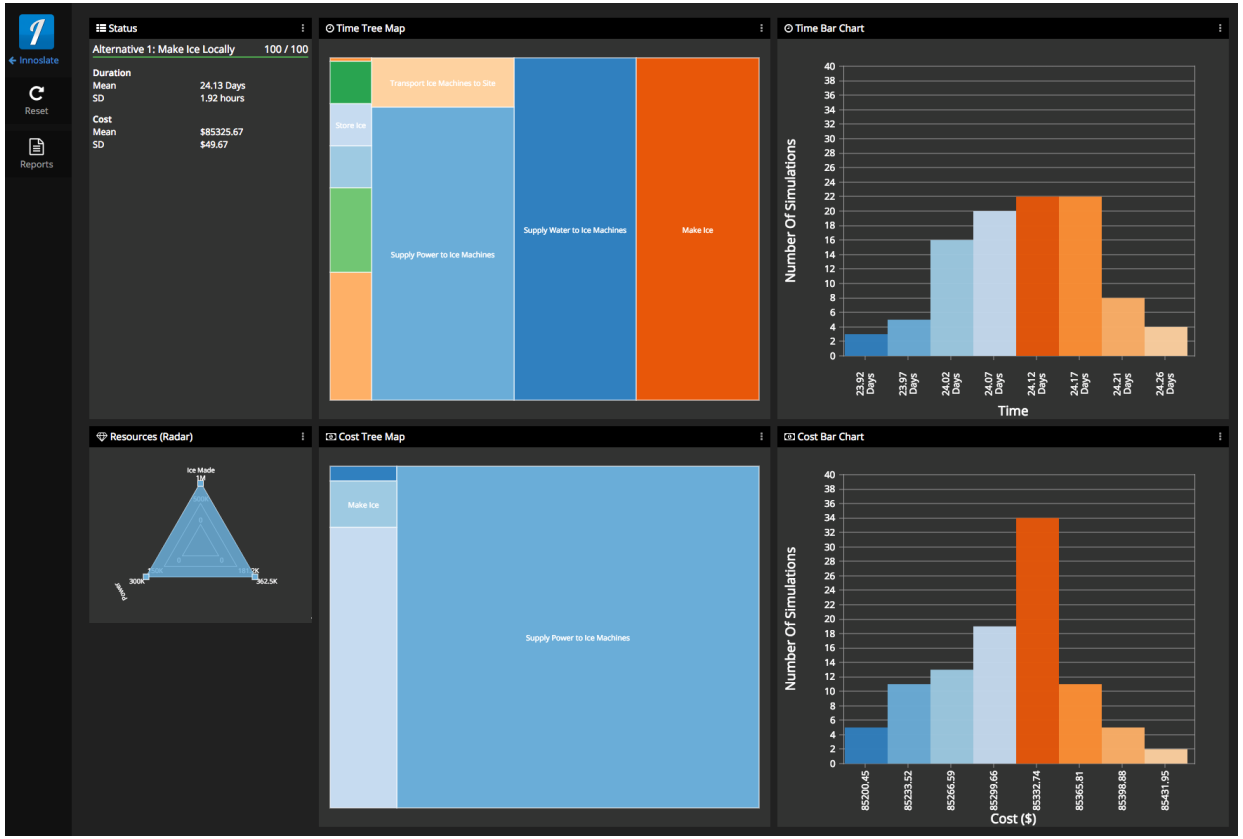
- Model processes
- Embed processes into test plan



Make Sure the Test Cases Work Using Simulation



Watch test case execute at all levels using the Discrete Event Simulator

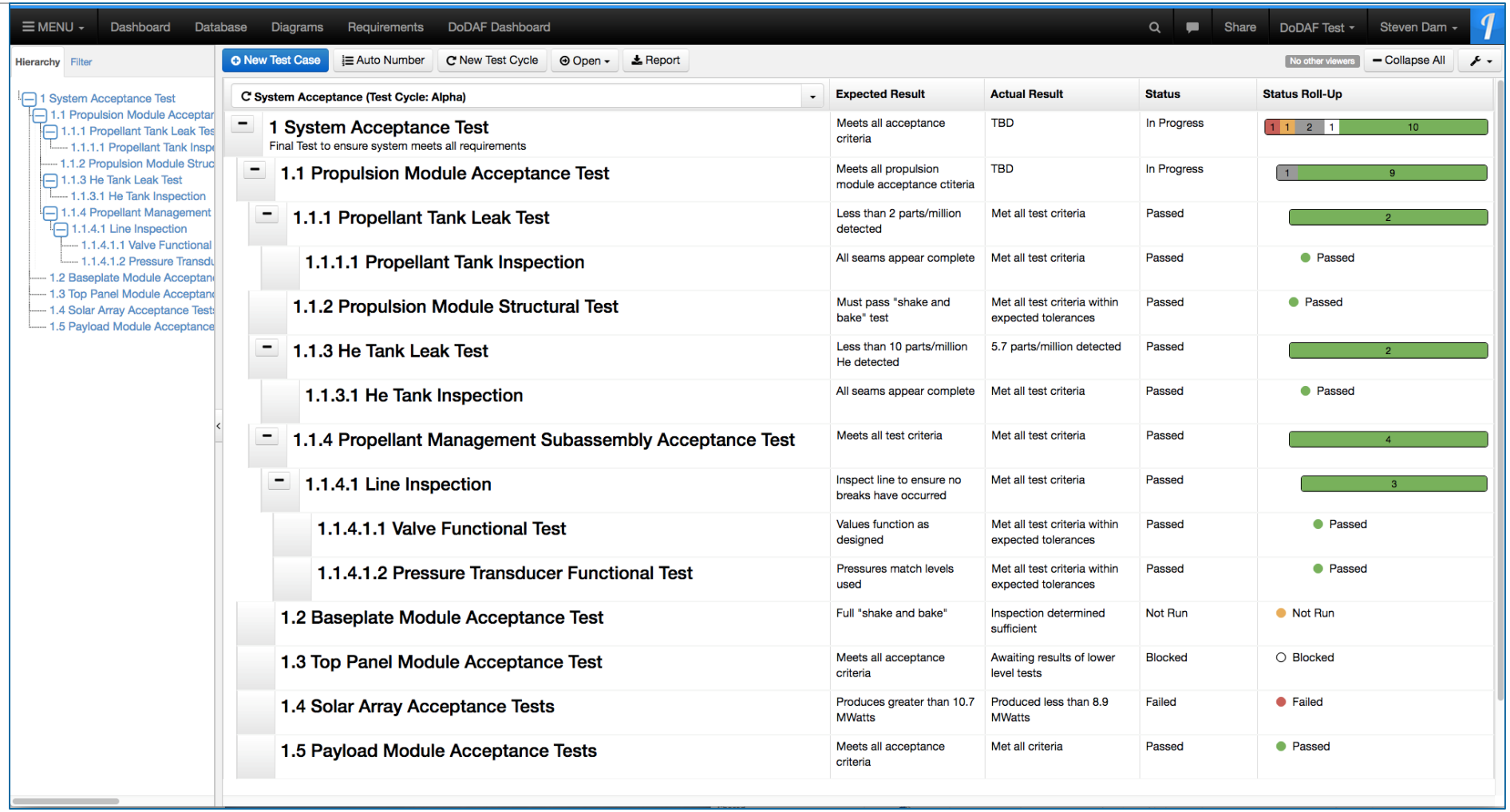


Explore the variation of individual steps to execute the model over many iterations using the Monte Carlo Simulator

You can add resources and costs to enhance your planning

Capture Actual Results and Status During V&V

- Capture actual results as part of test report



Other Information Needed for V&V Activities

- Test Equipment and Facilities (Assets)
- Test Organization (Assets) and Roles/Responsibilities (Statements)
- Risks and mitigations (Risk and many others)
- Criteria (Characteristics/Measures)
- Schedule (Timeline and/or process simulation output)
- Costs (WBS linked to processes)
- Data capture (actual results as Measures and Times)
- Artifacts
- Location(s)
- Decisions (assumptions, issues, etc.)

BENEFITS OF EARLY V&V



Benefits of Early V&V

1. Well defined plan for V&V
   - We know what data we need to capture
   - We know what test facilities we will need
   - We have modeled test scenarios to derive expected results
2. Well crafted verification requirements
   - Opportunity for early customer approval
   - Increase in stakeholder confidence
3. Reduced costs
   - Fewer errors in design
   - Fewer tests may be needed

Breaking Out

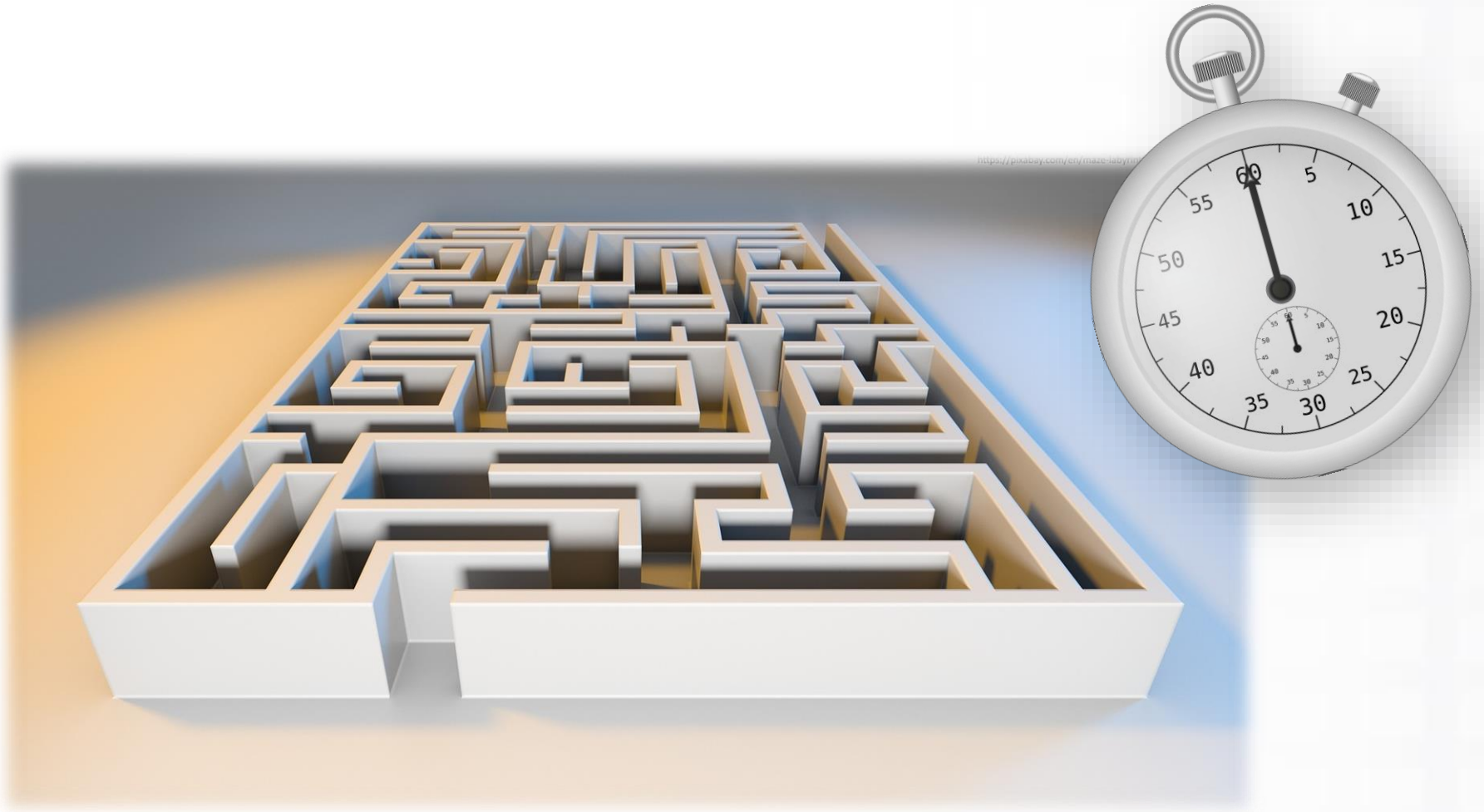
Systems Engineering To Go



Historical background

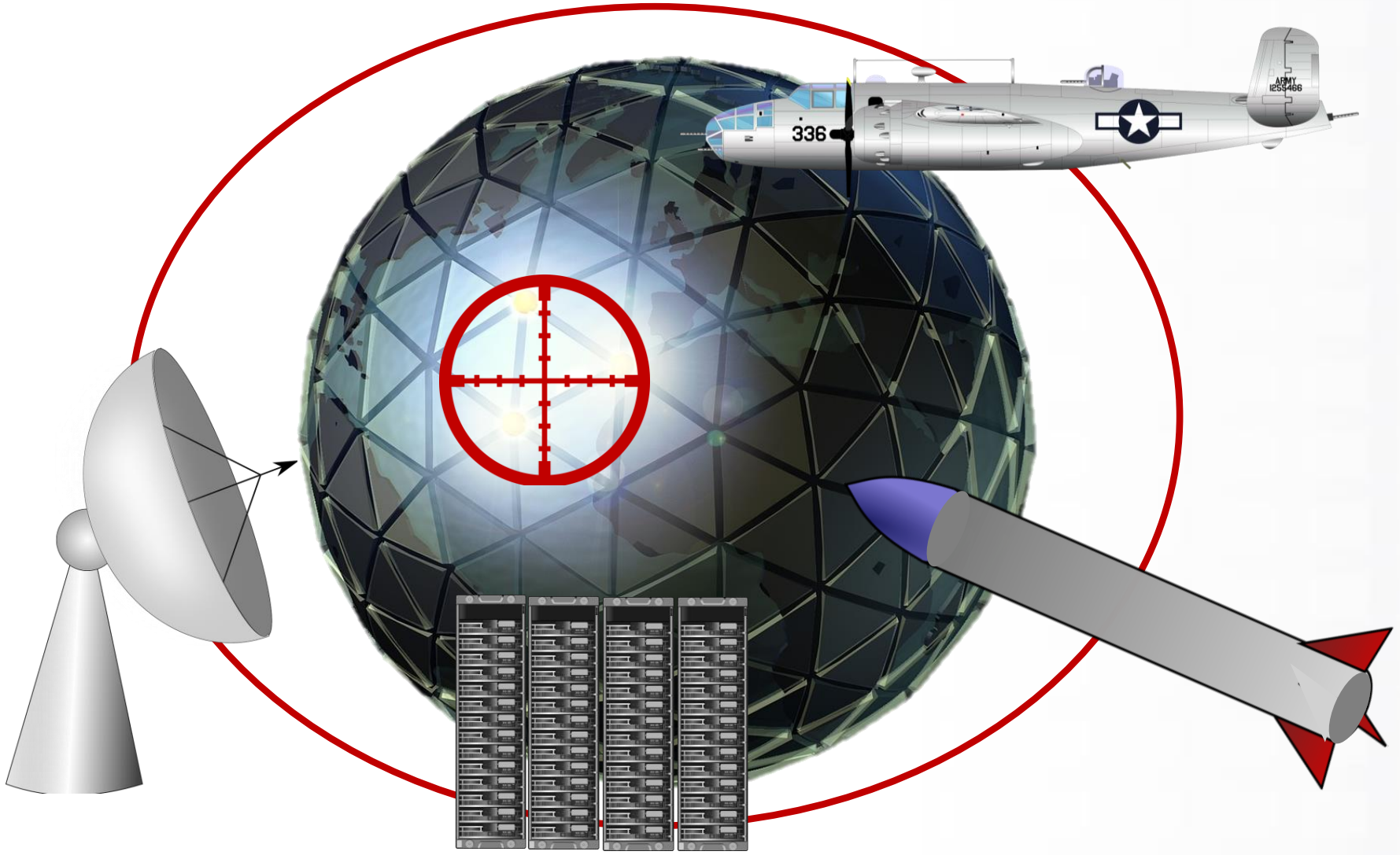
Copyright © 2017 by Vitech Corporation

Drivers = complexity + speed



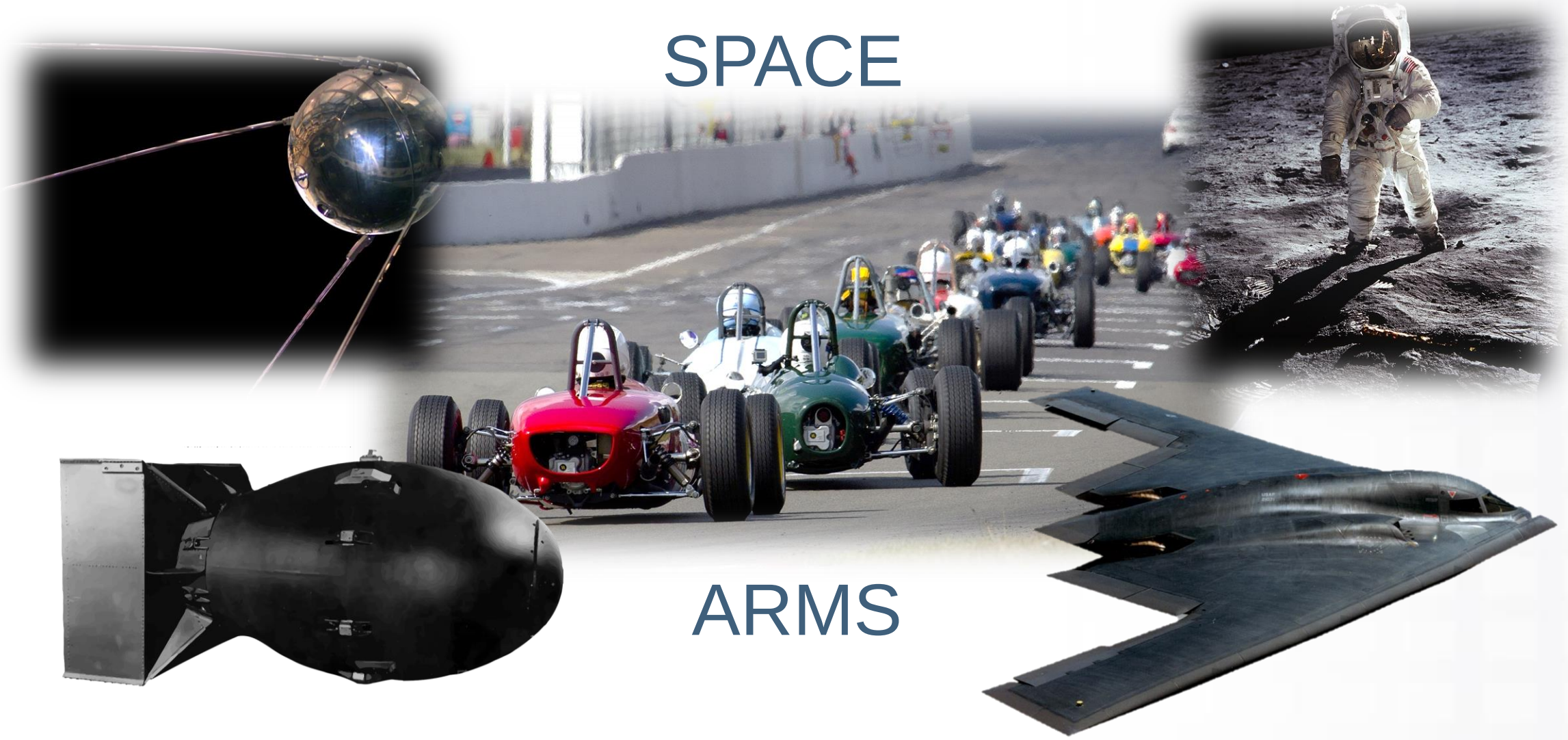
Copyright © 2017 by Vitech Corporation

Complexity



Copyright © 2017 by Vitech Corporation

Pace-Race



Copyright © 2017 by Vitech Corporation

Application-based transfer



Rockets Ships Vehicles Space Submarines

Copyright © 2017 by Vitech Corporation

Issues and Problems

Copyright © 2017 by Vitech Corporation

Baked-in

Heuristics Processes Algorithms

Product

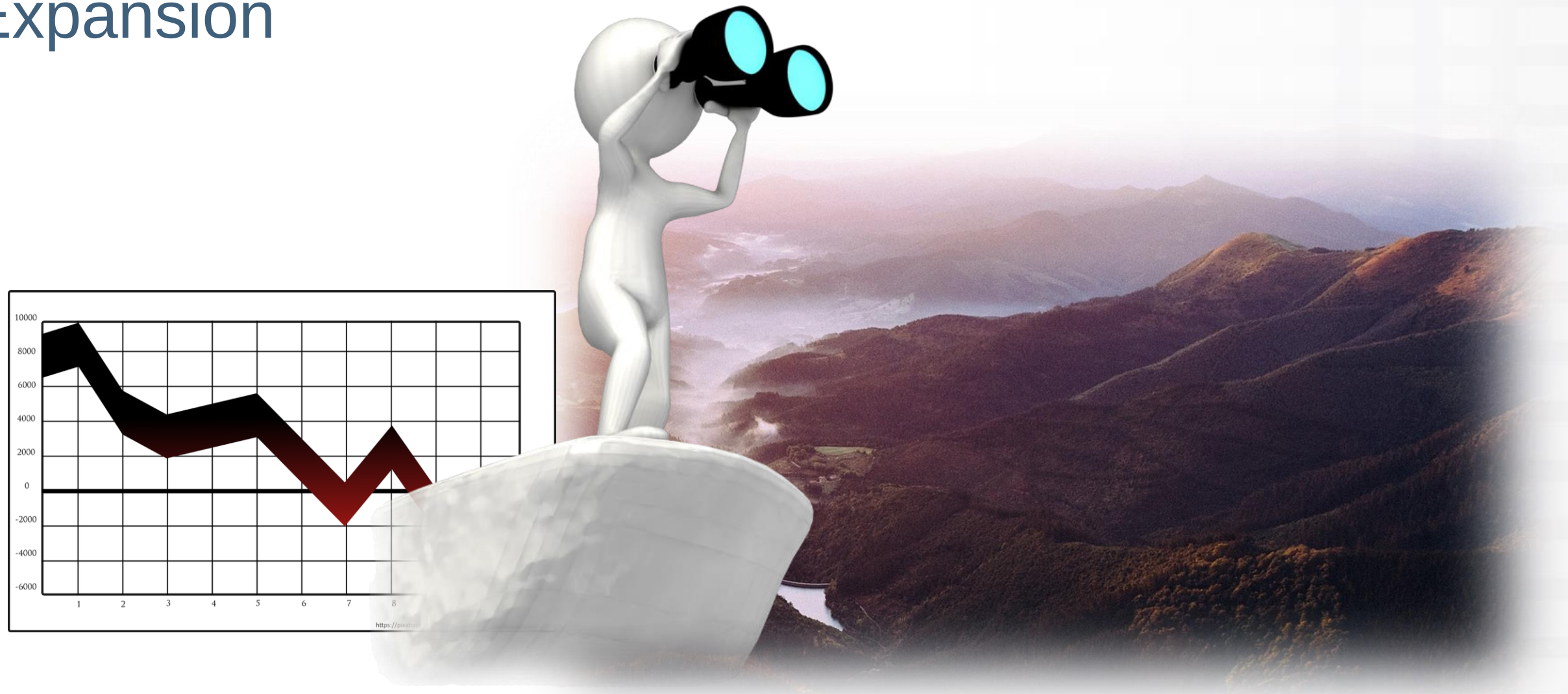


Software

Vocabulary

Copyright © 2017 by Vitech Corporation

Expansion

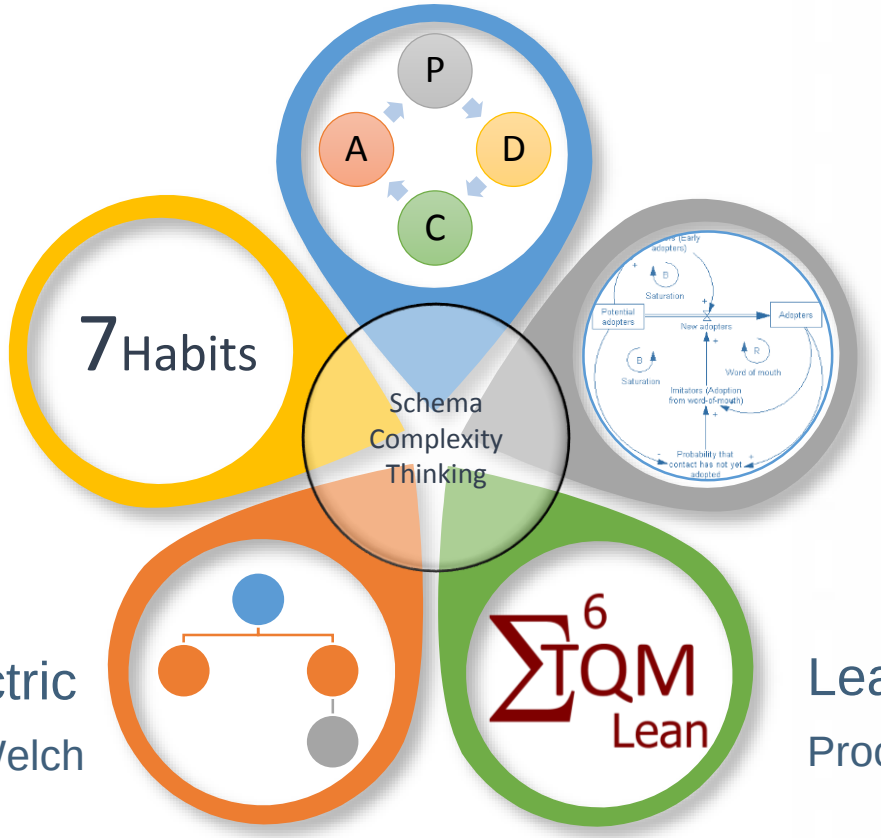


Copyright © 2017 by Vitech Corporation

Concepts Map To:

PDCA
Plan, Do, Check, Act

7 Habits of Highly Successful People
Steven Covey



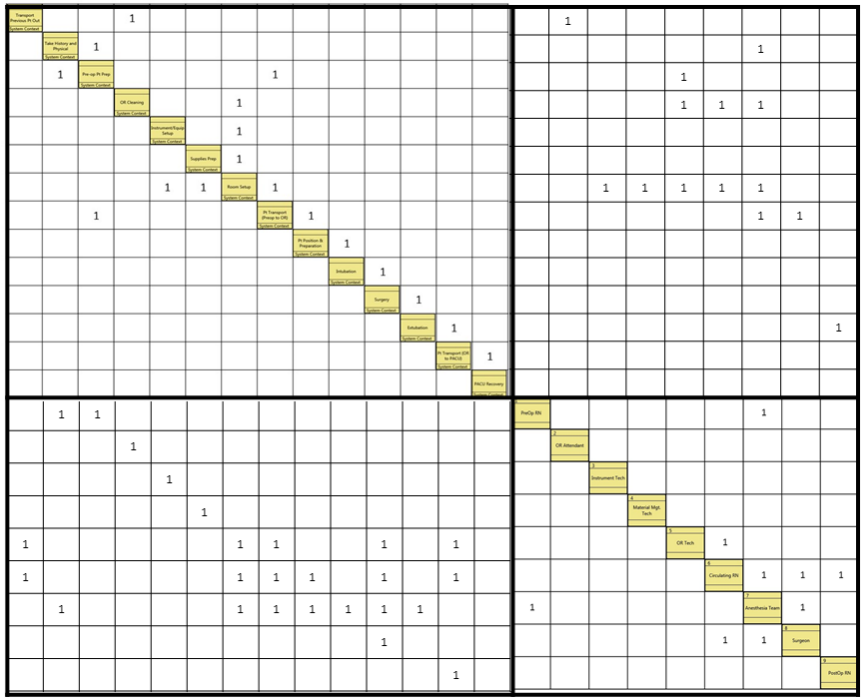
Systems Dynamics
5th Discipline
Peter Senge

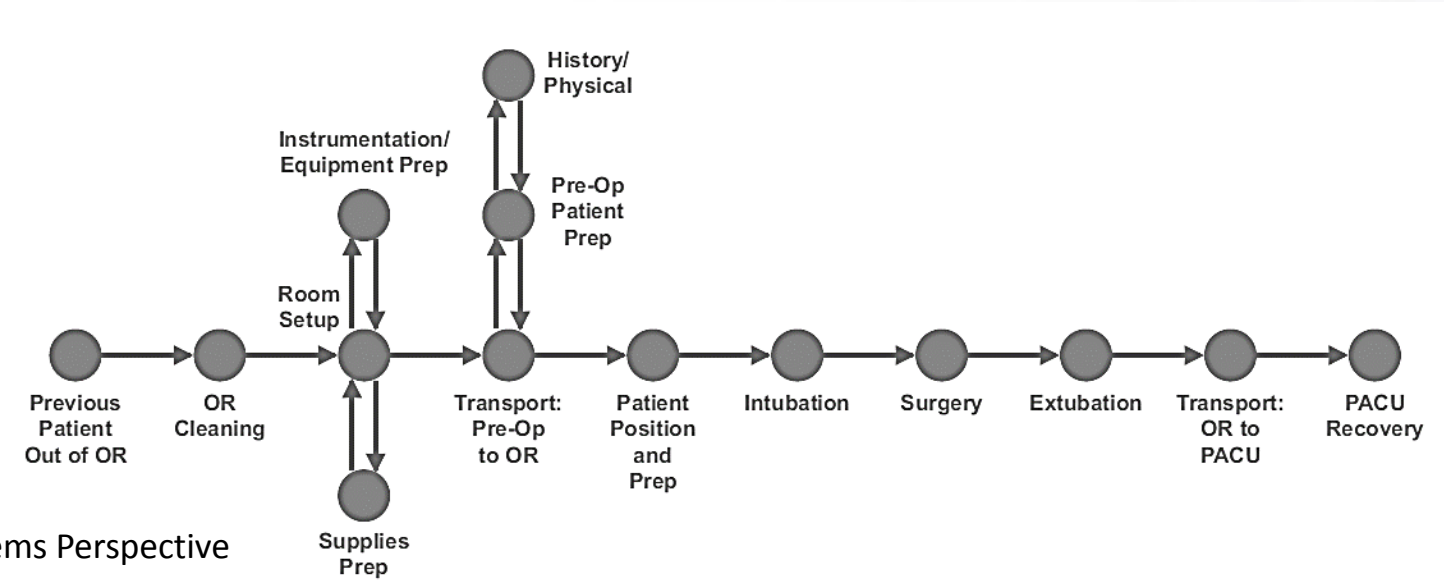
General Electric
Jack Welch

Lean Six Sigma/TQM
Process improvement

Copyright © 2017 by Vitech Corporation

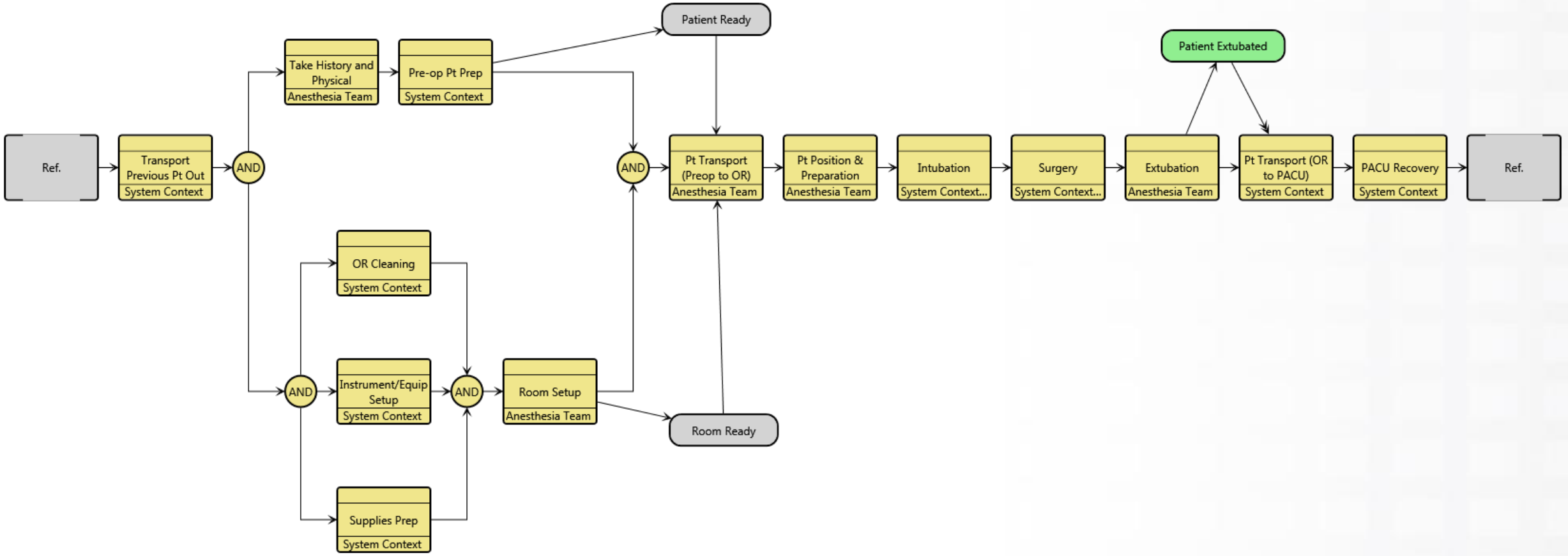
"While the DSM provides a valuable tool for visualizing complex processes, it actually is not the most intuitive means of graphically displaying dependencies in simpler systems like this one."





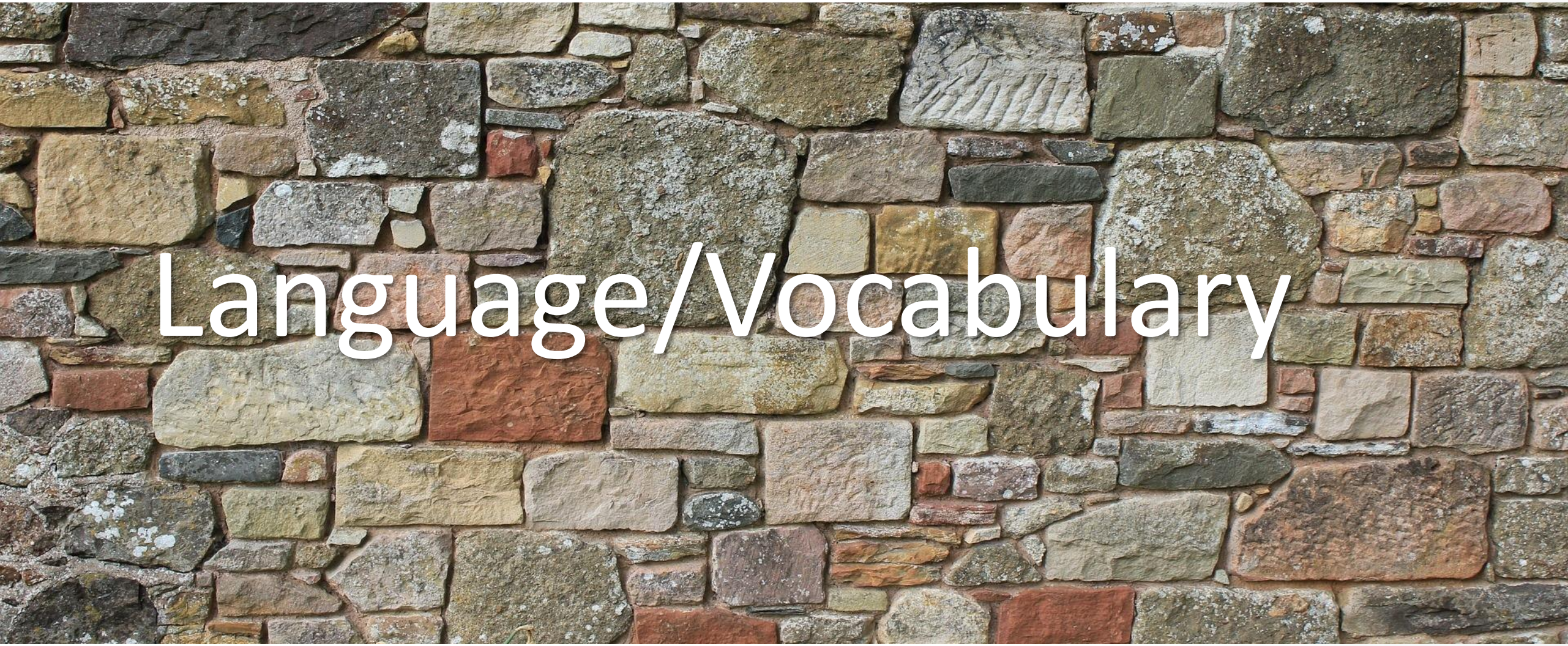
Process Modeling in the Operating Room: A Socio-Technical Systems Perspective
Sarah M. Bonzo, David McLain, Mark Avnet
Systems Engineering Vol. 19, No. 3, 2016

Copyright © 2017 by Vitech Corporation



Copyright © 2017 by Vitech Corporation

Impediment



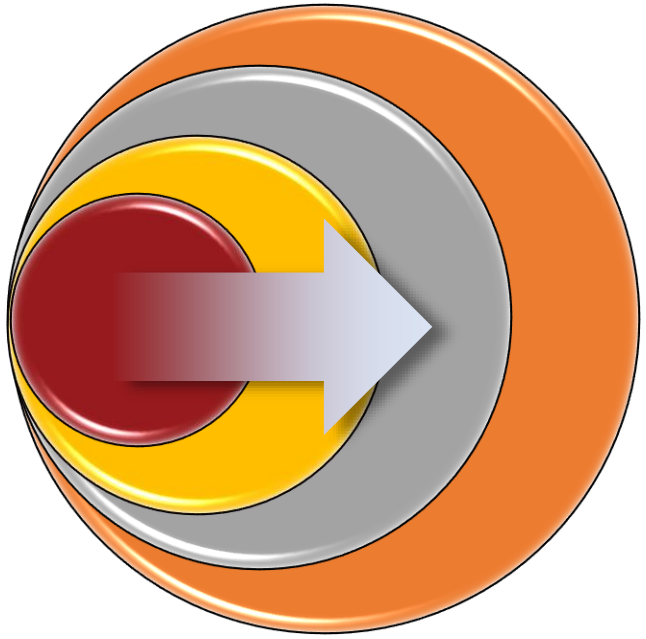
Copyright © 2017 by Vitech Corporation

Path Forward

Copyright © 2017 by Vitech Corporation

Path Forward- Step 1

Reproductive Thinking

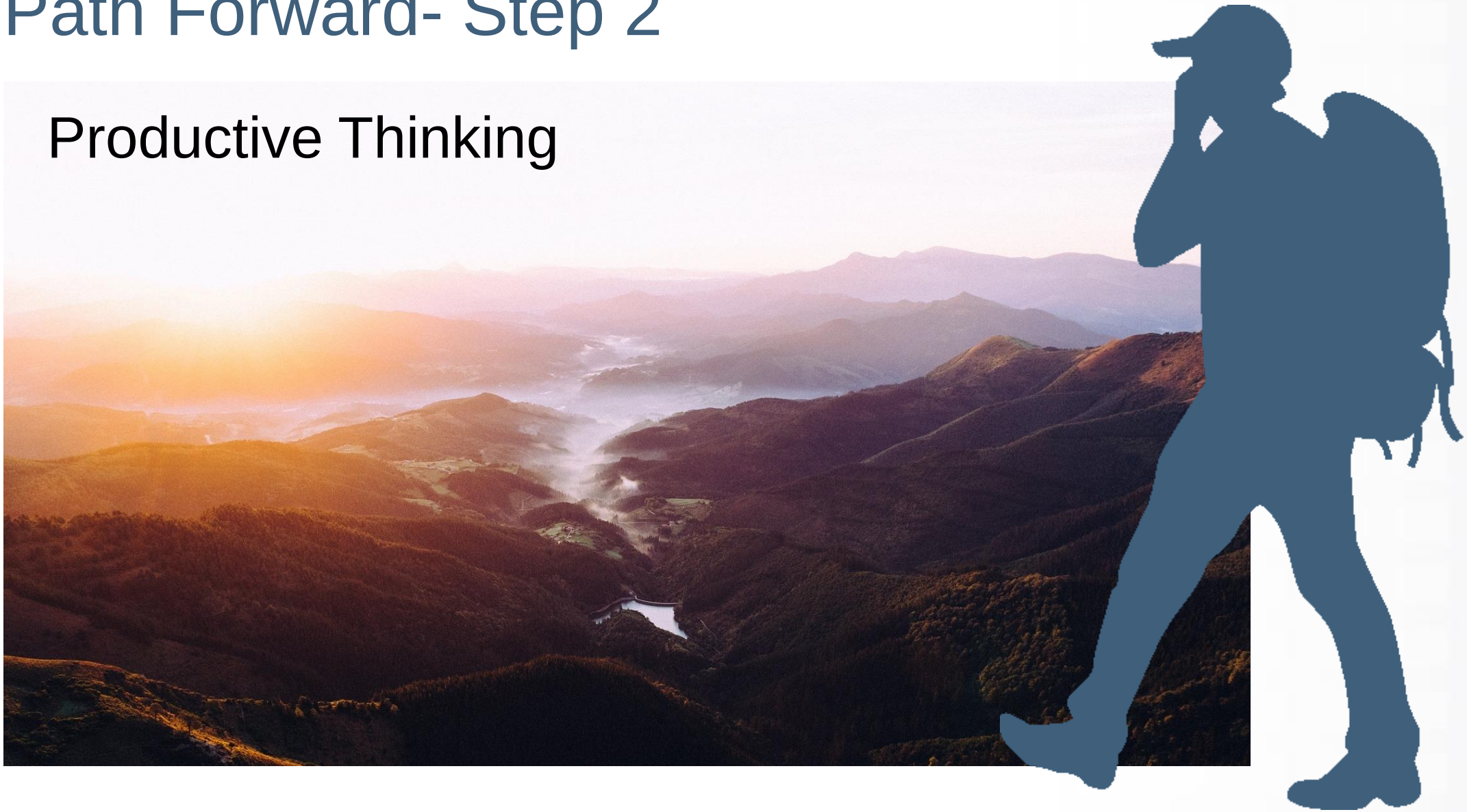


Incremental



Copyright © 2017 by Vitech Corporation

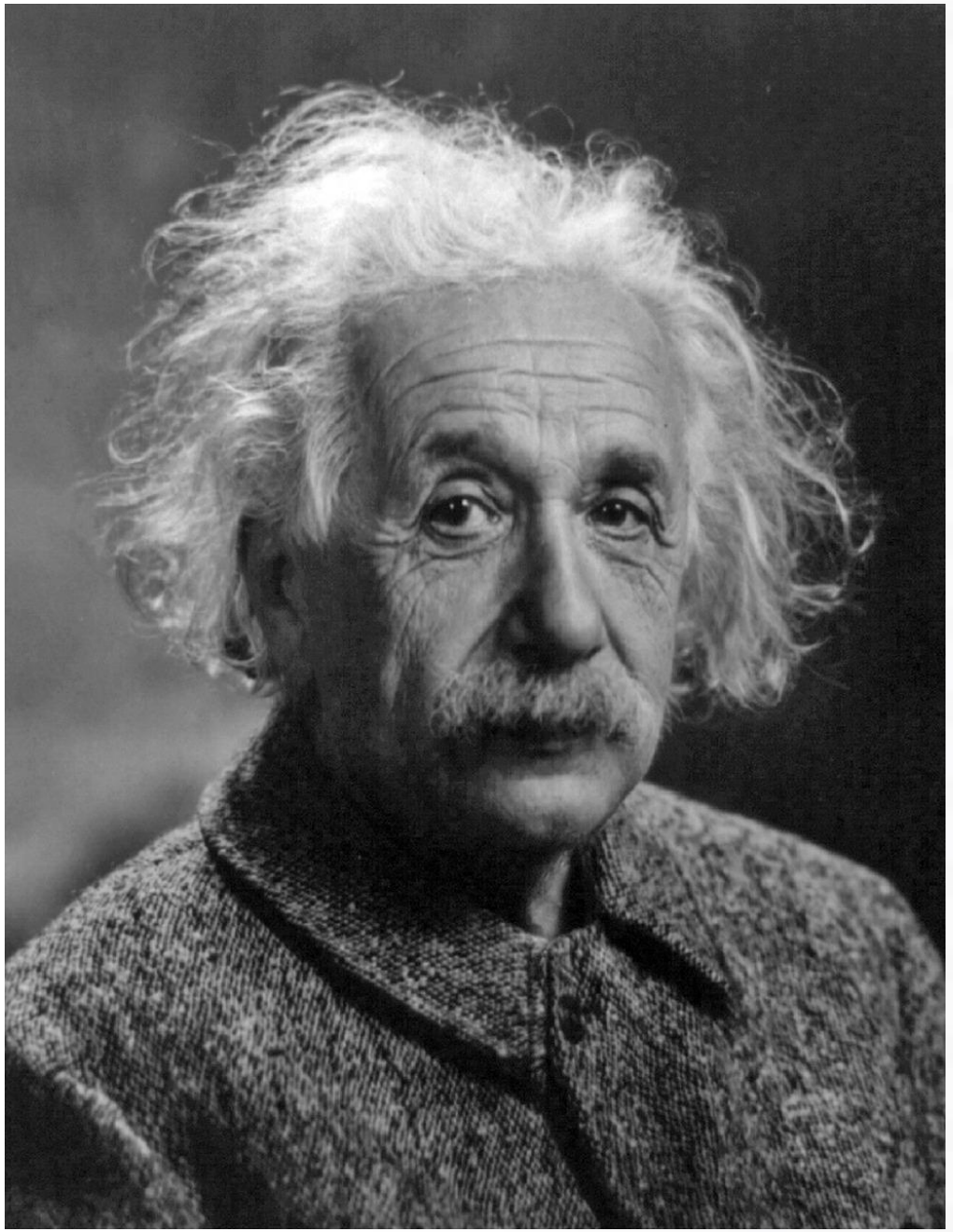
Path Forward- Step 2



Copyright © 2017 by Vitech Corporation

Combinatorial Play

"The first [principle is] that an idea is nothing more nor less than a new combination of old elements." (Vilfredo Pareto, 1935)



Copyright © 2017 by Vitech Corporation

James Webb Young

Five Steps for generating ideas:

1. Gather material
2. Digest material
3. Process unconsciously
4. Ah-Ha moment of insight
5. Tailor the idea to reality



Curiosity

Copyright © 2017 by Vitech Corporation

Warning!

- “But you didn’t offer examples of other areas”
- On purpose!
  - Encourages reproductive thinking
  - Plenty of examples (e.g.- A World In Motion)

Breaking Out: Systems Engineering To Go

Zane Scott, Vitech Corporation

www.vitechcorp.com | Blog: community.vitechcorp.com | Twitter: @VitechCorp
Vitech Corporation Celebrating 25 years of systems engineering excellence

Copyright © 2017 by Vitech Corporation

Educating Engineers or Training Technicians

Understanding at the Conceptual Level



Agenda

- Conceptual framework
- Bias toward practicality
- History of development
- Resulting barriers
- Path forward

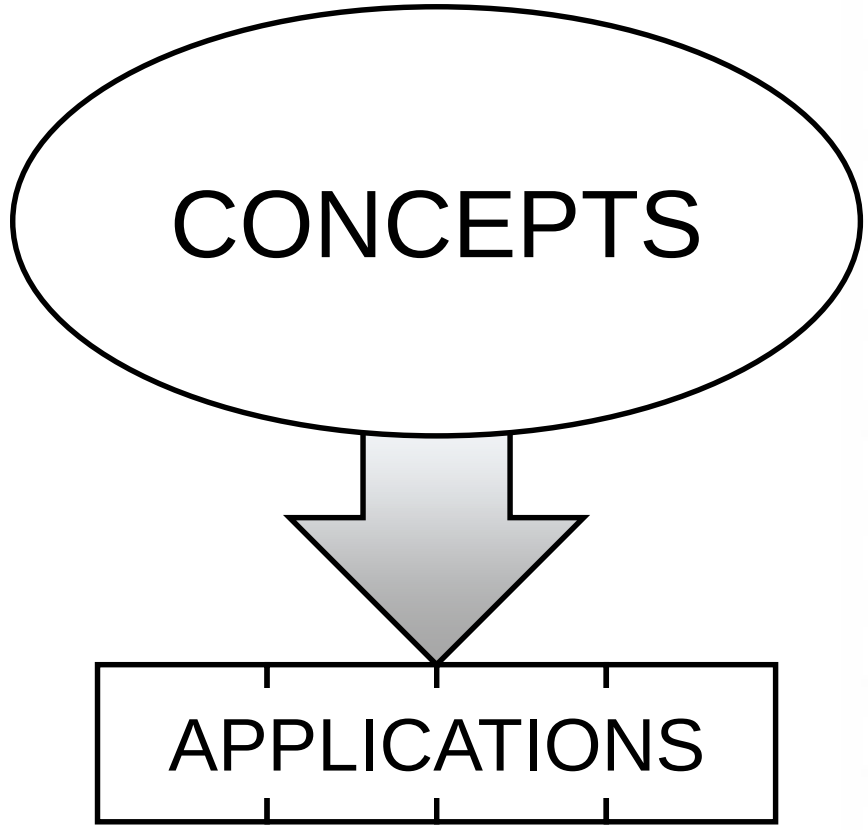


Conceptual Framework

Engineers v. Technicians

- US Dept. of Labor, Bureau of Labor Statistics
- Electrical engineer- “Research, design, develop, test, or supervise the manufacturing and installation of electrical equipment, components, or systems for commercial, industrial, military, or scientific use.”
- Electrician- “Install, maintain, and repair electrical wiring, equipment, and fixtures. Ensure that work is in accordance with relevant codes.”

Electrical Engineering = Concepts

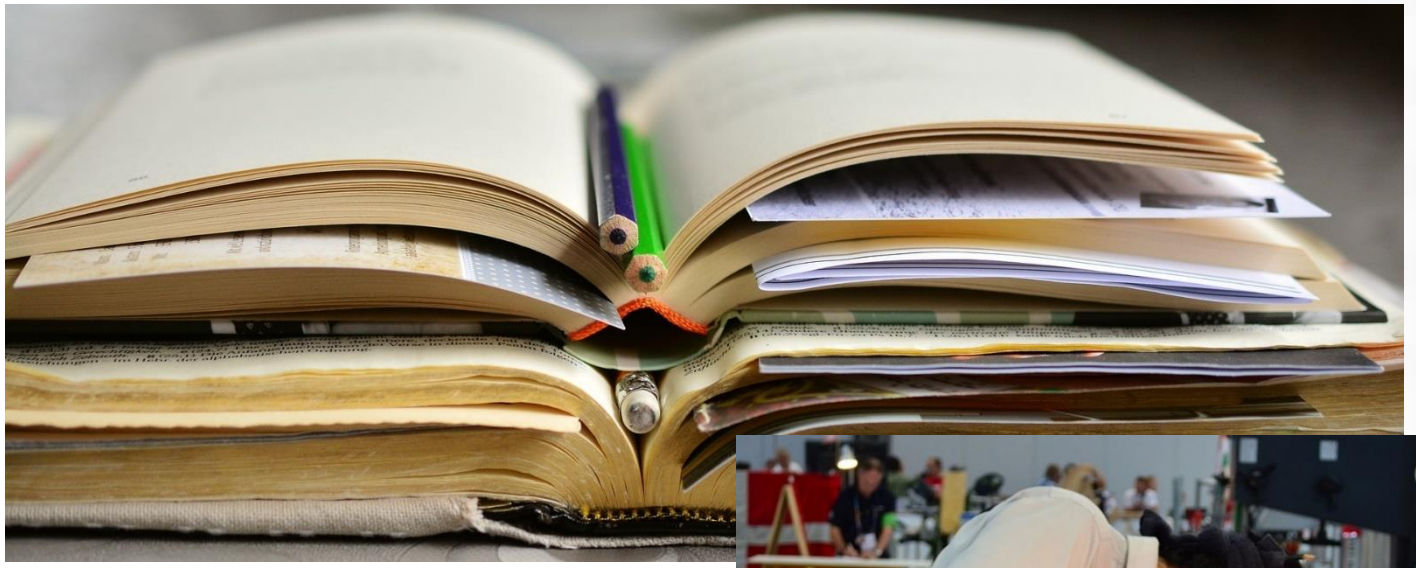

CONCEPTS
APPLICATIONS



Education v. Training

Definitions

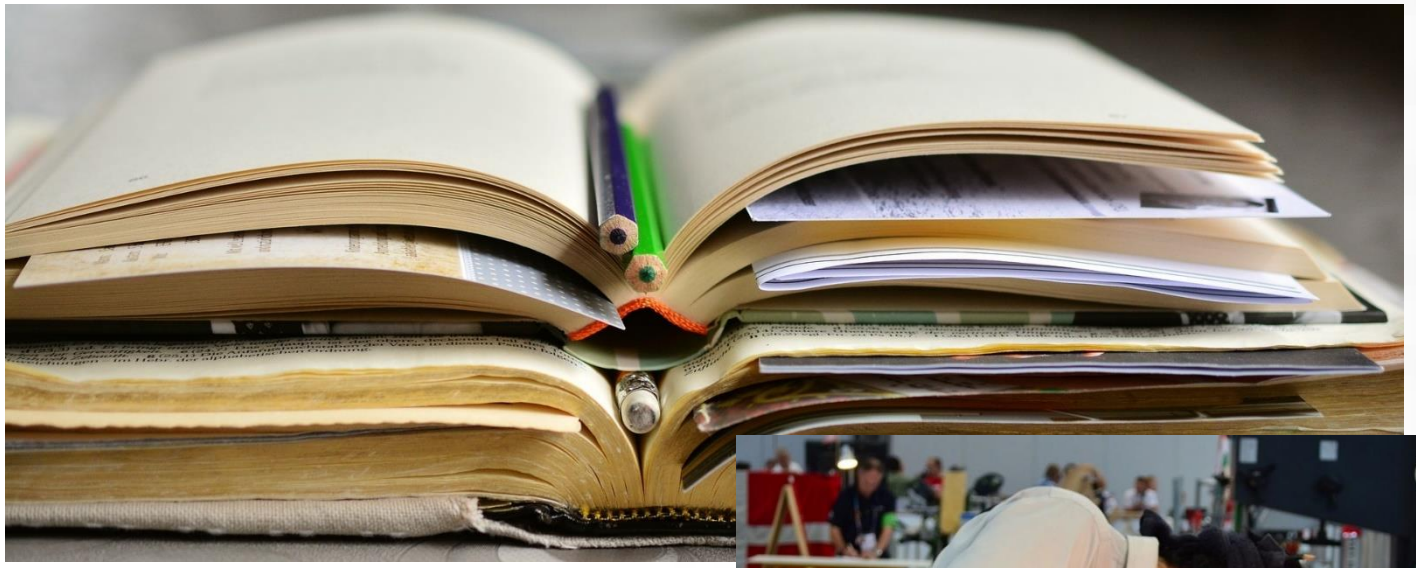
- Education- the act of imparting or acquiring general knowledge, developing the powers of reasoning and judgment
- Training- the action of teaching a person a particular skill or type of behavior
- Concepts v. skills





Bias

- “training gives you the skills to do something rather than just know about something”
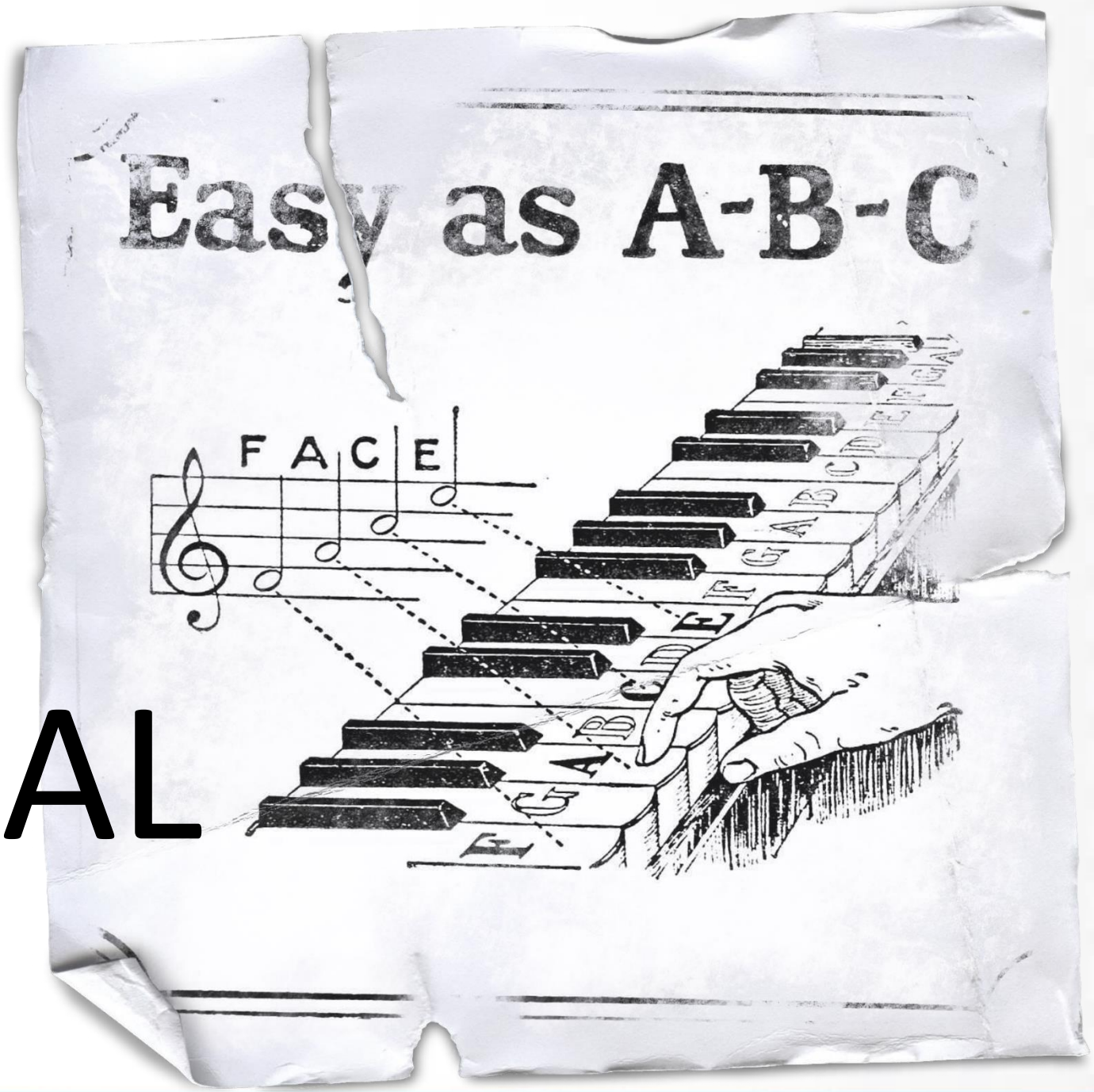




Do

rather than

just know

Vitech

PRACTICAL



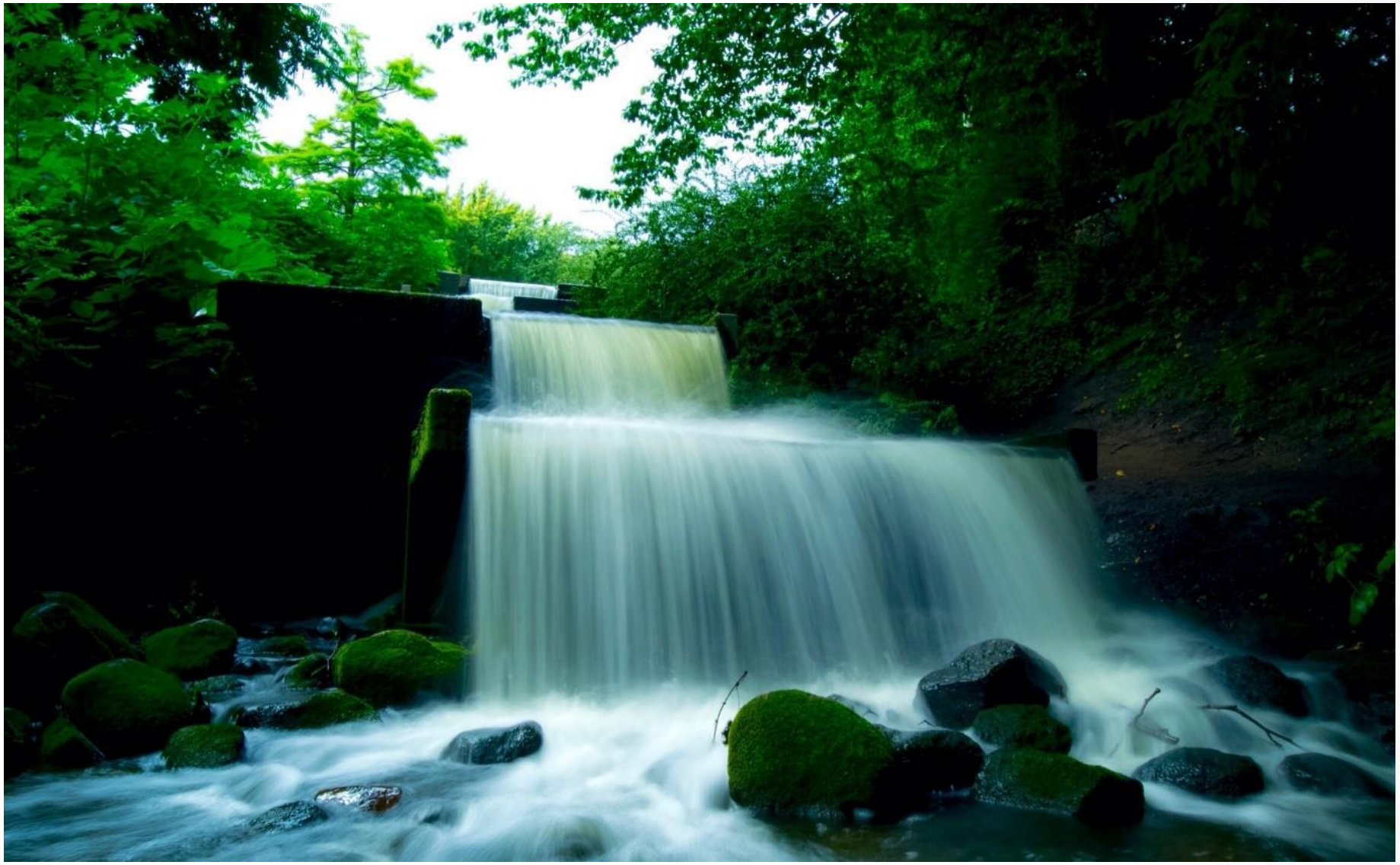
Vitech



Defining Systems Engineering-Process

History

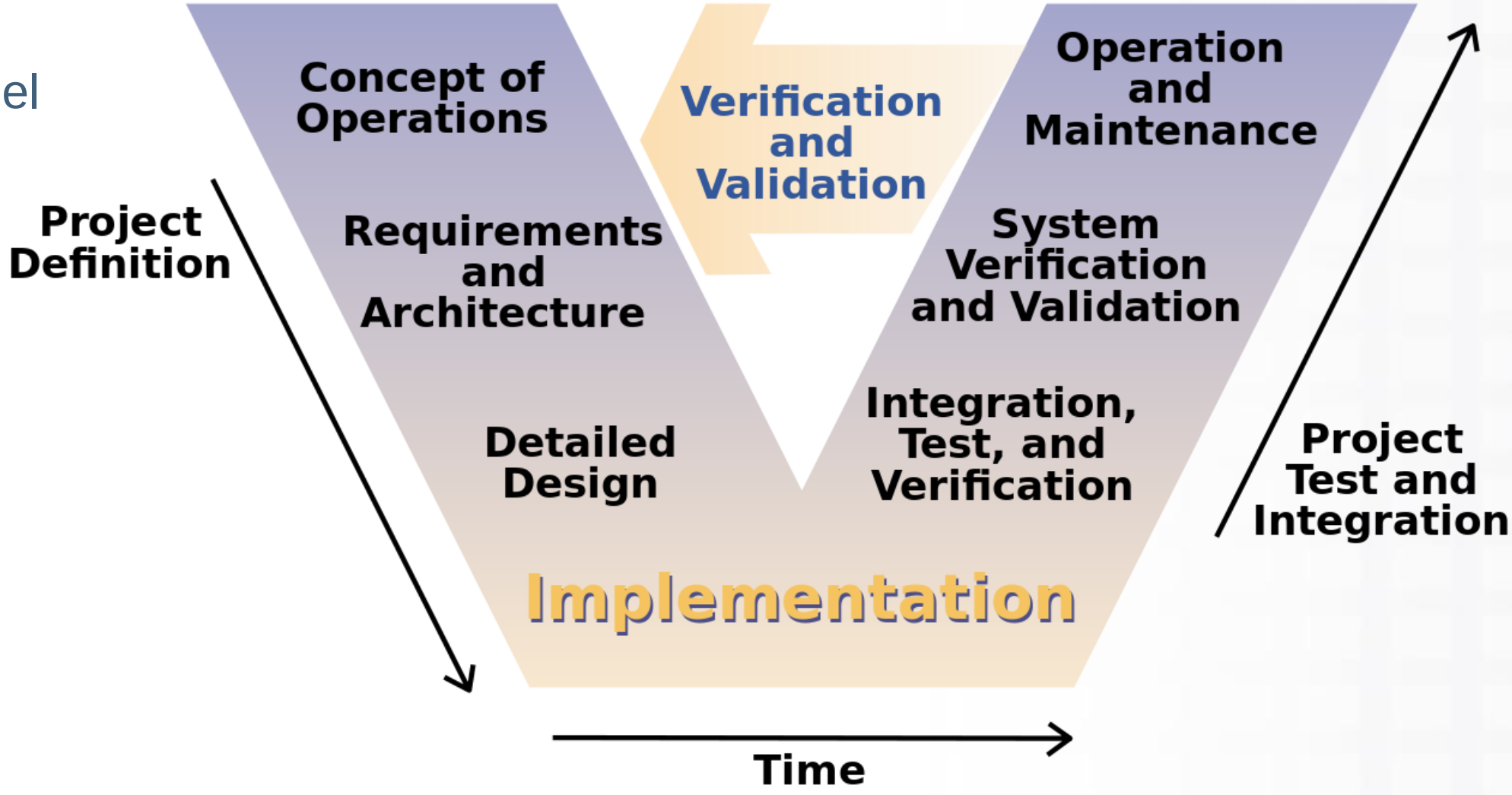
- Waterfall



Vitech

History

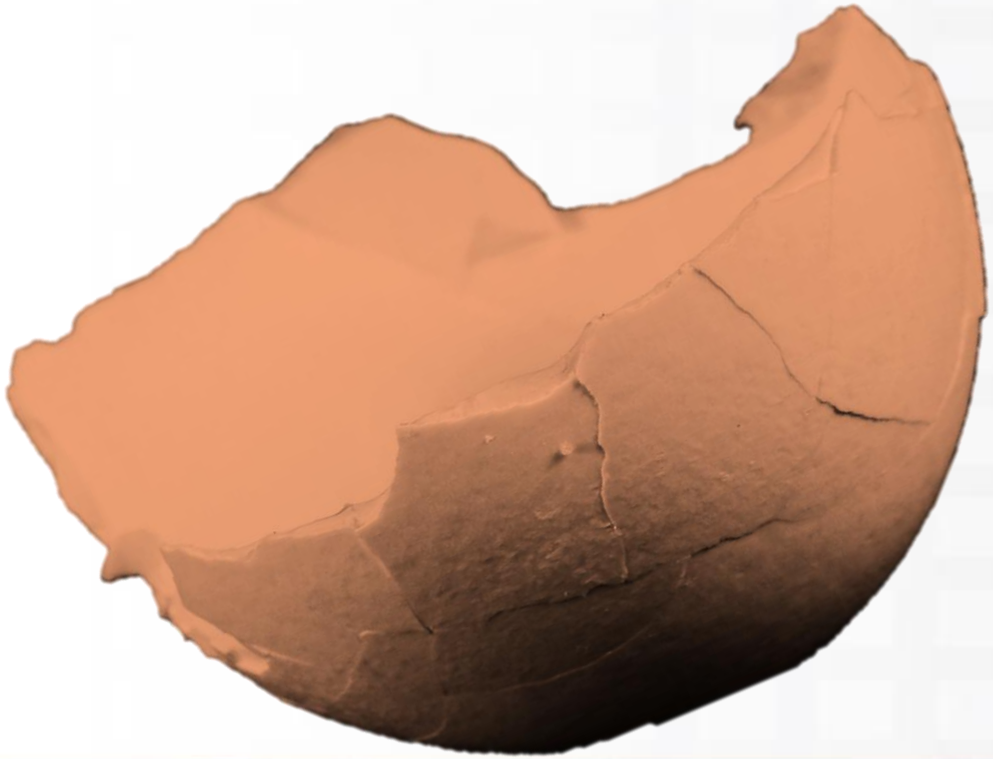
- Waterfall
- Vee- model

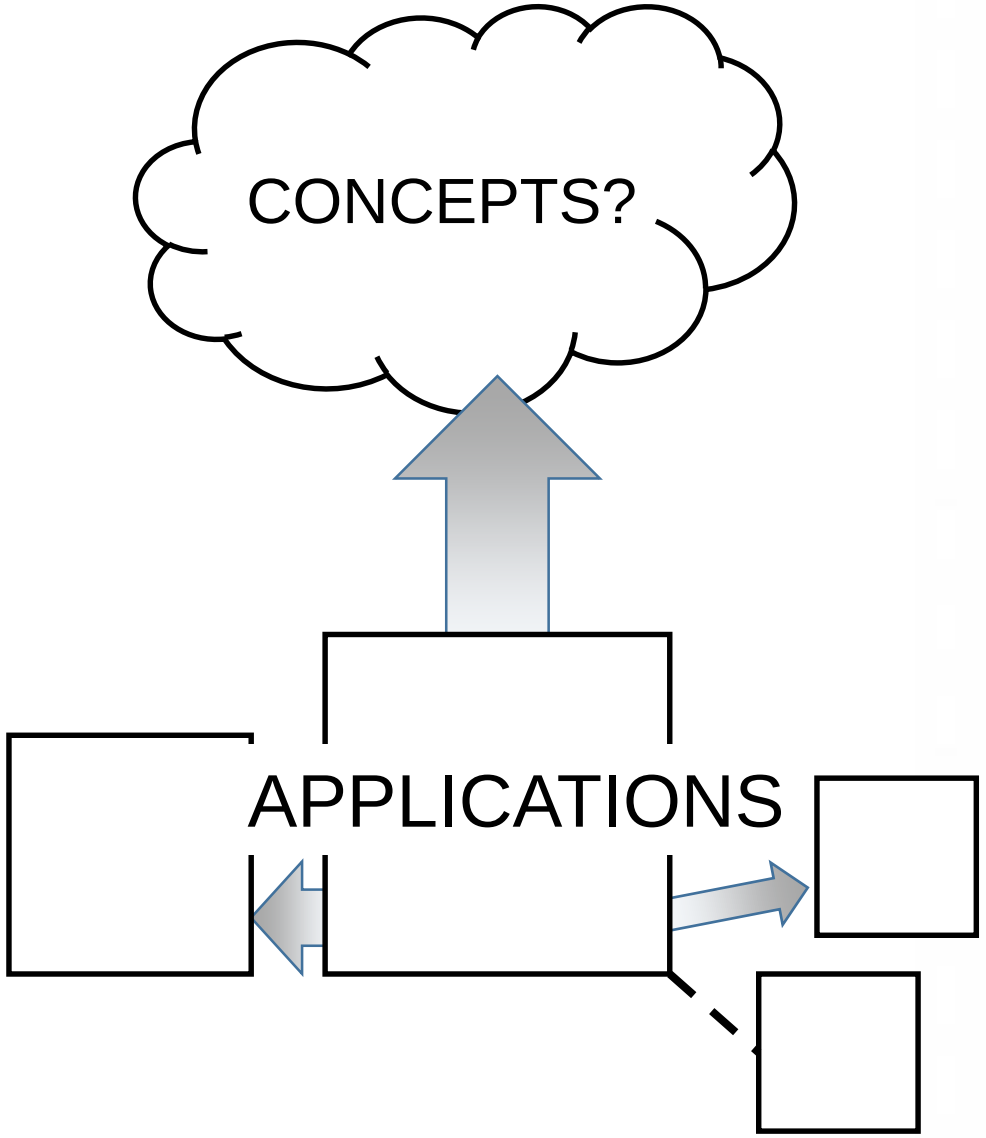


Early definitions

- MIL STD 499
- EIA 632 response to DoD cancellation of MIL STD 499
- Electronic Industries Alliance (EIA) composed of representatives from:
  - DoD,
  - Aircraft Industry Association (AIA),
  - National Security Industries Association (NDIA),
  - Institute of Electrical and Electronics Engineers (IEEE), and
  - INCOSE
- IEEE 1220 (1998), Standard for Application and Management of the Systems Engineering Process
- Process definition

Systems Engineering = Process



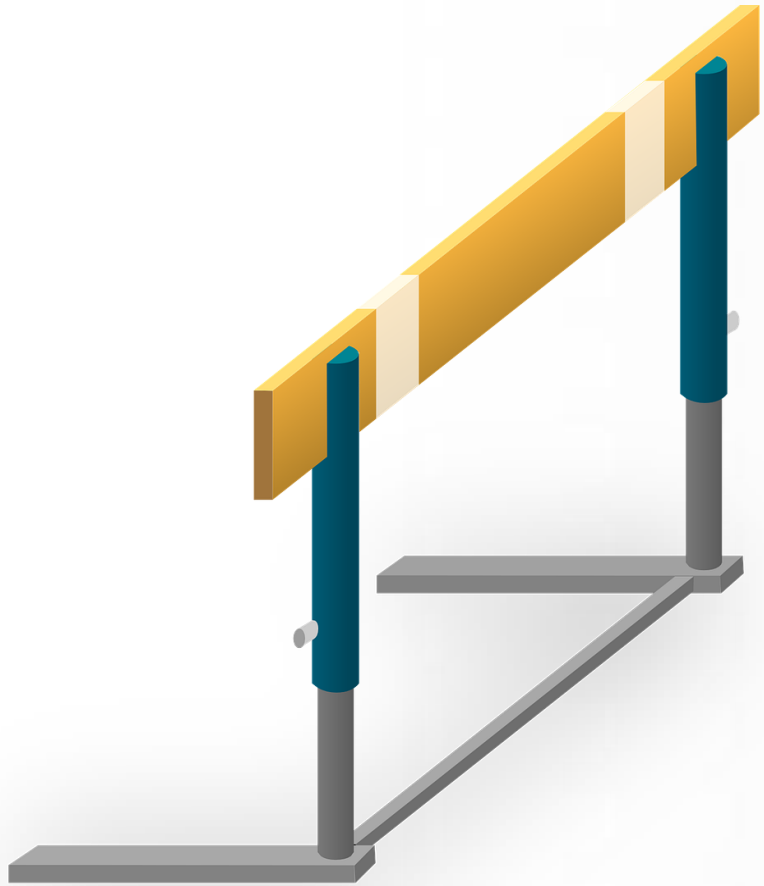

CONCEPTS?
APPLICATIONS

How is that a problem?

- Others don’t recognize processes
- Already tailored
  - Military
  - Aerospace
  - Electronics
  - Software



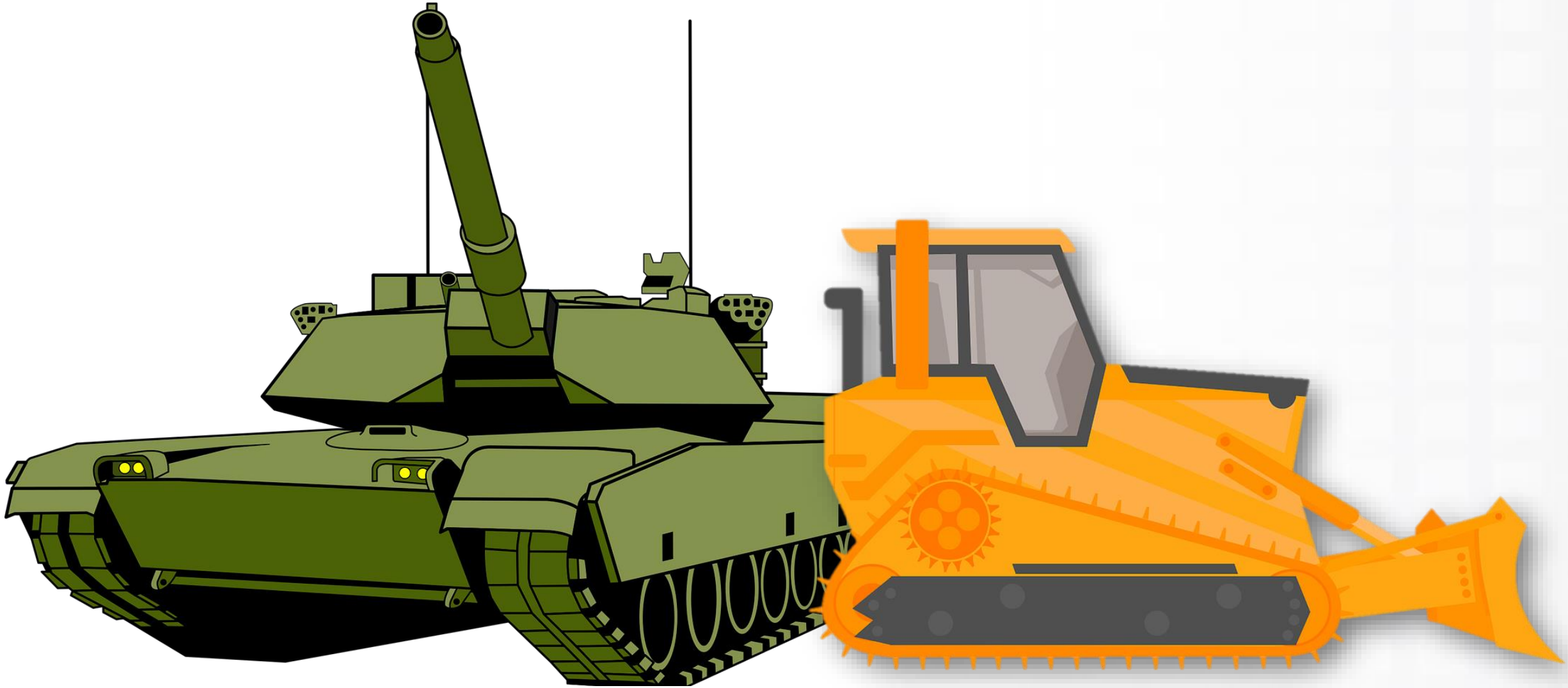
Hurdles



Language

- Jargon
  - SRS, SSDD, SSS
- Confusion
  - Ex.- Failure mode effects analysis (FMEA)
    - Meaning- ASQ, FDA, Oil and Gas, DoD (FMECA)
    - Mil Std 1629A cancelled- move to “commercial standard”
  - “Agnostic”

Contextual vision- This works

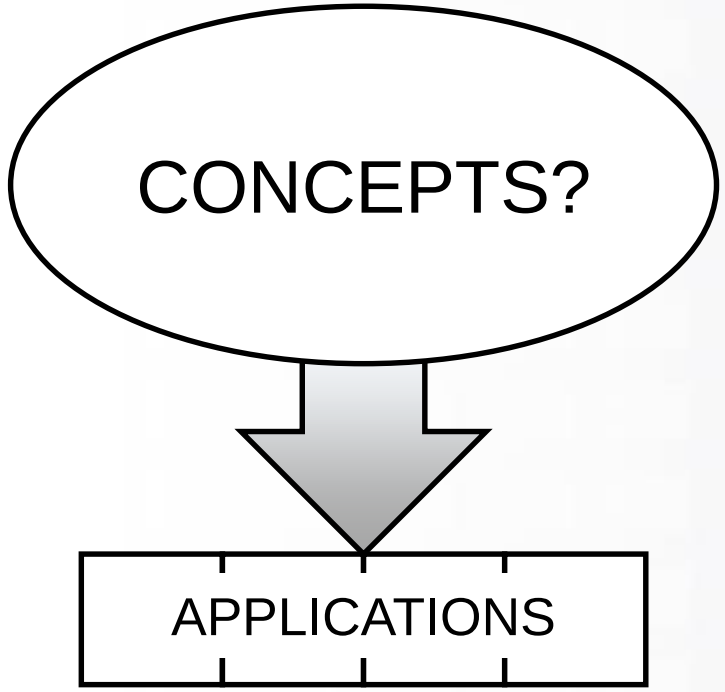


Vitech

Contextual vision- This? Not so much!



Vitech



Systems Engineering

Example- Systems Thinking

- “The standard systems engineering process breaks down a problem into parts, recursively, until the parts are simple enough that we understand them and can design solutions; we then re-assemble the parts to form the whole solution.” A Complexity Primer for Systems Engineers, INCOSE, Sheard, et al (2016)
- “In systems thinking, increases in understanding are believed to be obtainable by expanding the systems to be understood, not by reducing them to their elements. Understanding proceeds from the whole to its parts, not from the parts to the whole as knowledge does.” Russell Ackoff

Example- Complexity

- “But busy systems engineers rarely have the time to keep up with this literature, which is diffused across the many interdisciplinary applications of complex systems science.” A Complexity Primer for Systems Engineers, INCOSE, Sheard, et al (2016)
- Detail v. dynamic; physical v. adaptive
- All systems produce results not possible for any of their elements- this is particularly problematic for complex systems
- Managing complexity
- Desirable complexity- adaptability and resilience

Path Forward



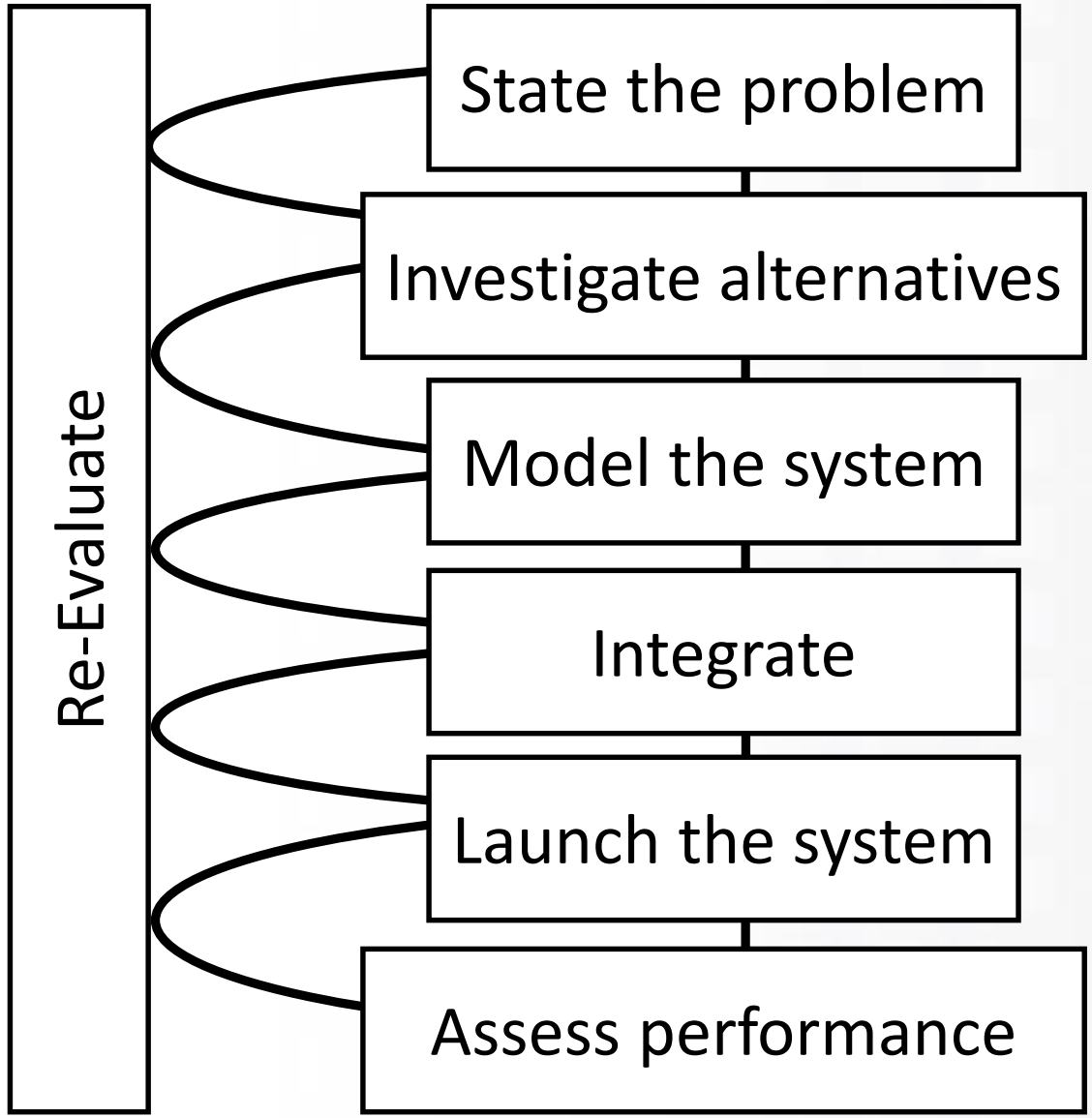
Vitech

Toward a more natural language

"Unless people can express themselves well in ordinary (language), they don't know what they are talking about." Russell Ackoff

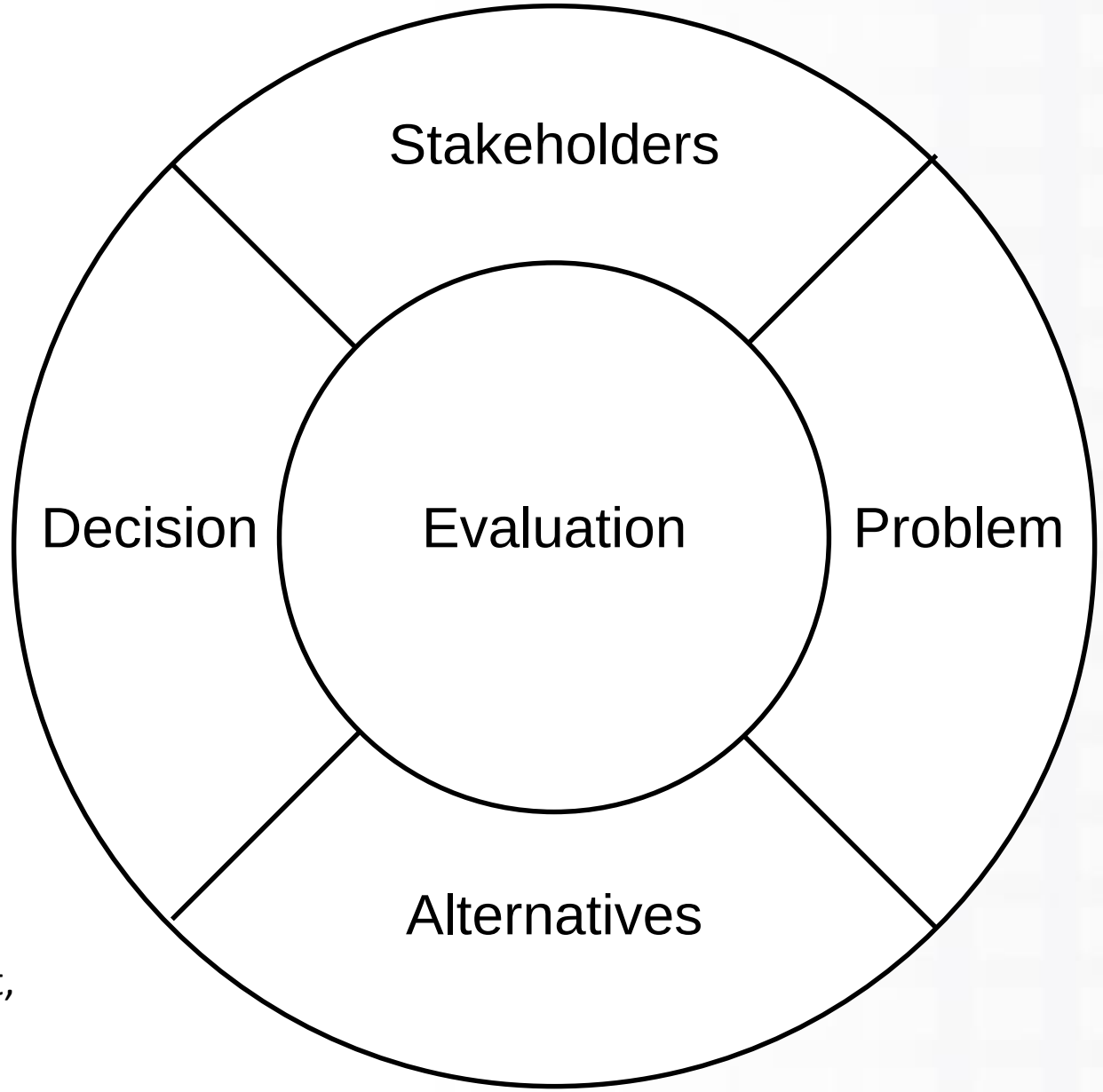
Example-SIMILAR Process

- Bahill & Gissing (1998)



Example- SPADE

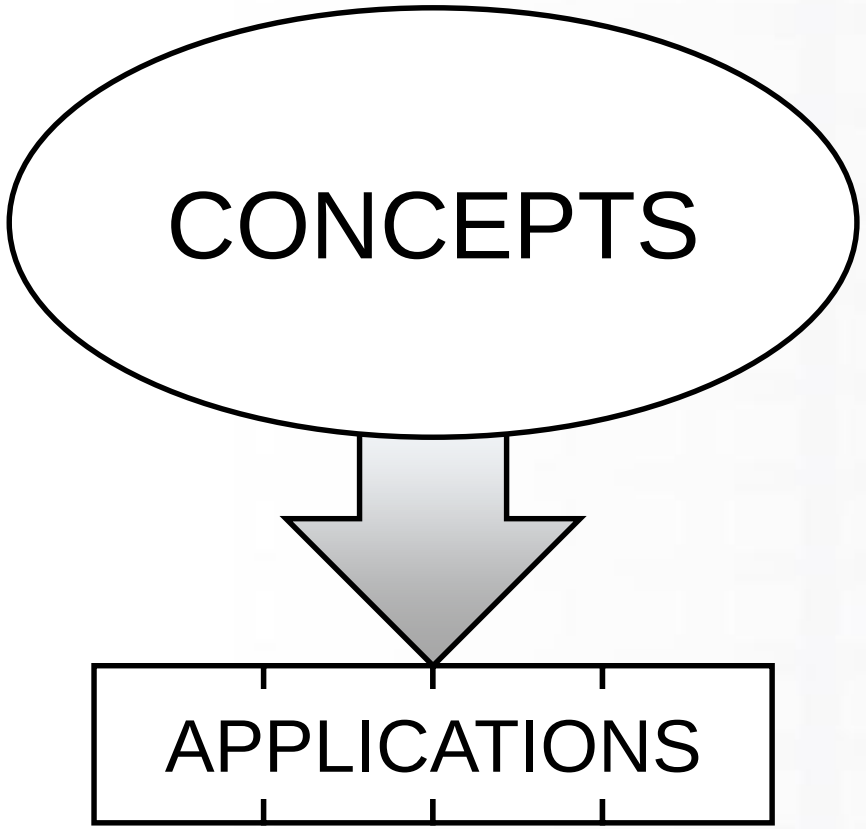
- Haskins (2008)*
  - Stakeholders
  - Problem
  - Alternatives
  - Decision-making
  - Evaluation



* Systems engineering analyzed, synthesized, and applied to sustainable industrial park development, Cecilia Haskins, PhD Thesis, NUST (2008)

Concepts first . . . then application

- Education
  - Systems thinking
  - Complexity
- Training
  - Processes
  - Tailoring



Summary

- Systems engineering developed largely in a specific market segment
- It was defined in terms of processes (as opposed to concepts)
- The processes were highly tailored
- Language was tailored as well
- Transferability (to other domains) is difficult
- We need to learn to see systems engineering at the concept level
- We need to learn to speak in a language (languages?) that others understand
- We need to tailor the solution to the need (not tailor the need to the solution)

Thank You!

Zane Scott

Vice President for Professional Services

Vitech Corporation

zscott@vitechcorp.com

Phone: 540.951.3322 x202

Web: www.vitechcorp.com/ | Blog community.vitechcorp.com | Twitter @VitechCorp

Vitech Corporation Celebrating 25 years of systems engineering excellence

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



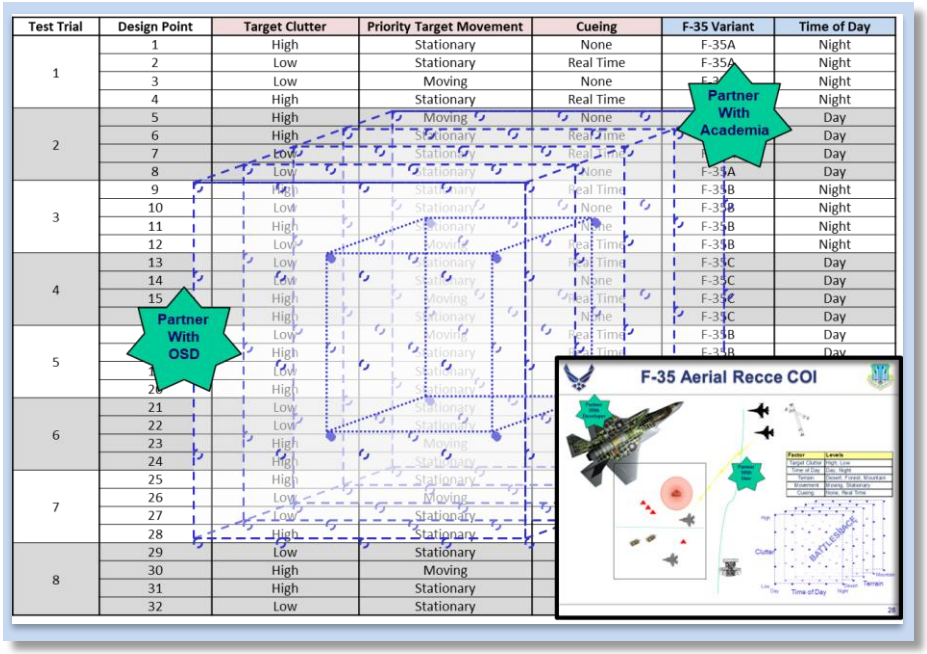
Topics

- Complexity awareness
- Elements of Adaptive V&V
- Importance of partnerships
- Action Plan



Complexity Awareness

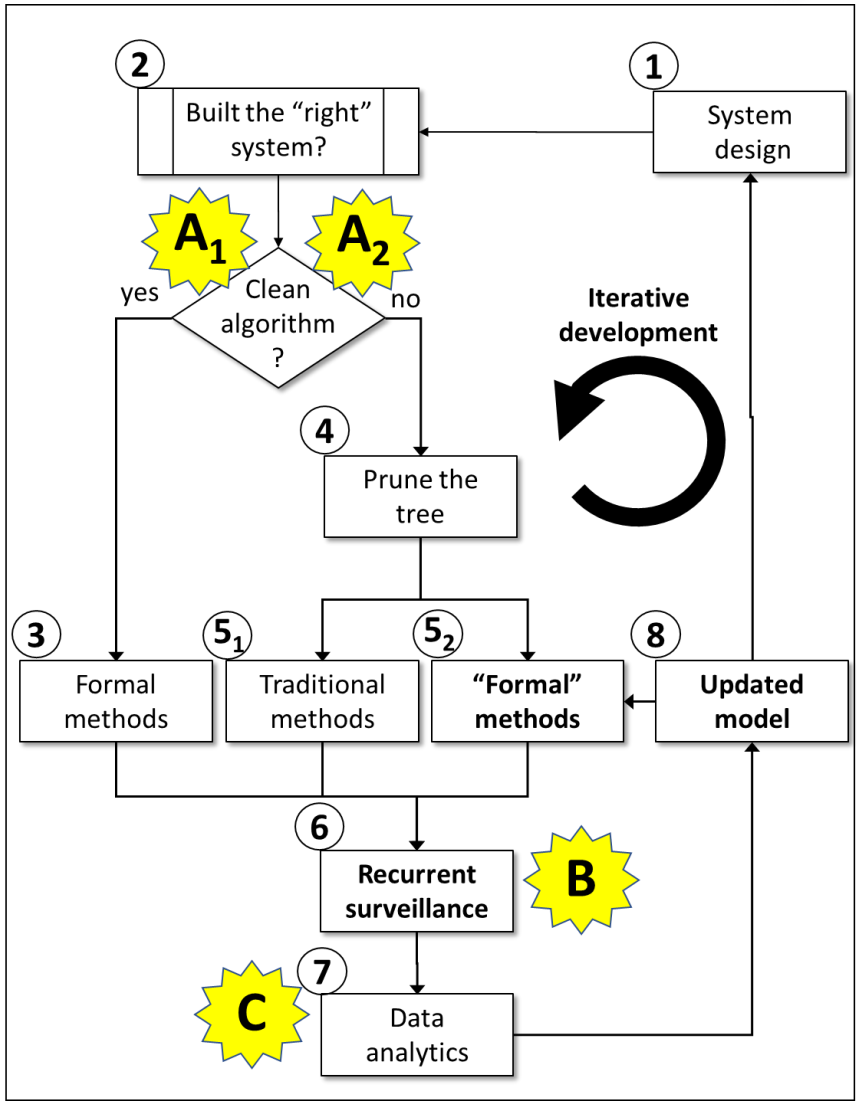
- Too many system states
- Don't have enough bandwidth to cover them all
- Fat tailed probabilities
- Dynamic, asynchronous, ad hoc exchange of digital data among constituents
- Surprises



AFOTEC concept of "hypercube" test matrix

A working model

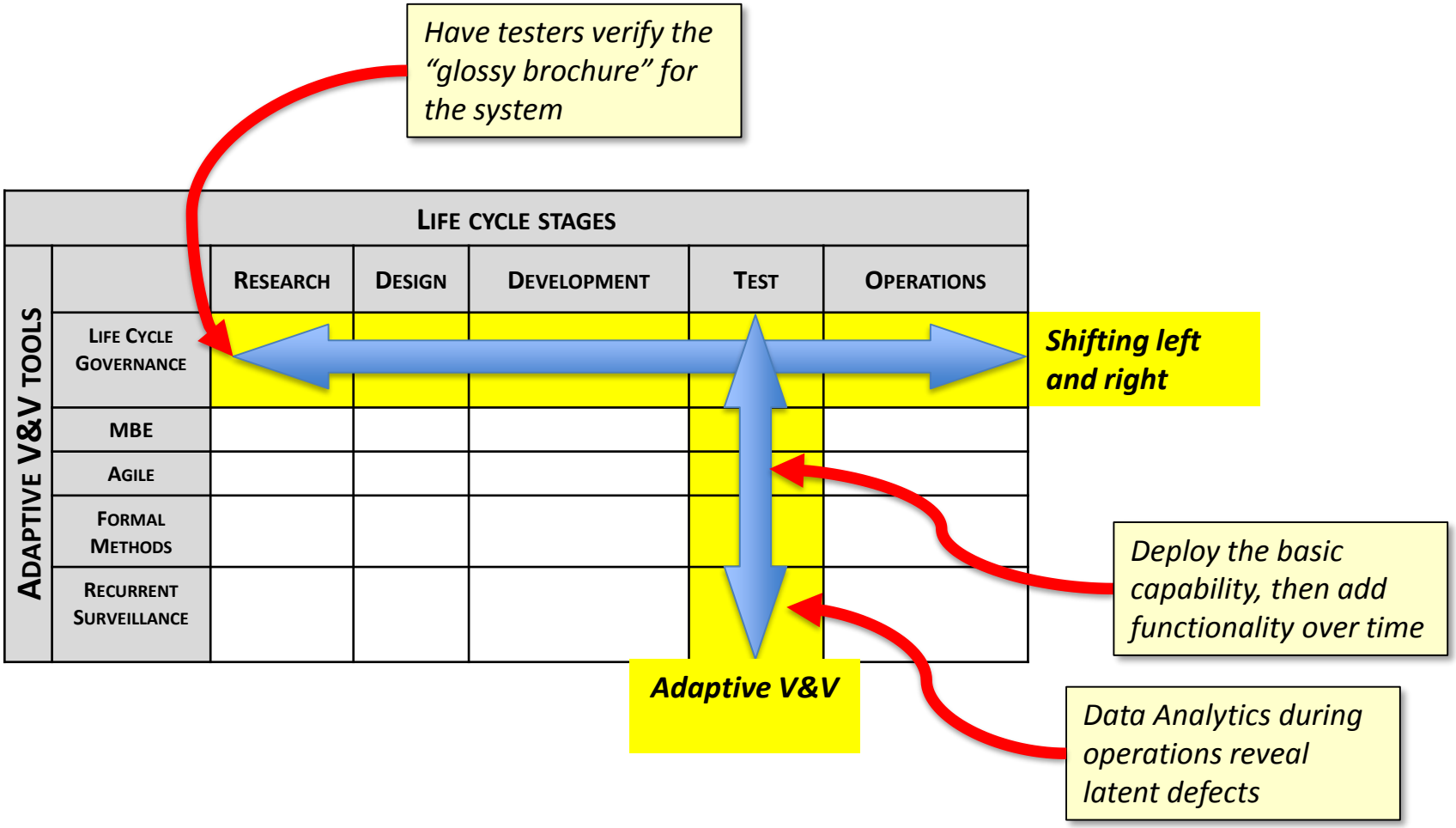
- How do we deal with the problem of complexity (perhaps unrecognized complexity)?
- Here's one possible approach…



Elements of Adaptive V&V



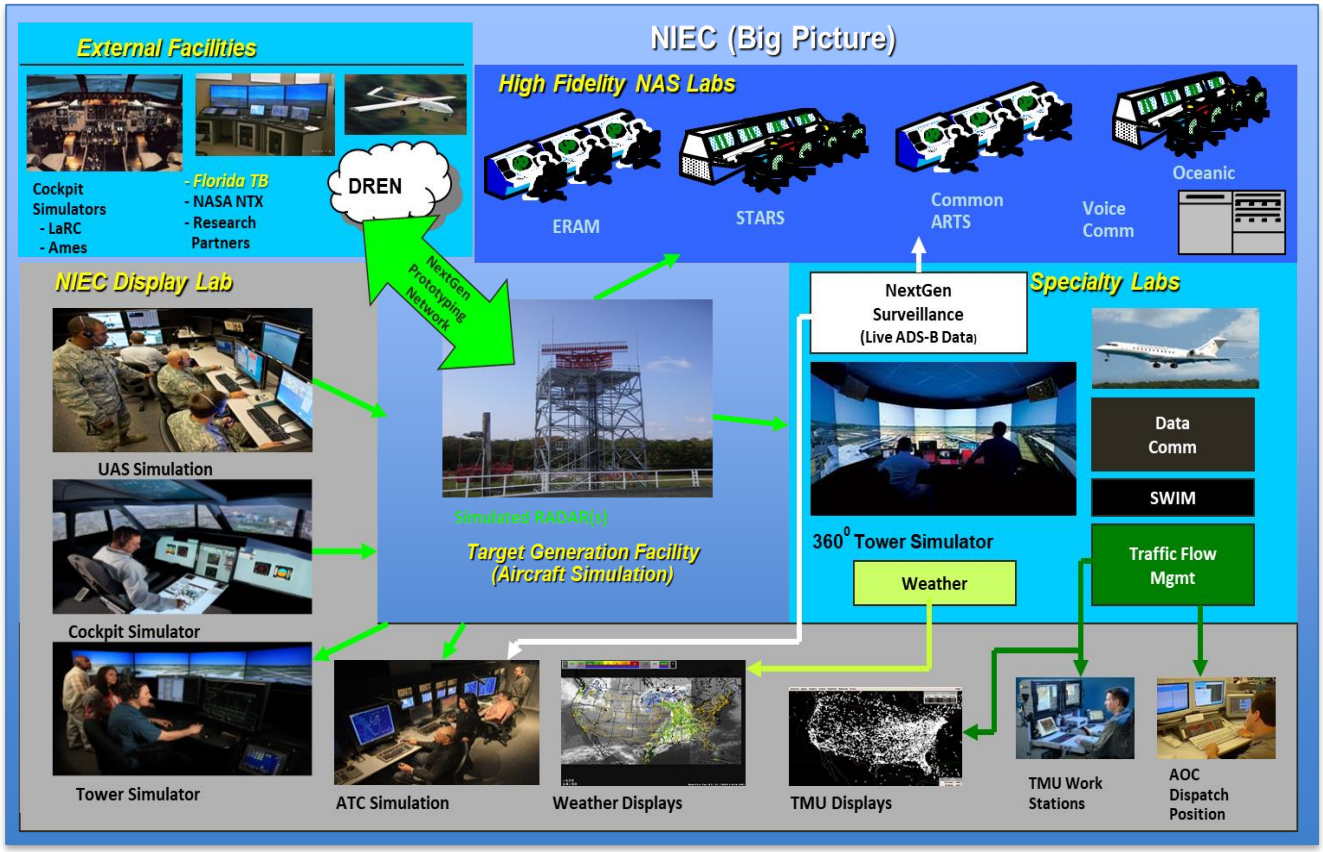
Life Cycle Governance



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

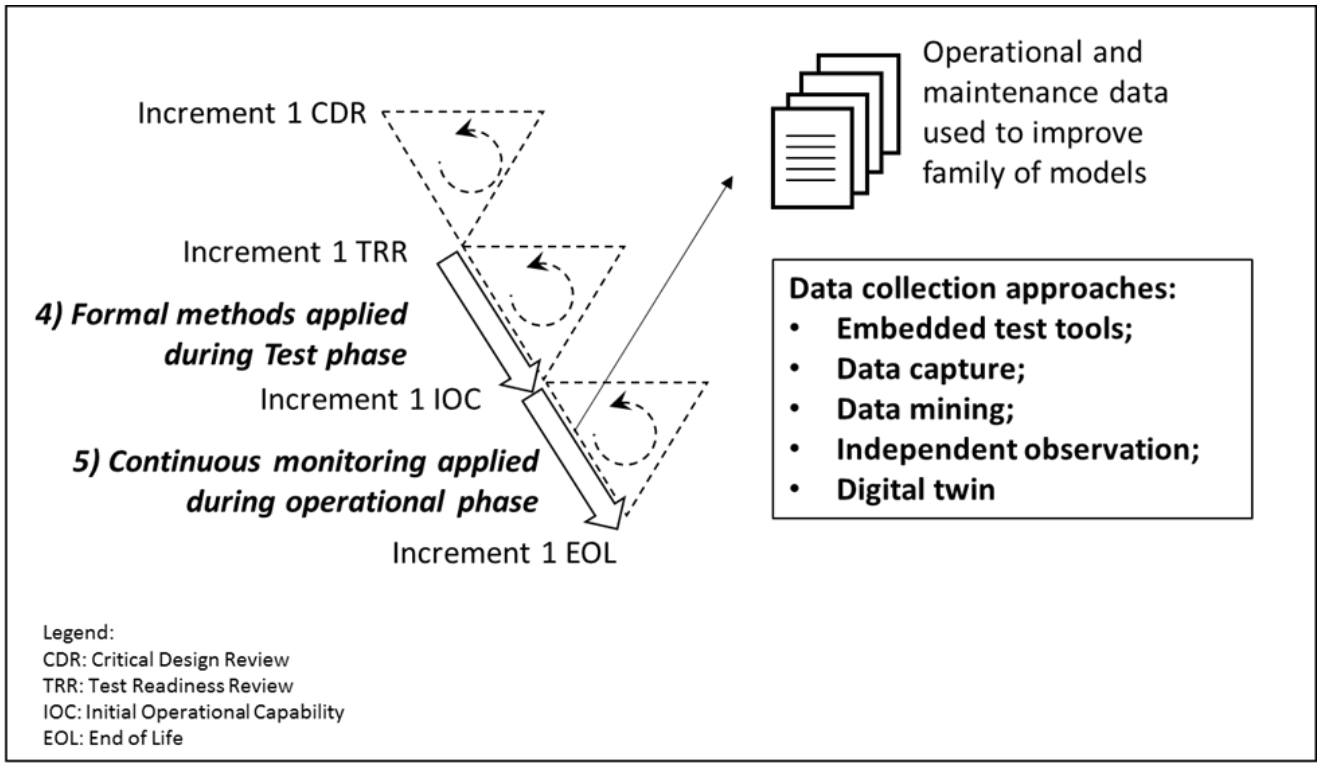
Model Based Engineering



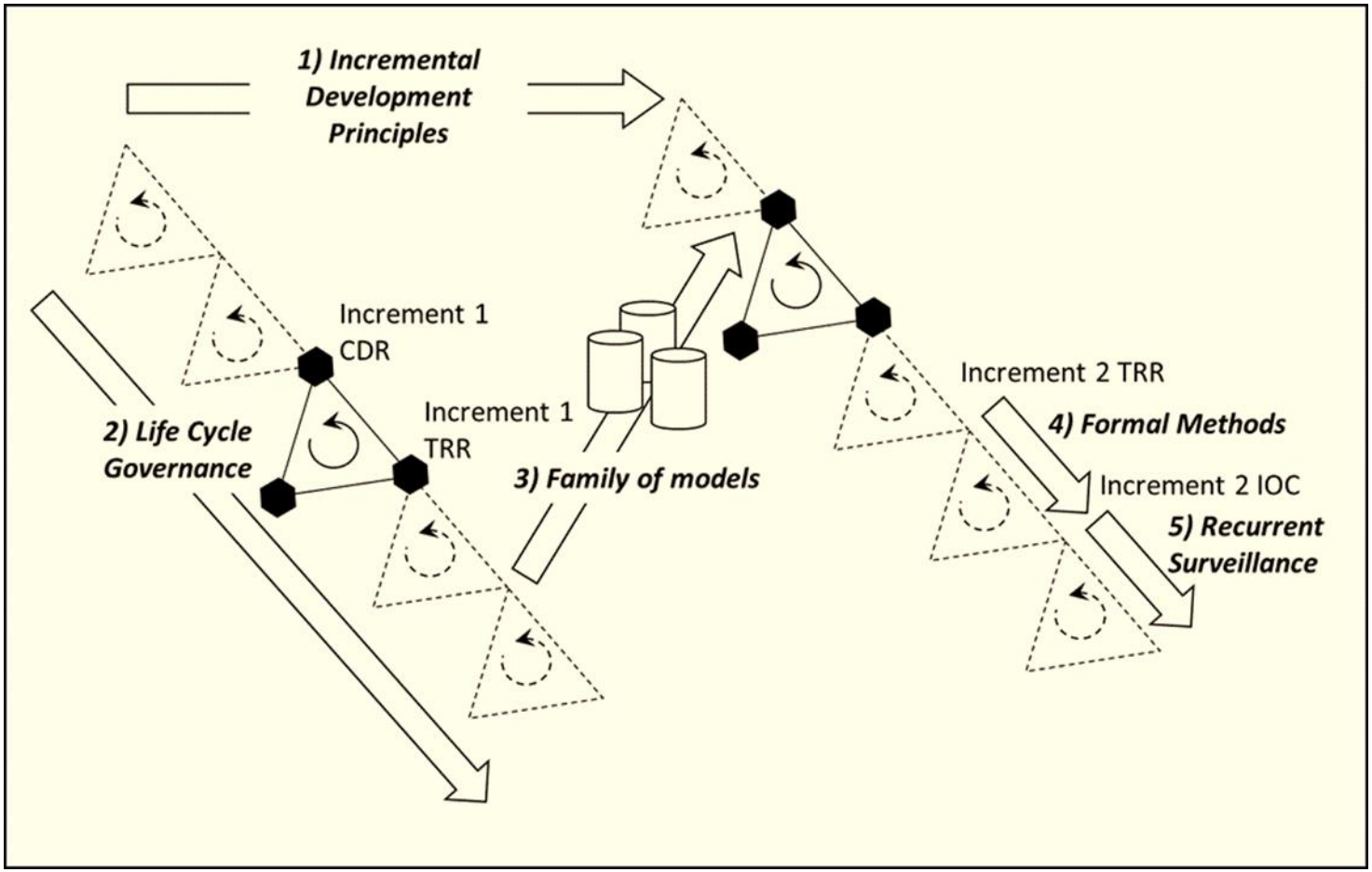
The FAA's NIEC/TGF complex *IS* the MBE core for the NAS!

NIEC – NextGen Integration and Evaluation Center
TGF – Target Generation Facility
MBE – Model Based Engineering
NAS – National Airspace System

Formal Methods and Recurrent Surveillance

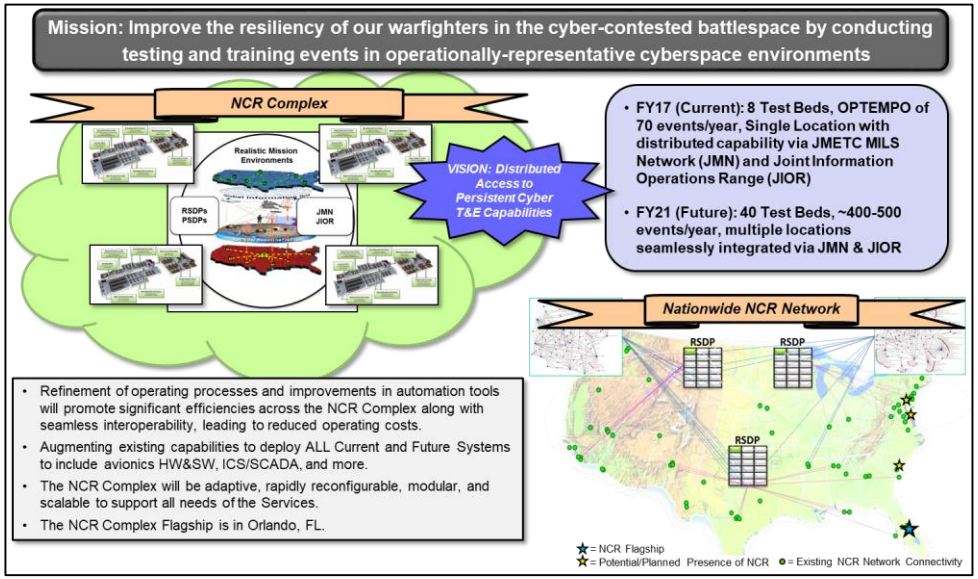


Summary:
The Adaptive V&V Framework



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

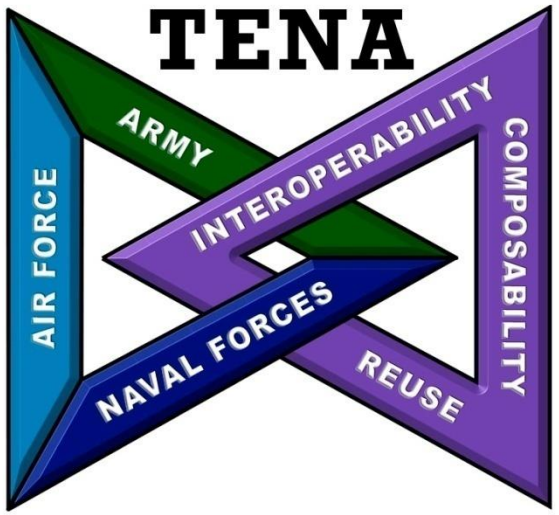
(240) 204-1145

Stevens Institute of Technology

wfelder@stevens.edu

Improving Distributed Test & Evaluation with JMETC & TENA





Ryan Norman

Deputy Program Manager, Joint Mission Environment Test Capability /

Director, Test & Training Enabling Architecture (TENA) Software Development Activity (SDA)

ryan.t.norman.civ@mail.mil

TRMC Missions
DoD (Charter) Directive 5105.71

MRTFB OVERSIGHT / T&E INFRASTRUCTURE

- ***Plan for and assess the adequacy*** *of the MRTFB to provide adequate testing in support of the development, acquisition, fielding, and sustainment of defense systems*
- Support the Department's objective of ensuring **compliance with DoDD 7000.14-R**
- ***Review proposed significant changes*** *to T&E facilities and resources of the MRTFB before they are implemented by the DoD Components*
- **Issue guidance** to the DoD Components, through the USD(AT&L), with respect to MRTFB planning
- Maintain an **awareness of other T&E facilities and resources**, within and outside the DoD, and their impacts on DoD requirements
- Serve as **Executive Agent for Cyber Test Ranges**

STRATEGIC PLAN

- *Complete a strategic plan for T&E not less often than once every 2 fiscal years*

BUDGET CERTIFICATION

- *Submit report to the SECDEF containing the comments of the Director concerning all such proposed budgets, together with the Director's certification as to whether such proposed budgets are* ***adequate***

PROGRAMS

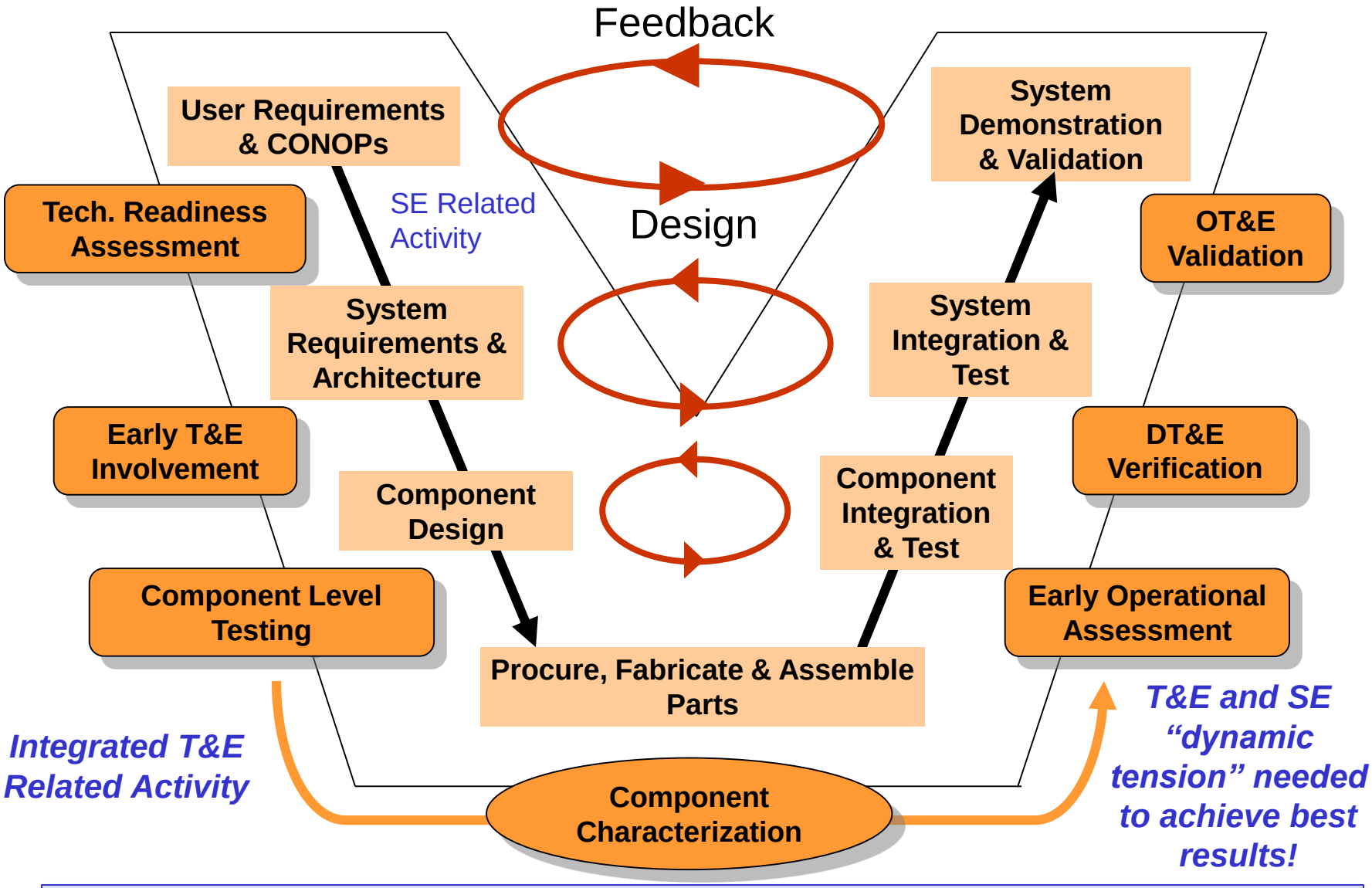
- *Administer the* ***CTEIP*** *(Central Test and Evaluation Investment Program) and* ***T&E/S&T Program***

CAPABILITIES

- Manage and operate the **JMETC** (Joint Mission Environment Test Capability) Multiple Independent Levels of Security (MILS) Network and the Regional Service Delivery Points (RSDP) cloud computing environments
- Manage and operate the **NCR** (National Cyber Range) (IAW RMD 407A1, Issue #1, Title: Cyber, Jan 12, 2015) to provide cyber test capability and capacity for the T&E Community

Statutory **Regulatory**

Why Are We Here?
Distributed T&E Supports Systems Engineering (SE)



T&E Integral to System Reliability Program & Overall Performance Verification

L. Weiss 2009

T&E at a Crossroads

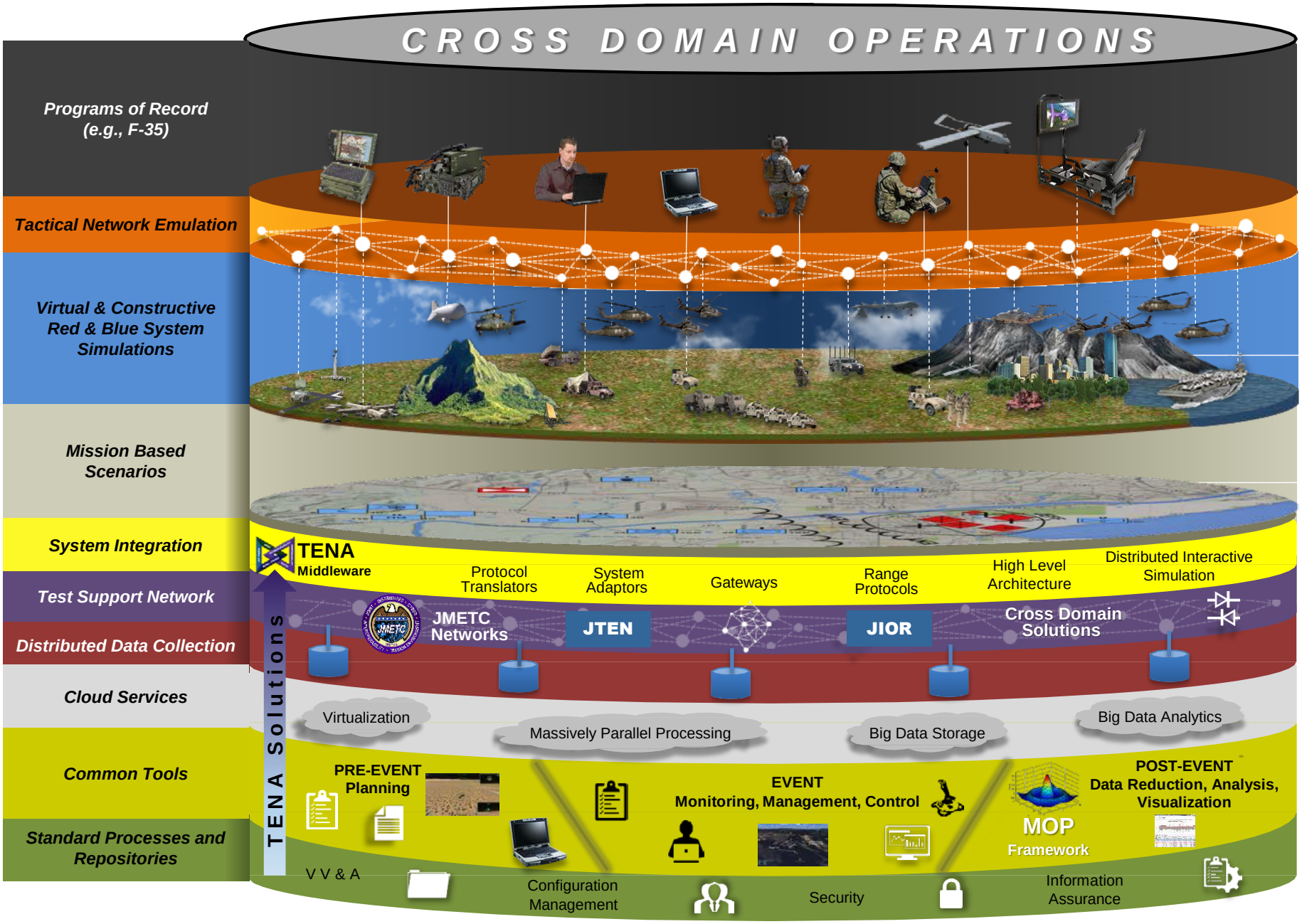
- **Live-Virtual-Constructive distributed T&E mitigates today's biggest testing limitations:**
  - We aren't challenging current generation acquisition systems with complex enough test environments
  - We have limited high priority / low availability assets to go around
  - Testing with multiple security levels / boundaries is too resource-intensive to be viable
  - Information Assurance & Cybersecurity is equal parts necessary and frustrating
  - "Traditional" T&E model not relevant in an agile acquisition world

- **<u>The Problem</u>: Distributed T&E is still "hard" so it isn't a critical part of every program's day-to-day test activities**
  - Connecting disparate lab & range networks needs to be easier & faster
  - Effort needs to shift from environment construction and test execution to improving data analysis capabilities
  - Cooperation & collaboration between facilities needs to be the norm rather than the exception

- **<u>Vision</u>: We must make distributed T&E routine**
  - **Before JMETC:** Months / Years to plan, execute, & analyze
  - **With JMETC Now:** Weeks / Months to plan, execute, & analyze
  - **Our Need:** Hours / Days to plan, execute, & analyze

T&E risks irrelevance if we don't address these limitations

Vision: Agile T&E Infrastructure that supports acquisition



Example Assets Available Through Distributed T&E Infrastructure



The right interface makes this environment available

Joint Mission Environment Test Capability (JMETC) Program



- **Distributed Testing (Events, Tools, etc.)**
- **JMETC Secret Network (JSN)**
- **Test & Training Enabling Architecture (TENA)**
  - TENA Object Models
  - TENA Web Services
  - TENA Software Repository
  - TENA Tools
- **Big Data / Knowledge Management Initiative**
- **National Cyber Range Complex (NCRC)**
  - National Cyber Range (NCR)
  - Regional Service Delivery Points (RSDPs)
  - NCR Expansion (Service Sites)
- **JMETC MILS Network (JMN)**
- **Executive Agent (EA) for Cyber Test Ranges**

Distributed T&E Ingredients Supporting the Vision

- **Connectivity: "Persistent MILS Network"**
  - Common network practices & procedures that reduce test execution risk
  - Shared Cross Domain Solutions (CDS) that reduce cost to use & maintain
  - Proactive monitoring & troubleshooting when things gone wrong
- **Analysis Capabilities: "Bring Big Data Analytics to T&E"**
  - Connections to physically disparate data sources
  - Automated analysis and reporting capabilities
  - Empower analysts to ask questions they never thought possible to ask
- **Information Assurance / Cybersecurity: "Balancing security & mission"**
  - Pre-negotiated security agreements with reciprocity across disparate domains
  - Common Risk Management Framework (RMF) Overlay for RDT&E Networks
  - Shared software certifications for common tools
- **Subject Matter Expertise: "JMETC is its people"**
  - Seasoned team with decades of hands-on distributed T&E experience
  - "Walking Encyclopedias" of available test assets & best practices

JMETC Benefits Acquisition Programs, Testers, & Evaluators

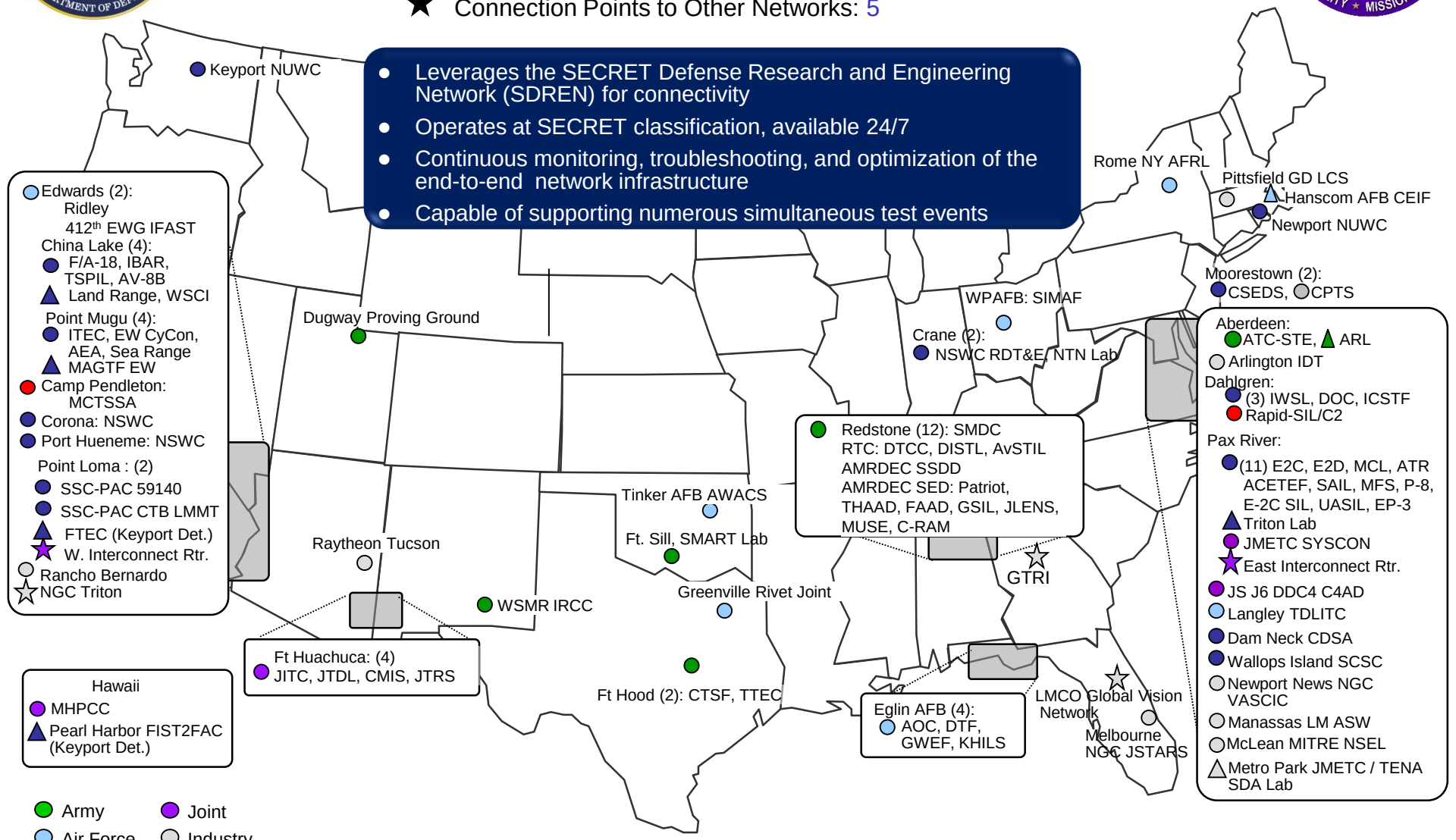
- Enables early verification that systems work in a Joint Environment
  - Test whether systems work well together
- Supports all aspects of testing
  - Rapid acquisition, Developmental Test, Operational Test, Interoperability Certification, Net-Ready Key Performance Parameters testing, Joint Mission Capability Portfolio testing
- Helps find problems early in acquisition – when they are less costly to fix
  - Customers have run as many as 20 independent test runs in a day and fixed interoperability issues overnight
- Reduces acquisition time and cost
  - Readily-available, persistent connectivity with standing network security agreements
  - Common integration software for linking sites
  - Accredited test tools for distributed testing
- Support to Acquisition Programs
  - Expertise to integrate distributed test facilities

JMETC is identified in T&E Master Plans (TEMPs) as the distributed infrastructure to be used to conduct Joint testing

JMETC SECRET Network (JSN) Site Map

- Functional JSN Locations: 46 (access to 79 labs/facilities)
- Planned JSN Locations: 9
- Connection Points to Other Networks: 5

- Leverages the SECRET Defense Research and Engineering Network (SDREN) for connectivity
- Operates at SECRET classification, available 24/7
- Continuous monitoring, troubleshooting, and optimization of the end-to-end network infrastructure
- Capable of supporting numerous simultaneous test events



As of 21 Aug 2017

DISTRIBUTION A. Approved for public release: distribution unlimited.

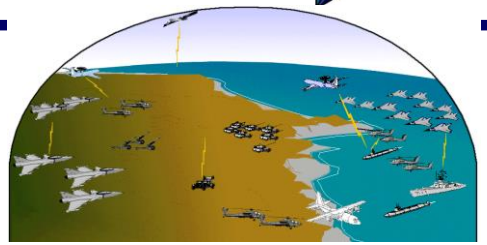
JMETC Uses TENA as its Distributed Test Architecture

Joint Operational Scenarios

Systems Under Test

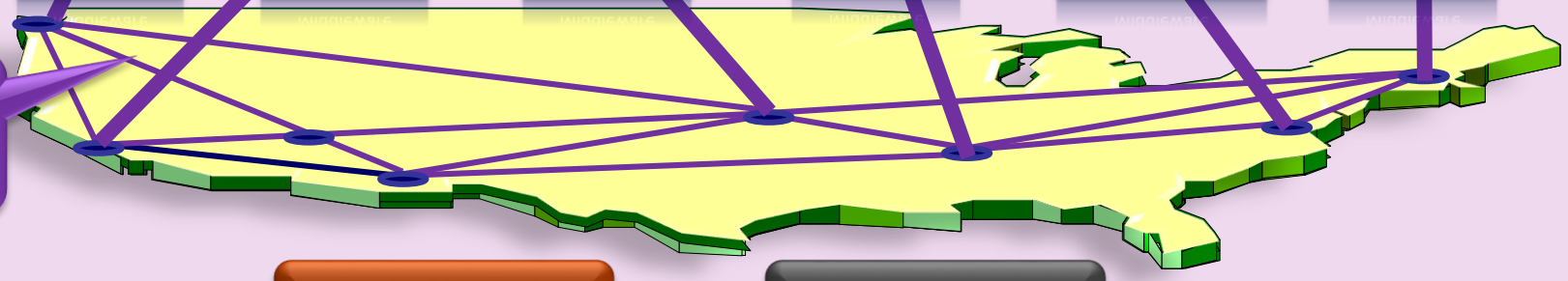






Integrated Test Resources

Virtual Prototype	Hardware in the Loop	Installed Systems Test Facility	Range	Environment Generator	Threat Systems
TENA Standard Interface Definitions	TENA Standard Interface Definitions	TENA Standard Interface Definitions	TENA Standard Interface Definitions	TENA Standard Interface Definitions	TENA Standard Interface Definitions
TENA Common Middleware	TENA Common Middleware	TENA Common Middleware	TENA Common Middleware	TENA Common Middleware	TENA Common Middleware



JMETC Infrastructure on DREN

Reuse Repository

Distributed Test Support Tools

* TENA: Test and Training Enabling Architecture

Enterprise Software Ingredients Supporting the Vision

- **System Integration Tools: "LVC Interoperability is our mission"**
  - Software that reduces test setup & design costs in a mixed architecture environment
  - Cross Domain Solutions that bridge classification levels and/or security boundaries
  - Adapters that enable communication without changing existing systems' behaviors
- **Common Tools: "Build once, use everywhere"**
  - Community tools readily available for download and use
  - Event Planning tools that simplify event integration and setup
  - Event Management tools that enable total awareness
  - Post-Test Event Analysis tools that embrace big data analytics techniques
- **Collaboration Tools: "The sum is better than the parts"**
  - Community-wide and DoD-only event collaboration
  - Community-wide and DoD-only source code collaboration
- **Cloud Services: "Embrace Testing as a Service (TaaS)"**
  - Immersive constructive environments available "on demand"
  - Re-hosted acquisition system software readily available for use (e.g. JSF system software)
  - Reduce local software footprint to mitigate Information Assurance headaches

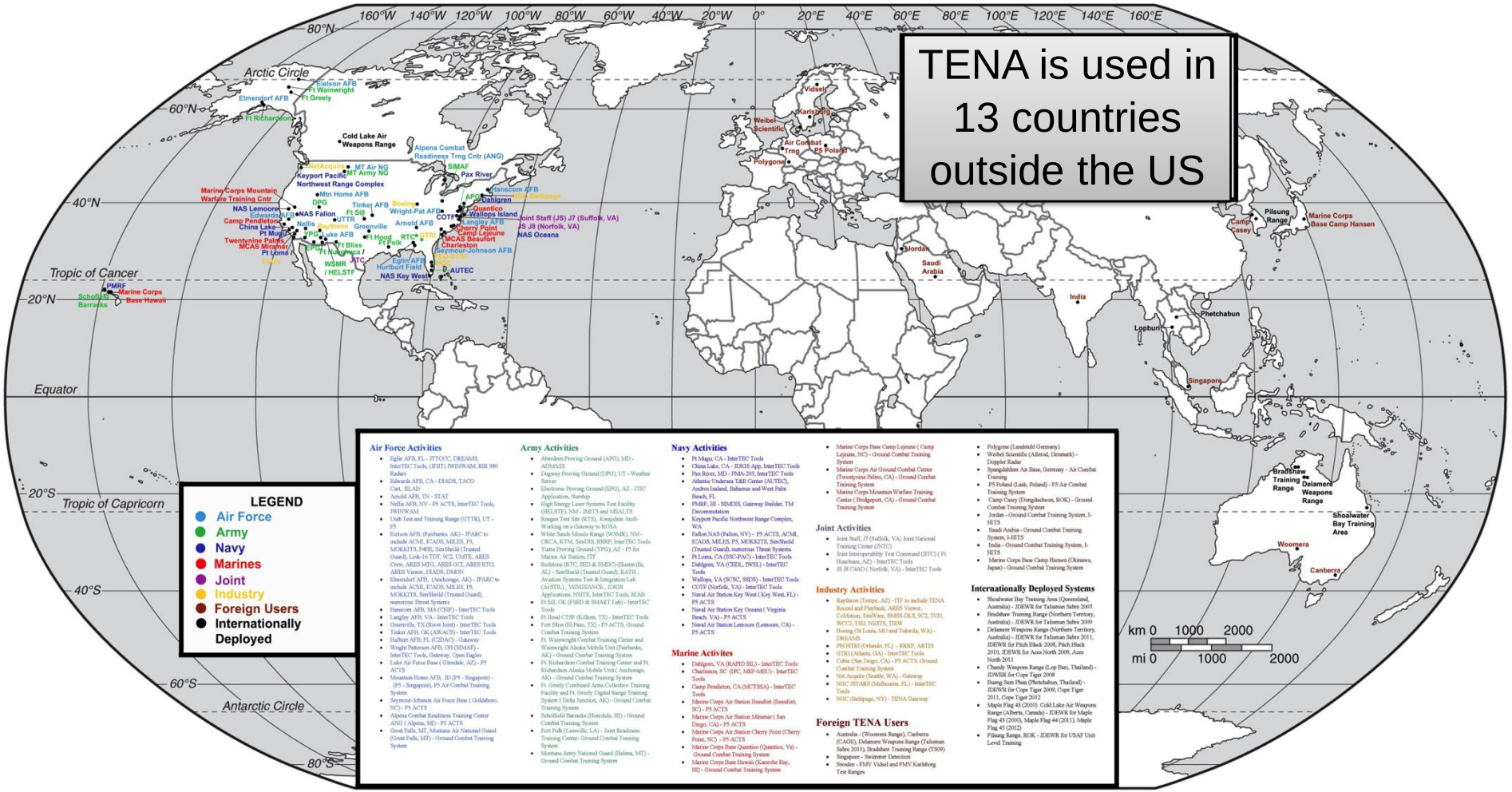
Test and Training Enabling Architecture (TENA) at a Glance

TENA is DoD's GOTS range integration architecture

- **What does TENA enable?**
  - Interoperability between inter- and intra-range assets
  - Elimination of proprietary interfaces to range instrumentation
  - Efficient incremental upgrades to test and training capabilities
  - Integration of Live, Virtual, and Constructive assets (locally or distributed)
  - Sharing and reuse of common capabilities across existing and new investments
- **What is included in the TENA architecture?**
  - Customizable "data contracts" that standardize repeatable information exchange
  - Interoperability-enabling, auto-code generated software libraries
  - A core set of tools that address common test and training requirements
  - Collaboration mechanisms that facilitate sharing and reuse
- **TENA has a plan for continued evolution and funding to execute this plan**

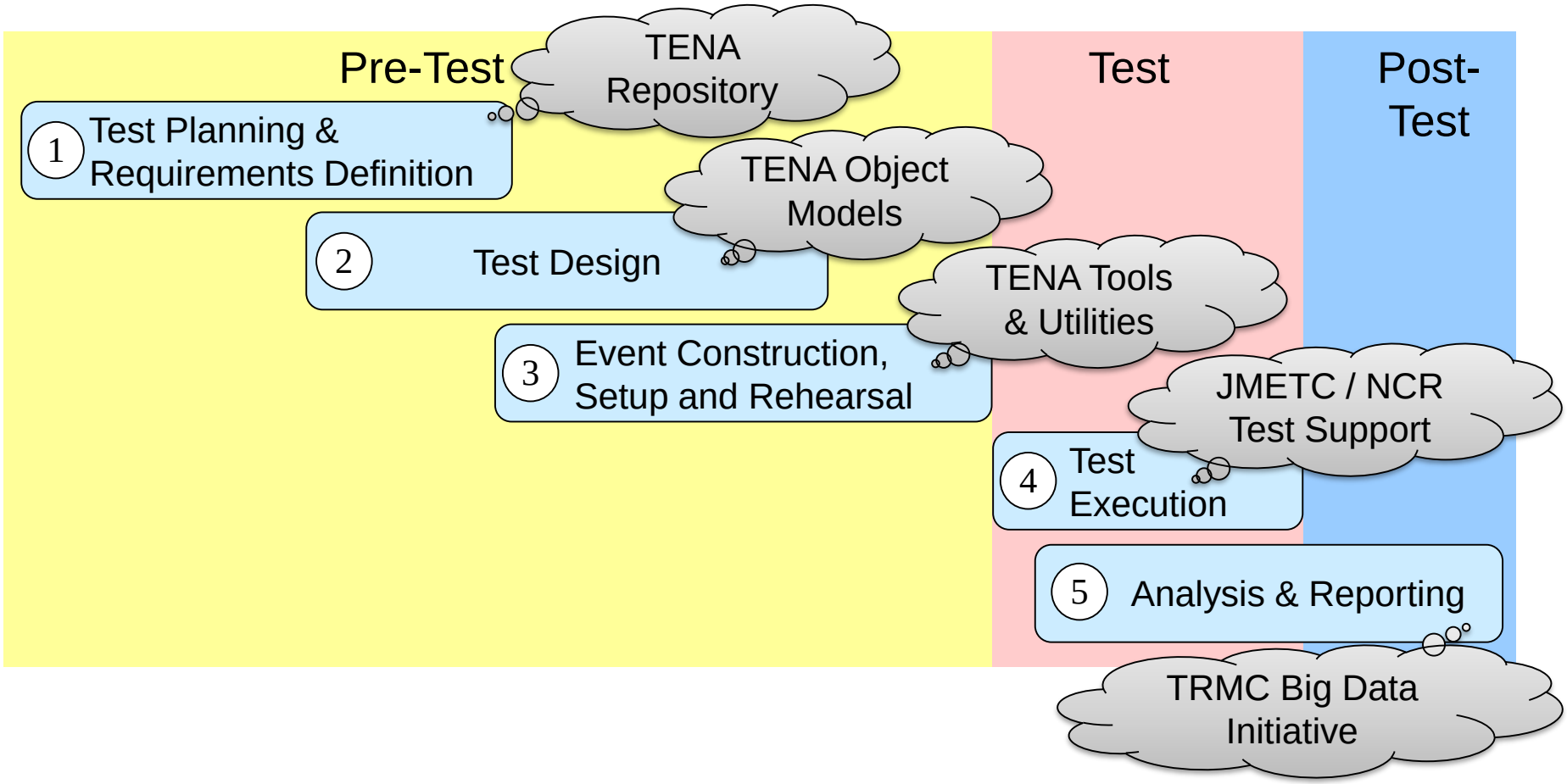
TENA ENABLED
Test and Training Enabling Architecture

Worldwide Use of TENA



How TRMC Supports T&E: Notional Test Walkthrough

TRMC Subject Matter Expertise (SME) supports entire process



JMETC Current Focus Areas

- **Investigating Information Assurance / Cybersecurity Services that would be value-added to the community**
  - Examples: TRMC software certifications, TRMC AO support, ATO / ISA assistance
- **Transitioning MLS-JCNE Cross Domain Solutions into JMETC SYSCON capabilities**
- **Considering how to bring distributed T&E into areas with limited network infrastructure and/or a single event need**
- **Researching where automation can lead to efficiencies**
  - Example: Ports-Protocol Verification Test Application
- **Reinstituting formal Post-Event User Feedback**
  - Examples: Post-Event Survey; Infrastructure After Action Review as-needed
- **Continually identifying areas where we can do things faster and/or cheaper**

TENA SDA Current Focus Areas

- Supporting capabilities development at ranges & labs
- Enabling TENA use in TRMC CTEIP and T&E S&T projects
- Expanding a GOTS library of range systems adapters
- Standardizing instrumentation remote monitoring and control
- Updating Object Models to better mix Virtual-Constructive with Live
- Improving enterprise tools & utilities
- Enhancing TENA Website Services
- Prototyping Enterprise Software Sharing Repository
- Exploring Software as a Service (SaaS) in the cloud
- Preparing for an enterprise Knowledge Management / Big Data Analytics capability
- Developing a “common language” for cyber T&E and training

JMETC / TENA Support Offer

- **The JMETC / TENA team is available to offer advice and assist any organization looking to use TENA**
  - Advice on overall design approach and trade-offs to consider
  - Recommended Object Models to reuse
  - Recommendations on how to design new Object Models
  - Implementation / Code Designs Reviews
  - Awareness of similar systems and lessons learned
  - Hands-on Training classes on TENA capabilities
  - Contract language to help ensure TENA-enabled solutions
  - Network connectivity to CONUS & OCONUS labs / ranges / facilities
  - Distributed event subject matter expertise

Need Assistance?

E-mail request to: feedback@trmc.osd.mil

Summary

- **<u>Vision</u>: An agile Test & Evaluation Infrastructure that support acquisition requirements**
  - Robust, Immersive, Easy-to-Construct Live-Virtual-Constructive Test Environments
  - Agility that supports rapid acquisition & experimentation along with traditional DT / OT
- **TENA provides the architecture and enterprise software foundation to achieve the vision**
- **JMETC provides the network and LVC expertise to achieve the vision**
- **The JMETC / TENA SDA Team is here to help**
  - TENA Upgrade support offer
  - Distributed Test Event Subject Matter Experts (SMEs)
  - Knowledge Management and Big Data Analytics support
  - Information Assurance / Cybersecurity assistance

JMETC Points of Contact

TENA Software Development Activity (SDA) Director
Ryan Norman
(571) 372-2725
ryan.t.norman.civ@mail.mil

JMETC Program Manager
George Rumford
(571) 372-2724
george.j.rumford.civ@mail.mil

National Cyber Range Complex (NCRC) Director
AJ Pathmanathan
(571) 372-2702
arjuna.pathmanathan.civ@mail.mil

Event Scheduling / Event Questions

Interoperability Events
Keith Poch
(850) 389-6044
keith.poch@tena-sda.org

Distributed Tests
Linking Sites

Cyber Events
Lizann Messerschmidt
(571) 451-4295
lizann@mitre.org

NCR Events
RSDP Events

NCRC Expansion / Site Questions

NCRC, Deputy Director
Rob Tamburello
(501) 372-2753
robert.n.tamburello.civ@mail.mil

TENA Products / Software Repository

TENA Software Development Manager
Steve Bachinsky
(703) 253-1068
steve.bachinsky@tena-sda.org

Connectivity / Network Questions

JMETC Secret Network (JSN)
Jeff Braget
(850) 389-6031
jeff.braget@tena-sda.org

Secret Only
Always Connected

JMETC MILS Network (JMN)
Ben Wilson
(757) 492-7621
bennett.wilson@navy.mil

Above Secret (TS/SCI/SAP)
Connected Only During Event

Miscellaneous Questions

For JMETC questions: feedback@jmetc.org
For TENA questions: feedback@tena-sda.org

Websites

Unclassified, FOUO, DoD-Restricted (CAC required): https://www.trmc.osd.mil
Distribution A, Industry, non-DoD (username/password required): https://www.tena-sda.org

Help Desk

Action Items, Questions, Tasks, Software Needs, Bug Reports: https://www.tena-sda.org/helpdesk

The Systems of Systems (SoS) Primer: A Guide to SoS for all Expertise Levels

October 2017

Laura Antul lantul@mitre.org
Dr. Judith Dahmann jdahmann@mitre.org
Dr. Aleksandra Markina-Khusid amk@mitre.org
Dr. Ryan Jacobs rjacobs@mitre.org

NDIA 20th Annual Systems Engineering Conference
http://www.ndia.org/events/2017/10/23/20th-systems-engineering-conference

MITRE

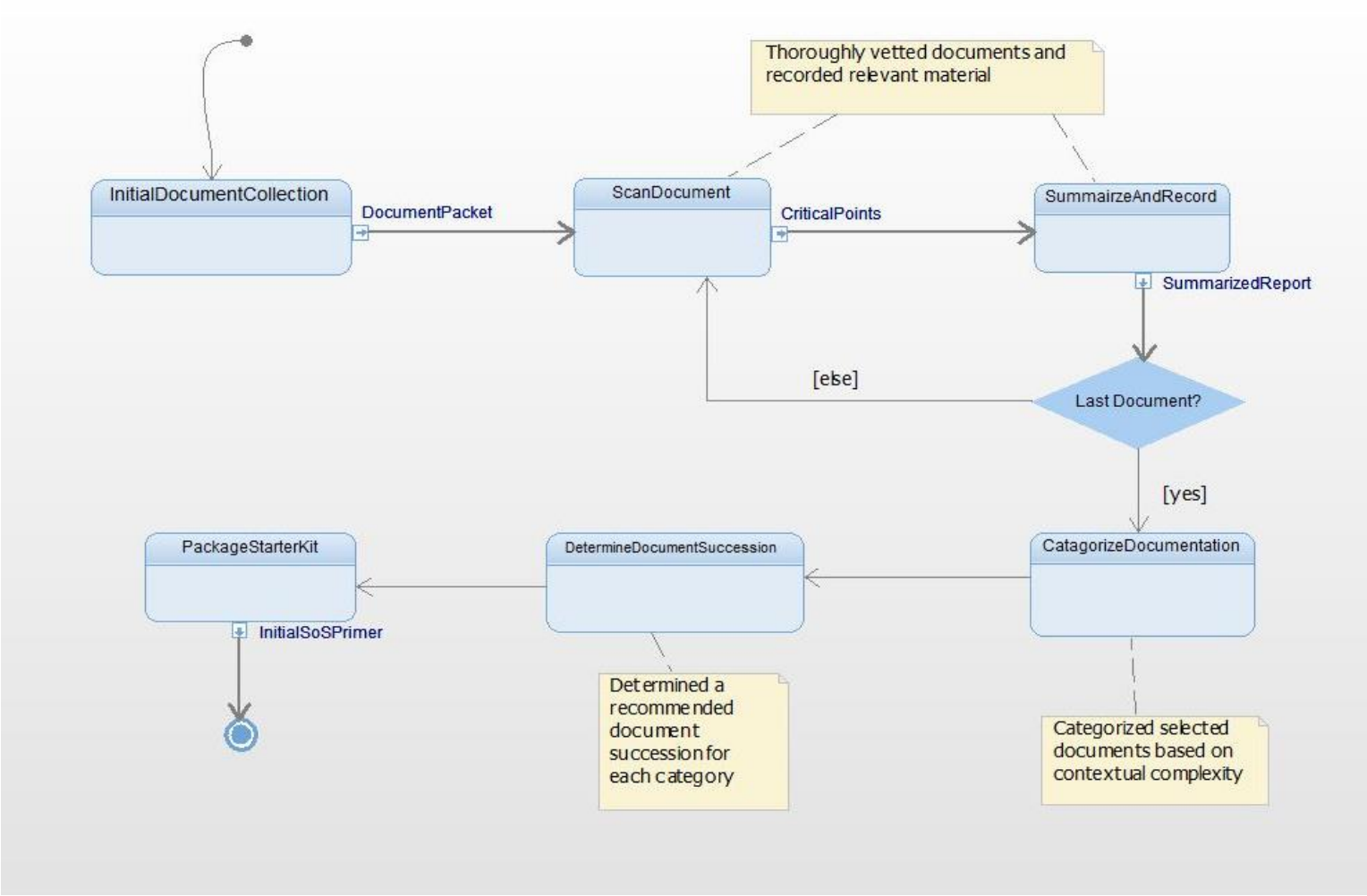
For Internal MITRE Use.
© 2017 The MITRE Corporation. All rights reserved.

Overview

- **Objective:**
  - Develop a “SoS Primer” to serve as a guide for SoS concepts and practices with content that accommodates users of all expertise levels
- **Intended to be a living document that is updated**
  - Following user feedback
  - To reflect the most recent advances in the state of the practice

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

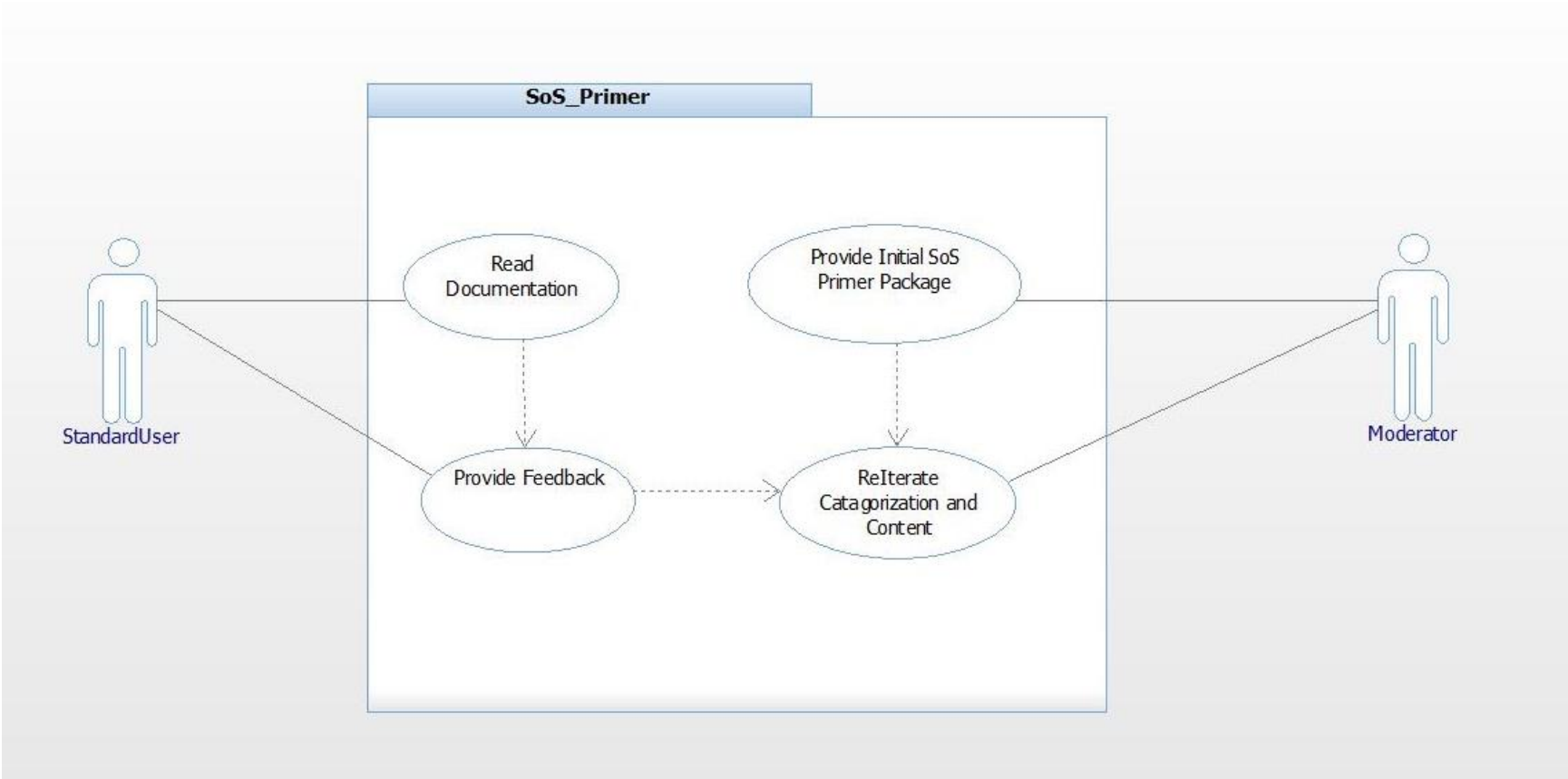
SoS Primer: Developmental Workflow



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

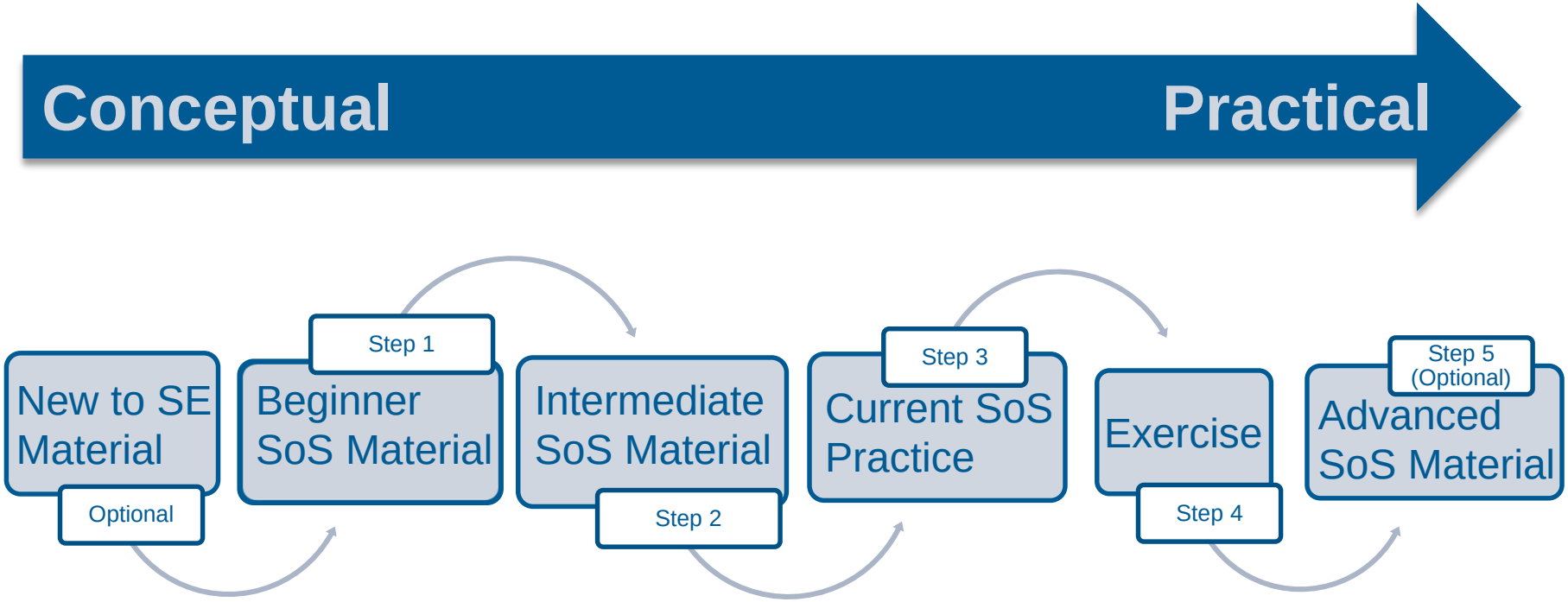
MITRE

SoS Primer: User Roles



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Document Categorization



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Recommended Document Succession

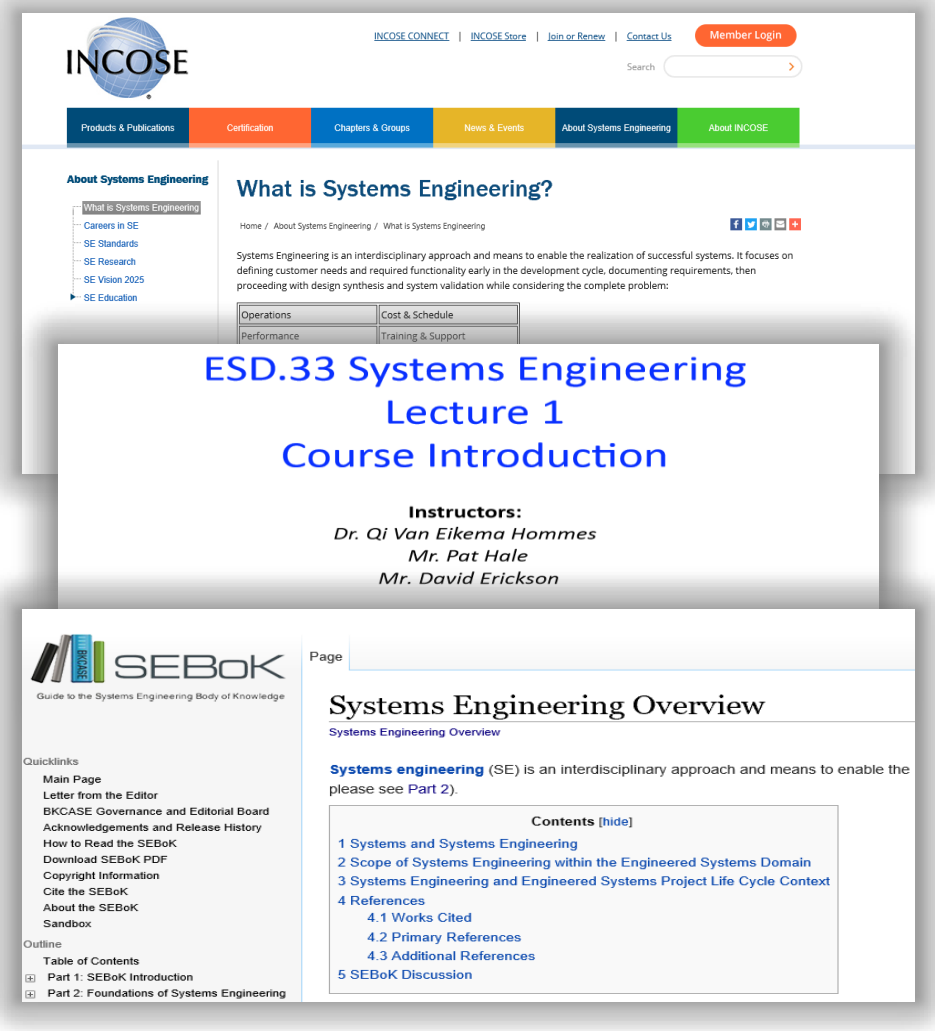
Proposed Order

New to SE Material	Beginner SoS Material	Intermediate SoS Material	Current SoS Practice	Advanced SoS Material
INCOSE: What is SE?	MITRE: Overview of SoS (Summarized PPT)	MITRE: Understanding SOP	INCOSE INSIGHT SoSE	INCOSE Systems Engineering Journal
MIT: Systems Introduction	MITRE: Am I dealing with a SoS?	MITRE: Implementer View SoSE (Summarized PPT)		IEEE Xplore
SEBoK: Systems Engineering Overview		INCOSE: SoS Pain Points Study (Summarized PPT)		INCOSE Journal of Enterprise Transformation
				International Journal of Systems of Systems Engineering

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

New To SE Material*

1. **INCOSE: What is SE?**
   - Definition of Systems and SE
   - The SIMILAR Process
2. **MIT: Systems Introduction**
   - Characteristics and Applications
   - Process Models
3. **SEBoK: Systems Engineering Overview**
   - SE Scope and Project Lifecycle



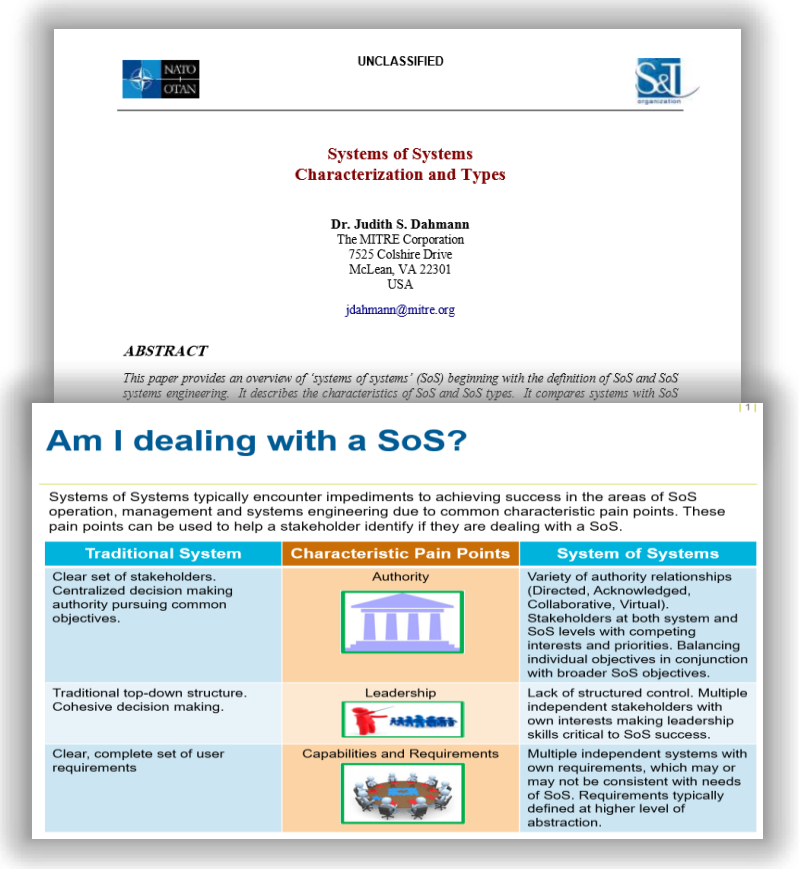
*Optional for individuals new to systems and systems engineering concepts

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Beginner SoS Material

1. **MITRE: Overview of SoS**
   - SoS Definitions
   - Characteristics and Attributes
   - Scope and Domains
   - Types and Aspects of SoS SE
   - Challenges
2. **MITRE: Am I dealing with a SoS?**
   - Pain Points



UNCLASSIFIED

NATO OTAN

S&T organization

Systems of Systems
Characterization and Types

Dr. Judith S. Dahmann
The MITRE Corporation
7525 Colshire Drive
McLean, VA 22301
USA

jdahmann@mitre.org

ABSTRACT

This paper provides an overview of 'systems of systems' (SoS) beginning with the definition of SoS and SoS systems engineering. It describes the characteristics of SoS and SoS types. It compares systems with SoS

Am I dealing with a SoS?

Systems of Systems typically encounter impediments to achieving success in the areas of SoS operation, management and systems engineering due to common characteristic pain points. These pain points can be used to help a stakeholder identify if they are dealing with a SoS.

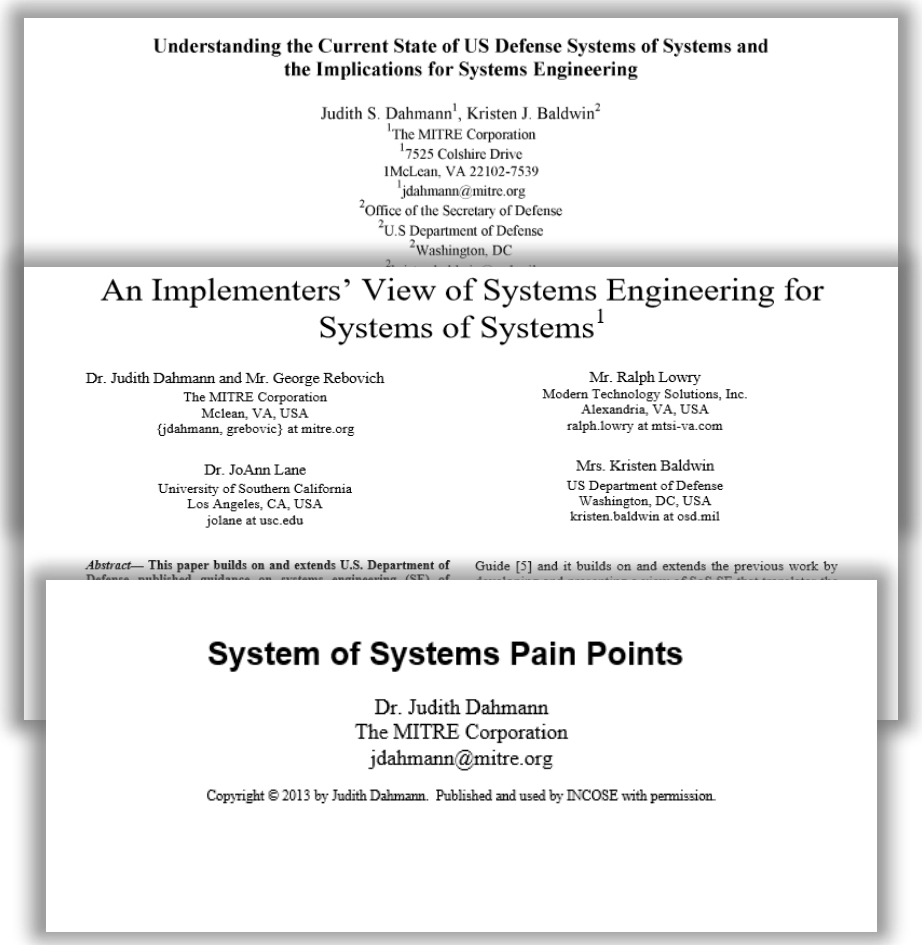
Traditional System	Characteristic Pain Points	System of Systems
Clear set of stakeholders. Centralized decision making authority pursuing common objectives.	Authority	Variety of authority relationships (Directed, Acknowledged, Collaborative, Virtual). Stakeholders at both system and SoS levels with competing interests and priorities. Balancing individual objectives in conjunction with broader SoS objectives.
Traditional top-down structure. Cohesive decision making.	Leadership	Lack of structured control. Multiple independent stakeholders with own interests making leadership skills critical to SoS success.
Clear, complete set of user requirements	Capabilities and Requirements	Multiple independent systems with own requirements, which may or may not be consistent with needs of SoS. Requirements typically defined at higher level of abstraction.

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Intermediate SoS Material

1. **MITRE: Understanding SOP**
   - Acknowledged SoS in the DoD
   - SE Challenges for Acknowledged SoS
2. **MITRE: Implementer View SoSE**
   - Wave Model
3. **INCOSE: SoS Pain Points Study**
   - Origins of Pain Points



Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering

Judith S. Dahmann[1], Kristen J. Baldwin[2]
[1]The MITRE Corporation
[1]7525 Colshire Drive
IMcLean, VA 22102-7539
[1]jdahmann@mitre.org
[2]Office of the Secretary of Defense
[2]U.S Department of Defense
[2]Washington, DC

An Implementers' View of Systems Engineering for Systems of Systems[1]

Dr. Judith Dahmann and Mr. George Rebovich
The MITRE Corporation
Mclean, VA, USA
{jdahmann, grebovic} at mitre.org

Mr. Ralph Lowry
Modern Technology Solutions, Inc.
Alexandria, VA, USA
ralph.lowry at mtsi-va.com

Dr. JoAnn Lane
University of Southern California
Los Angeles, CA, USA
jolane at usc.edu

Mrs. Kristen Baldwin
US Department of Defense
Washington, DC, USA
kristen.baldwin at osd.mil

Abstract— **This paper builds on and extends U.S. Department of**

Guide [5] and it builds on and extends the previous work by

System of Systems Pain Points

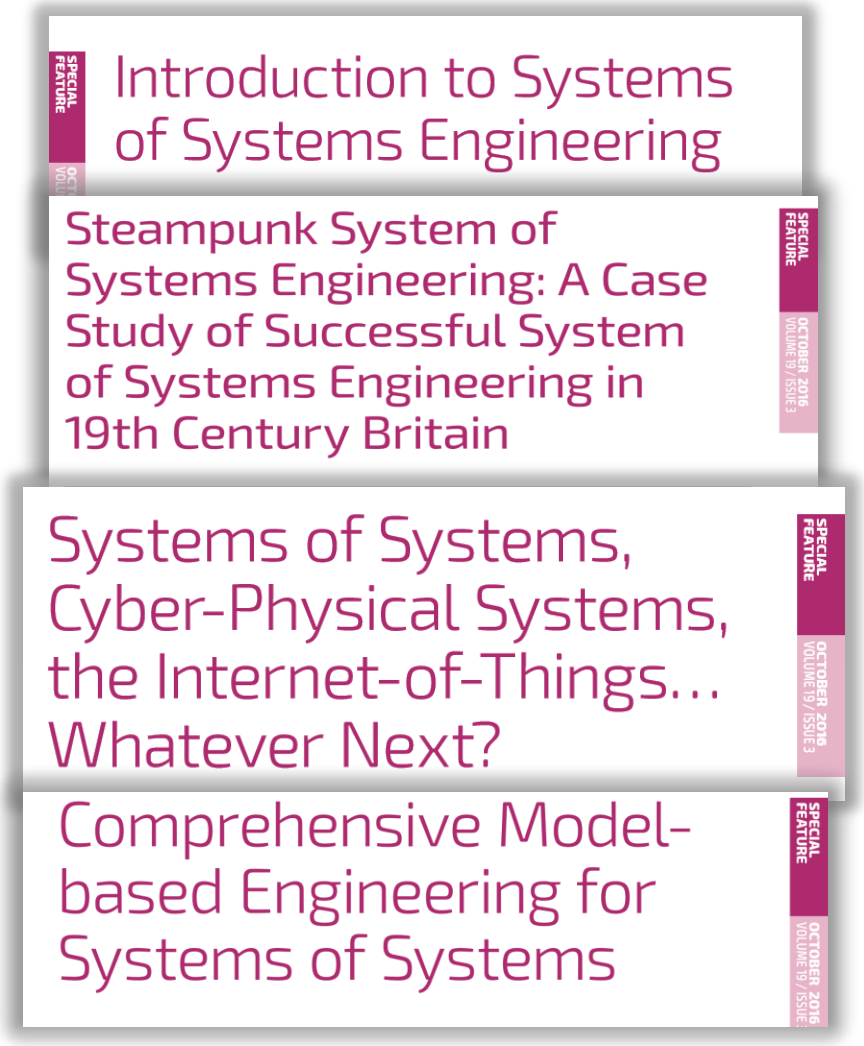
Dr. Judith Dahmann
The MITRE Corporation
jdahmann@mitre.org

Copyright © 2013 by Judith Dahmann. Published and used by INCOSE with permission.

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Current SoS Practice

1. **INCOSE: INSIGHT**
   - SoS Background
   - SoS/SoSE Case Studies
   - Emerging Ideas in SoS/SoSE
   - SoSE Tools, Techniques, and Approaches



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Advanced SoS Material

- **INCOSE Systems Engineering Journal**
  - International Council on Systems Engineering's (INCOSE) quarterly journal publications
- **IEEE Xplore**
  - Online database of articles published on systems through the Institute of Electrical and Electronics Engineers (IEEE)
- **INCOSE Journal of Enterprise Transformation**
  - INCOSE quarterly publication that focuses on enterprise transformation in academic fields including systems engineering
- **International Journal of Systems of Systems Engineering**
  - Inderscience quarterly publication whose articles are centered around ground-breaking changes and areas of interest within the field of SoS engineering

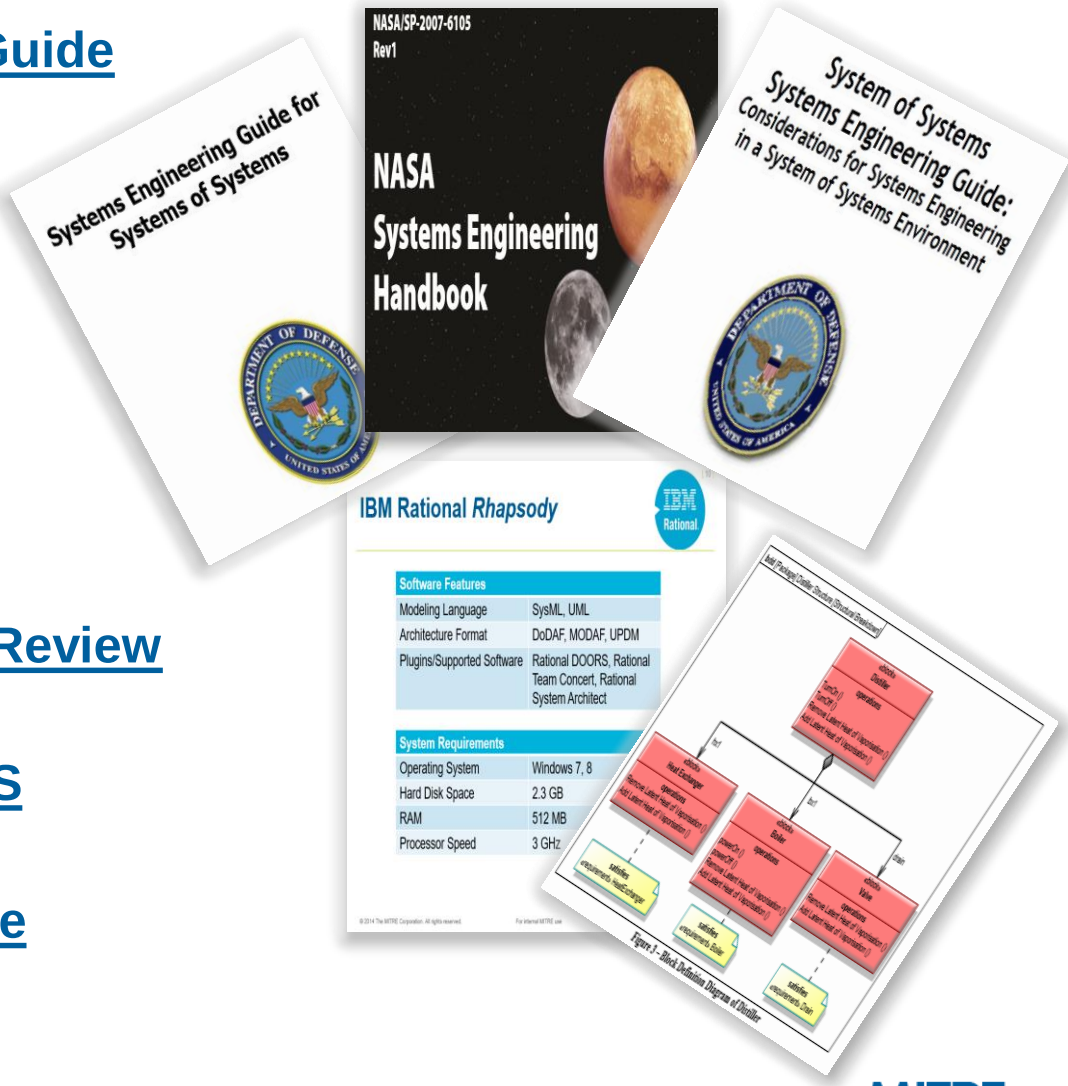


© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Optional SoS Material

- DAU: Systems Engineering Guide For Systems of Systems
- NASA: Systems Engineering Handbook
- DSIAC: System of Systems Systems Engineering Guide: Considerations for Systems Engineering in a System of Systems Environment
- MITRE: Analytic Workbench Review
- MITRE: Software Tools for Modeling and Analysis of SoS Architecture
- MITRE: SoS Modeling Mhause
  - SysML Resource



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

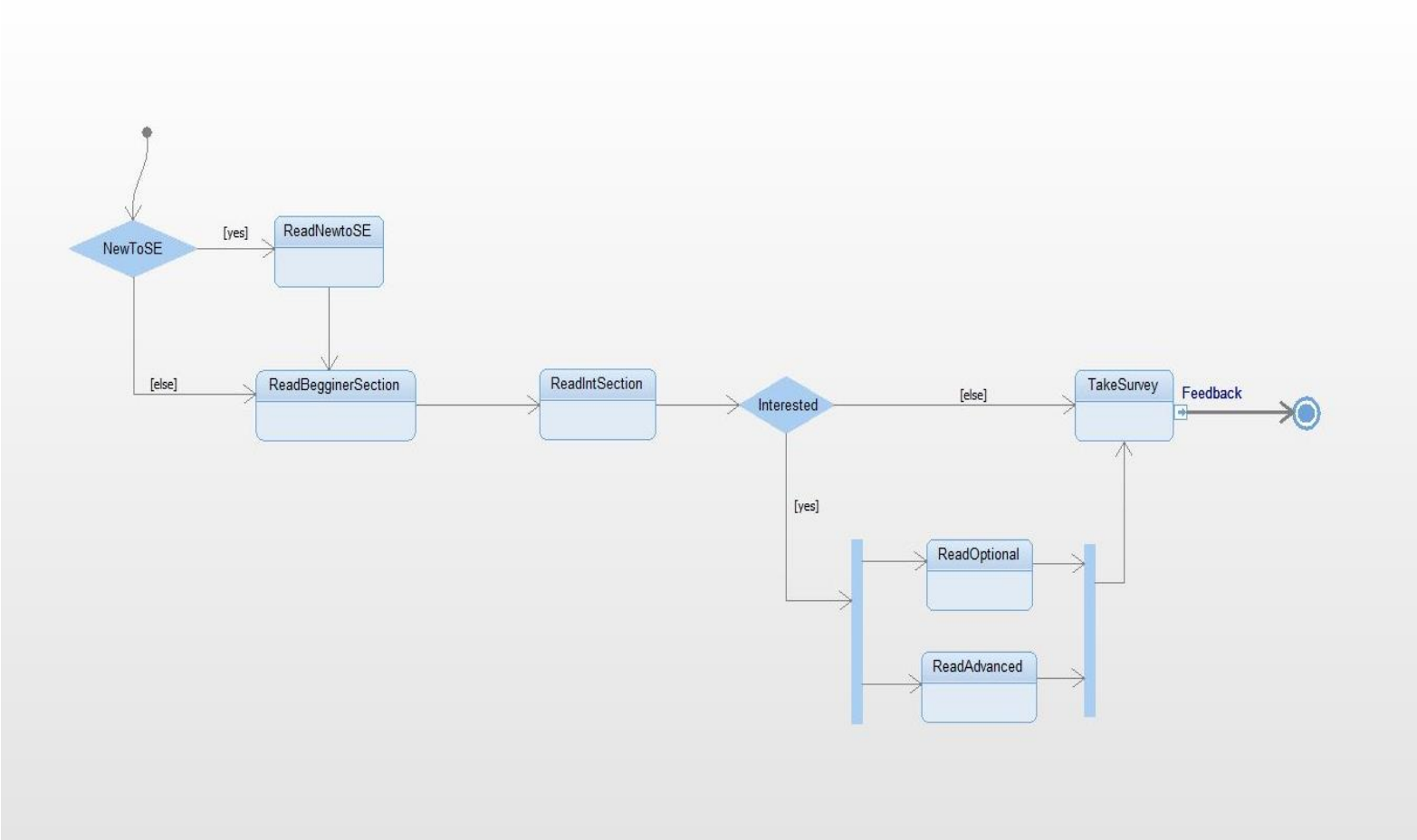
Acronyms

- **COTS** – Commercial Off-the-Shelf
- **INCOSE** – International Council on Systems Engineering
- **SE** – System Engineering
- **SoS** – System of System
- **DoDAF** – Department of Defense Architecture Framework
- **MoDAF** – Ministry of Defense Architecture Framework
- **SEBoK** – System Engineering Body of Knowledge
- **IOC** – Initial Operational Capability
- **SoSE** – System of Systems Engineering
- **DoD** – Department of Defense
- **TTCP** – The Technical Cooperation Program
- **CONOPS** – Concept of Operations
- **IMS** – Integrated Master Schedule
- **SOP –** Standard Operating Procedure
- **DAG –** U.S. Defense Acquisition Guidebook
- **EC –** European Commission
- **COMPASS –** Comprehensive Modeling for Advanced Systems of Systems
- **DANSE –** Designing for Adaptability and evolutioN in System of systems Engineering
- **IT –** Information Technology
- **T-AREA-SoS –** Trans-Atlantic Research and Education Agenda in Systems of Systems
- **E2E –** End to End
- **SoSWG –** System of Systems Working Group
- **COI –** Communities of Interest
- **AOC –** Air Operations Center
- **SEP –** Systems Engineering Plan
- **V&V –** Verification and Validation

© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

SoS Primer: User Workflow

- **Piloting with New Hire or Employee New to SoS**



© 2017 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Scaling Model-Based System Engineering Practices for System of Systems Applications: Analytic Methods

October 2017

Laura Antul lantul@mitre.org
Dr. Aleksandra Markina-Khusid amk@mitre.org
Dr. Ryan Jacobs rjacobs@mitre.org
Janna Kamenetsky jannak@mitre.org

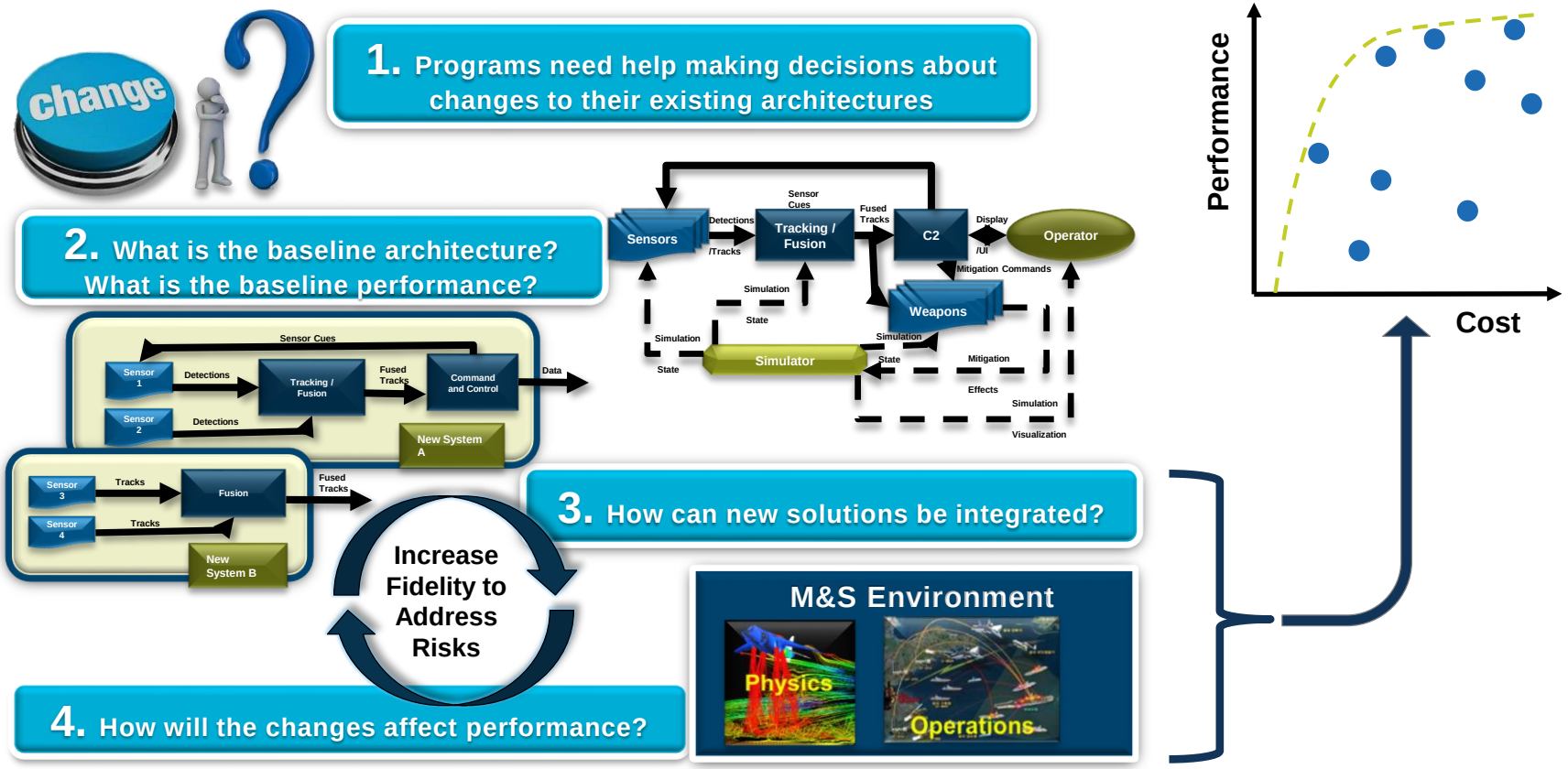
NDIA 20th Annual Systems Engineering Conference
http://www.ndia.org/events/2017/10/23/20th-systems-engineering-conference

MITRE

Approved for Public Release; Distribution Unlimited Case #

© 2016 The MITRE Corporation. All rights reserved.

Motivation



© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

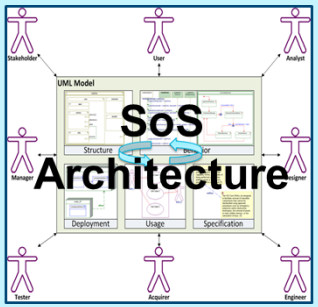
MITRE

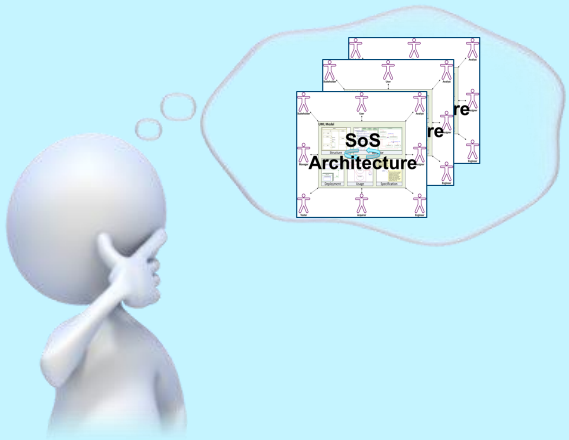
As-is for Evaluating Architectures

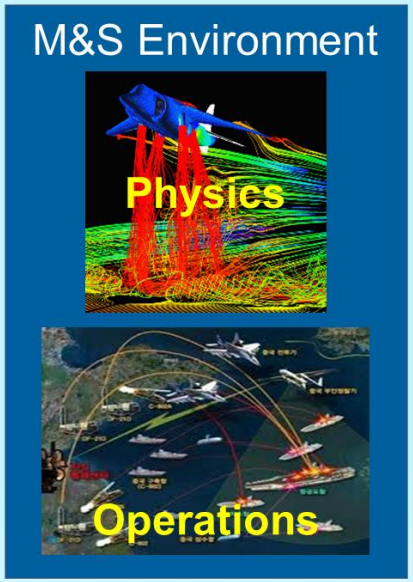


© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

SoS Analysis of Alternatives



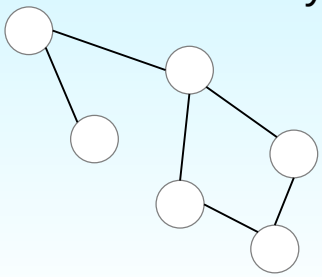




Establish baseline SoS architecture

Generate SoS architecture alternatives

SoS graph abstraction and network analysis



MIP contribution: inform prioritization of alternatives using lightweight analytics

Detailed evaluation with M&S environment

Informed architecture selection

© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Robustness Metric (Algebraic Connectivity Value)

- **Represents average difficulty of isolating a node**
  - Second smallest eigenvalue of a Laplacian Matrix
- **Inputs:**
  - Degree Matrix
    - Diagonal matrix that contains the number of nodes adjacent to a given node

$$D_{ij} = \begin{cases} d_i & \text{degree of component } i \text{ when } i = j \\ 0 & \text{otherwise} \end{cases}$$

  - Adjacency Matrix
    - Symmetric matrix that contains a 1 if two given nodes are adjacent and 0 otherwise

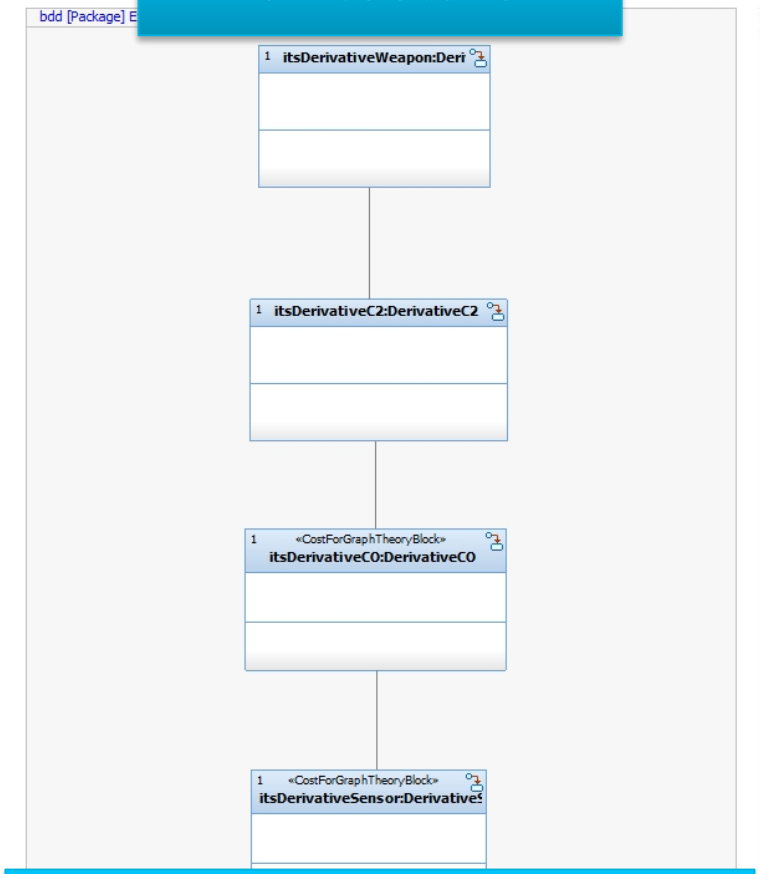
$$A_{ij} = \begin{cases} 1 & \forall[(i,j)|(i \neq j) \quad \text{and} \quad (i,j) \in \Delta] \\ 0 & \text{otherwise} \end{cases}$$

Reference: H. Mehrpouyan, B. Haley, A. Dong, I. Y. Tumer, and C. Hoyle, "Resiliency analysis for complex engineered system design," *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*, vol. 29, no. 01, pp. 93–108, Jan. 2015.

© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

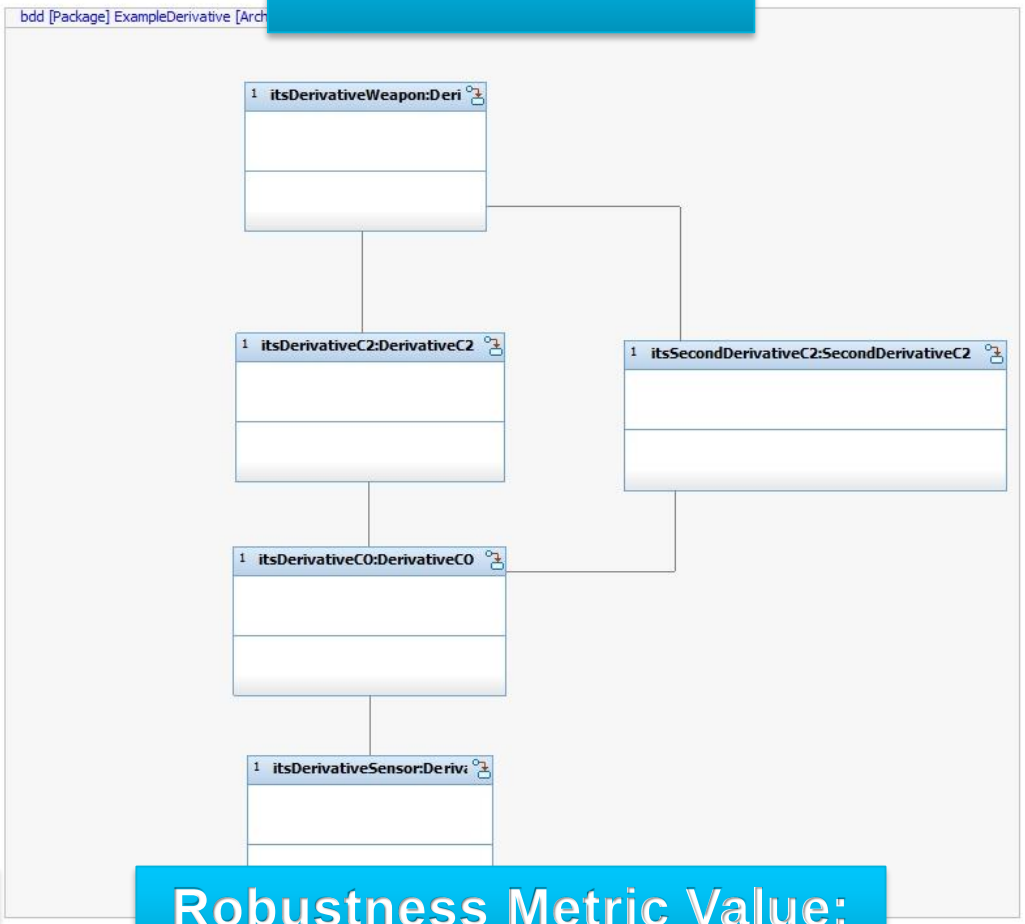
Identifying Robust SoS Architectures

Architecture 1



Robustness Metric Value: 0.5858

Architecture 2



Robustness Metric Value: 0.8299

© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

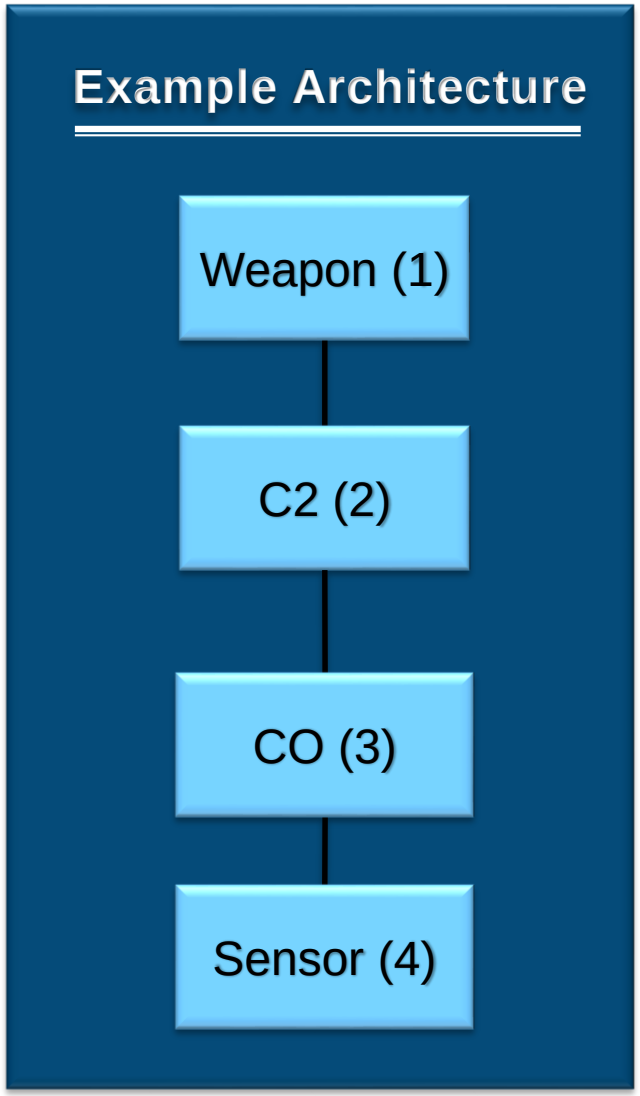
Multi-layer Architectural Analysis

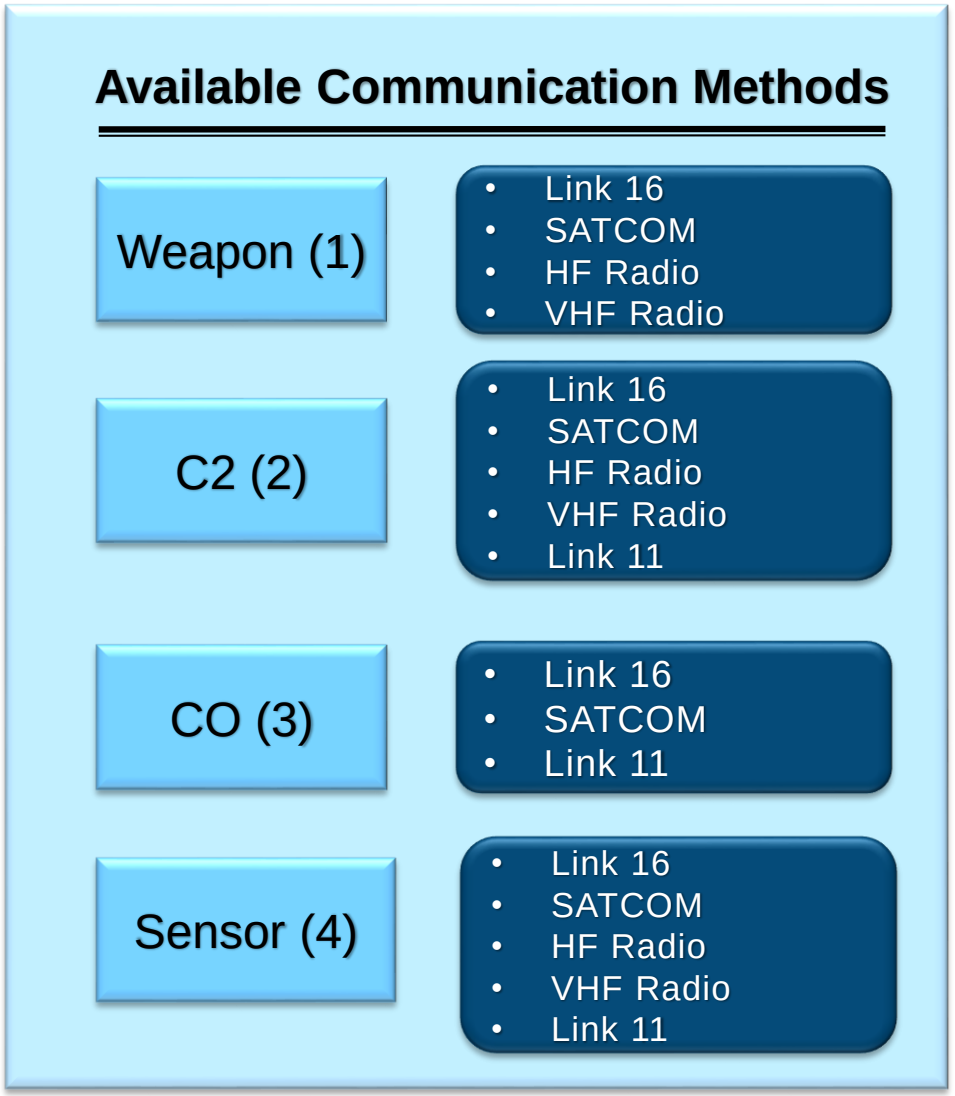
MITRE

For Internal MITRE Use.

© 2016 The MITRE Corporation. All rights reserved.

Example Architecture

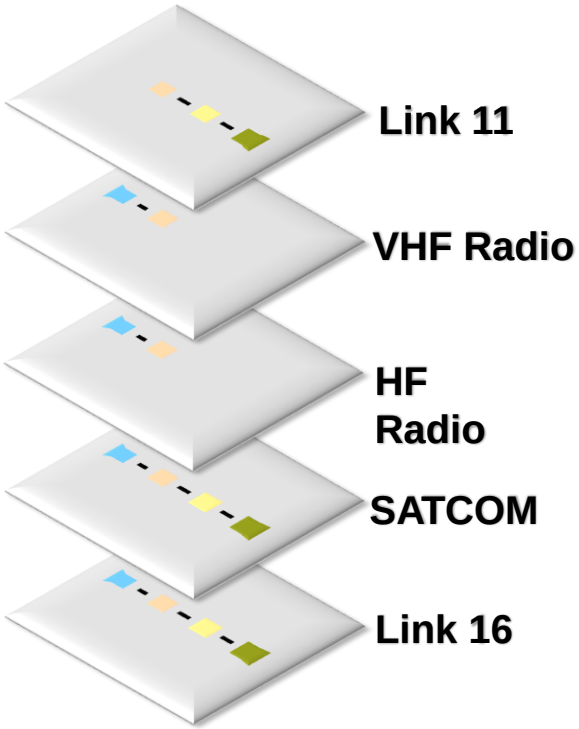




© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Mapping Architecture to Multilayer Graph – Intralayer Graph Representation

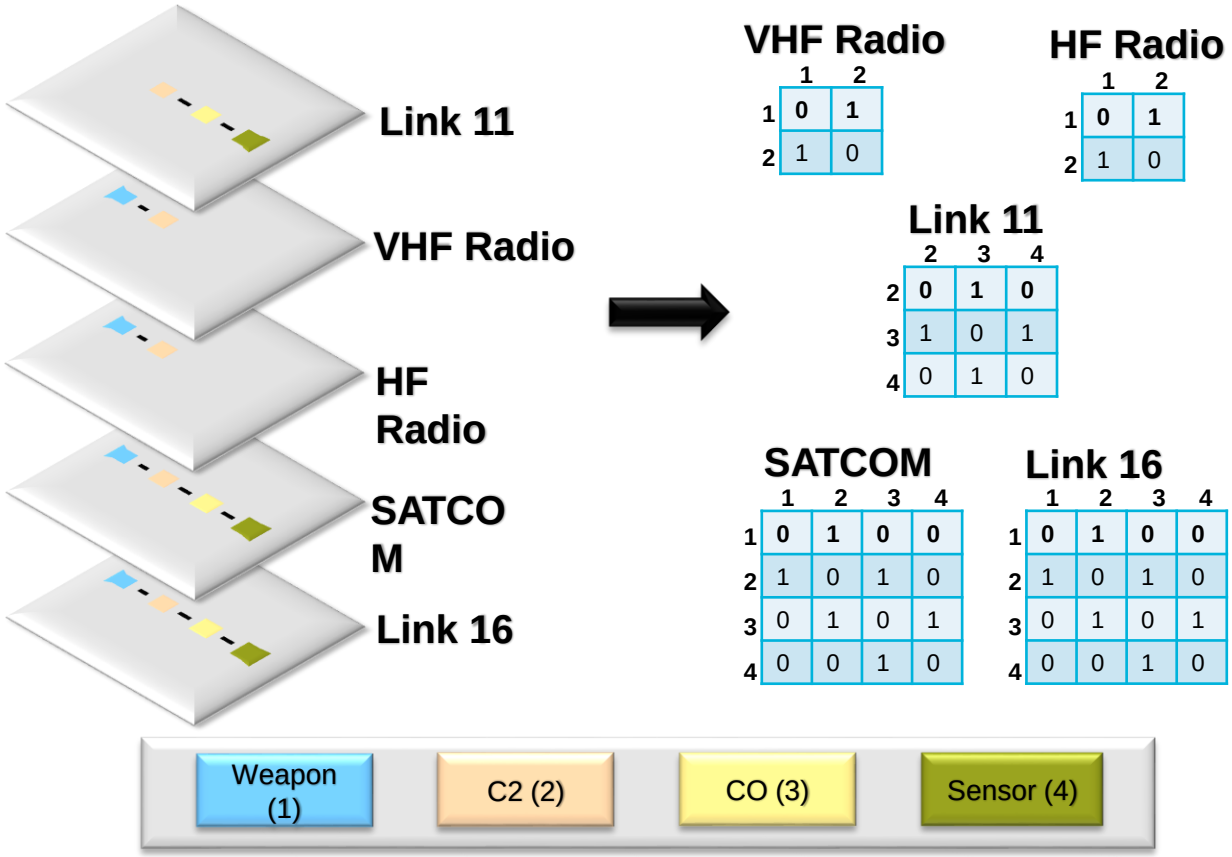


Available Communication Methods

Weapon (1)	• Link 16 • SATCOM • HF Radio • VHF Radio
C2 (2)	• Link 16 • SATCOM • HF Radio • VHF Radio • Link 11
CO (3)	• Link 16 • SATCOM • Link 11
Sensor (4)	• Link 16 • SATCOM • HF Radio • VHF Radio • Link 11

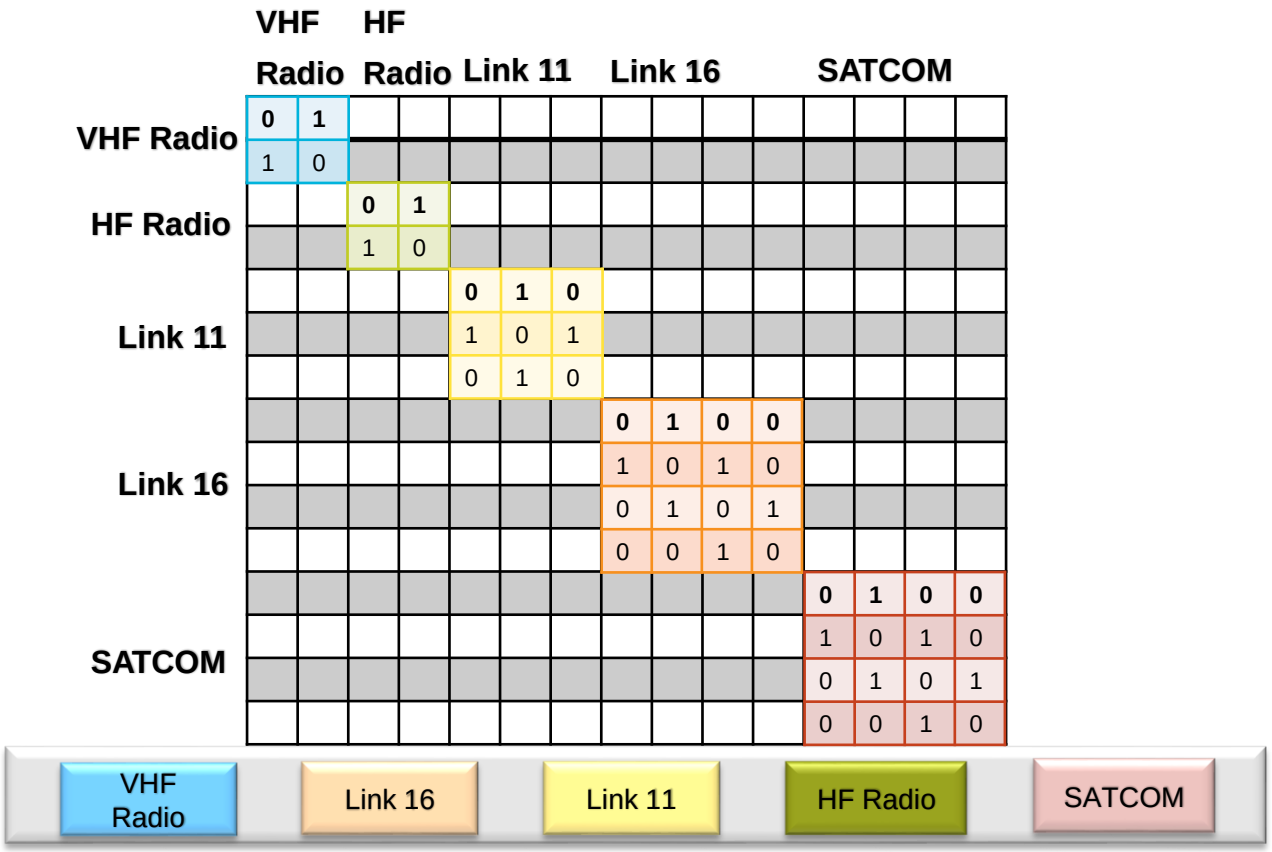
© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Mapping Architecture to Multilayer Graph – Intralayer Adjacency Representation



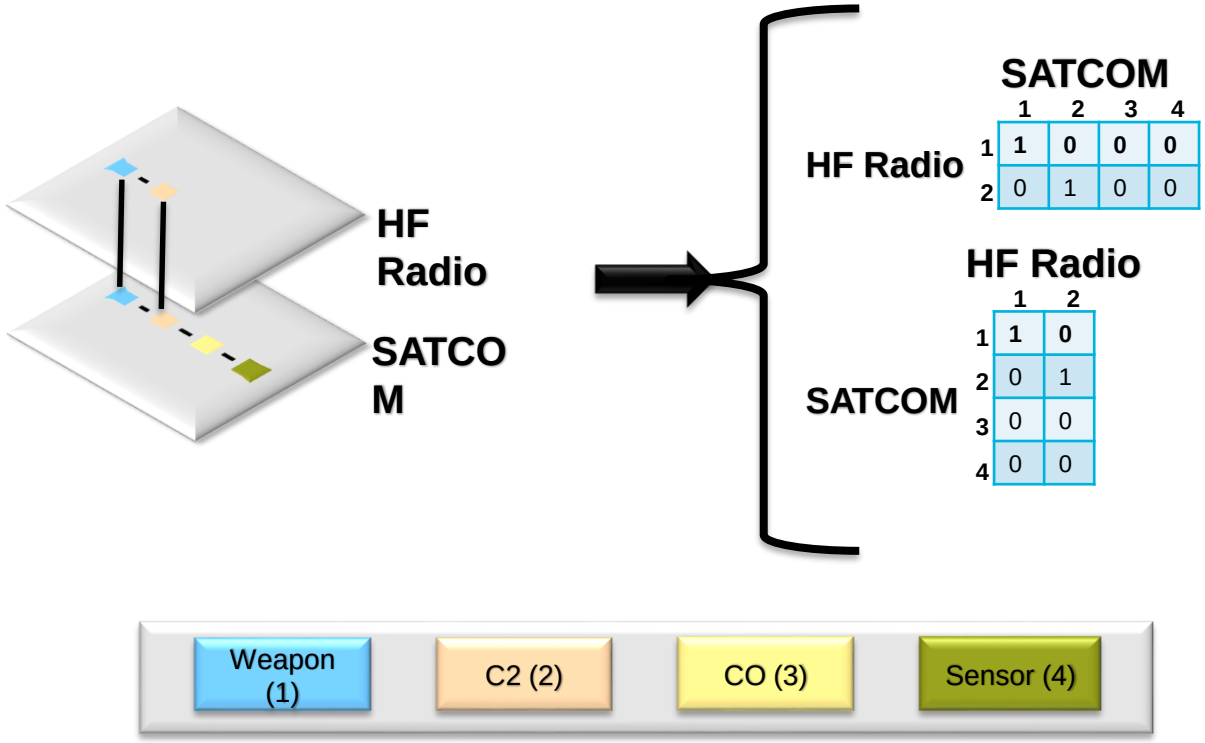
© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Mapping Architecture to Multilayer Graph – Intralayer Adjacency Representation



© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

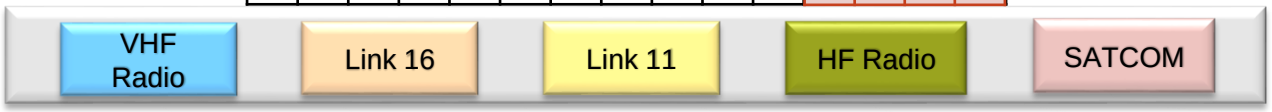
Mapping Architecture to Multilayer Graph – Interlayer Matrix Representation



© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Mapping Architecture to Multilayer Graph – Adding Interlayer to Intralayer in Matrix

	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



© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

MITRE

Summary

- **Results**
  - Developed a scalable rapid analysis capability for MBSE software tools
  - Identified a proxy for resilience that can be measured using lightweight analysis techniques
  - Tested the analysis method on notional architectures and compared the results with a low fidelity operational modeling and simulation tool
- **Lessons Learned**
  - Detailed analysis will have to accompany the graph theoretic analysis to account for operationally critical architectural components
  - Based on the domain the optimal graph theoretic value may vary

© 2016 The MITRE Corporation. All rights reserved. For Internal MITRE Use.

Physics and Model-Based Aerodynamic Design and Analysis





Presented:

NDIA Systems Engineering 2017

October 26, 2017



This document does not contain U.S. export controlled technical data.

GENERAL ATOMICS AERONAUTICAL

General Atomics Aeronautical Systems

Predator A Piston (In Production)



International



U.S. ARMY



U.S. ARMY

Predator B/C Turboprop/fan (Production/Dev)



U.S. Air Force



Type-Certifiable



Turbofan

Small/Large UAVs (In Dev)


DARPA

Artist's Concept


U.S. NAVY

This document does not contain U.S. export controlled technical data.

GENERAL ATOMICS AERONAUTICAL

Product Aerodynamic Lifecycle

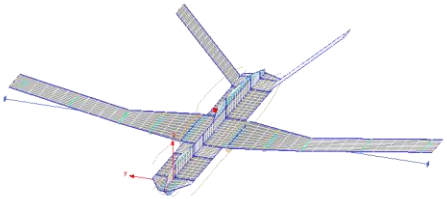
- Requirements
- Conceptual Design
- Prelim/Detailed Design
- Test
- Sustainment / Growth

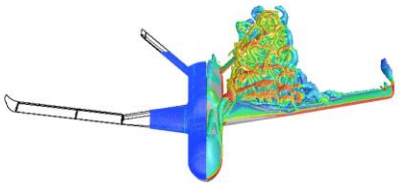
- **Aerodynamic design and analysis relevant to all stages of the product life cycle**
- **Ideally need a set of "multi" tools**
  - Multi-fidelity (low → high fidelity)
  - Multi-physics (aero → aero+)
  - Multi-cost (sec/min → days/weeks)
  - Multi-user/org (aero vs. struct SME)
  - Multi-product (Aircraft A vs. Aircraft B)

This document does not contain U.S. export controlled technical data.

Aerodynamic Pre-Flight Tool belt

Physics Based





Test Based

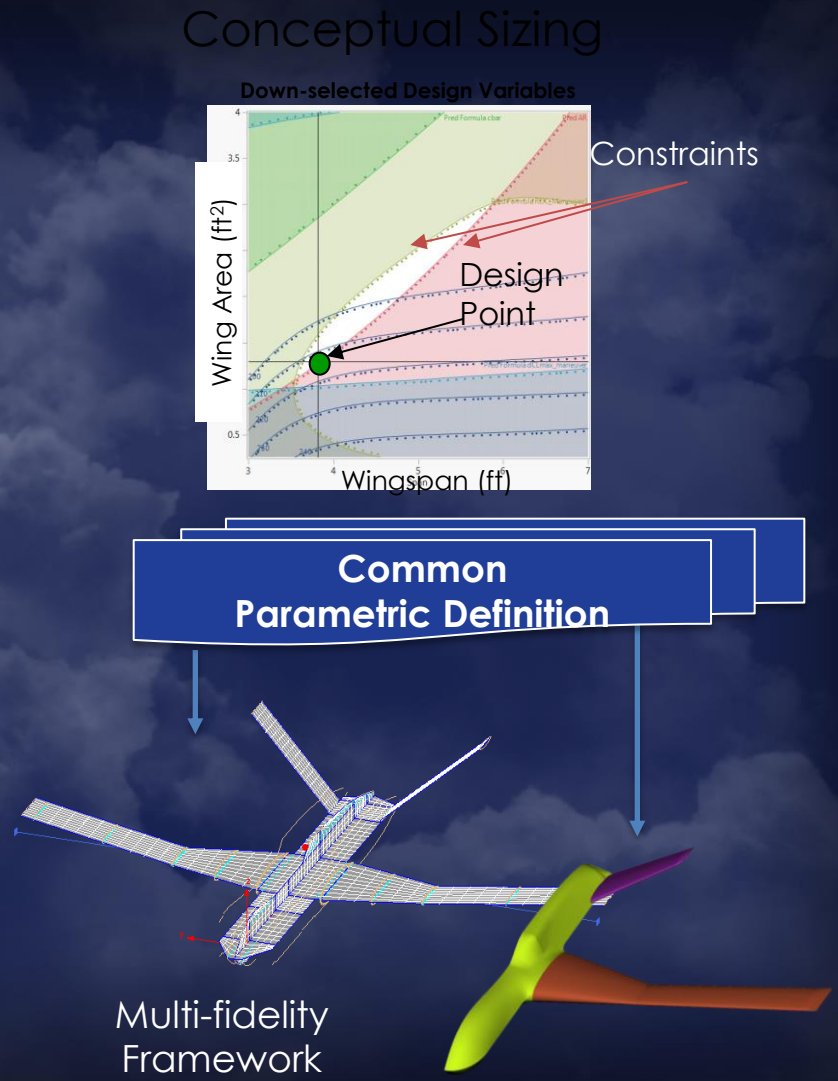


Physics	Vortex Lattice / Panel	CFD	Wind Tunnel
Inputs	Conceptualize → Run	CAD → Mesh → Run → Post	Plan → CAD/Build → Test → Post
Outputs	**Steady/Unsteady** Linear aero **Quick** prelim results	Steady/Unsteady **Non-linear aero** **Validation required**	Typically steady aero **Non-linear aero** **Established data source**
Scale (Reynolds #)	Full-scale (Inviscid i.e. Re→∞)	**Full-Scale** (Flight Re)	Sub-scale or partial model (Variable Re adds **cost**)
Compressibility	Incompressible or compressibility corrected	Compressible (Flight Mach)	Compressible. Separate tests depending on Ma
Viscous Effects	Inviscid or viscous corrected	Typically fully turbulent Recent RANS transition models	Typically tripped or natural transition at test Re
Geometry	Panel representation and **simple shapes**	Geometric complexity increases meshing cost; smooth	Smooth; gaps/slots sizes may need to be Re scaled
Propulsion	Faired; no or limited prop effects	Faired or flow-through; can model propulsion effects	Faired or flow-through; separate tests for prop effects
Environment	Modeled in farfield	Modeled in farfield	Corrected for tunnel effects

This document does not contain U.S. export controlled technical data.

Requirements / Conceptual Design

- **Semi-empirical methods drive requirements and sizing**
  - High level
  - Grounded in actuals
  - Good for derivative designs
  - Good for high level trades
- **Opportunities**
  - Multi-fidelity framework at GA-ASI
  - Others successfully options exist e.g. MIT TASOPT

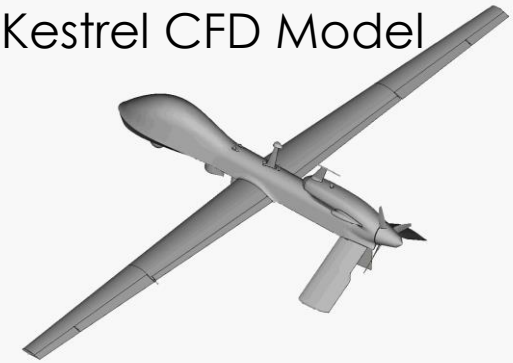


This document does not contain U.S. export controlled technical data.

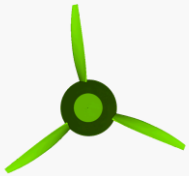
Preliminary / Detailed Design

- **CFD and wind tunnel test drive design**
  - Analysis for design trades
  - Test for database generation
  - Test for perf verification
- **Challenges**
  - Managing multiple models… CREATE-AV enabling multi-disciplinary analysis
  - Physics!.. the RANS plateau LES/DDES still costly

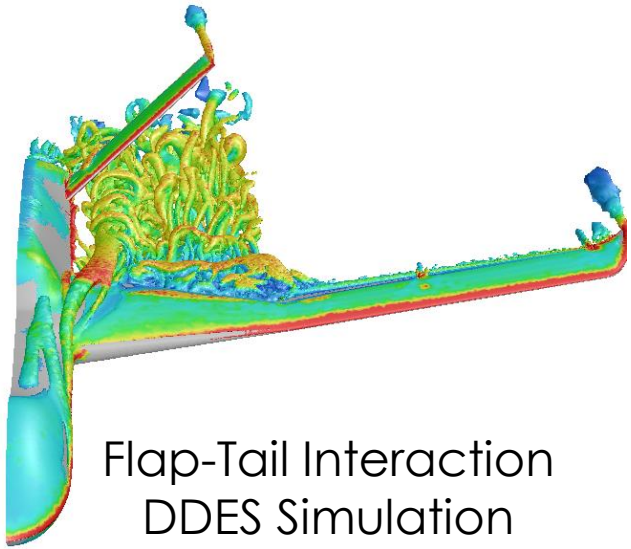
Kestrel CFD Model



Animated gif



Overset allows moving control surfaces and props

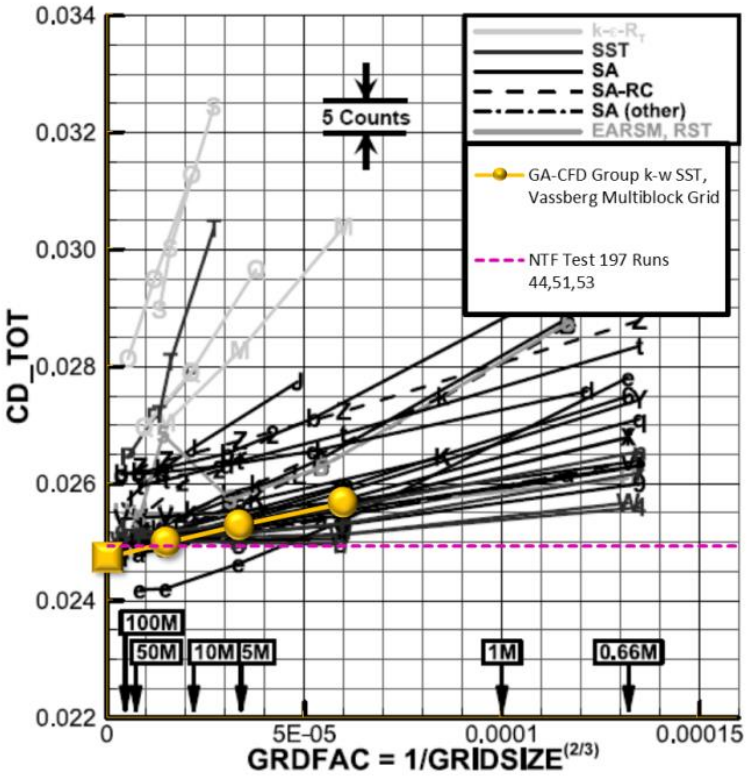


Flap-Tail Interaction DDES Simulation

This document does not contain U.S. export controlled technical data.

Prelim / Detailed Design (Cont.)

- **Challenges (Cont.)**
  - Scalability… Wind tunnel cheaper than CFD for large databases.
  - Trust… CFD meshing treated as an "art." Mesh convergence ≠ Solution accuracy. Test validation remains essential.
  - Expectations… CFD not fast enough to be in-exact.
  - Process… CFD treated as virtual wind-tunnel.



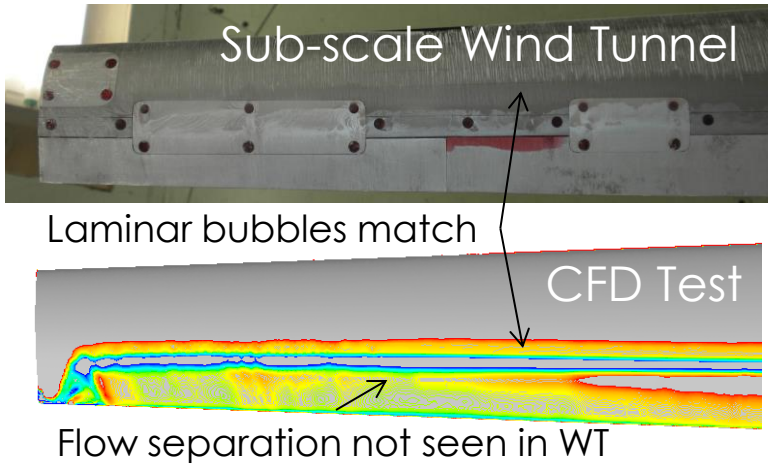
AIAA Drag Prediction Workshop (DPW5)

Graphic from: https://aiaa-dpw.larc.nasa.gov/Workshop5/presentations/DPW5_Presentation_Files/14_DPW5%20Summary-Draft_V7.pdf

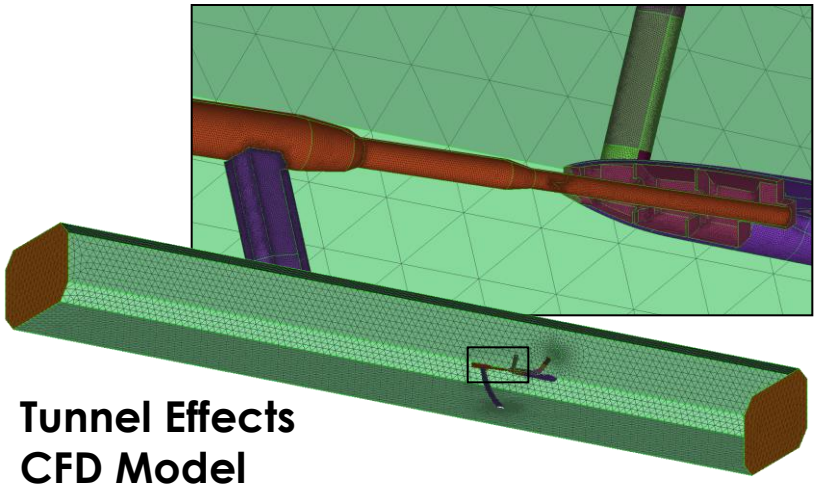
This document does not contain U.S. export controlled technical data.

Test

- **Pre-test predictions inform test focus areas**
- **Test helps CFD**
  - Separated flows
  - Interaction effects
  - Transition
- **CFD helps test**
  - Wind tunnel corrections
  - Propulsion effects
  - Aero-static effects



Tunnel Flow Viz Comparison



Tunnel Effects CFD Model

Graphic from: https://aiaa-dpw.larc.nasa.gov/Workshop5/presentations/DPW5_Presentation_Files/14_DPW5%20Summary-Draft_V7.pdf

This document does not contain U.S. export controlled technical data.

Closing the Loop on Performance

Requirements

Conceptual Aero

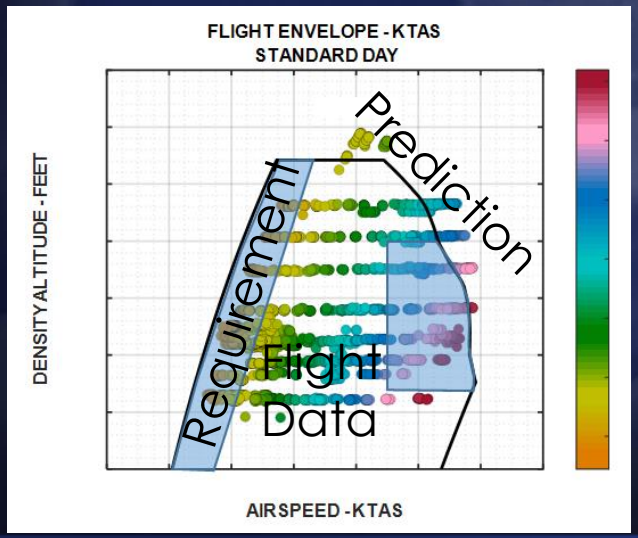
RANs Aero

Wind Tunnel Aero

Flight Test Aero

All aero models contribute to:

- Understanding of aircraft flow-field
- Support modeling for perf and S&C
- Air-data integration

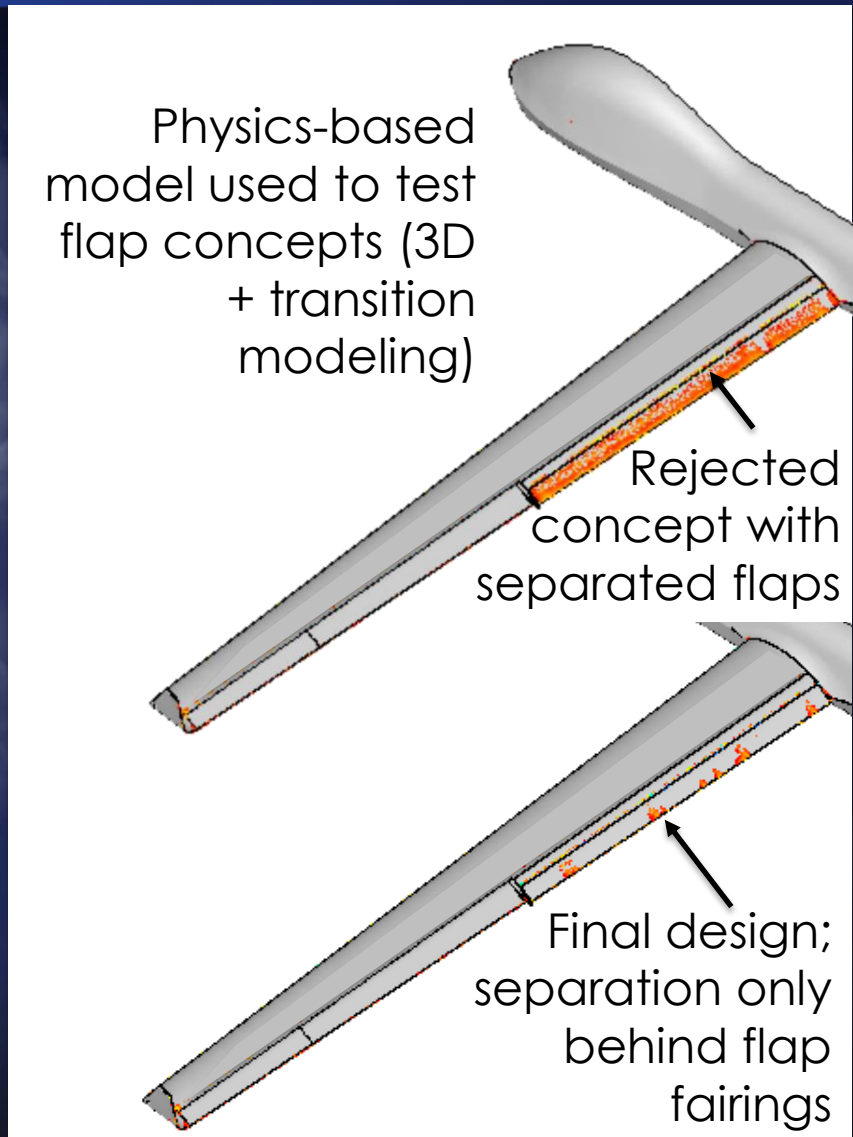


Aero + Weights + Propulsion
= Performance

This document does not contain U.S. export controlled technical data.

Sustainment / Growth

- **New tools provide opportunities to improve existing systems and match evolving customer needs**
- **GE → GE-ER Case Study**
  - GE double slotted flap designed with 2D CFD
  - GE-ER reconfigured existing hardware to a single slotted flap with 3D CFD
  - Wind tunnel and flight test in both cases
  - Meet current customer needs



This document does not contain U.S. export controlled technical data.

Future Needs

- **Medium fidelity needs**
  - Fast 3D methods (can include fuselages)
  - Non-linear unsteady options (damping deriv, loads spectra)
- **Promising Candidates**
  - Coarsely auto-meshed RANS/URANS with wall functions
  - Auto-meshed Euler+IBLT3
  - Probabilistic multi-fidelity methods like Kriging
- **High fidelity needs**
  - More efficient algorithms (e.g. multi-grid)
  - Less reliance on hardware solutions (costly)
  - Faster CAD clean-up (time consuming)
- **Transition modeling essential for GA-ASI**
  - RANS based models promising from computational cost perspective
  - Need models robust to Re 5e5-10e6 (current γ-Reθ not there)
  - Natural transition covering TS, CF, laminar bubbles, attachment line contamination
  - Forced transition covering trip, surface roughness/defects
  - Non-dissipative methods for high level for freestream turbulence in RANS

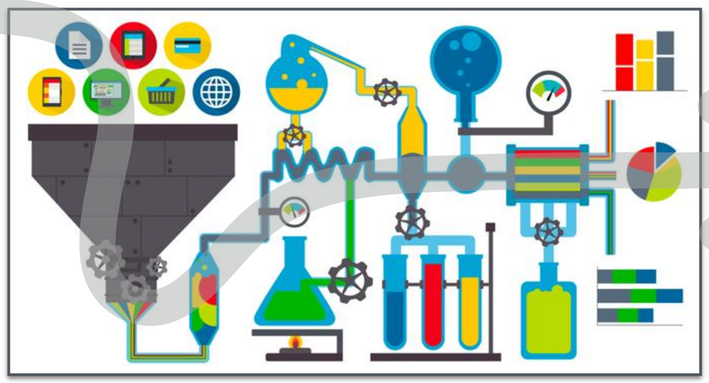
This document does not contain U.S. export controlled technical data.

Scaling Data Analytics for ERS

David Stuart

ERS Software Architecture

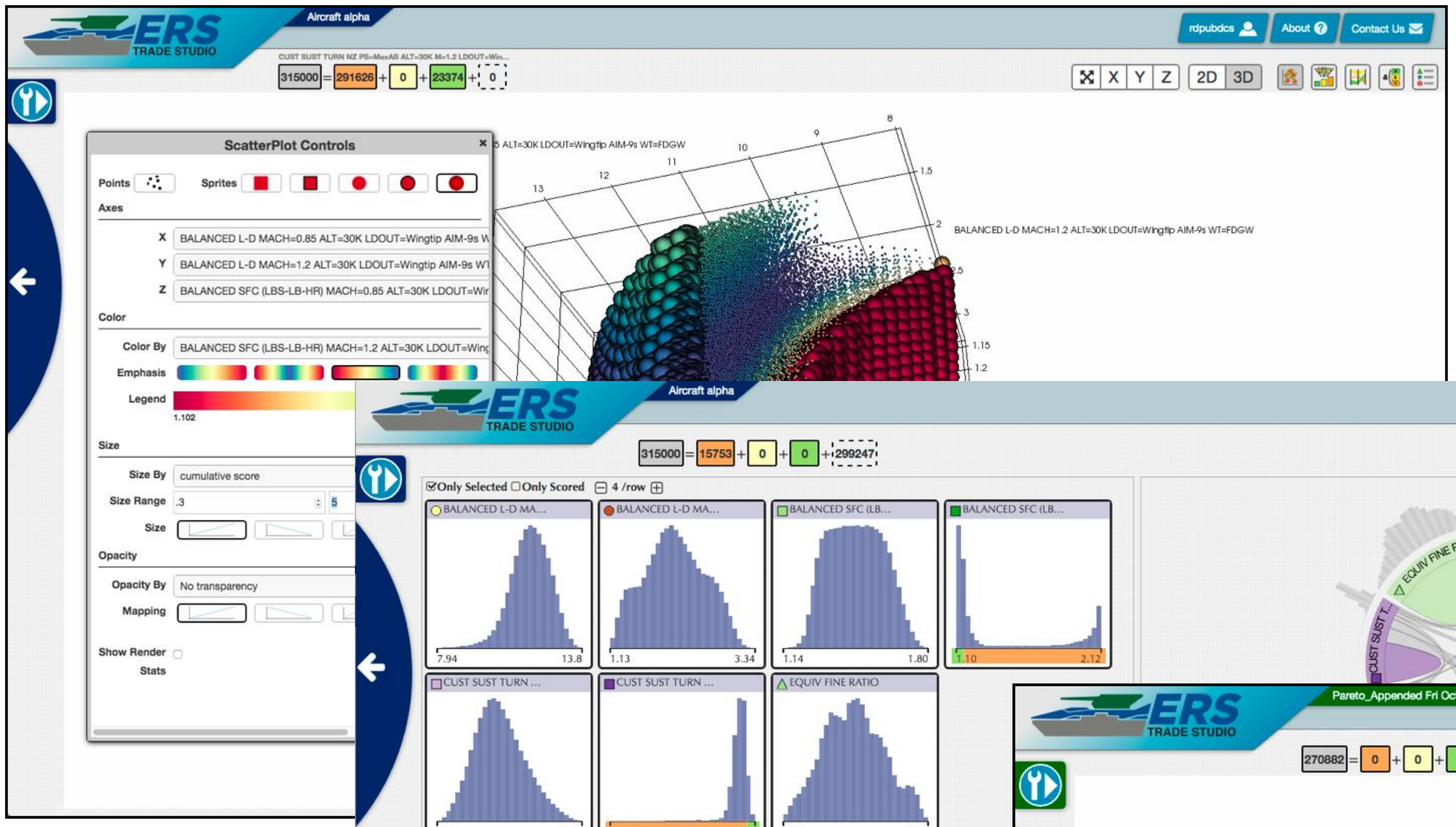
Data

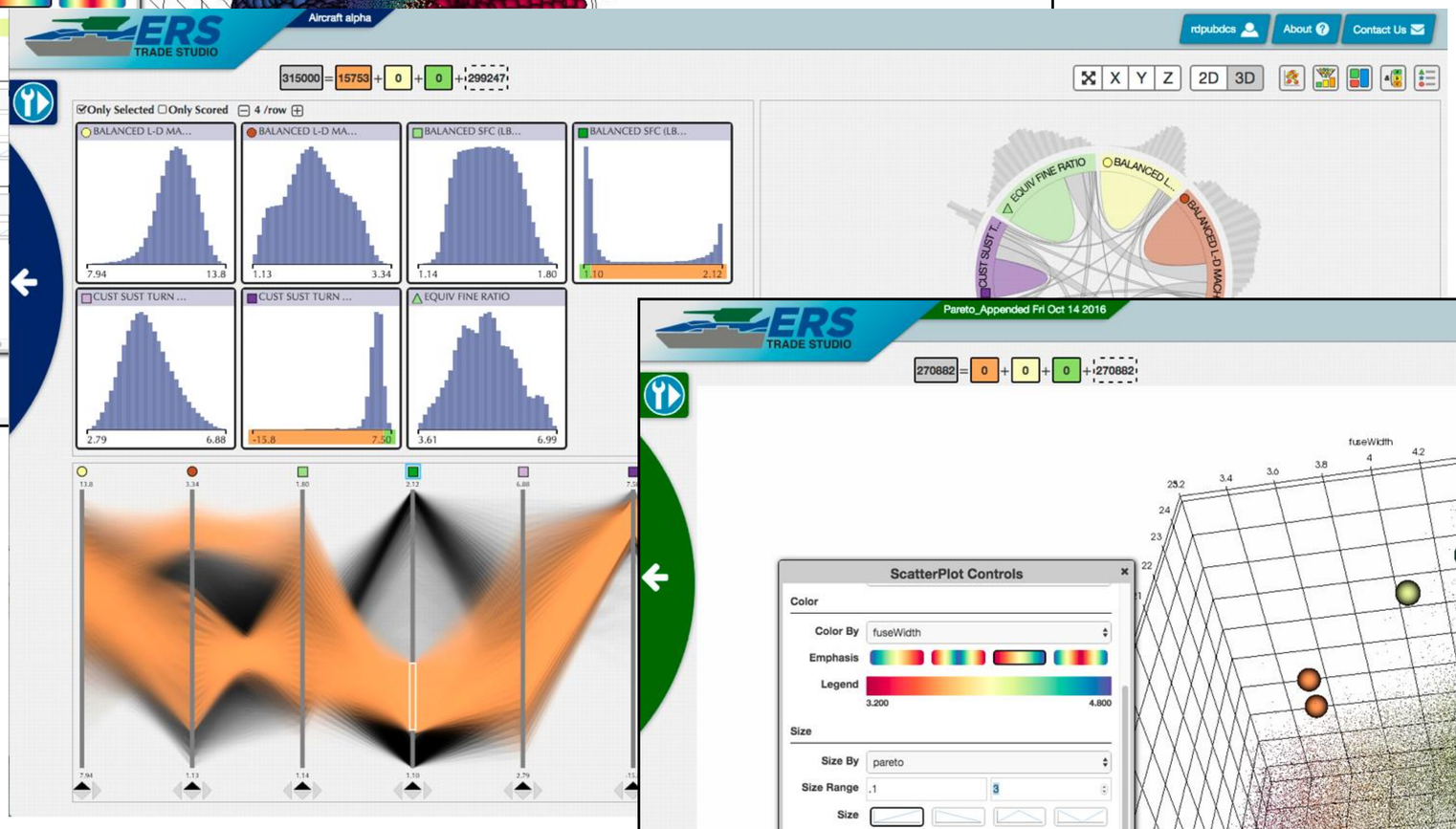


Insights

Distribution Statement

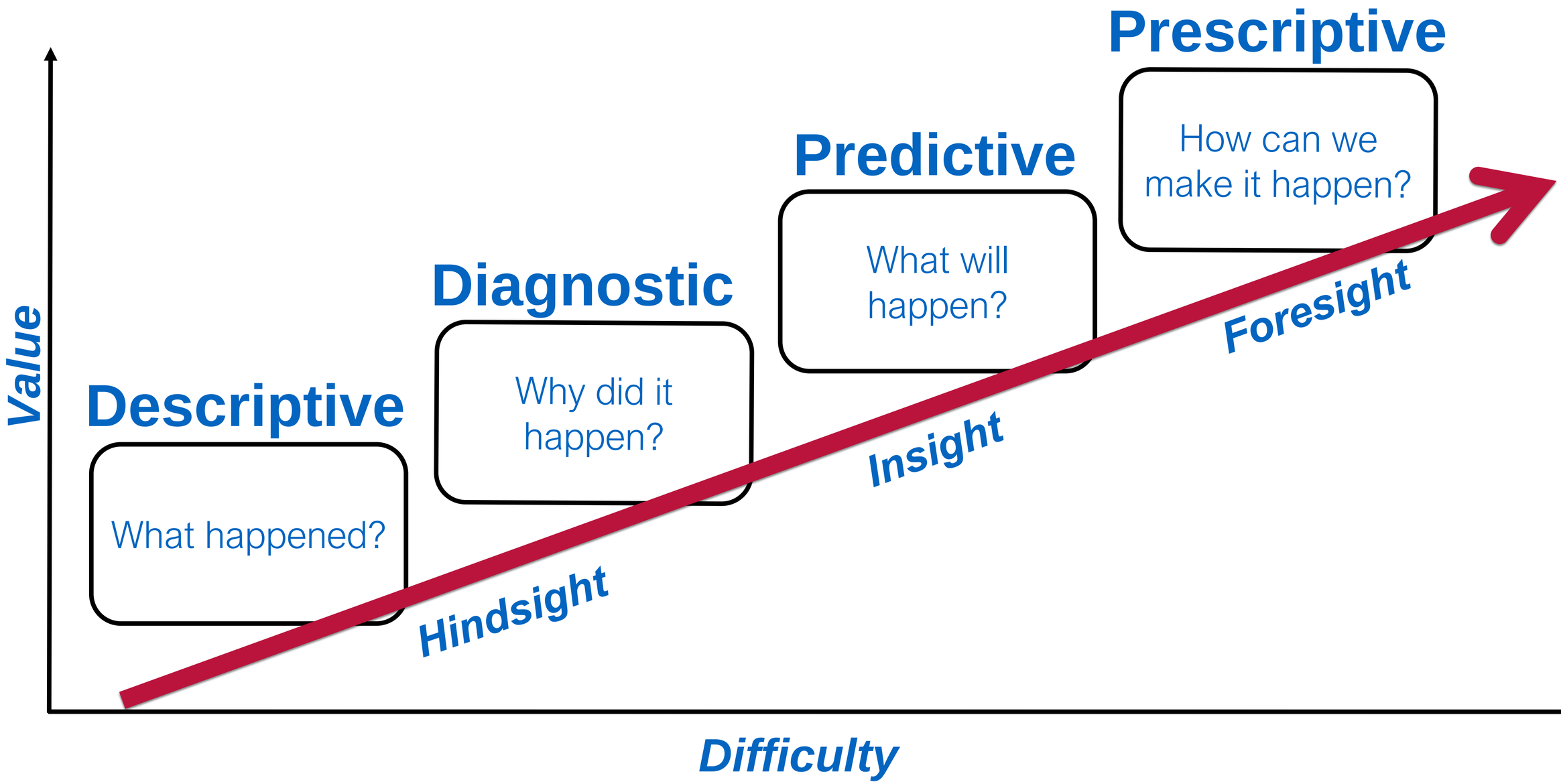
Current Tools - heavy visualization





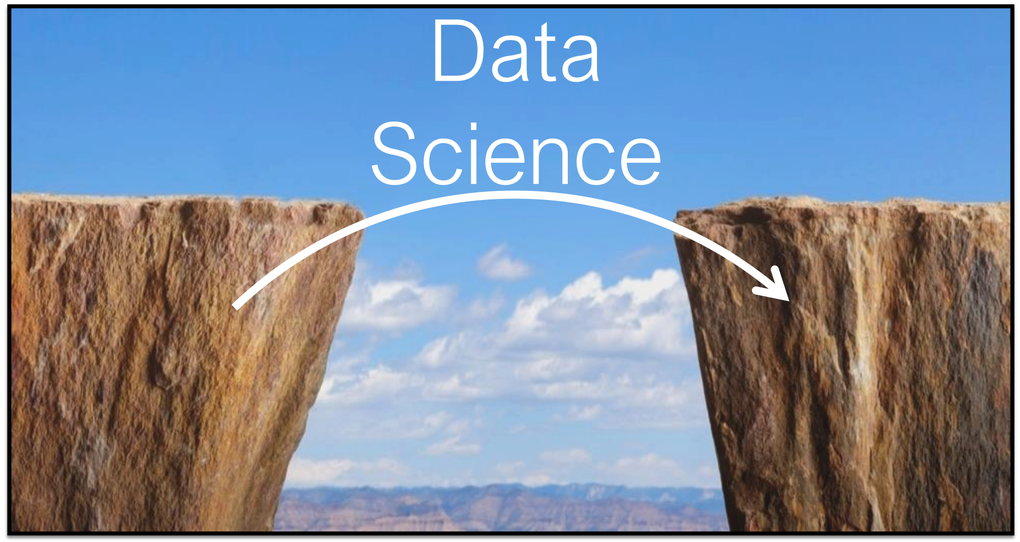
Distribution Statement

Data Analytics



Data Analytics Overview

- Significant investments in computational capabilities have resulted in unprecedented growth in data.
- Transitioning model results into decision making continues to be a challenge.
- Data science provides the underlying methodologies to produce actionable data for informed decision making.
- It includes machine learning, deep learning, large-scale data analysis, statistics, applied mathematics, and high-performance computing.
- Directly supportive of decision making - applicable to many current and future DoD problems.



Computational Science and Engineering

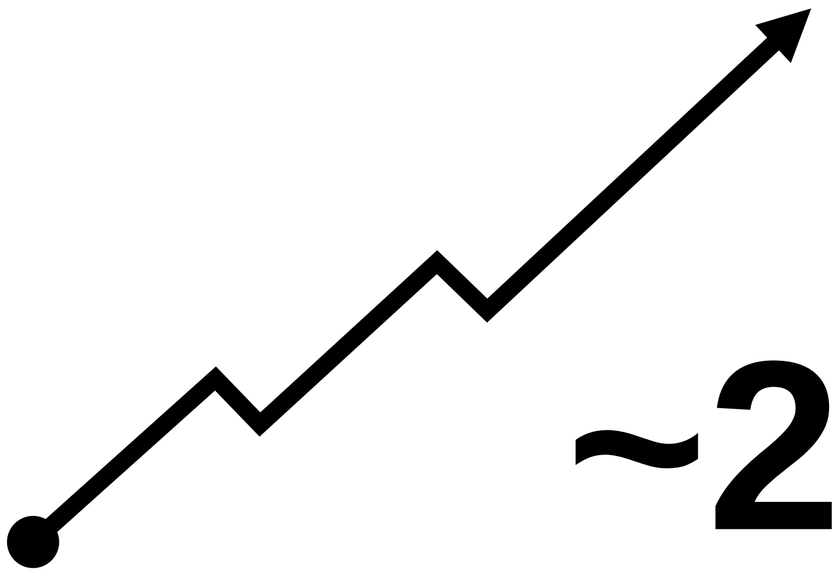
Data-informed Decisioning

Data Deluge

1. Quantity of information is soaring
2. Just managing the information is a challenge
3. Accessibility to information is a problem as well
4. However, integrating and preprocessing of the information are the primary bottleneck
5. Analyzing it, to spot patterns and extract useful information, is severely limited due to the challenges above



We are great at creating data!



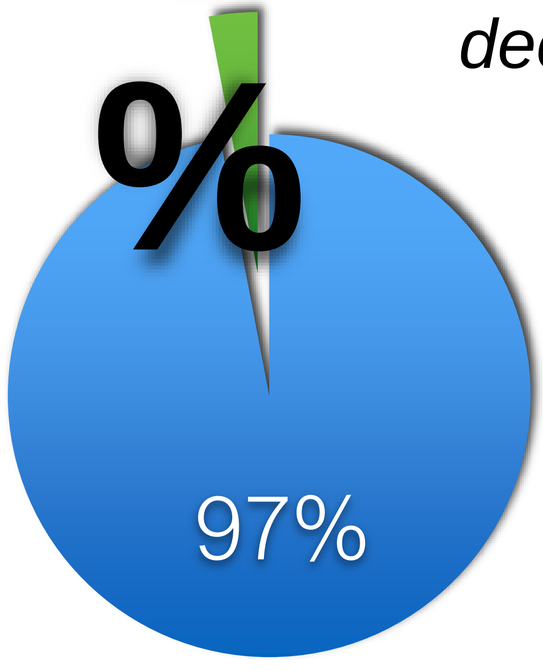
~25%

annual growth in data

3%

of the data is used to make decisions

**IDC Study*



The FOUR V's of Big Data

From traffic patterns and music downloads to web history and medical records, data is recorded, stored, and analyzed to enable the technology and services that the world relies on every day. But what exactly is big data, and how can these massive amounts of data be used?

As a leader in the sector, IBM data scientists break big data into four dimensions: **Volume, Velocity, Variety and Veracity**

Depending on the industry and organization, big data encompasses information from multiple internal and external sources such as transactions, social media, enterprise content, sensors and mobile devices. Companies can leverage data to adapt their products and services to better meet customer needs, optimize operations and infrastructure, and find new sources of revenue.

By 2015
4.4 MILLION IT JOBS
will be created globally to support big data, with 1.9 million in the United States



Volume
SCALE OF DATA

40 ZETTABYTES
[43 TRILLION GIGABYTES]
of data will be created by 2020, an increase of 300 times from 2005

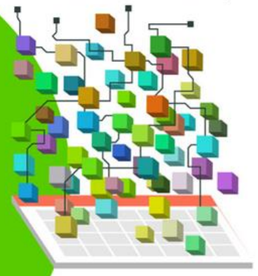


6 BILLION PEOPLE
have cell phones



WORLD POPULATION: 7 BILLION

It's estimated that
2.5 QUINTILLION BYTES
[2.3 TRILLION GIGABYTES]
of data are created each day





Most companies in the U.S. have at least
100 TERABYTES
[100,000 GIGABYTES]
of data stored

Velocity
ANALYSIS OF STREAMING DATA

The New York Stock Exchange captures
1 TB OF TRADE INFORMATION
during each trading session





Modern cars have close to
100 SENSORS
that monitor items such as fuel level and tire pressure

By 2016, it is projected there will be
18.9 BILLION NETWORK CONNECTIONS
– almost 2.5 connections per person on earth



Variety
DIFFERENT FORMS OF DATA

As of 2011, the global size of data in healthcare was estimated to be
150 EXABYTES
[161 BILLION GIGABYTES]



30 BILLION PIECES OF CONTENT
are shared on Facebook every month



By 2014, it's anticipated there will be
420 MILLION WEARABLE, WIRELESS HEALTH MONITORS



4 BILLION+ HOURS OF VIDEO
are watched on YouTube each month





400 MILLION TWEETS
are sent per day by about 200 million monthly active users

Veracity
UNCERTAINTY OF DATA

1 IN 3 BUSINESS LEADERS
don't trust the information they use to make decisions



Poor data quality costs the US economy around
$3.1 TRILLION A YEAR





in one survey were unsure of how much of their data was inaccurate

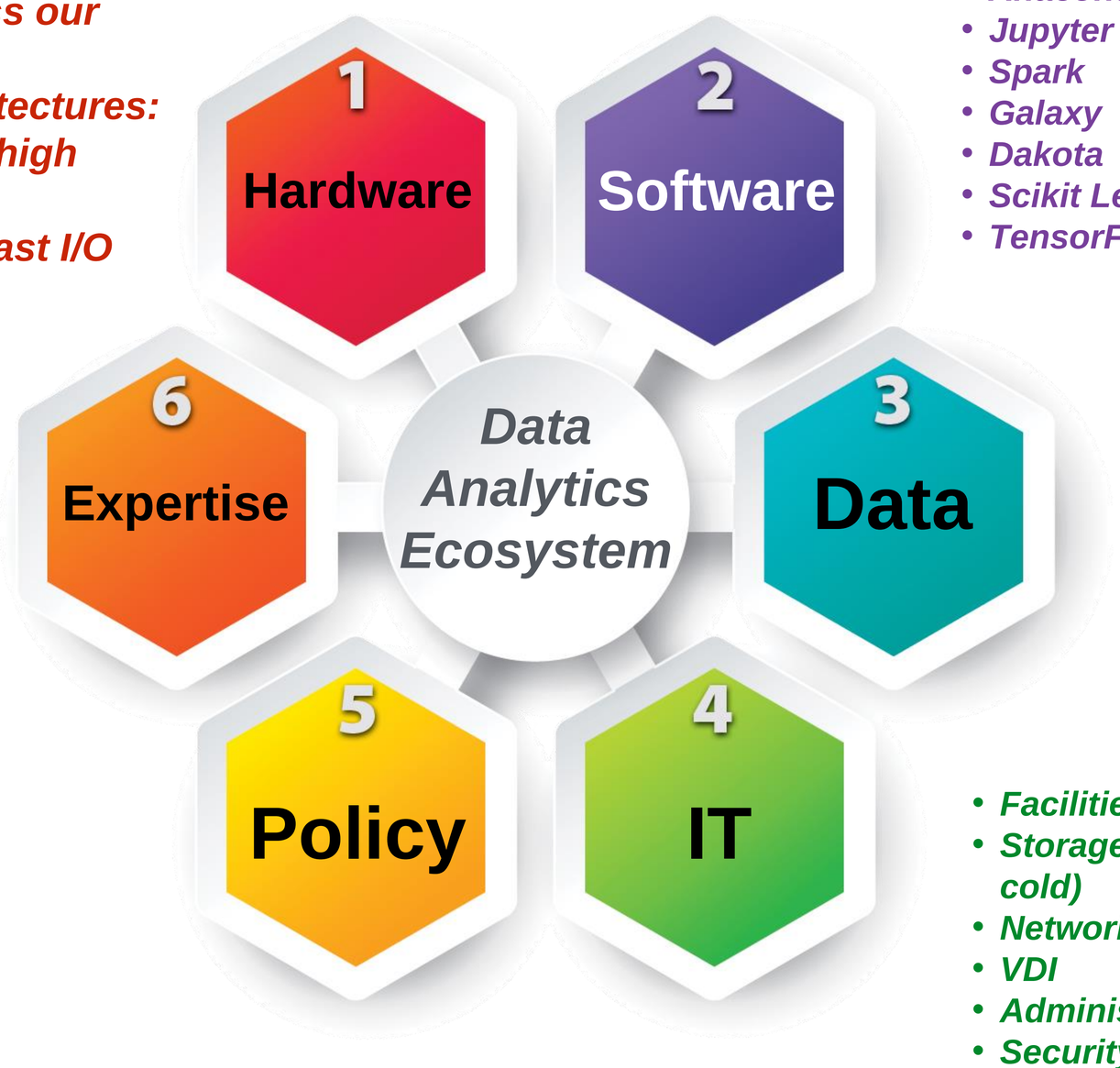
Sources: McKinsey Global Institute, Twitter, Cisco, Gartner, EMC, SAS, IBM, MEPTEC, QAS

IBM

Building blocks

- *Machines that can address our largest problems*
- *Blended computing architectures:*
  - *Numerical - distributed, high speed interconnects*
  - *Data - shared memory, fast I/O*

- *Leverages open source capabilities*
- *Python ,R, and C/C++ (when needed)*
- *Anaconda - package management*
- *Jupyter Notebooks*
- *Spark*
- *Galaxy*
- *Dakota*
- *Scikit Learn (machine learning)*
- *TensorFlow (deep learning)*



- *Terabytes collected - Unorganized and unaccessible*
- *Streamline data wrangling*
- *Minimize the movement of data*
- *Leverage database technologies*
  - *SQL and noSQL*

- *Computational and data scientists assist in problem step up, execution, and visualization*

- *Integrate necessary policies*

- *Facilities*
- *Storage (hot, warm, and cold)*
- *Networks (10G+)*
- *VDI*
- *Administration of machines*
- *Security - (monitoring, patching, etc.)*

Data Analytics Ecosystem



Mass Storage Services

- ERDC's MSAS System (Gold)
- 1PB SAMFS filesystem
- 25PB current on tape (80 PB capacity)
- 3 Oracle T54 servers running Solaris 11
- Data transfers are equally distributed among the 3 T54 servers)

Data Analytics



- Anaconda Enterprise
- Spark
- Machine Learning
- Deep Learning

High Speed Network (100G)

General Computing Services



- Virtualization
- Persistent Services
- Data Management
- Interactive Access

Computational Science



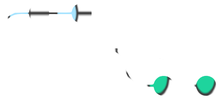
- 126,192 compute cores
- 544 Knights Landing nodes
- 32 GPGPUs
- 437 terabytes of memory

Models



Dakota
(optimizer)

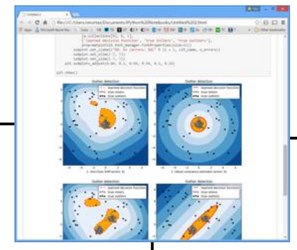
Galaxy
(workflow)



Computational Science & IT

Decision Gateways

Jupyter Notebooks



Web or VDI connection

Data Scientists





Web connection

Decision Makers



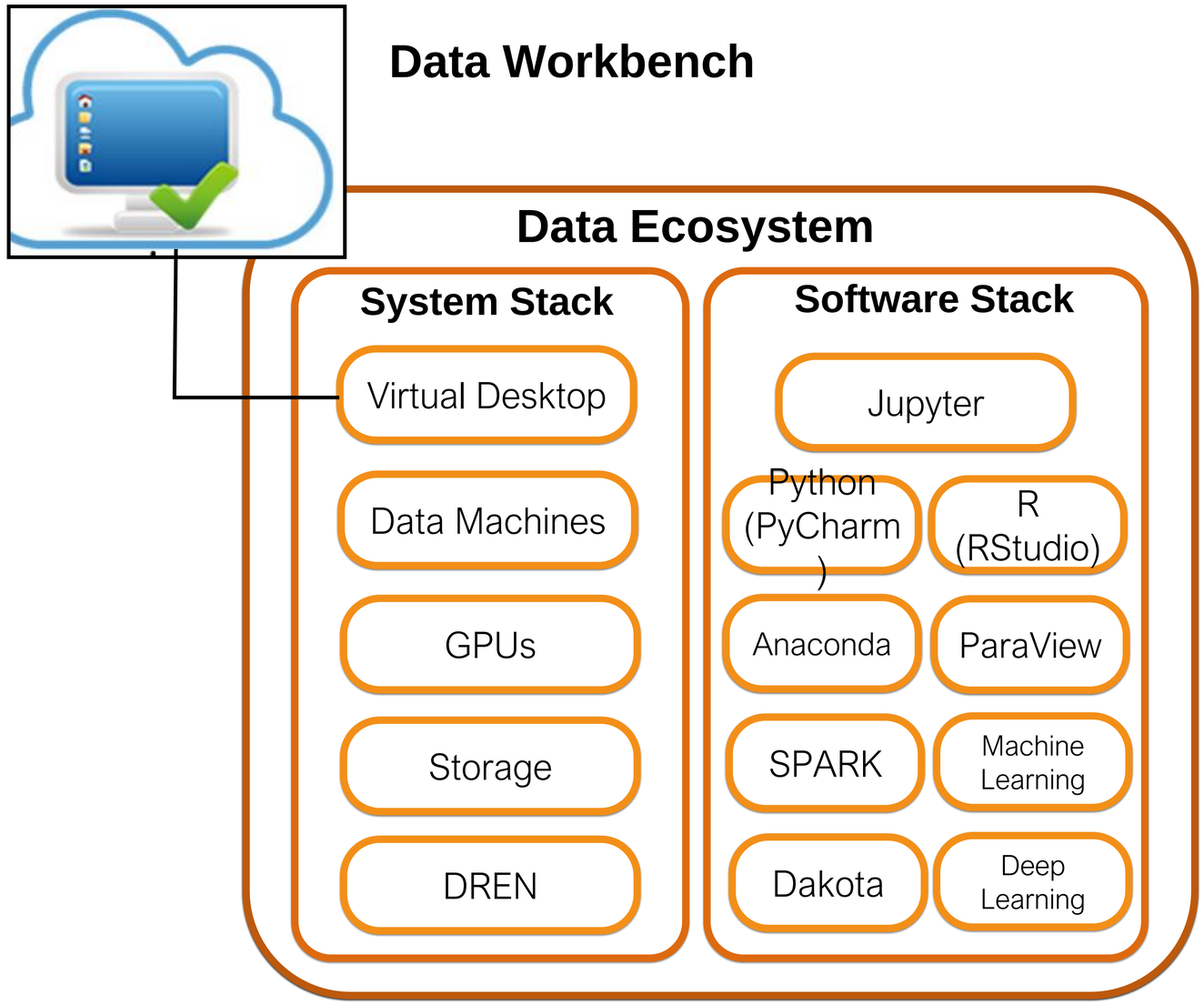
Data Workbench

Data Science & Decision Making

Distribution Statement

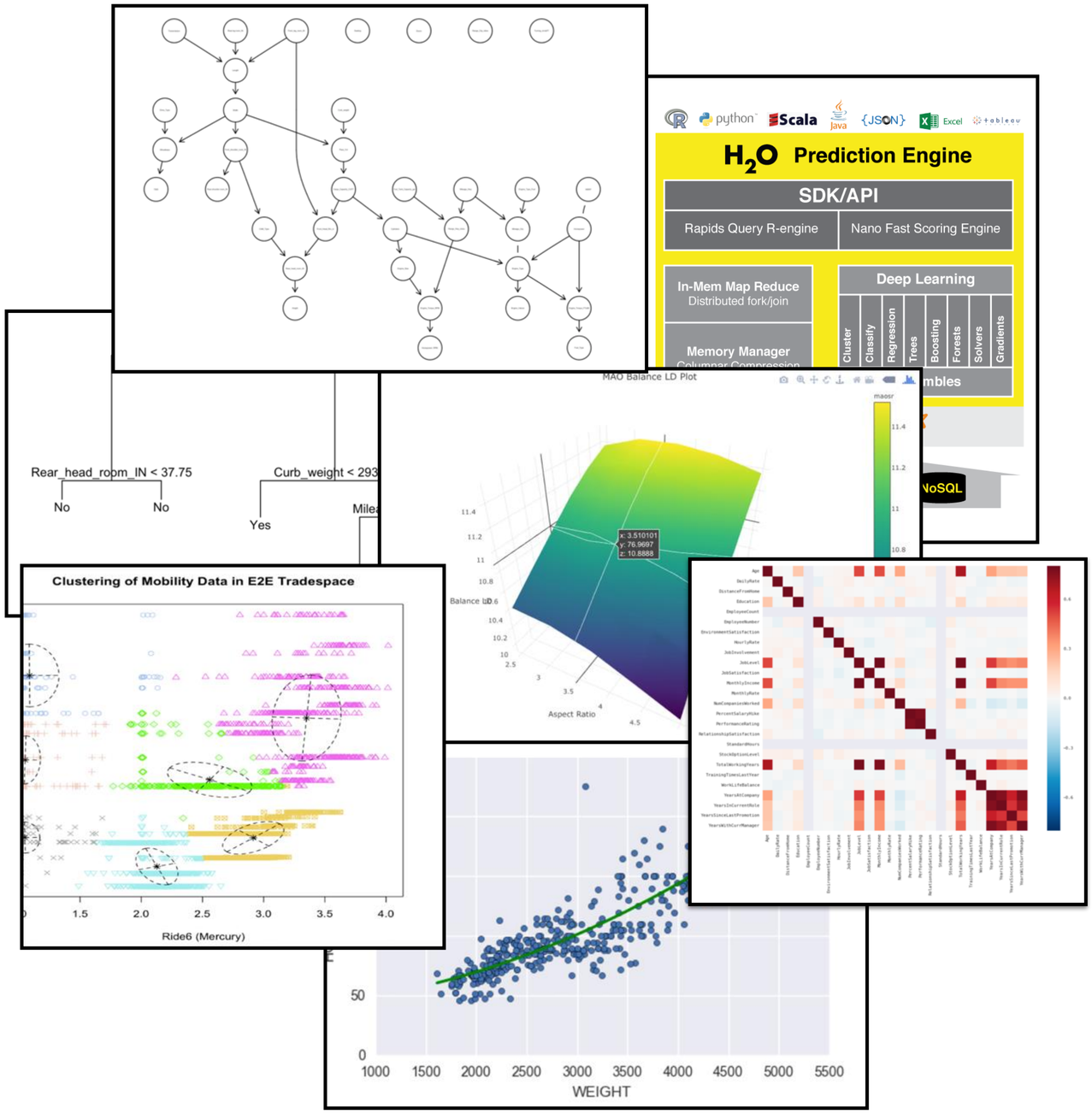
High-Performance Data Analytics Workbench

- Provides a DoD ecosystem for conducting large-scale data analytics
- Extends existing DoD investments in HPC to include data-intensive computing
- Provides users remote desktop access to *Workbench*
- Allows for the development of data analytics training curriculum based on *Workbench*
- Enables the deployment of *Workbench* on designated HPCMO machines



H2O for Machine Learning

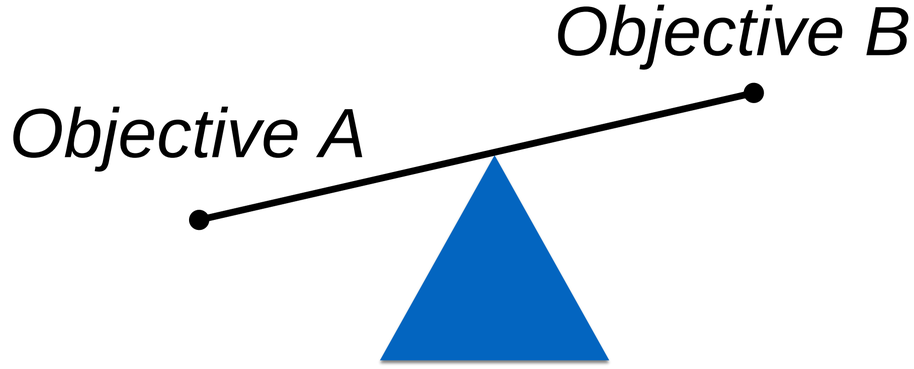
- Open source, written in Java
- Seamless integration with Hadoop and Spark
- Use common programming languages or web-based GUI
- Massively scalable – train on billions of rows of data
- Optimal efficiency - fine-grain distributed processing using in-memory processing combined with fast serialization between nodes and clusters
- Export models to Java objects for fast, real-time scoring
- Visual inspection of models during training through H2O Flow GUI



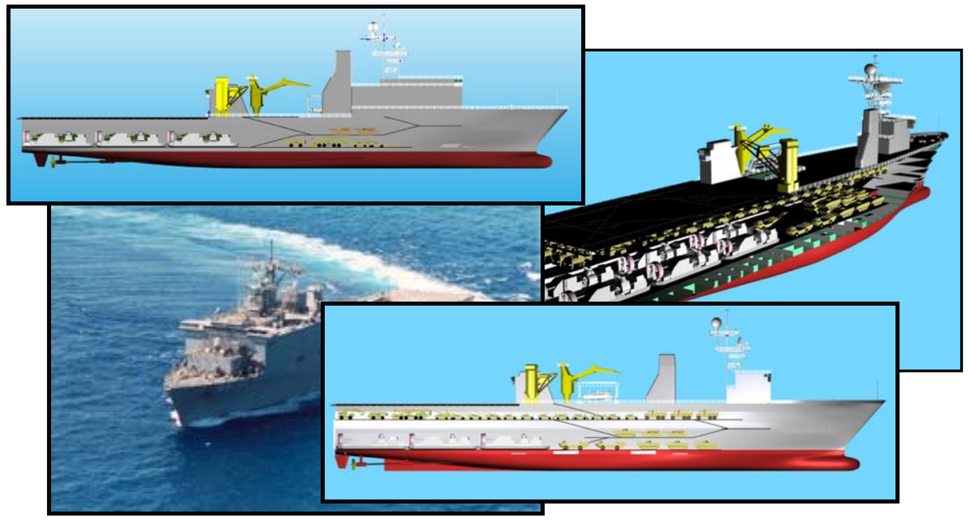
Trade-off Analytics

A technique of reducing or forgoing one or more desirable outcomes in exchange for increasing or obtaining other…

- Helps people make better choices when faced with multiple, often conflicting, goals and alternatives.
- Uses mathematical filtering techniques to identify the best candidate options based on different criteria,
- Allows users to explore the trade-offs between options to make complex decisions.
- Combines smart visualization and analytical recommendations for easy and intuitive exploration of trade-offs.

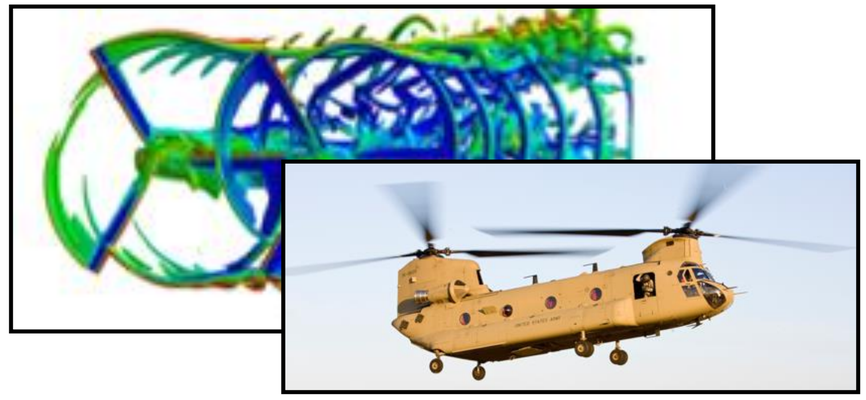


Trade-off Examples

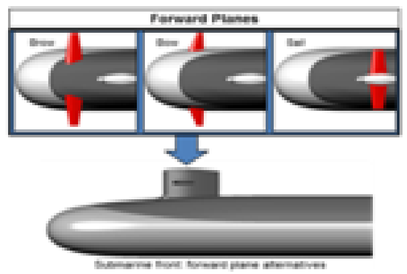


LX(R) Analysis of Alternatives (AoA): Navy researchers collaborated with the Engineered Resilient Systems (ERS) program for the initial LX(R) AoA. The AoA focused on understanding the trade-offs among 19 ship performance attributes, survivability specification levels, and cost. The Navy benefited from a detailed understanding of LX(R) requirements, performance, and cost trade-offs for 22,000 different design concepts – all produced and evaluated within 3 months. *This assessment included potential cost-performance benefits of new technologies early in the development of the system.*

CH-47F Performance Improvement: Army and Boeing researchers used CREATE rotorcraft software to confirm helicopter performance predictions for new Boeing proposed rotor blades, which are expected to provide 2,000 pounds of improved hover thrust for potentially 400+ CH-47Fs (Chinooks). *Additional lift directly translates to 10% more combat capability from the same platform*.







Ohio Replacement Submarine: Noise is the crucial element in detection of submarines – the quieter the submarine, the better chance it has to survive and provide a deterrent option to the National Command Authority. Detailed hydrodynamic evaluations using CREATE software are being used to provide guidance in hull, appendage, and propulsor design and testing for the Ohio Replacement Program (ORP). *These assessments evaluated maneuvering and vibration implications of different configurations directly impacting the design of ORP.*

ERDC

INFORMATION TECHNOLOGY LABORATORY

david.c.stuart@erdc.dren.mil







Engineered Resilient Systems

Influencing Acquisition Innovation

20th Annual NDIA Systems Engineering Conference
October 26, 2017

Owen Eslinger, PhD
ERS Program Manager
US Army Engineer Research and Development Center (ERDC)

ERS Platform: Innovation & Acquisition Reform

ENGINEERED RESILIENT SYSTEMS
DEPARTMENT OF DEFENSE

DoD current goals of acquisition reform and innovation are supported in six major thrusts within ERS

Non-linear Engineering
Promotes Model-based Engineering

Data-driven Analytics and Machine Learning Data Analytics
Deeper insights into decisions

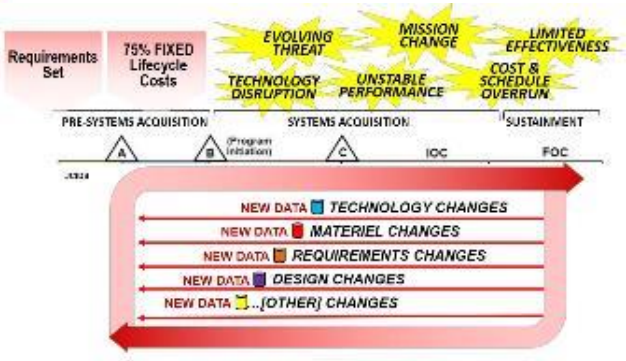
Physics-based Modeling
Enables design accuracy earlier in the process.

Big Data Visualization
Enhances communication and understanding in decision-making

Workflow Solutions
Breaks down barriers to HPC use

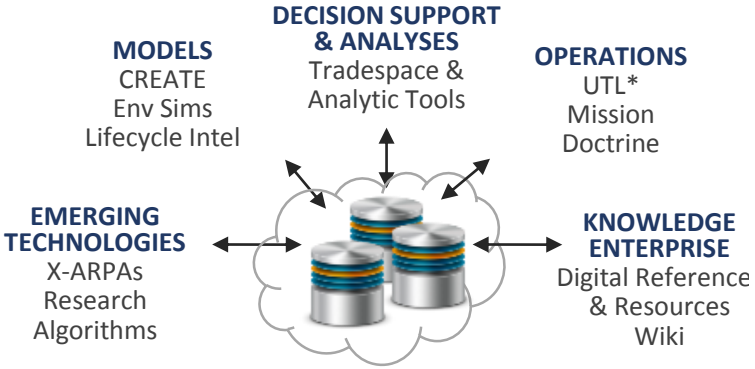
Govt-Industry Collaboration
Amplifies communication with common understanding and goals

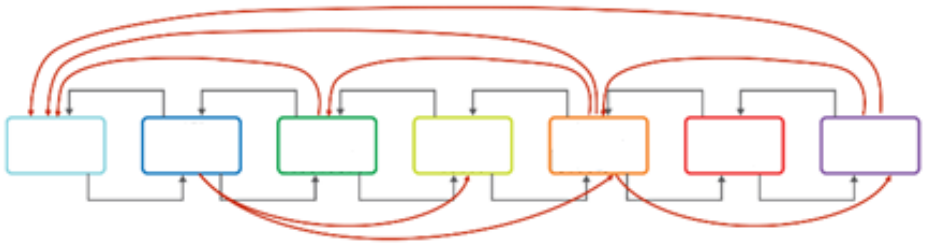
Non-linear, Model-based Engineering



Linear Engineering does not support today's complex system engineering and analytics

Maximize the use of data and models for large scale analytics





Facilitates non-linear engineering processes

* Universal Task List

Relevant ERS NDIA Talks

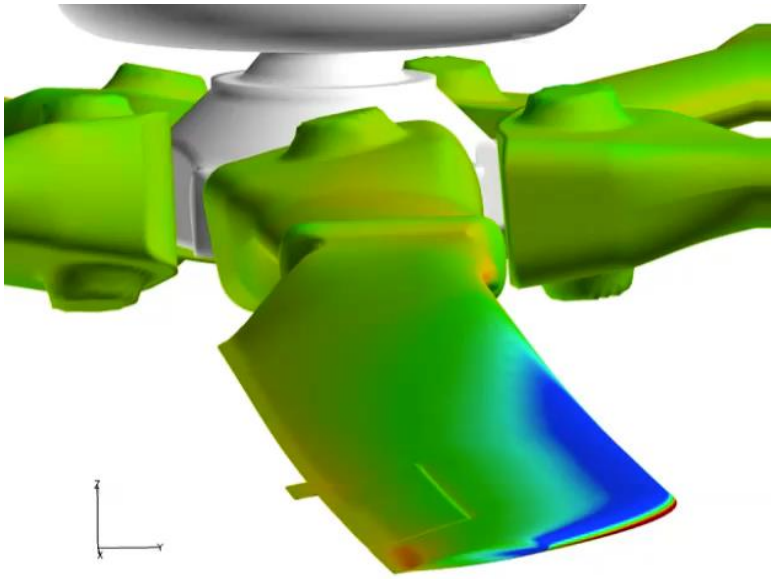
11:05 - Introducing Lifecycle Cost to Early Conceptual Tradespace Exploration
Alex Baylot - ERDC

1:00 - The Language of Complexity: Ontology in Systems Design & Engineering
Abe Wu - Raytheon Missile Systems

4:30 – ERS & MBE: Opportunities, Risks and Best Practices
Mark Halpern- Gartner

Physics-based Modeling

Provides confidence in performance and viability assessments early in the process



- **Realistic Insights:**
  - **Effectiveness (performance) and efficiency (time & cost) are critical measurements in the concept design phase**
- **Test/Eval Confidence:**
  - **Makes supporting virtual flight certification processes for new or modified platforms achievable**

Relevant ERS NDIA Talks

1:20 - Physics and model based aerodynamic design and analysis at GA *Pritesh Mody - General Atomics*	2:15 - Application of CREATE Tools for High Fidelity Design Space Exploration *Antonio De La Garza III - Lockheed Martin*	3:15 - Clustering Analysis in ERS Tools for Enhanced Trade Space Exploration of GVs *Andrew Pokoyoway - TARDEC*

Workflow Solutions for Computational Environments

New workflow solutions lower the barriers to working in high-performance environments

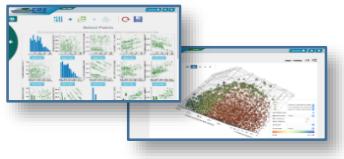
Requirements & Systems Modeling



Tradespace Creation

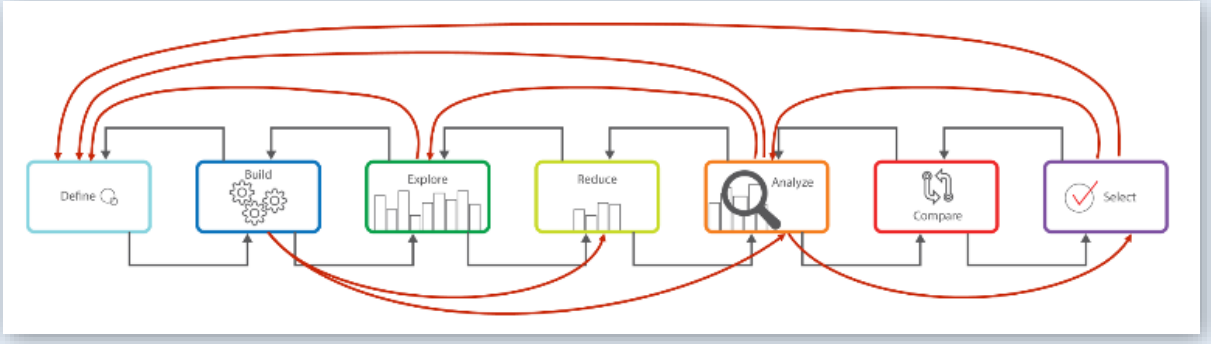


Tradespace Analysis



INTEGRATION AUTOMATION COLLABORATION

INDUSTRY
Develop & integrate tools to support complex system design processes



GOVERNMENT
Invest in future computing environments; communicate needs

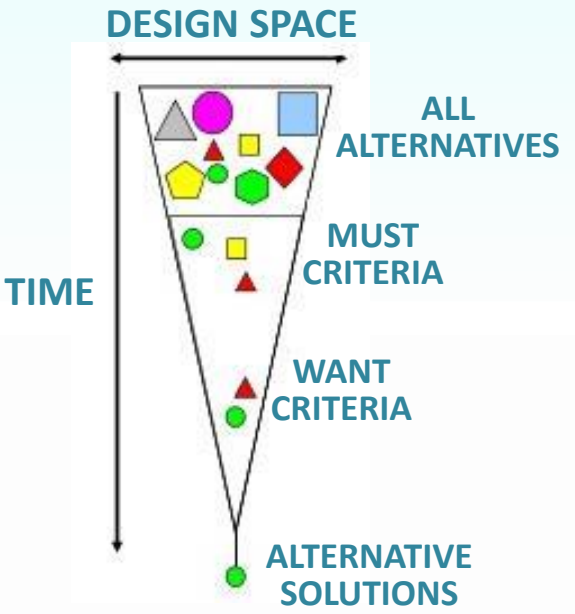
Relevant ERS NDIA Talks

1:50 - Automation and Integration for Complex System Design
Scott Radon - Phoenix Integration

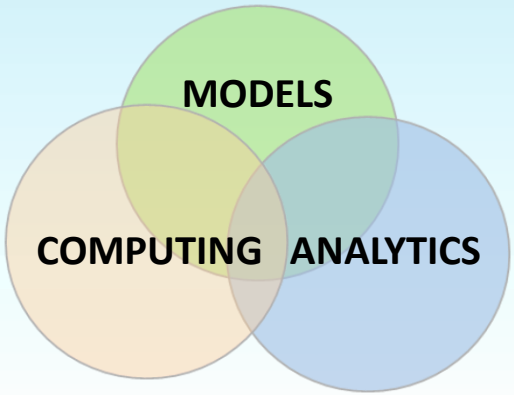
Data-driven Analytics
Machine Learning Data Analytics

Data-driven, tradespace analytics – provides greater insights earlier in the design process, e.g., cost vs risk

DATA-RICH ASSESSMENTS



INTEGRATED TOOLS & RESOURCES



MACHINE LEARNING TECHNIQUES

Humans - 10s of Options

Excel - 100s of Options

Data Analysis Tools - 1000s of Options

Hyper-dimensional space - Millions of Options

Relevant ERS NDIA Talks

8:50 - Scaling Data Analytics for Engineered Resilient Systems
David Stuart – ERDC

10:15 - Tradespace: Informed Decision-making for Acquisition
Timothy Garton - ERDC

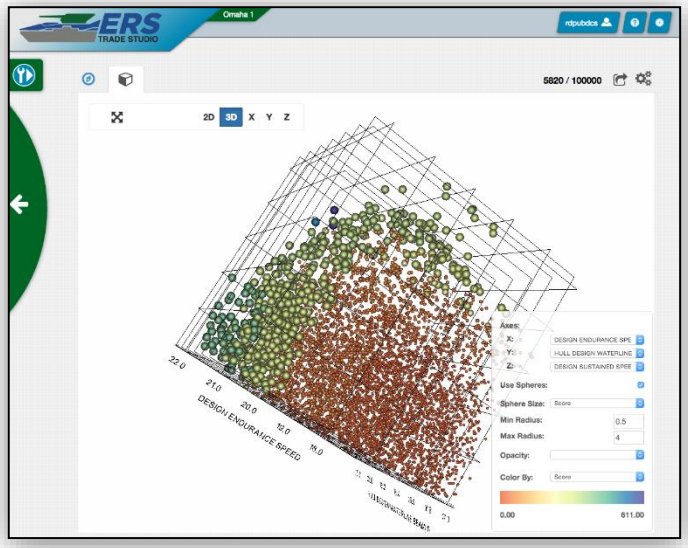
Distribution Statement A: Approved for Public Release

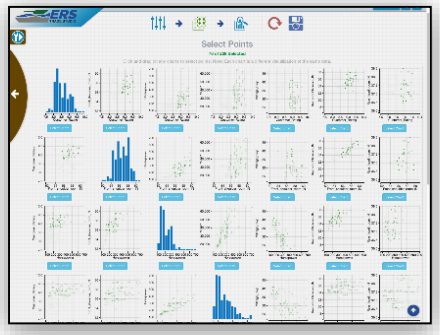
Big Data Visualization

Data Visualization builds accurate representations for the human mind

ERS Visualization of multi-dimensional data enables:

- Deeper comprehension (required for use of big data analytics)
- Higher level interpretation of multi-dimensional data representations for human consumption
- Critical communication in decision-making





ERS TradeAnalyzer provides automatic insights into design decisions for the user.*

***Beta Release completed Sep 2017**

Relevant ERS NDIA Talks

8:50 - Scaling Data Analytics for Engineered Resilient Systems
David Stuart – ERDC

10:15 - Tradespace: Informed Decision-making for Acquisition
Timothy Garton - ERDC

3:15 - Clustering Analysis in ERS Tools for Enhanced Trade Space Exploration of GVs
Andrew Pokoyoway - TARDEC

Govt-Industry Collaboration Infrastructure

Synthesizes community-wide goals with common data sources, analyses, assessments, and improved understanding.



Relevant ERS NDIA Talks

11:30 - Overcoming the Government-Industry Collaboration Hurdle
Patrick Martin, PhD - BAE

1:25 - Physics and model based aerodynamic design and analysis at GA
Pritesh Mody - General Atomics

2:15 - Application of CREATE Tools for High Fidelity Design Space Exploration
Antonio De La Garza III - Lockheed Martin

ERS in DoD Acquisition Context

DESIGN ENGINEERING ANALYTICAL ENVIRONMENT
Conceptual Design
Analysis of Alternatives
Value Engineering

HIGH-FIDELITY COMPUTATIONAL ENVIRONMENT
Prototyping
Test & Evaluation
Operational Analysis

PLATFORM DOMINANCE
Leverage domain expertise across DoD

USER-BASE STAKE HOLDERS

- SENIOR DECISION MAKERS
- PEOs, PMs
- ACQUISITION ENGINEERS
- SMEs
- ANALYSTS

WEB INTERFACE

ALTERNATIVES

DECISIONS

INDUSTRY Cloud Services

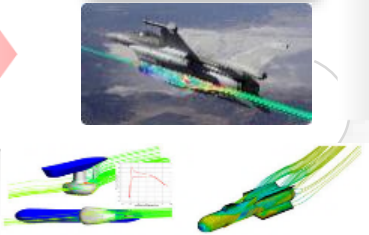
IP PROTECTED

RMF COMPLIANT

- CAPABILITIES GENERATION
- TRADESPACE ANALYSIS
- MISSION ENGINEERING
- ENGINEERING ANALYSES
- COST ANALYSIS
- WORKFLOW PRODUCTIVITY

Domain-specific Design and Engineering Support

MAKE PROTOTYPING COMPUTATIONAL





ENTERPRISE DATA AND KNOWLEDGE ENVIRONMENT









DIGITAL THREAD – DIGITAL TWIN









DOCUMENTATION **SEARCH** **STORAGE** **DISTRIBUTION** **RETRIEVAL** **TUTORIAL**

ENGINEERING A RESILIENT SYSTEM

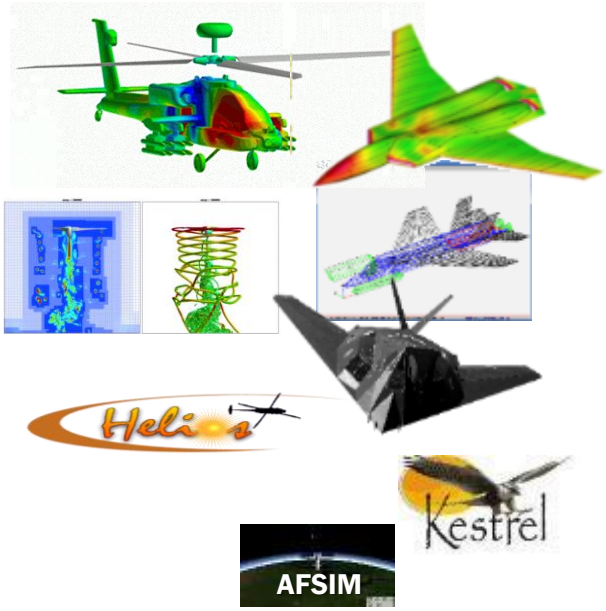
Distribution Statement A: Approved for Public Release

ERS: Developing Domain-specific Design Environments

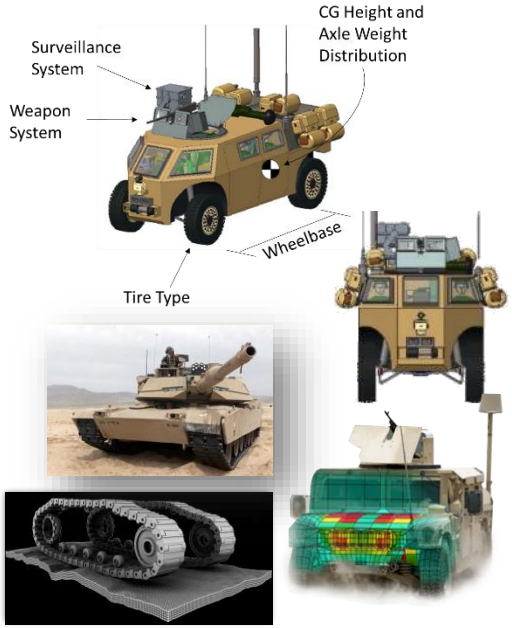
Each domain has unique processes and toolsets

Air

Rotorcraft – Fixed Wing



Land



Sea

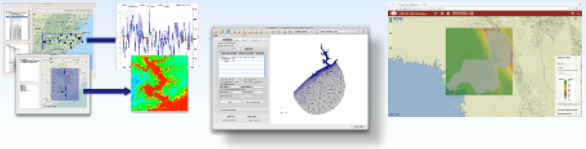


TOOLS AND PROCESSES **HPC** **ENVIRONMENTAL SIMULATOR**

TradeStudio

CREATE





SUPPORT BY COMMON, INTEGRATED RESOURCES

Distribution Statement A: Approved for Public Release

ERS Industry Participation

Industry partners are working with the Government in the ERS environment development and implementation

BAE SYSTEMS

11:30 - Overcoming the Government-Industry Collaboration Hurdle
Patrick Martin, PhD - BAE

Raytheon

1:00 - The Language of Complexity: Ontology in Systems Design & Engineering
Abe Wu - Raytheon Missile Systems

GENERAL ATOMICS AERONAUTICAL

1:25 - Physics and model based aerodynamic design and analysis at GA
Pritesh Mody - General Atomics

PHOENIX INTEGRATION

1:50 - Automation and Integration for Complex System Design
Scott Radon - Phoenix Integration

LOCKHEED MARTIN

2:15 - Application of CREATE Tools for High Fidelity Design Space Exploration
Antonio De La Garza III - Lockheed Martin

Senate Arms Services Committee Statement on Pentagon Acquisition System Report

"…Without ongoing reform and innovation, the Department of Defense cannot hope to maintain the technological advantages that underpin our nation's military superiority."

Senator John McCain
Majority Chairman, SASC
August 2017

Distribution Statement A: Approved for Public Release

Questions



ERS NDIA
FUELING INNOVATION & COLLABORATION

Implementation of Clustering Analysis in Engineered Resilient Systems Tools for Enhanced Trade Space Exploration of Military Ground Vehicles

Mr. Andy Pokoyoway*, Dr. Matt Castanier
US Army Tank Automotive Research, Development, and Engineering Center (TARDEC)

Abstract ID: 19712 *** Lead author contact info:** 586-282-3765 <andrew.p.pokoyoway.civ@mail.mil>

NDIA Systems Engineering Conference
Springfield, VA 26 OCT 2017

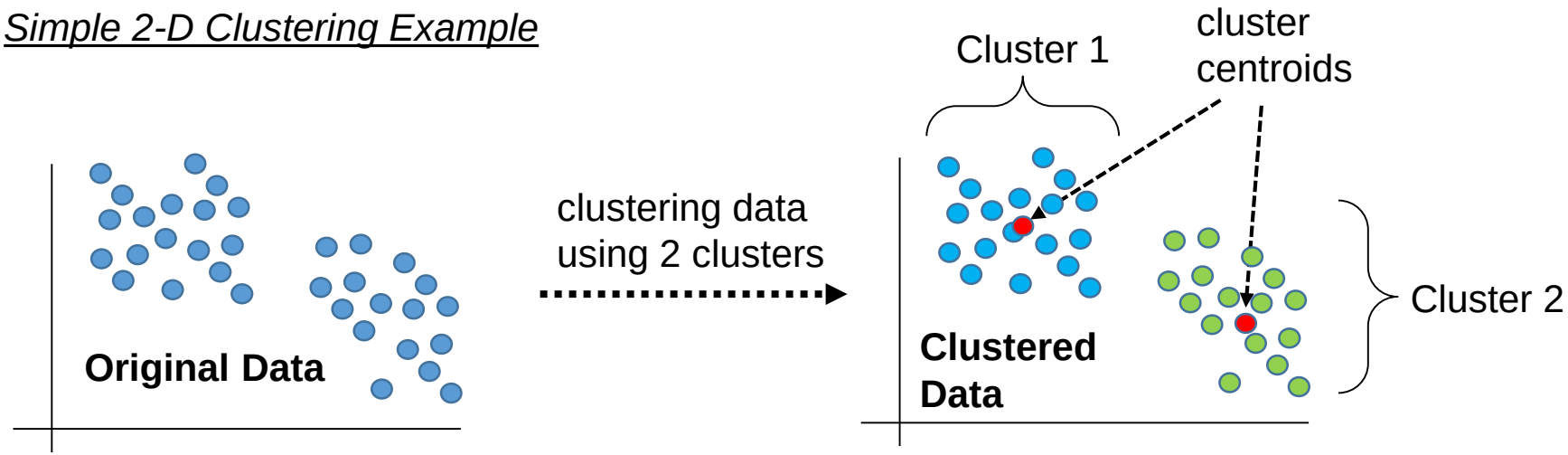
Background and Motivation

- Performing multidisciplinary design optimization of a military ground vehicle is extremely challenging
- One challenge is related to analyzing large, highly dimensional vehicle design datasets
- Analysis questions to answer regarding these datasets:
  - Do my highest-ranked designs reside in multiple regions of the trade space?
  - How many promising regions are there?
  - Does each region represent variations on a single design concept or multiple design concepts?
  - How can I best characterize the unique features of each design concept?

Clustering

- Simply put, clustering is the process of assigning data points to groups based on how closely their values are to a common group centroid
- A way to group data that is highly dimensional
- Different algorithms available
- Machine learning technique

Simple 2-D Clustering Example



Clustering for Trade Space Design Populations

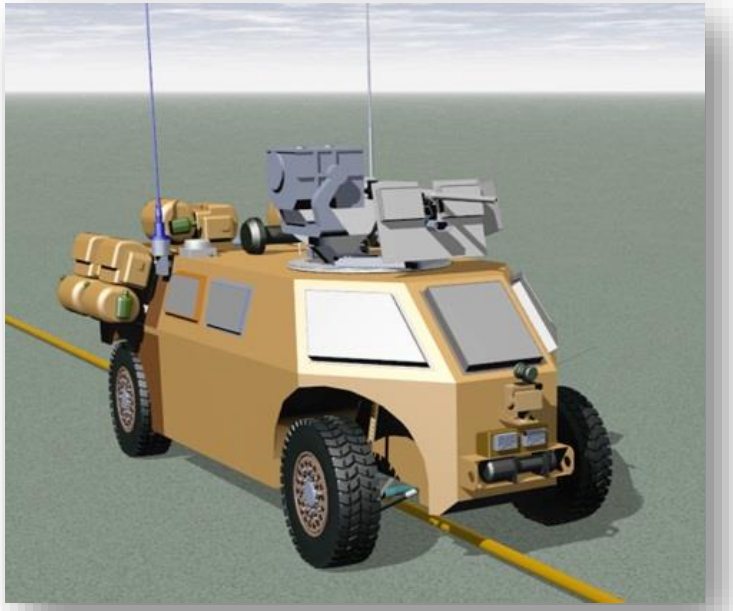
- Reduce large, highly dimensional datasets to more manageable, digestible sizes. This can make it easier to draw conclusions

- Automated way of quantifying and qualifying design differences - ***characterizing***; may help answer the question of : "How different are the top ranked vehicle designs?"

- Clusters could be used to provide promising vehicle design groups, and therefore promising characteristics, to be taken to the next stage of vehicle development

Objectives

- Learn, evaluate, and provide feedback to developers of **CREATE-GV and ERS Tools**
- Apply these tools to the **LRV notional concept vehicle** to perform **trade space exploration**
- Develop new trade space exploration methods for ground vehicles



CREATE-GV: Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles

ERS: Engineered Resilient Systems

LRV: Light Reconnaissance Vehicle

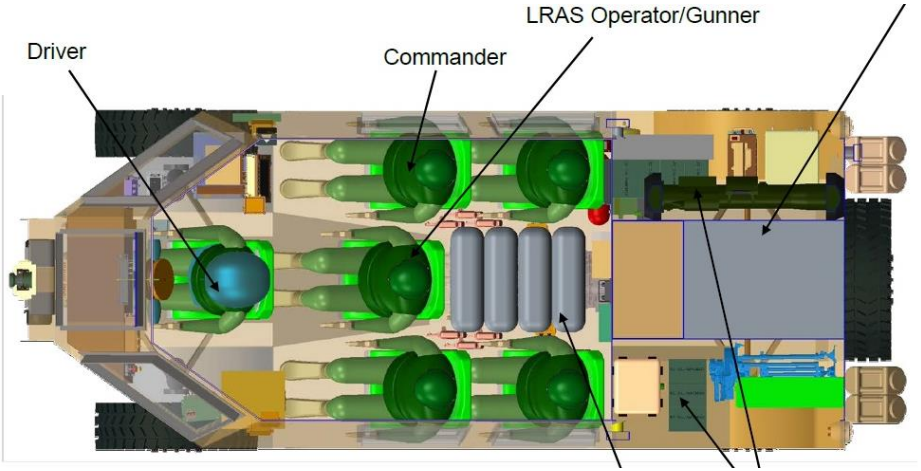
UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

LRV – A Notional Concept for a New-Start Vehicle

Notional concept was initially developed based on these requirements:

- Crew of 6
- Power for 96-hour mission
- Silent watch, silent move
- Advanced reconnaissance & surveillance equipment package
- CH-47 internal transport and sling-load transport





Trade Space Exploration Process

Reviewed initial concept & requirements

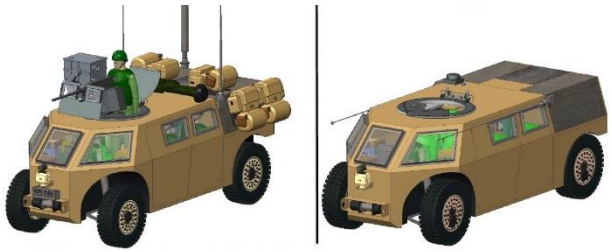
Performed analysis to build trade space

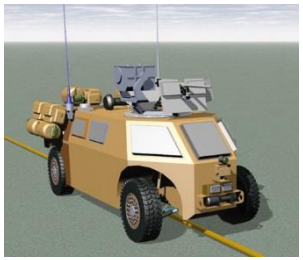
Revisited concept & varied requirements

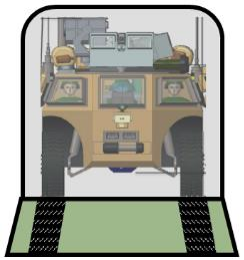
Performed analysis to expand trade space

Generated new design set = new concept

Iterative Concept-Analysis Loop











ENGINEERED RESILIENT SYSTEMS

Trade Space Exploration Process

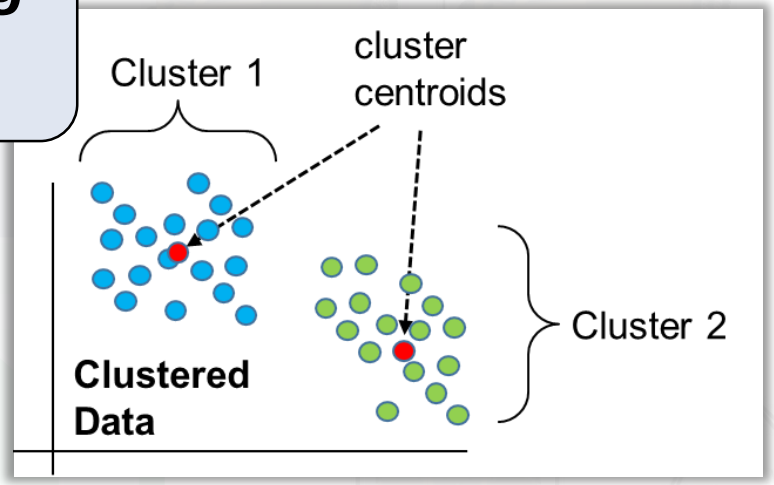
Reviewed initial concept & requirements

Performed analysis to build trade space

Revisited concept & varied requirements

Iterative Concept-Analysis Loop

Clustering Analysis



Performed analysis to expand trade space

Generated new design set = new concept

UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Trade Space Construction in ERS TradeBuilder

CREATE-GV	
1	On-Road Speed
2	Off-Road Speed
3	Max Sandy Grade
4	Off-Road No-Go %
5	Soft-soil mobility

ERS TradeBuilder	
1	Surveillance
2	Crew
3	Stability
4	Silhouette
5	Power density
6	Survivability
7	Transportability
8	Lethality

Performance Metrics imported from result files

Performance Metrics evaluated in ERS TradeBuilder

Design Variables

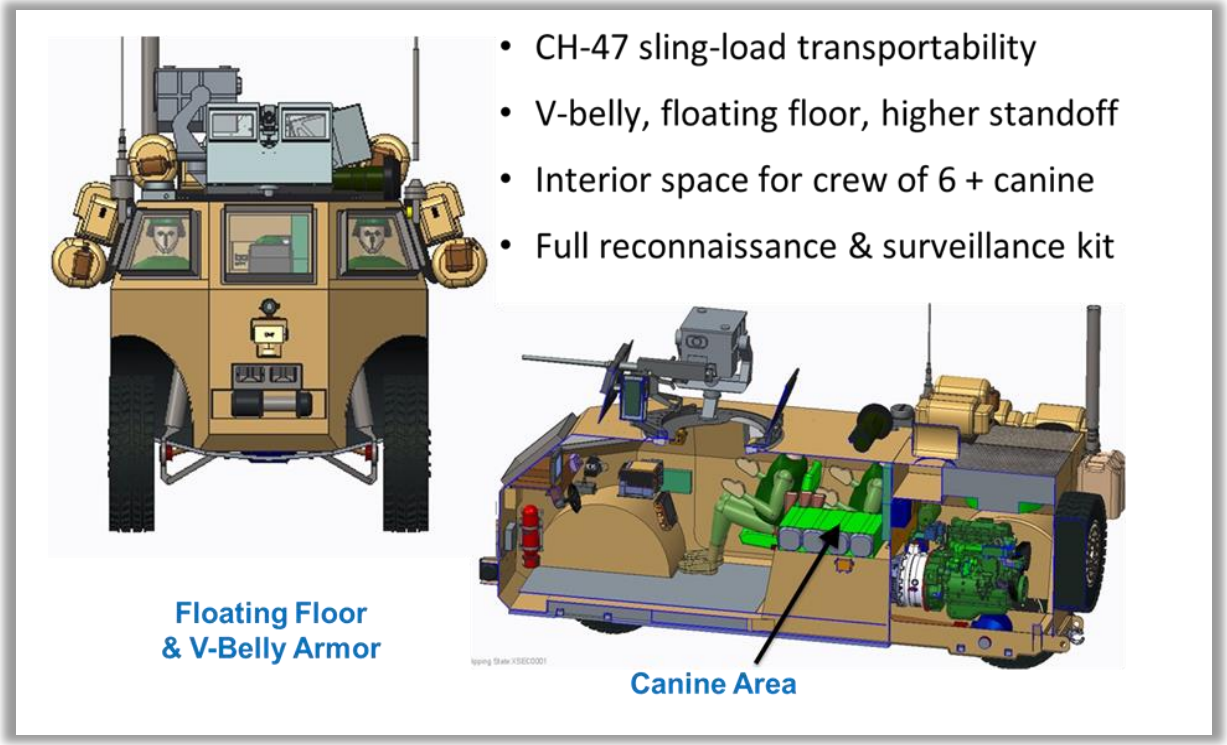
#	H	L	W	…											
1	H_1	L_1	W_1												
2	H_2	L_2	W_2												
3	H_3	L_3	W_3												
4	H_4	L_4	W_4												

Designs

UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Trade Space Vehicle Design Characterization

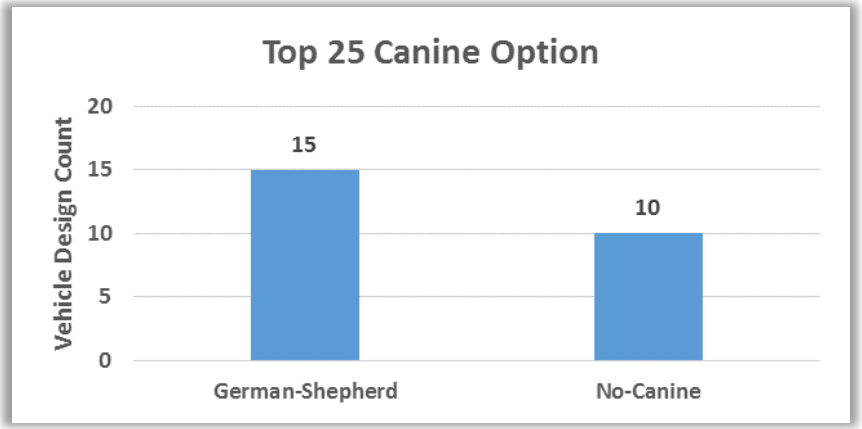
- Common features from highest-ranked designs:

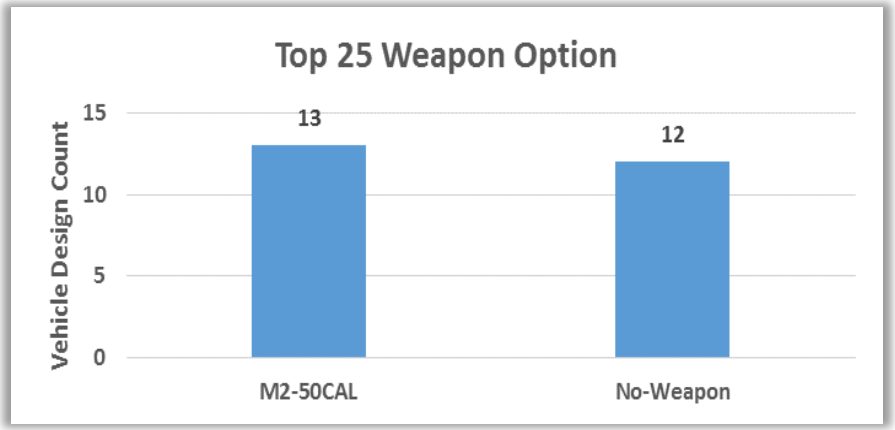


These are general features typically seen in the top 25 ranked vehicles, **though not all of the top 25 designs had the same features**

Trade Space Vehicle Design Characterization

- Two areas where differences are seen in the top 25 designs :



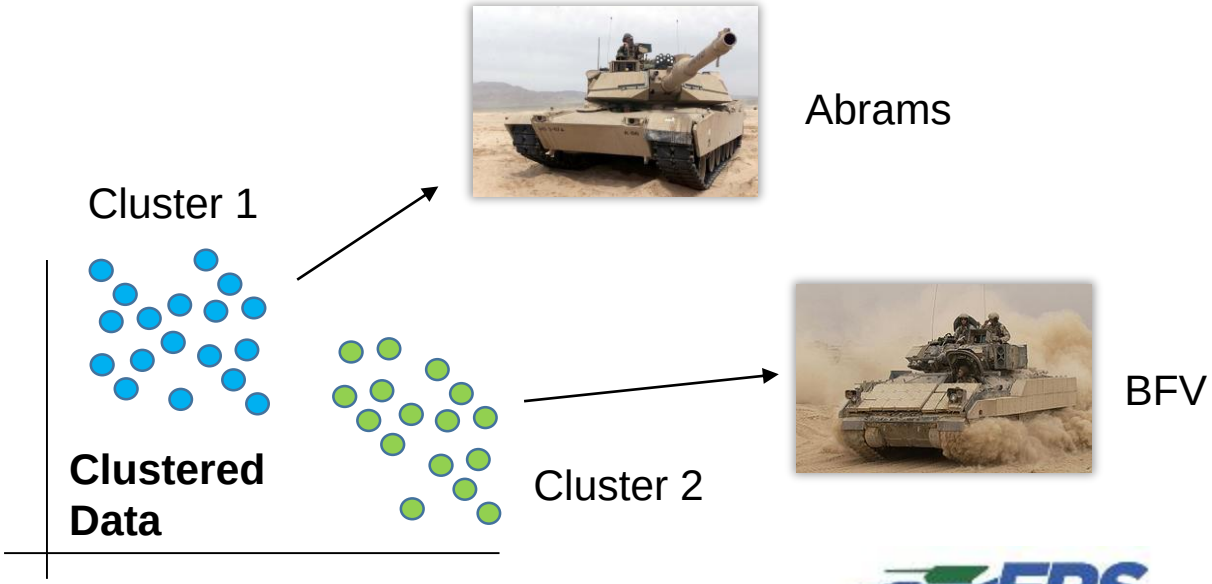


- Characterizing the top ranking designs as a whole may not lead to as useful conclusions regarding which features a single vehicle design should have
- We could be **unintentionally characterizing multiple vehicle designs, multiple variants**, *a potential outcome when performing multi-objective design optimization*

Trade Space Vehicle Design Characterization

- Early in the concept development phase, the trade space is large, with a design space that could be spanning regions consisting of two or more completely different vehicle designs
- … and this is not apparent
- We want to understand if potential regions exist early on in the analysis process to understand what unique concepts we may have

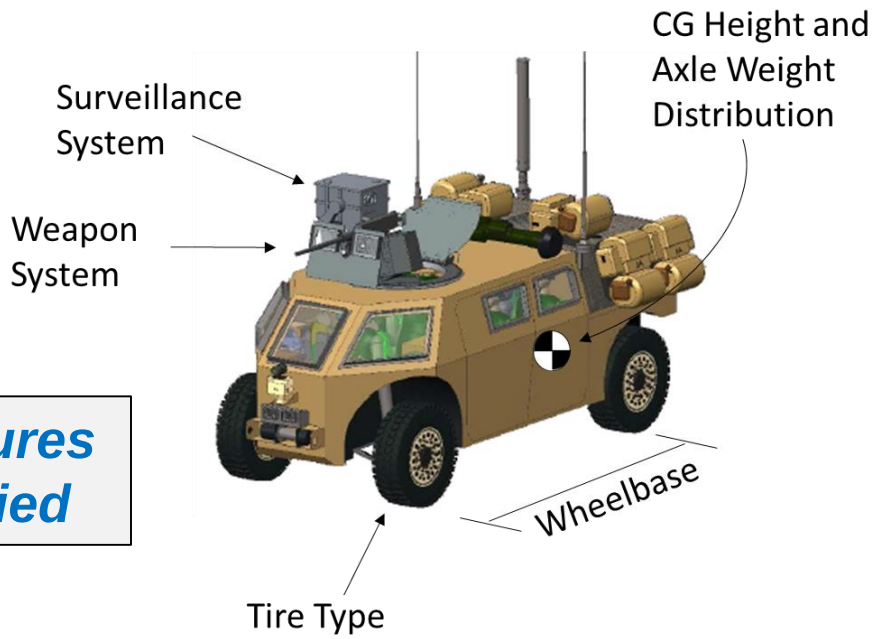
Potential example outcome of early concept, highly dimensional, multi-object design optimization



UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Analysis - Setup

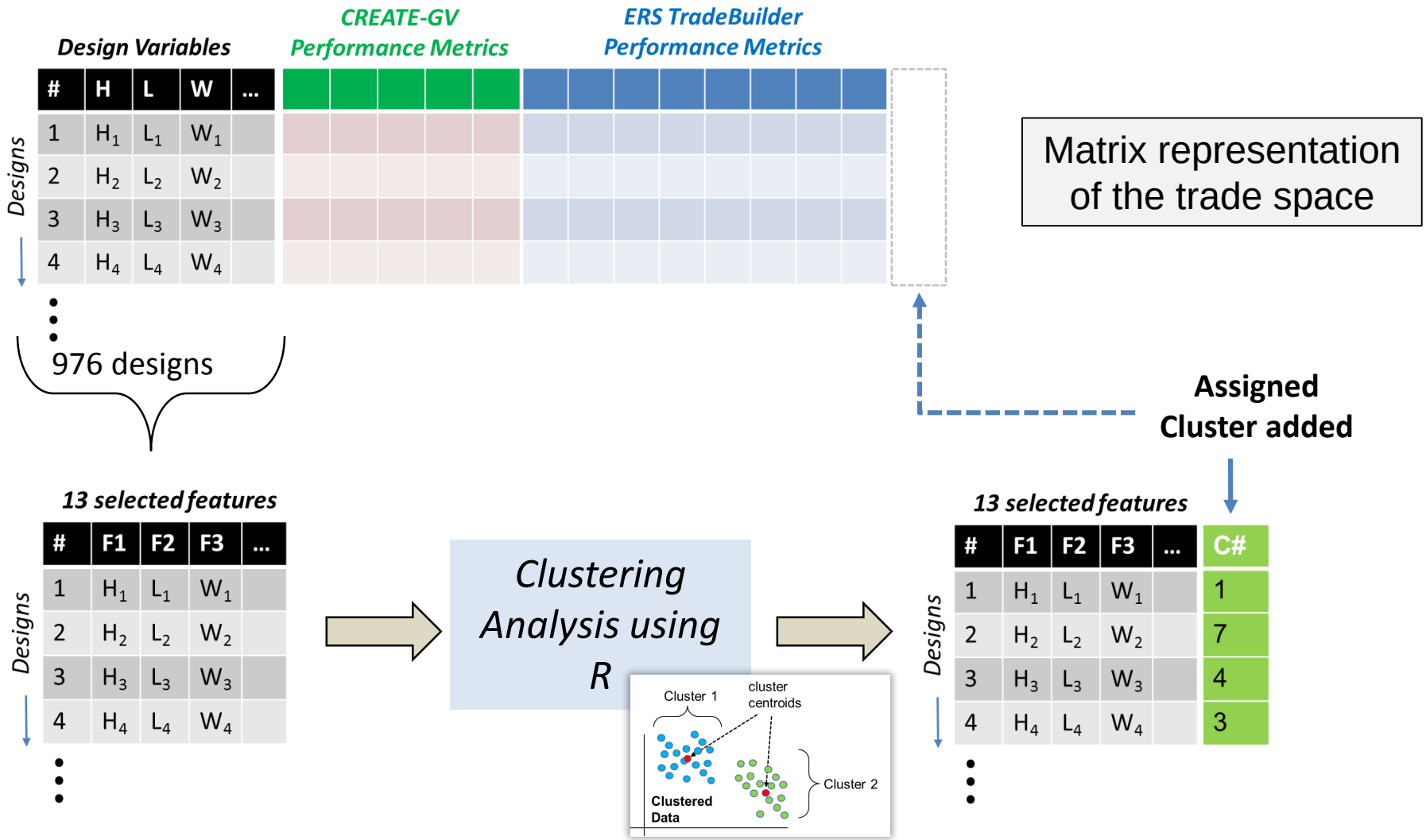
- **K-means clustering** algorithm used within R ("Hartigan-Wong" version)
- **Chose to generate 10 clusters** based on the "within sum of squares (WSS)" count selection method
- Design variables and characteristics chosen for features:



13 features specified

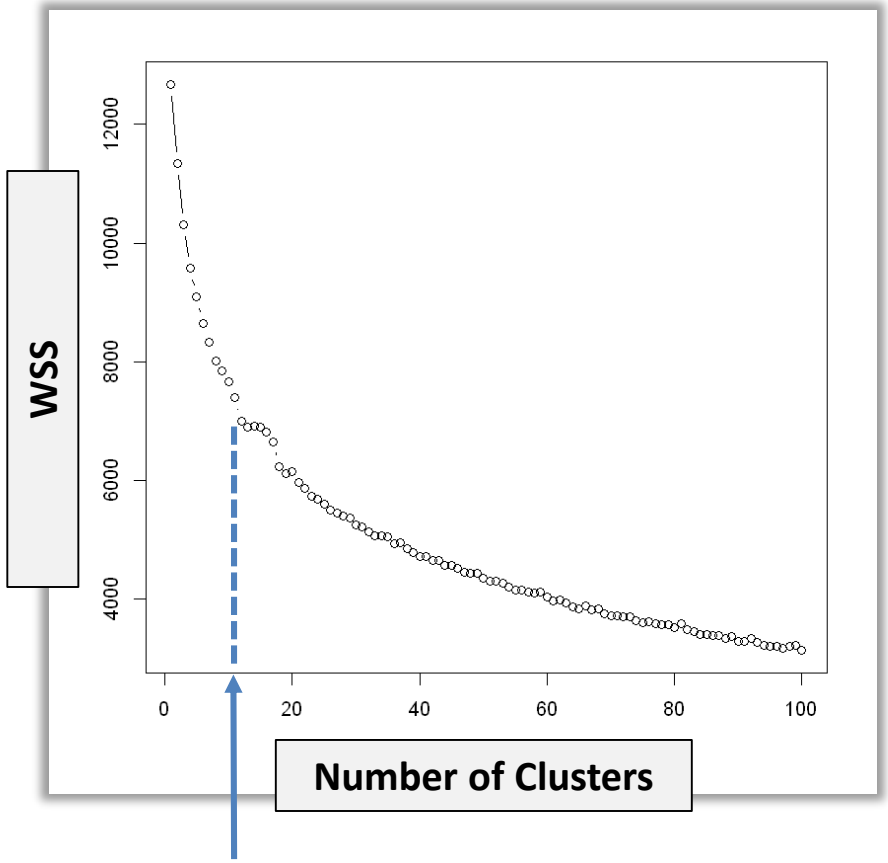
- Suspension characteristics (damping ratio and ride frequency) for the front and rear axles
- Canine
- Crew size
- Armor weight

Clustering Analysis - Setup



Clustering Analysis – Selecting Cluster Count

- Within Sum of Squares cluster count selection method (WSS)

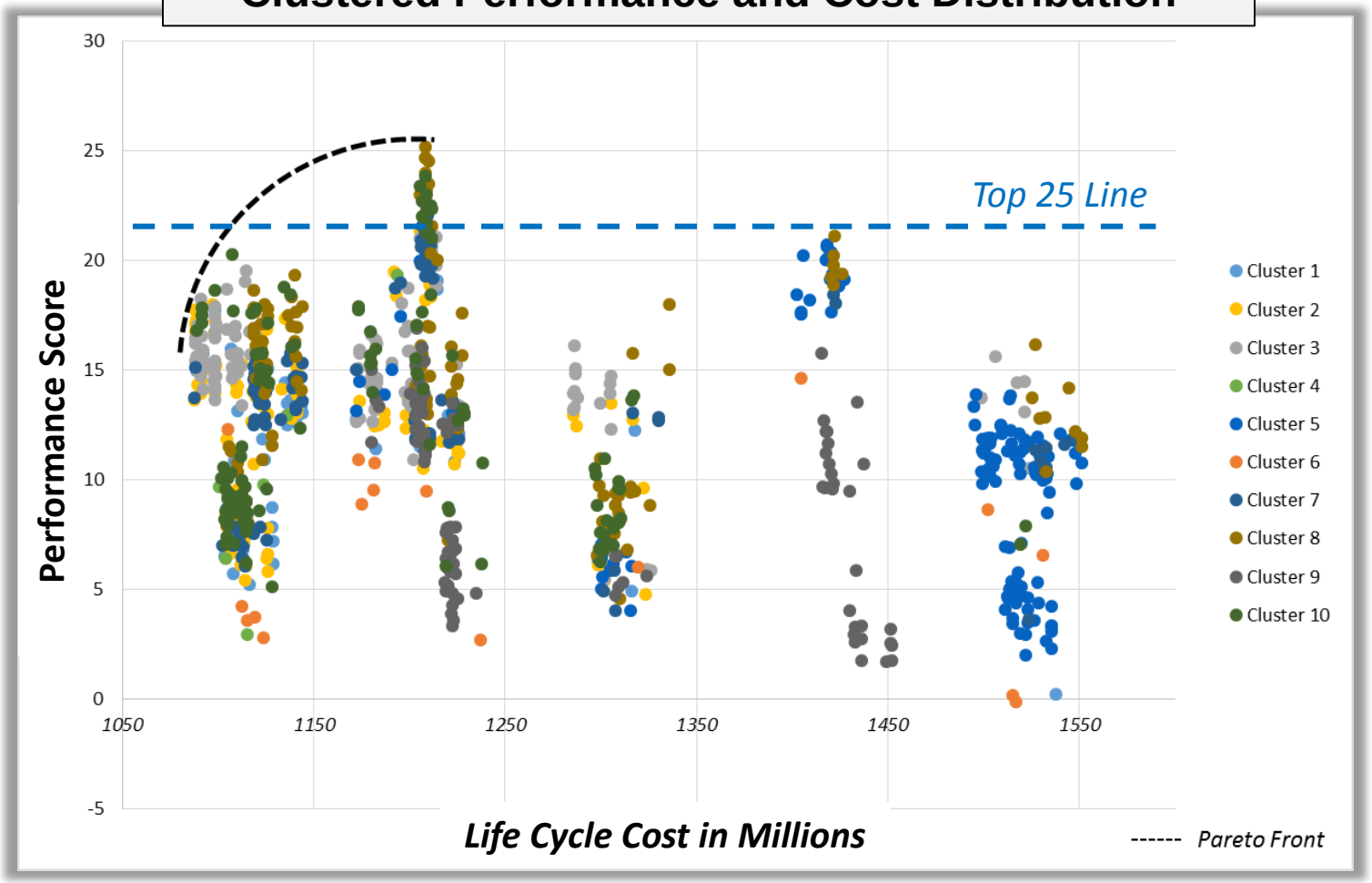


… at 976 clusters, the sum of squares value would equal 0

10 Clusters

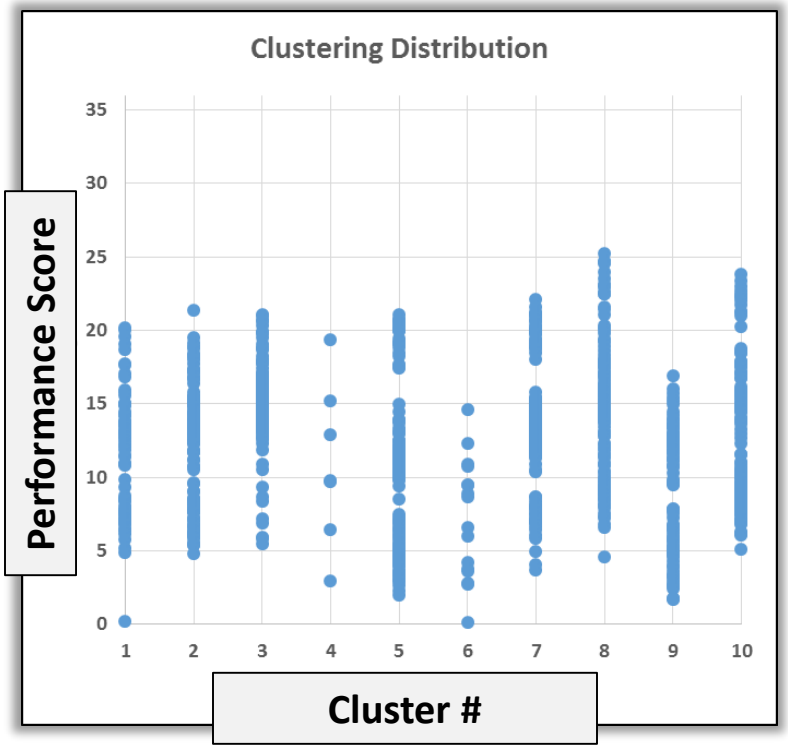
Clustering Analysis – Results

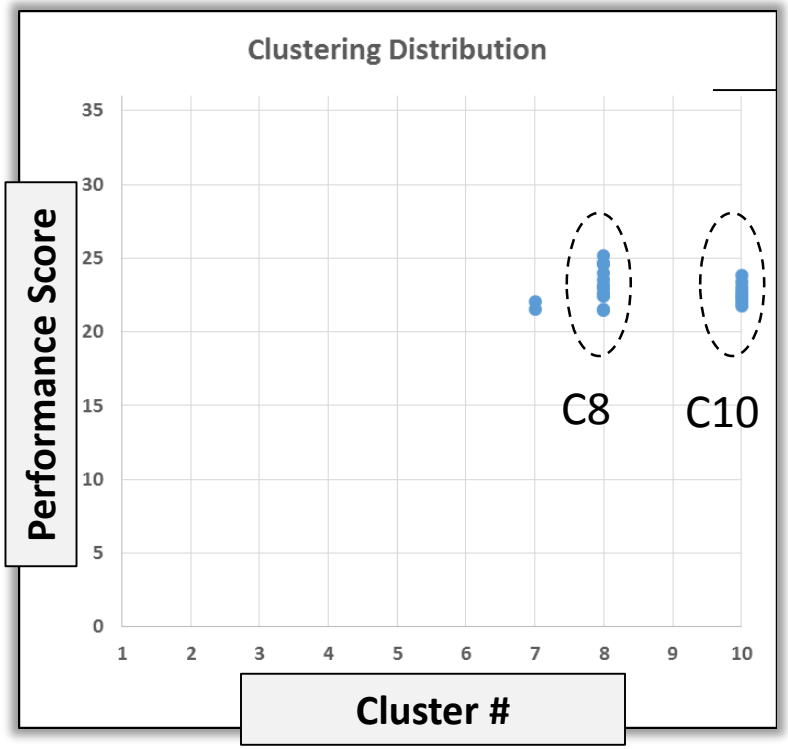
Clustered Performance and Cost Distribution



UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Analysis – Characterization





36: Highest Possible Score

Plot shows clustering results using 10 specified clusters for the 976 vehicles designs investigated

Showing 3 clusters in the top 25:

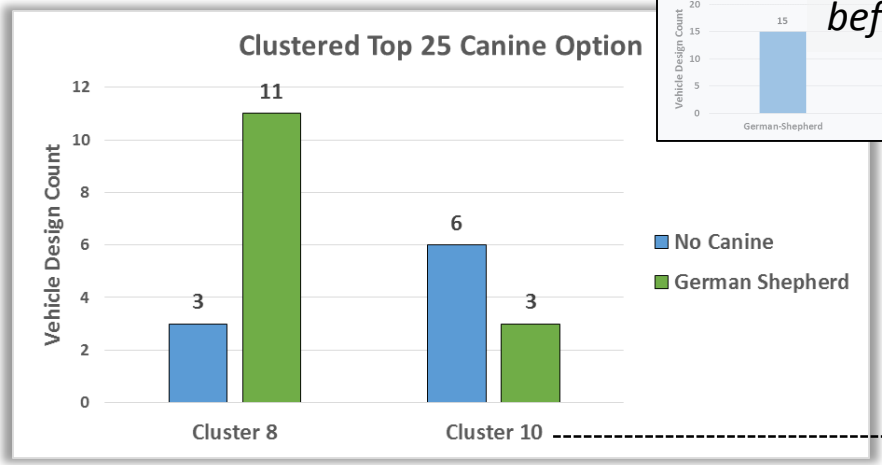
Cluster 7 (C7) : 2 designs

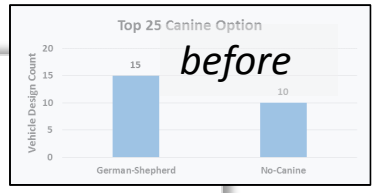
Cluster 8 (C8) : 14 designs

Cluster 10 (C10) : 9 designs

Clustering Characterization Comparison

- *Looking at the same two features as before…*



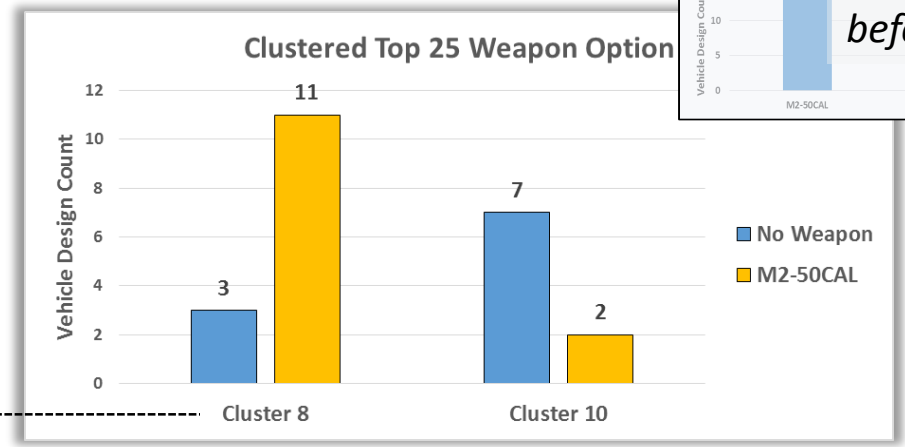


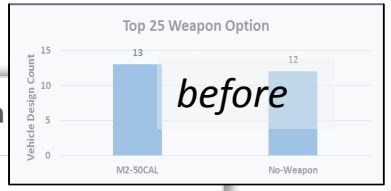
Cluster 10 Designs:

Mostly <u>do not</u> include a weapon or canine

Cluster 8 Designs:

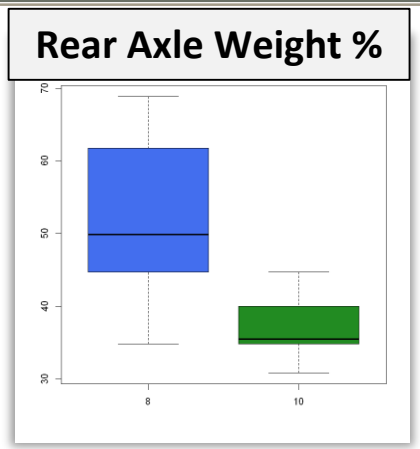
Mostly include weapon and canine

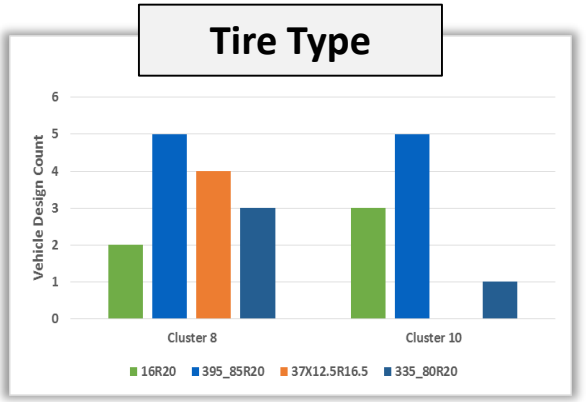


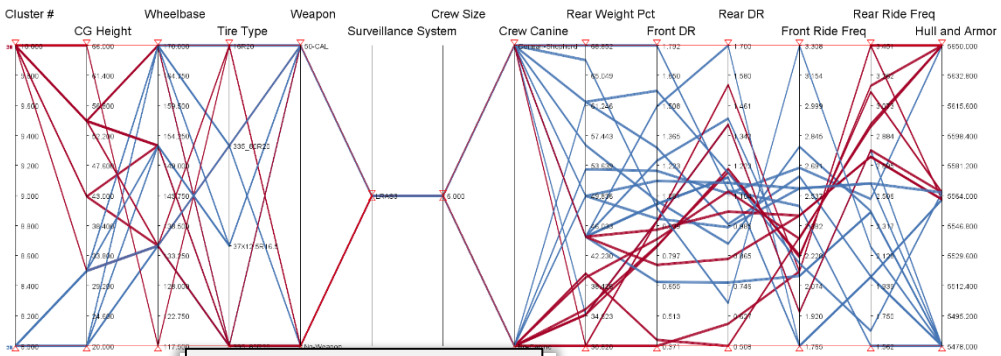


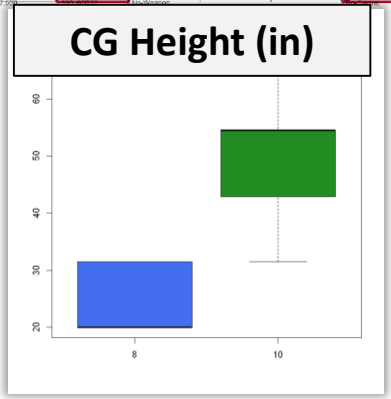
Clustering Characterization - Features

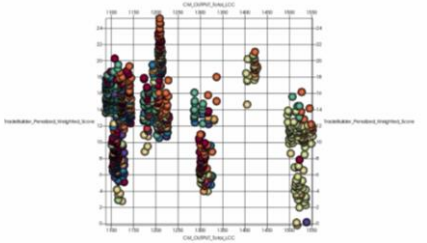
- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *design variables and characteristics*











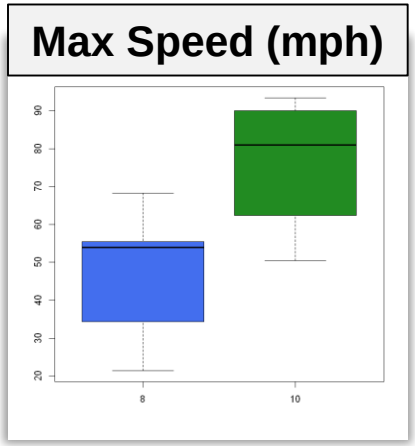
Clustering Characterization - Features

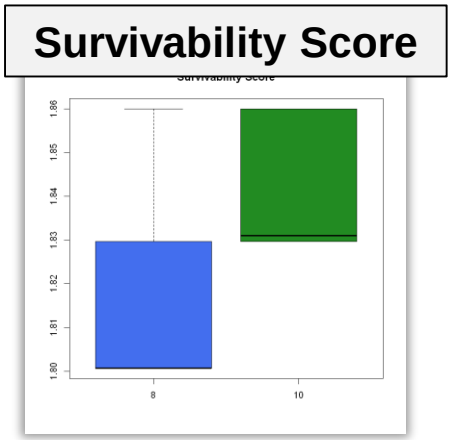
Feature	Cluster 8	Cluster 10
Weapon	Most designs include the M2-50 Cal	Most designs don't include a weapon
Canine	Most designs include a German Shepherd	Most designs don't include a canine
CG Height	Low	High
Wheelbase Length	Longer	Medium
Weight Distribution	More centered to rear heavy designs	More front heavy designs
Front Axle Ride Characteristics	Stiff, Mostly Overdamped	Less Stiff, Underdamped
Rear Axle Ride Characteristics	Stiff, Mostly Overdamped	Very Stiff, Mostly Overdamped

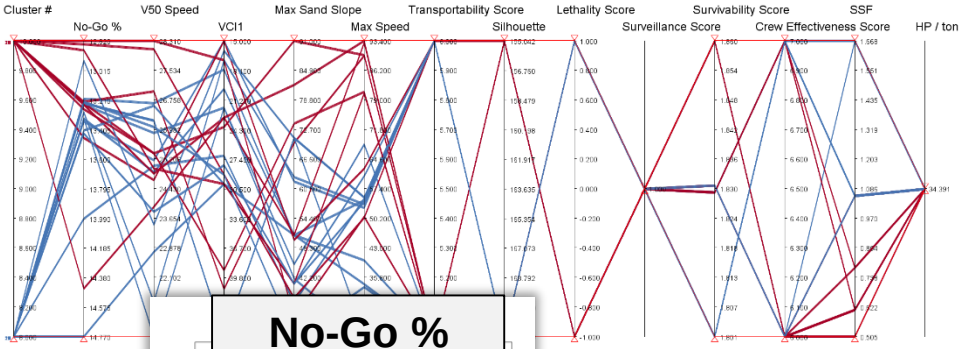
These clustered designs were **similar regarding the Tires, Hull and Armor Weight, Crew Size, and Surveillance System** features

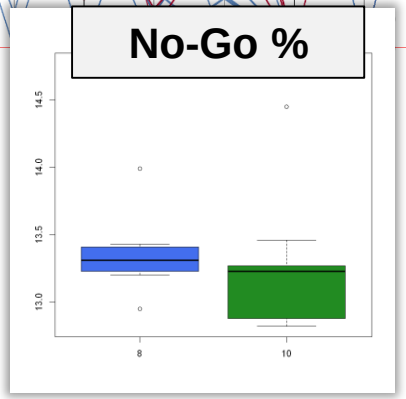
Clustering Characterization - Performance

- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *performance*









UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Characterization - Performance

Performance	Cluster 8	Cluster 10
Crew Effectiveness	Highest score	Meets requirements
Max Speed	Lower to moderate	Moderate to high
Max Sand Slope	Medium	Medium to high
SSF	High	Medium to low
Visibility (Silhouette)	Larger profile	Smaller profile
Lethality	Higher	Lower

These clustered designs were **similar regarding the Surveillance, No-Go %, VCI1, V50 Speed, HP / ton, Survivability, and Transportability** performance metrics

Clustered Characterization - Conclusions

- Highlighted two main clusters in the top 25 ranked vehicle designs and analyzed their features and performance
- Instead of describing one LRV design, now describing two LRV design variations in the top 25 – two designs that have some distinct differences, but with similar overall performance scores

Cluster 8

Well-rounded design concerning all of the areas of performance considered



Two potential variants

Cluster 10

Fast, mobile design, with smaller profile



Conclusions

New trade space exploration process *which utilized a* ***clustering technique*** *highlighted* ***two main vehicle variants*** *out of a set of top performing vehicle designs*

- Clustering is a promising trade space analysis process addition to help improve and further automate trade space characterization
- Can help answer important questions about a trade space
- And lead to improved optimal design extraction from trade spaces, and overall improved concept design development
- More to look into : clustering technique tuning and feature selection

Acknowledgments: ERS, CREATE-GV, ECO

US Army TARDEC

- Stuart Parkhurst
- Jacob Woten
- Stephanie Loewen
- Joe Raymond
- Scott Shurin
- Ian Stranaly
- Tom Skorupa
- Gary Bronstetter
- MAJ Roy
- COL Vanyo
- …

US Army ERDC

- Alex Baylot
- Owen Eslinger
- Justin Foster
- Willie Brown
- Daniel Chaussé
- Jody Priddy
- Chris Goodin
- Jessica Johnson
- Glover George
- Timothy Garton
- …

Thank you!

Implementation of Clustering Analysis in Engineered Resilient Systems Tools for Enhanced Trade Space Exploration of Military Ground Vehicles

Mr. Andy Pokoyoway*, Dr. Matt Castanier
US Army Tank Automotive Research, Development, and Engineering Center (TARDEC)

Abstract ID: 19712 *** Lead author contact info:** 586-282-3765 <andrew.p.pokoyoway.civ@mail.mil>

NDIA Systems Engineering Conference
Springfield, VA 26 OCT 2017

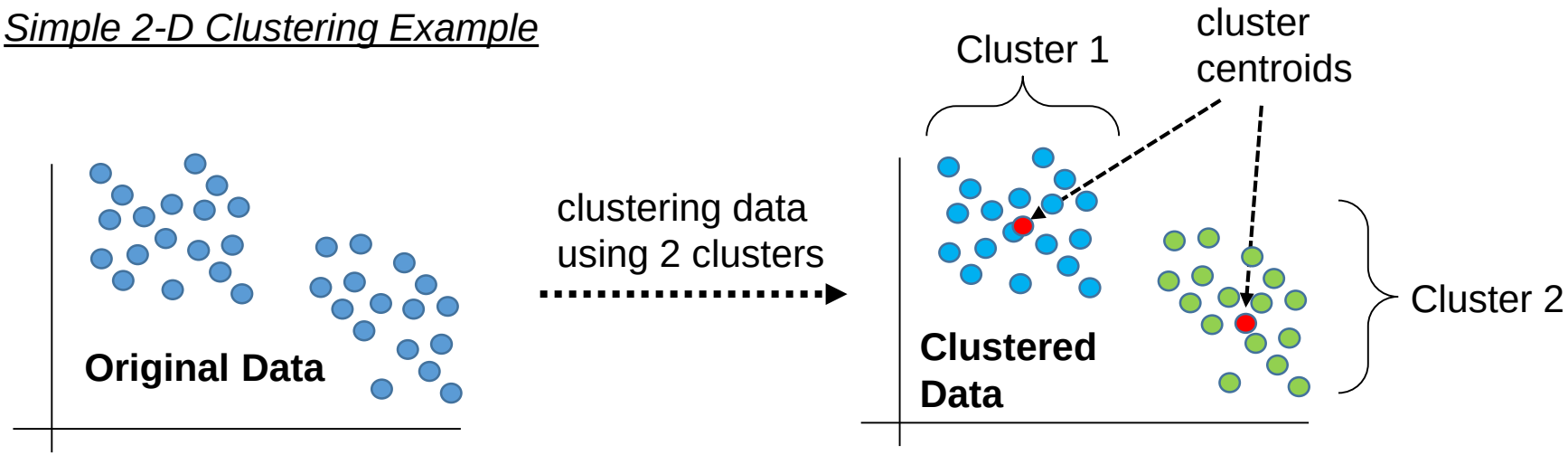
Background and Motivation

- Performing multidisciplinary design optimization of a military ground vehicle is extremely challenging
- One challenge is related to analyzing large, highly dimensional vehicle design datasets
- Analysis questions to answer regarding these datasets:
  - Do my highest-ranked designs reside in multiple regions of the trade space?
  - How many promising regions are there?
  - Does each region represent variations on a single design concept or multiple design concepts?
  - How can I best characterize the unique features of each design concept?

Clustering

- Simply put, clustering is the process of assigning data points to groups based on how closely their values are to a common group centroid
- A way to group data that is highly dimensional
- Different algorithms available
- Machine learning technique

Simple 2-D Clustering Example



Clustering for Trade Space Design Populations

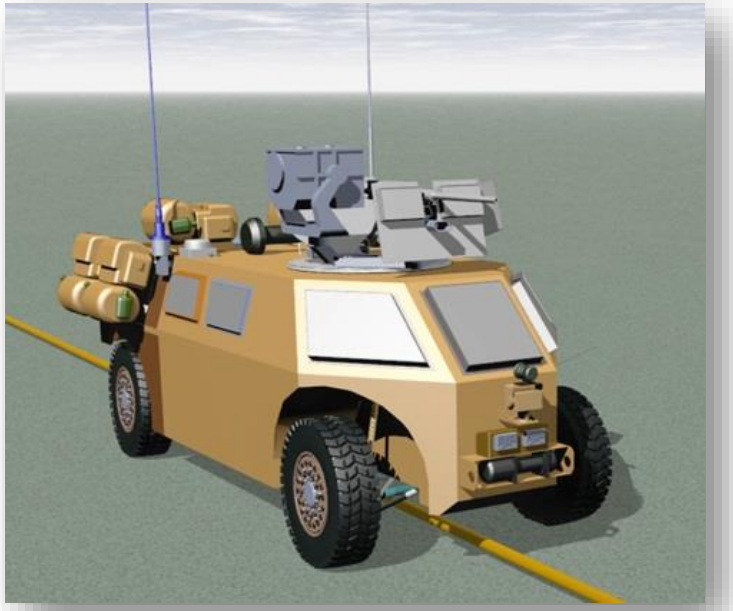
- Reduce large, highly dimensional datasets to more manageable, digestible sizes. This can make it easier to draw conclusions

- Automated way of quantifying and qualifying design differences - ***characterizing***; may help answer the question of : "How different are the top ranked vehicle designs?"

- Clusters could be used to provide promising vehicle design groups, and therefore promising characteristics, to be taken to the next stage of vehicle development

Objectives

- Learn, evaluate, and provide feedback to developers of **CREATE-GV and ERS Tools**
- Apply these tools to the **LRV notional concept vehicle** to perform **trade space exploration**
- Develop new trade space exploration methods for ground vehicles



CREATE-GV: Computational Research and Engineering Acquisition Tools and Environments – Ground Vehicles

ERS: Engineered Resilient Systems

LRV: Light Reconnaissance Vehicle

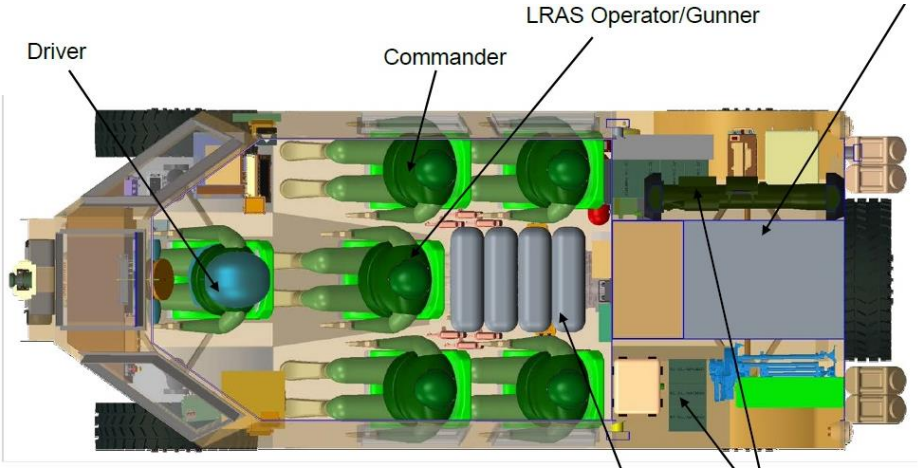
UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

LRV – A Notional Concept for a New-Start Vehicle

Notional concept was initially developed based on these requirements:

- Crew of 6
- Power for 96-hour mission
- Silent watch, silent move
- Advanced reconnaissance & surveillance equipment package
- CH-47 internal transport and sling-load transport





Trade Space Exploration Process

Reviewed initial concept & requirements

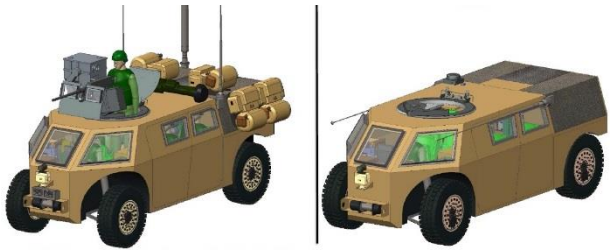
Performed analysis to build trade space

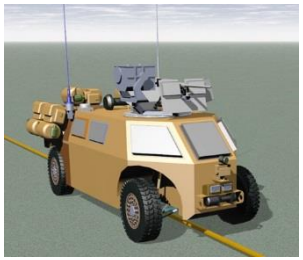
Revisited concept & varied requirements

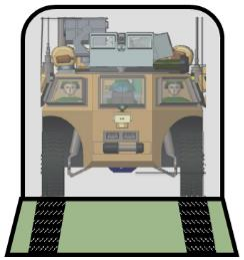
Performed analysis to expand trade space

Generated new design set = new concept

Iterative Concept-Analysis Loop











ENGINEERED RESILIENT SYSTEMS

Trade Space Exploration Process

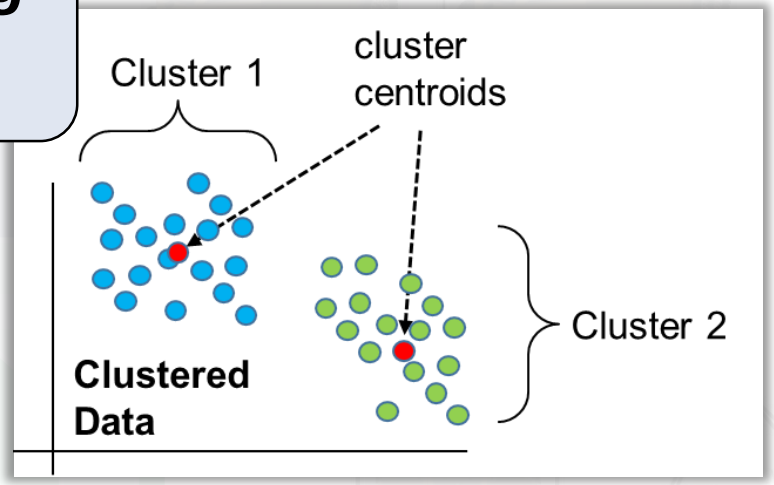
Reviewed initial concept & requirements

Performed analysis to build trade space

Revisited concept & varied requirements

Iterative Concept-Analysis Loop

Clustering Analysis



Performed analysis to expand trade space

Generated new design set = new concept

UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Trade Space Construction in ERS TradeBuilder

CREATE-GV	
1	On-Road Speed
2	Off-Road Speed
3	Max Sandy Grade
4	Off-Road No-Go %
5	Soft-soil mobility

ERS TradeBuilder	
1	Surveillance
2	Crew
3	Stability
4	Silhouette
5	Power density
6	Survivability
7	Transportability
8	Lethality

Performance Metrics imported from result files

Performance Metrics evaluated in ERS TradeBuilder

Design Variables

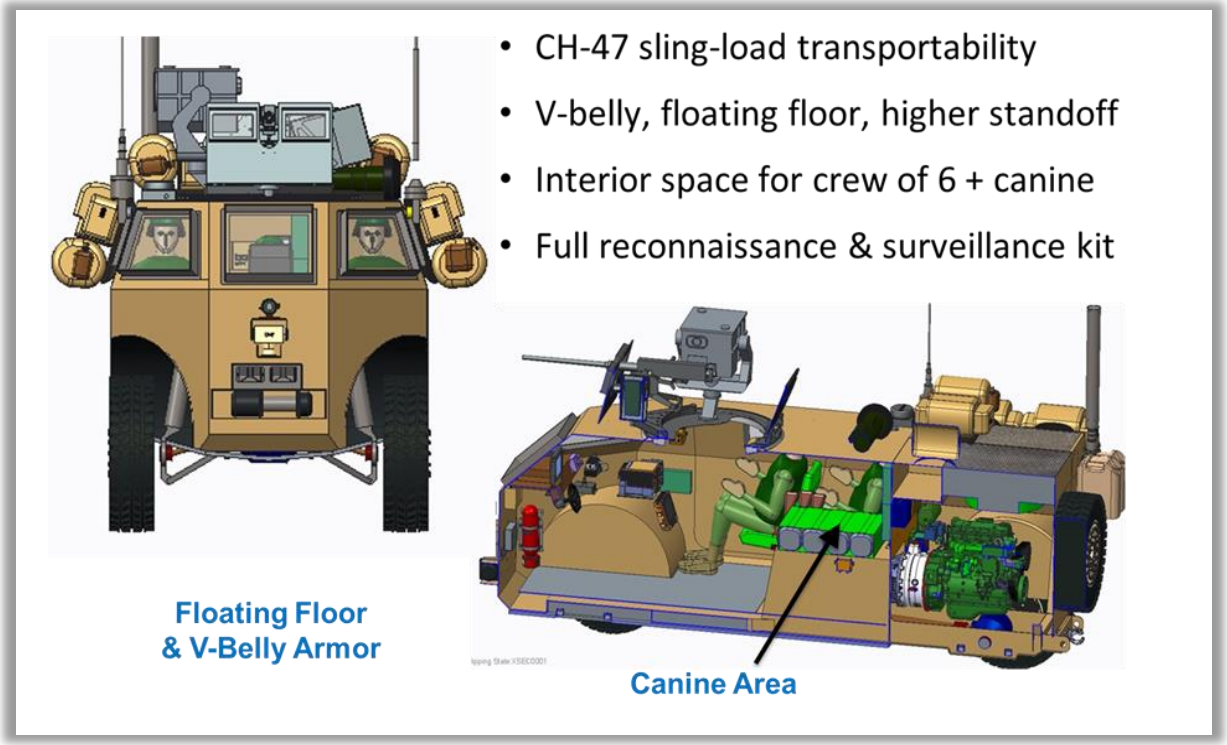
#	H	L	W	…											
1	H_1	L_1	W_1												
2	H_2	L_2	W_2												
3	H_3	L_3	W_3												
4	H_4	L_4	W_4												

Designs

UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Trade Space Vehicle Design Characterization

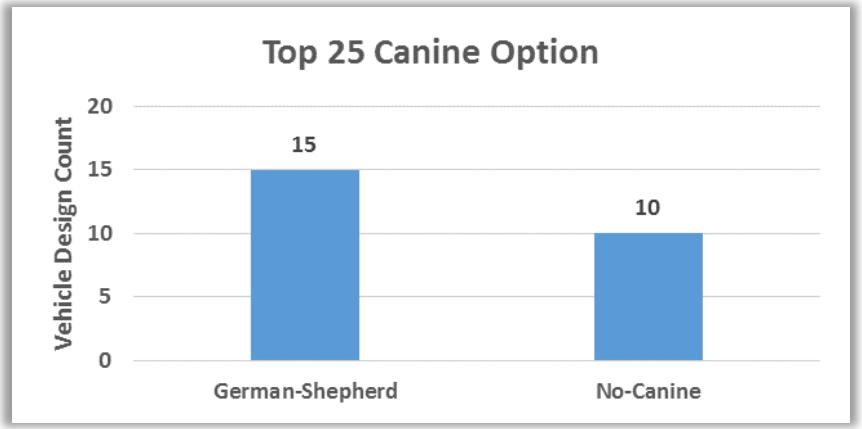
- Common features from highest-ranked designs:

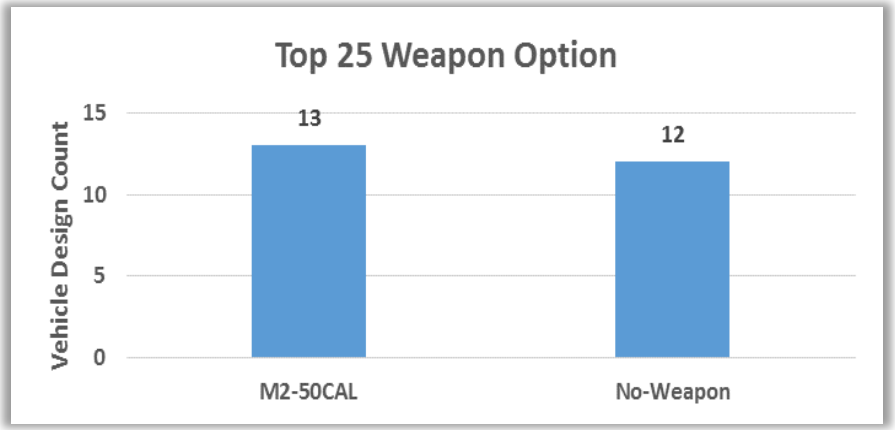


These are general features typically seen in the top 25 ranked vehicles, **though not all of the top 25 designs had the same features**

Trade Space Vehicle Design Characterization

- Two areas where differences are seen in the top 25 designs :



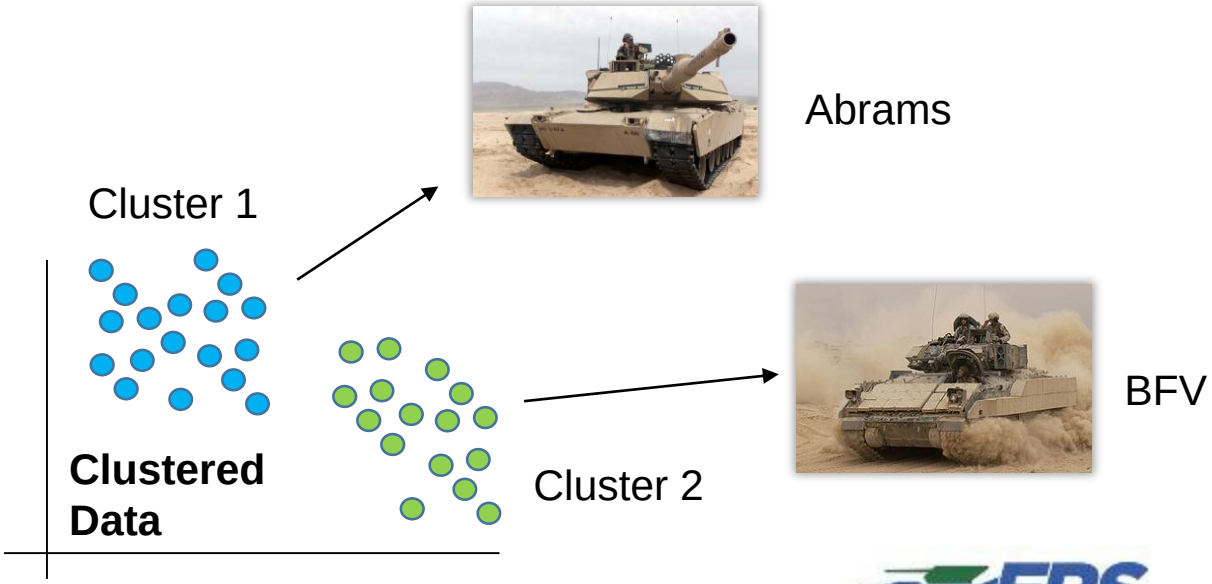


- Characterizing the top ranking designs as a whole may not lead to as useful conclusions regarding which features a single vehicle design should have
- We could be **unintentionally characterizing multiple vehicle designs, multiple variants**, *a potential outcome when performing multi-objective design optimization*

Trade Space Vehicle Design Characterization

- Early in the concept development phase, the trade space is large, with a design space that could be spanning regions consisting of two or more completely different vehicle designs
- … and this is not apparent
- We want to understand if potential regions exist early on in the analysis process to understand what unique concepts we may have

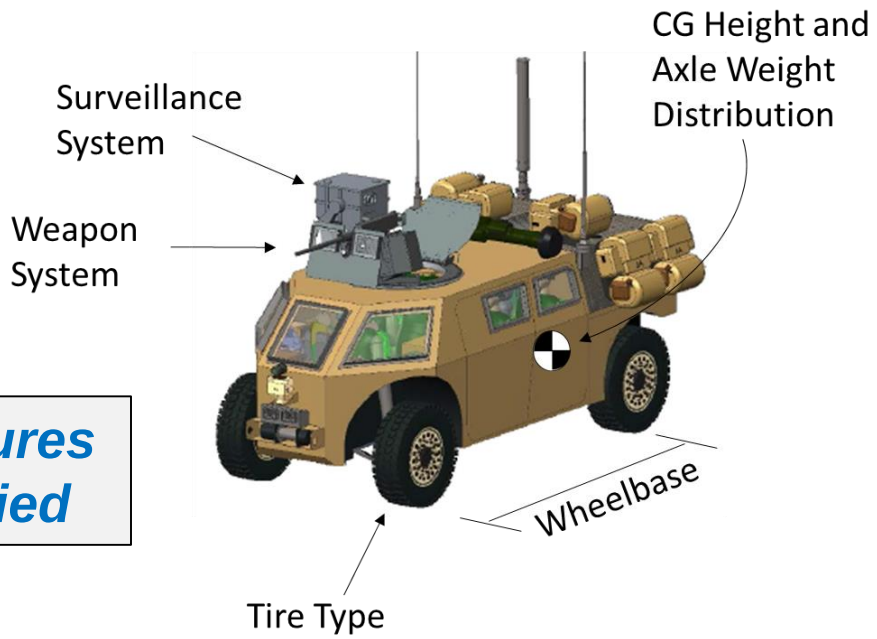
Potential example outcome of early concept, highly dimensional, multi-object design optimization



UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Analysis - Setup

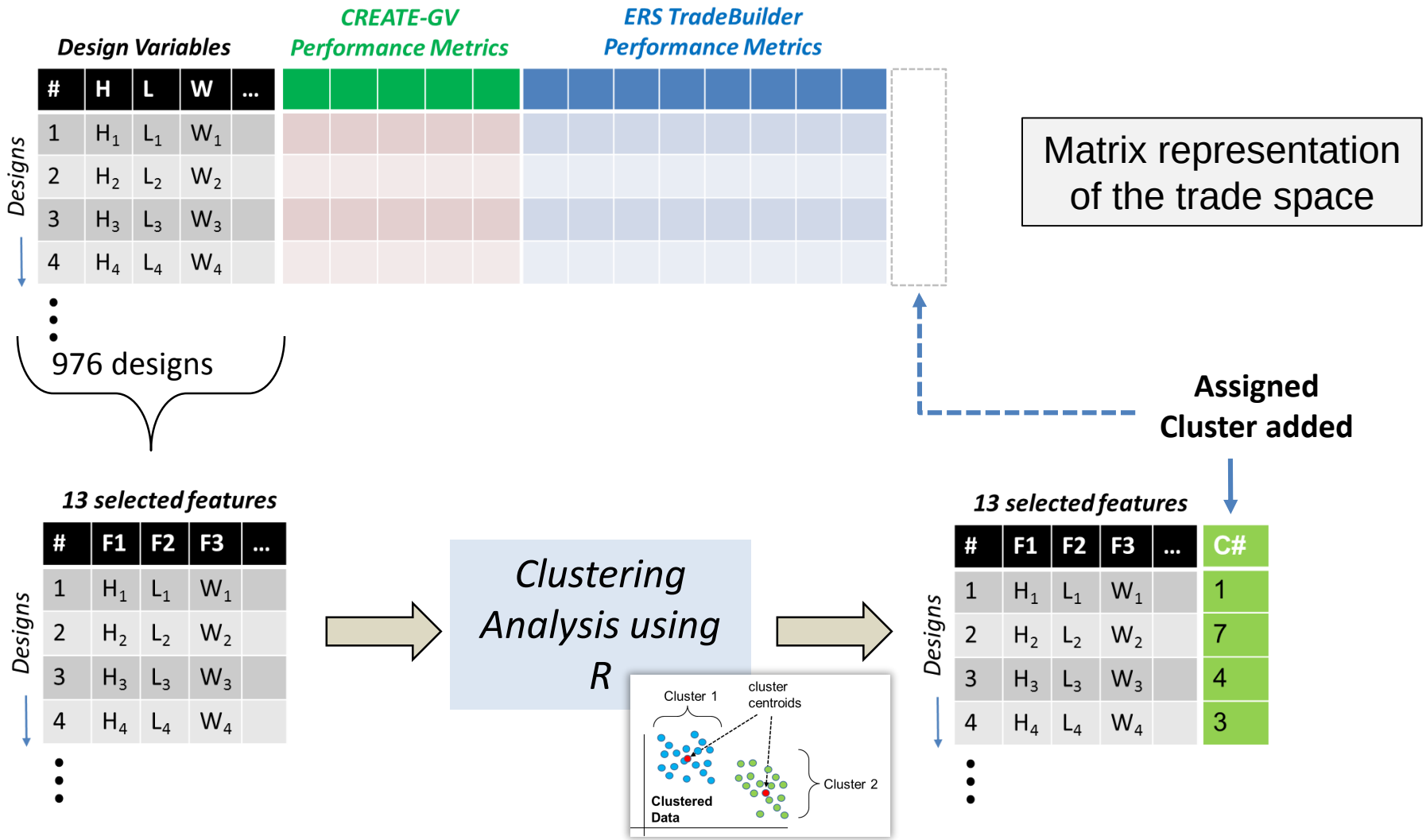
- **K-means clustering** algorithm used within R ("Hartigan-Wong" version)
- **Chose to generate 10 clusters** based on the "within sum of squares (WSS)" count selection method
- Design variables and characteristics chosen for features:



13 features specified

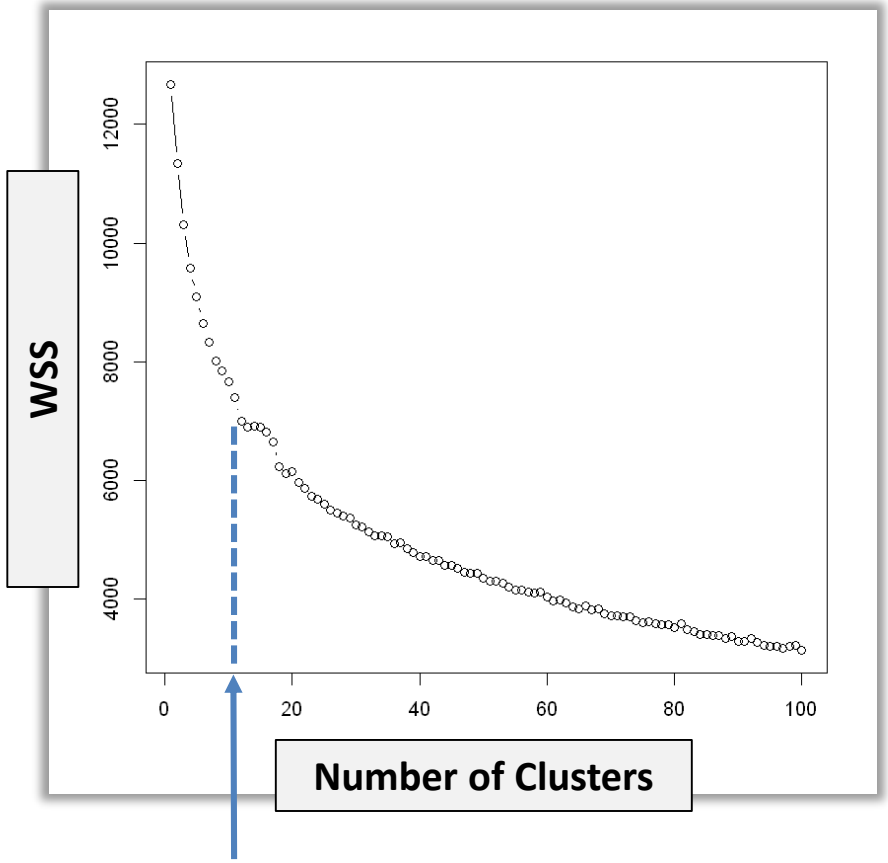
- Suspension characteristics (damping ratio and ride frequency) for the front and rear axles
- Canine
- Crew size
- Armor weight

Clustering Analysis - Setup



Clustering Analysis – Selecting Cluster Count

- Within Sum of Squares cluster count selection method (WSS)

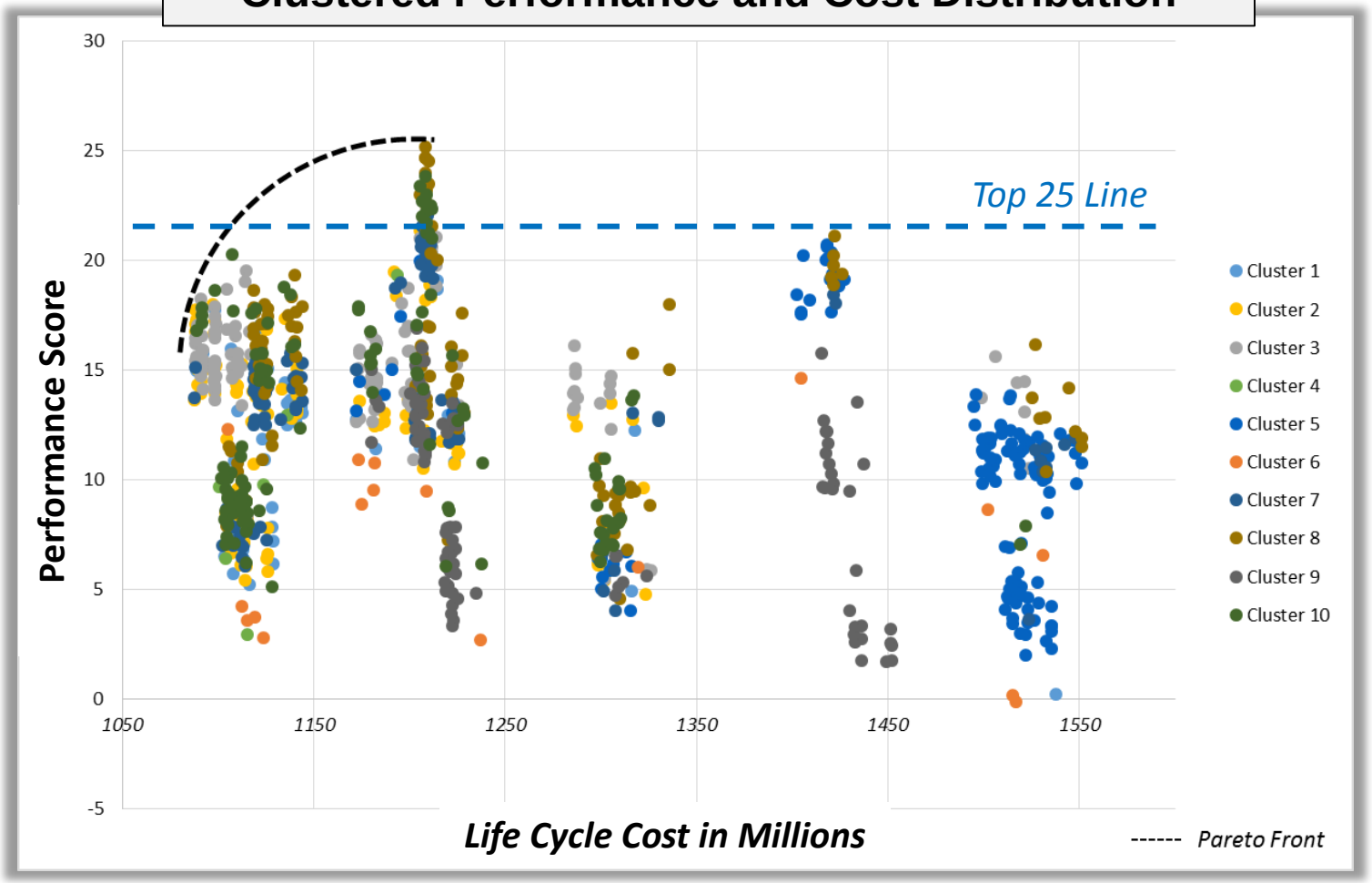


… at 976 clusters, the sum of squares value would equal 0

10 Clusters

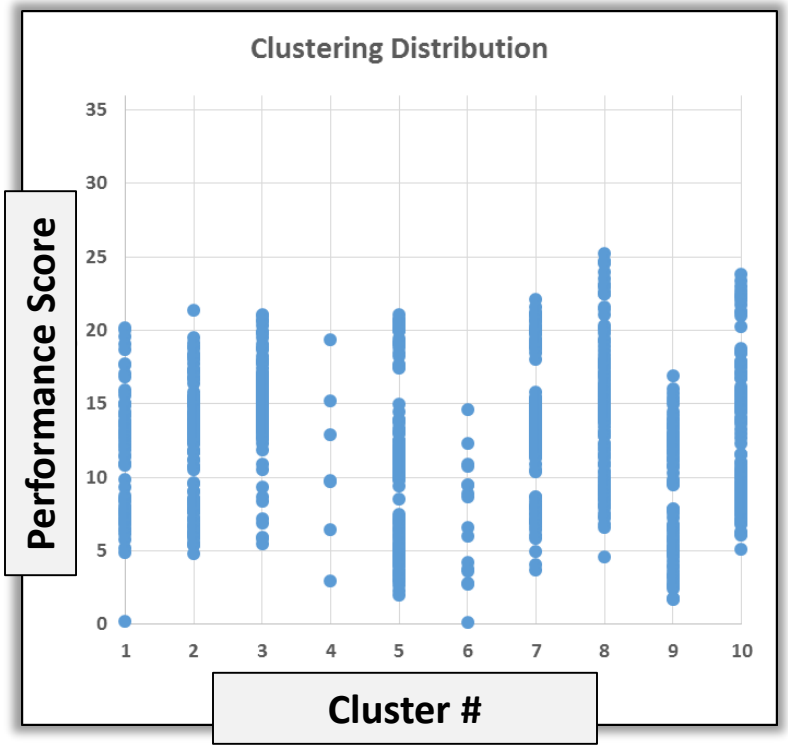
Clustering Analysis – Results

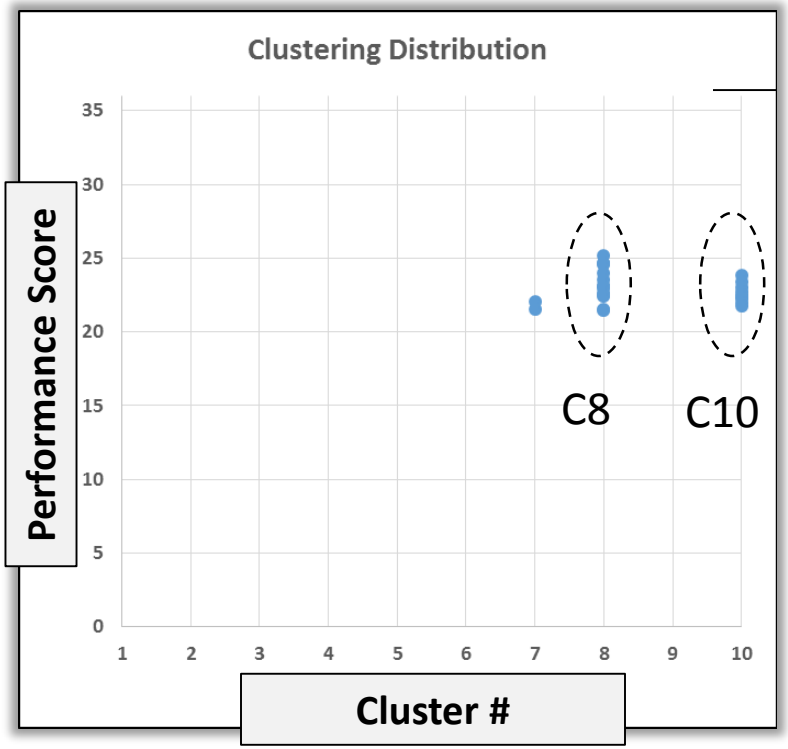
Clustered Performance and Cost Distribution



UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Analysis – Characterization





36: Highest Possible Score

Plot shows clustering results using 10 specified clusters for the 976 vehicles designs investigated

Showing 3 clusters in the top 25:

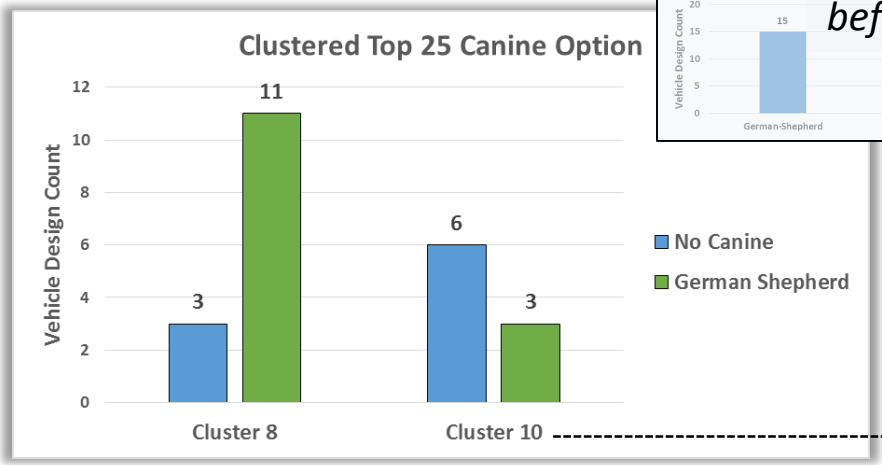
Cluster 7 (C7) : 2 designs

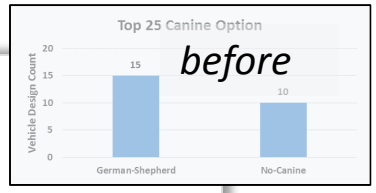
Cluster 8 (C8) : 14 designs

Cluster 10 (C10) : 9 designs

Clustering Characterization Comparison

- *Looking at the same two features as before…*



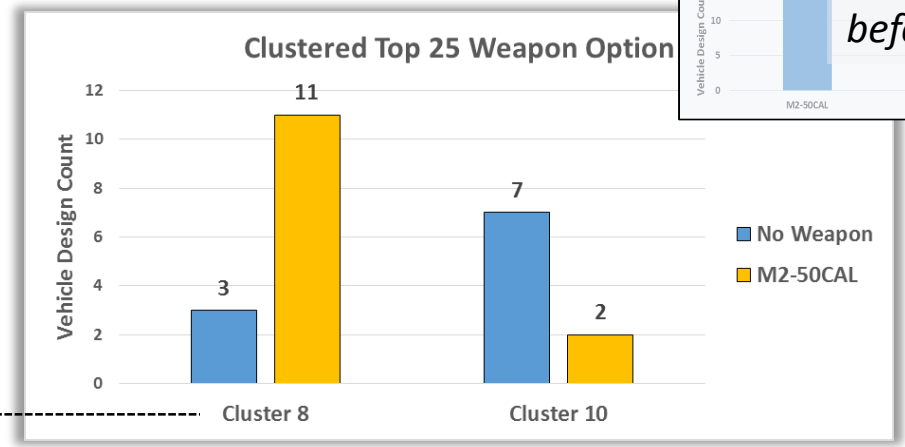


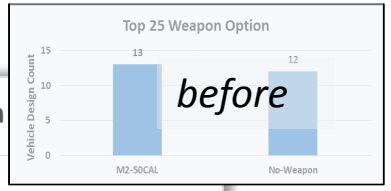
Cluster 10 Designs:

Mostly <u>do not</u> include a weapon or canine

Cluster 8 Designs:

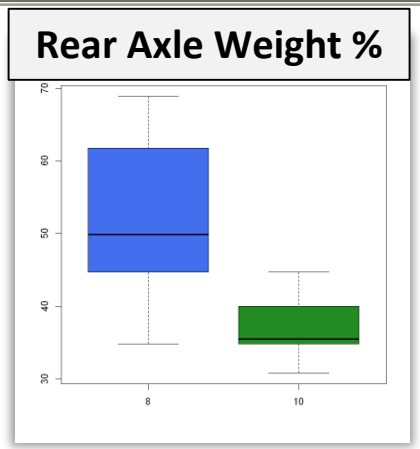
Mostly include weapon and canine

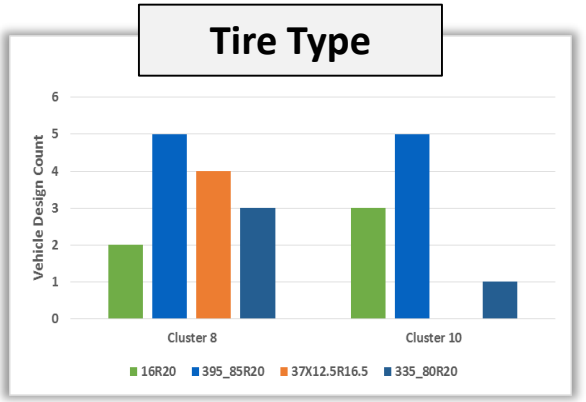


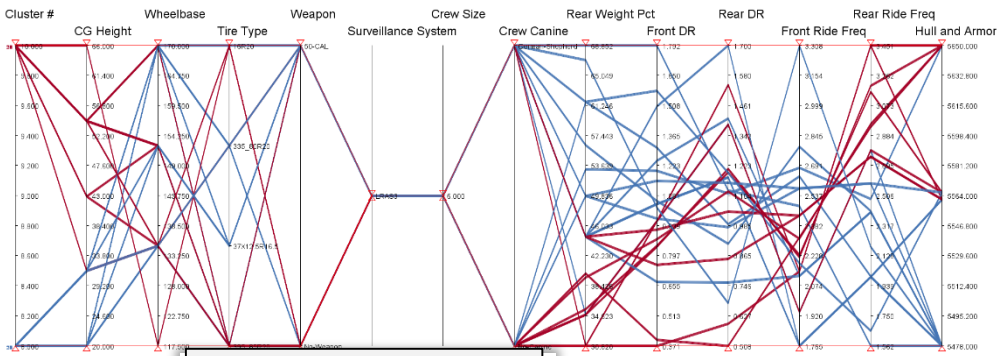


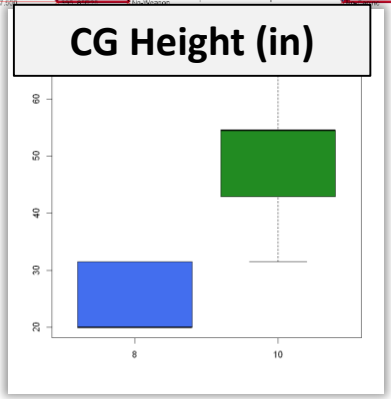
Clustering Characterization - Features

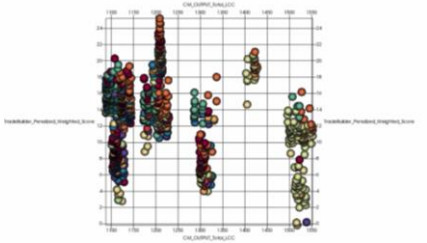
- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *design variables and characteristics*











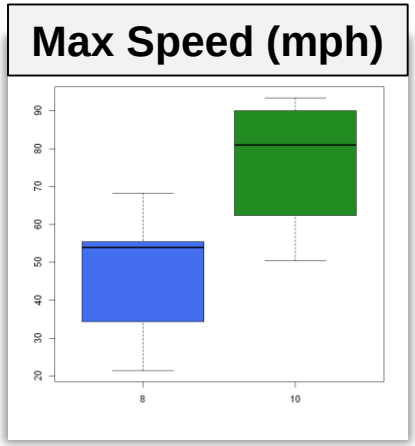
Clustering Characterization - Features

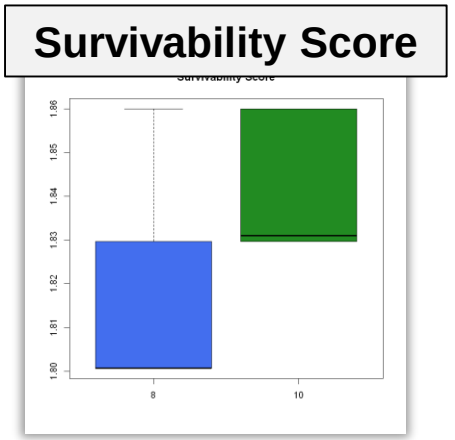
Feature	Cluster 8	Cluster 10
Weapon	Most designs include the M2-50 Cal	Most designs don't include a weapon
Canine	Most designs include a German Shepherd	Most designs don't include a canine
CG Height	Low	High
Wheelbase Length	Longer	Medium
Weight Distribution	More centered to rear heavy designs	More front heavy designs
Front Axle Ride Characteristics	Stiff, Mostly Overdamped	Less Stiff, Underdamped
Rear Axle Ride Characteristics	Stiff, Mostly Overdamped	Very Stiff, Mostly Overdamped

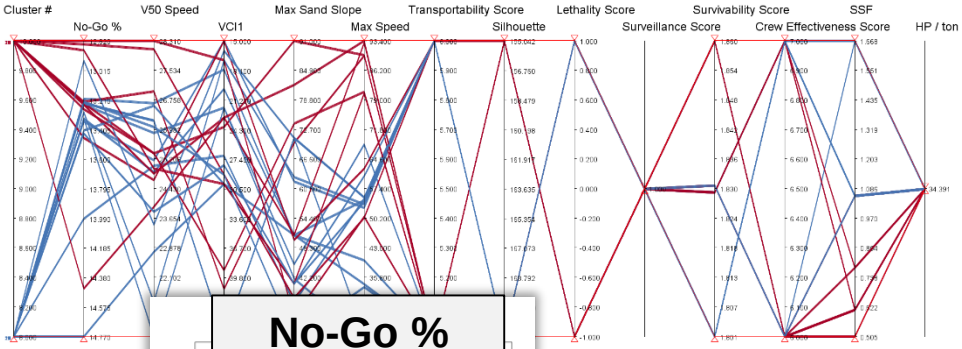
These clustered designs were **similar regarding the Tires, Hull and Armor Weight, Crew Size, and Surveillance System** features

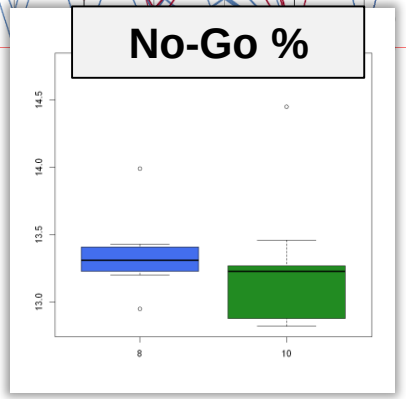
Clustering Characterization - Performance

- Various visualizations used to distinguish the differences between the top 25 designs within **clusters 8** and **10** concerning their *performance*









UNCLASSIFIED: Distribution A. Approved for public release; distribution is unlimited

Clustering Characterization - Performance

Performance	Cluster 8	Cluster 10
Crew Effectiveness	Highest score	Meets requirements
Max Speed	Lower to moderate	Moderate to high
Max Sand Slope	Medium	Medium to high
SSF	High	Medium to low
Visibility (Silhouette)	Larger profile	Smaller profile
Lethality	Higher	Lower

These clustered designs were **similar regarding the Surveillance, No-Go %, VCI1, V50 Speed, HP / ton, Survivability, and Transportability** performance metrics

Clustered Characterization - Conclusions

- Highlighted two main clusters in the top 25 ranked vehicle designs and analyzed their features and performance
- Instead of describing one LRV design, now describing two LRV design variations in the top 25 – two designs that have some distinct differences, but with similar overall performance scores

Cluster 8

Well-rounded design concerning all of the areas of performance considered



Two potential variants

Cluster 10

Fast, mobile design, with smaller profile



Conclusions

New trade space exploration process *which utilized a* ***clustering technique*** *highlighted* ***two main vehicle variants*** *out of a set of top performing vehicle designs*

- Clustering is a promising trade space analysis process addition to help improve and further automate trade space characterization
- Can help answer important questions about a trade space
- And lead to improved optimal design extraction from trade spaces, and overall improved concept design development
- More to look into : clustering technique tuning and feature selection

Acknowledgments: ERS, CREATE-GV, ECO

US Army TARDEC

- Stuart Parkhurst
- Jacob Woten
- Stephanie Loewen
- Joe Raymond
- Scott Shurin
- Ian Stranaly
- Tom Skorupa
- Gary Bronstetter
- MAJ Roy
- COL Vanyo
- …

US Army ERDC

- Alex Baylot
- Owen Eslinger
- Justin Foster
- Willie Brown
- Daniel Chaussé
- Jody Priddy
- Chris Goodin
- Jessica Johnson
- Glover George
- Timothy Garton
- …

Thank you!



Tradespace: Informed Decision-making for Acquisition

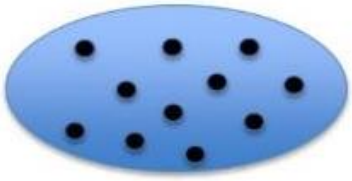
20th Annual NDIA Systems Engineering Conference
October 26, 2017

Timothy Garton
Computer Scientist
US Army Corps of Engineers
Engineer Research Development Center

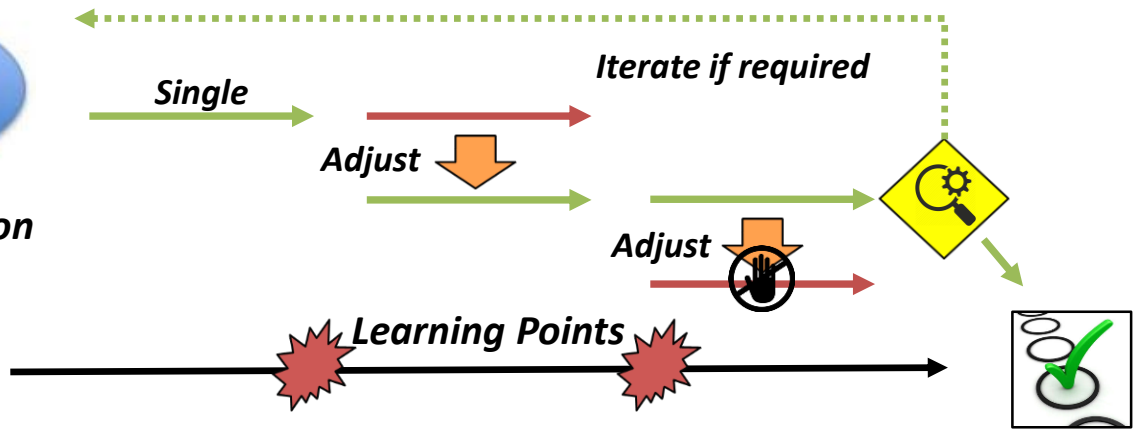
Tradespace Analytics - Set-Based Design

Tradespace - the set of processes, program and system parameters, attributes, and characteristics required to satisfy mission profile

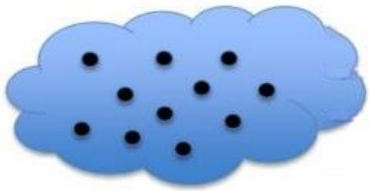
POINT-BASED DESIGN



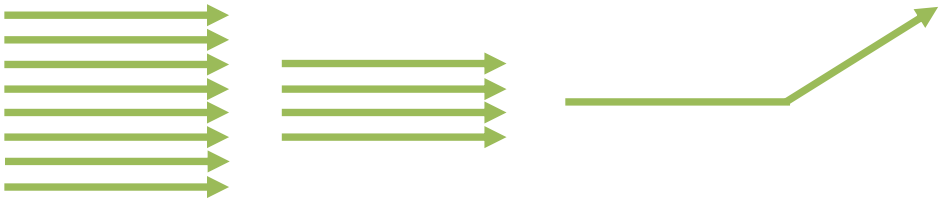
Potential Solution Space



SET-BASED DESIGN



The space spanned by completely enumerated design variables



Advanced analytics allow engineers to investigate more thorough design solutions sets

ERS Tradespace Concept

- Architecture
- Tradespace Analytics
- Advanced Modeling
- Environmental Rep.
- Mission Context

Cost models
-ilities
….other

ERS CLOUD COMPUTING ENVIRONMENT (CCE)

10,000x *Improvement in productivity in Analysis of Alternatives*



Efficiently discover key performance parameters (KPPs)

HPCMP and S&T Resources

Currently Applied ERS Advanced Tradespace Analytics

DEFINE



- Early concept tool
- Functional / component breakdown
- Explore tradespace edges

Expand Tradespace Fully



Performance Assessments
Performance Metrics

High-fidelity Models
Parameter Sweeps:
Design Variations



ANALYZE

- Highly computational
- Sifts through millions of designs
- Refined set of specifications for viable design solutions

Tradespace Exploration Processes

physics-based models analyze new designs

known designs are used in formulating the tradespace

Seeding

High-Fidelity Simulations

Historical Data

evaluated in various performance scenarios

Performance Modeling

analyzed from a systems perspective

Systems Properties "ilities"

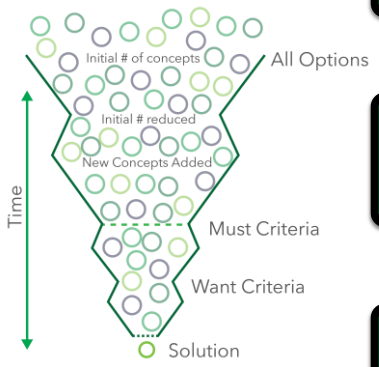
assessed in the context of possible operational missions

Mission Modeling

Tradespace Creation *"Define"*



Tradespace Analysis *"Partition"*



Exclusion

Selection

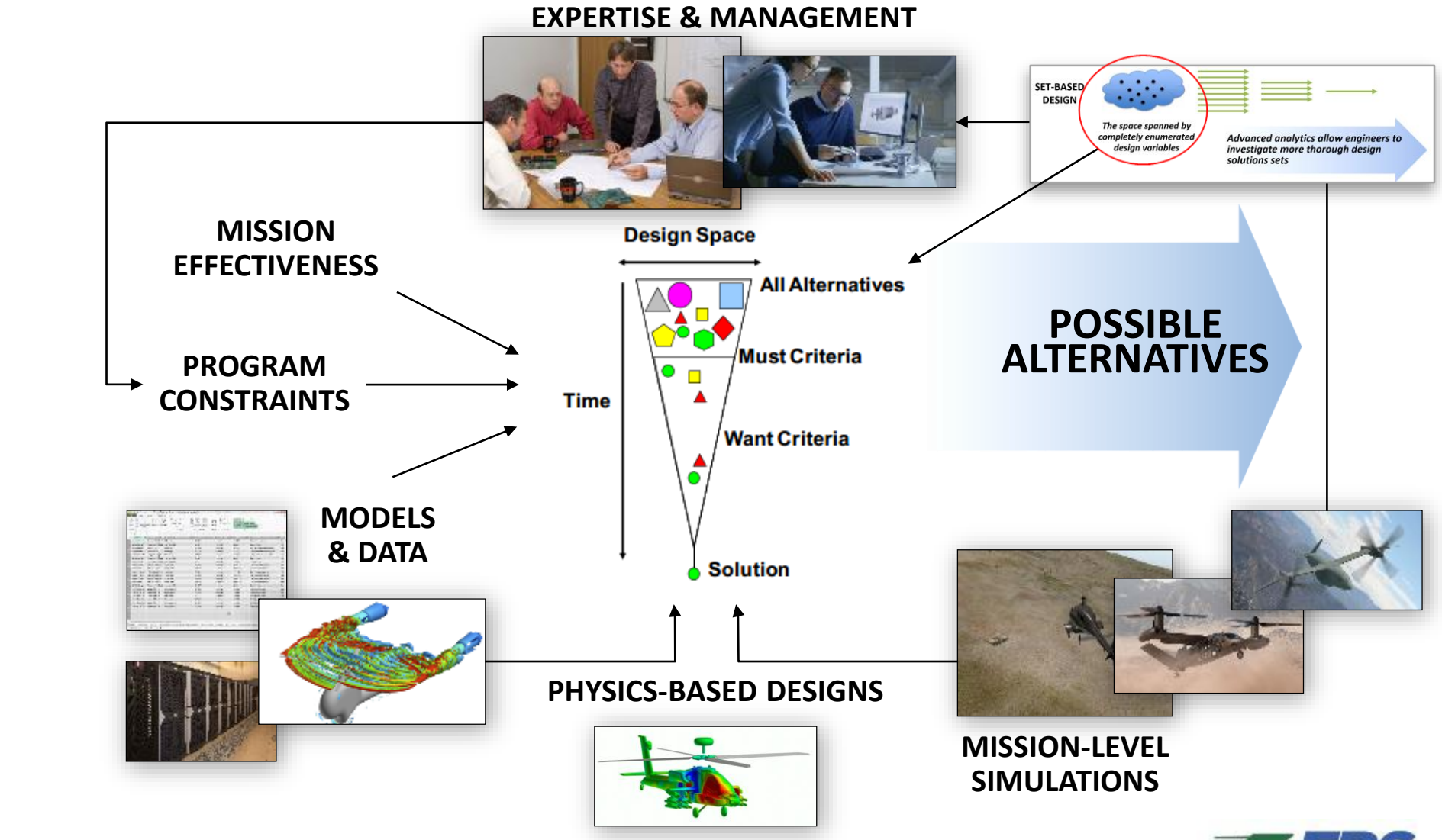
Comparison

Tradespace is gradually narrowed

Globally optimum solutions are revealed

Remaining designs are compared and contrasted

Decision Analysis: Integrated Processes with Trade Analytics



Technical Requirements of Data-Driven Decisions Tools



Trace Requirements and link systems to output



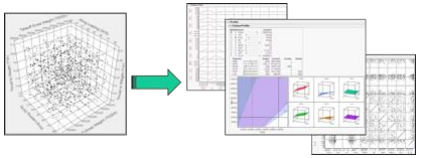
Visualize trades between dominant variables and requirements



Allow novice and advanced data exploration



Quickly find dominant variables



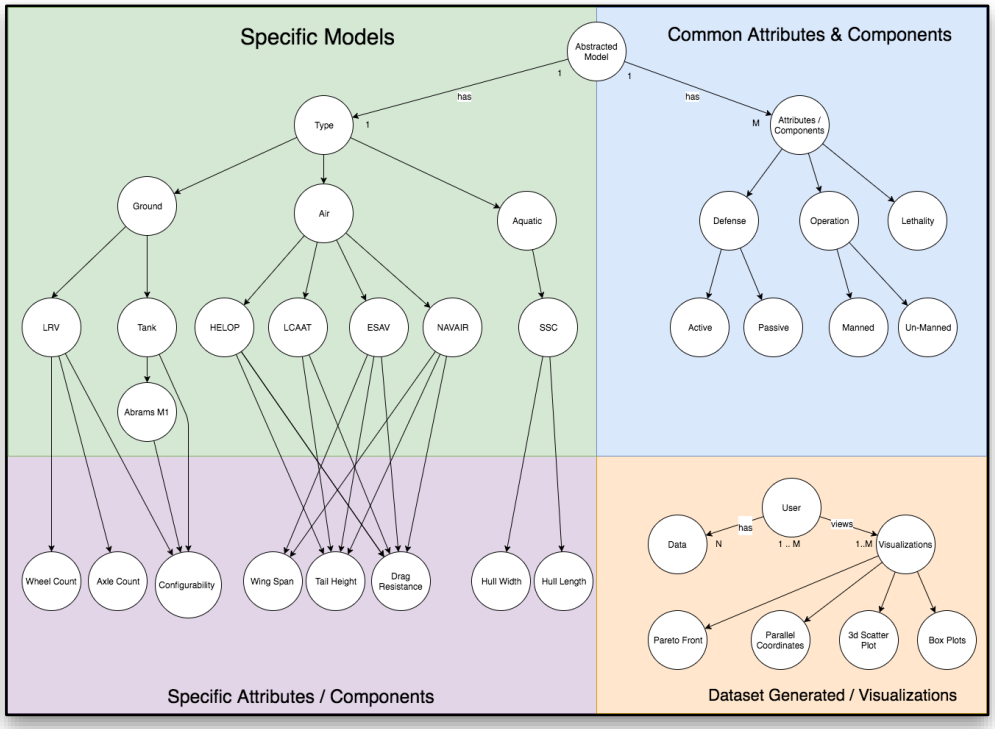
Tradespace tools must:

- Have a traceable history
- Utilize cutting edge search and decision analytics

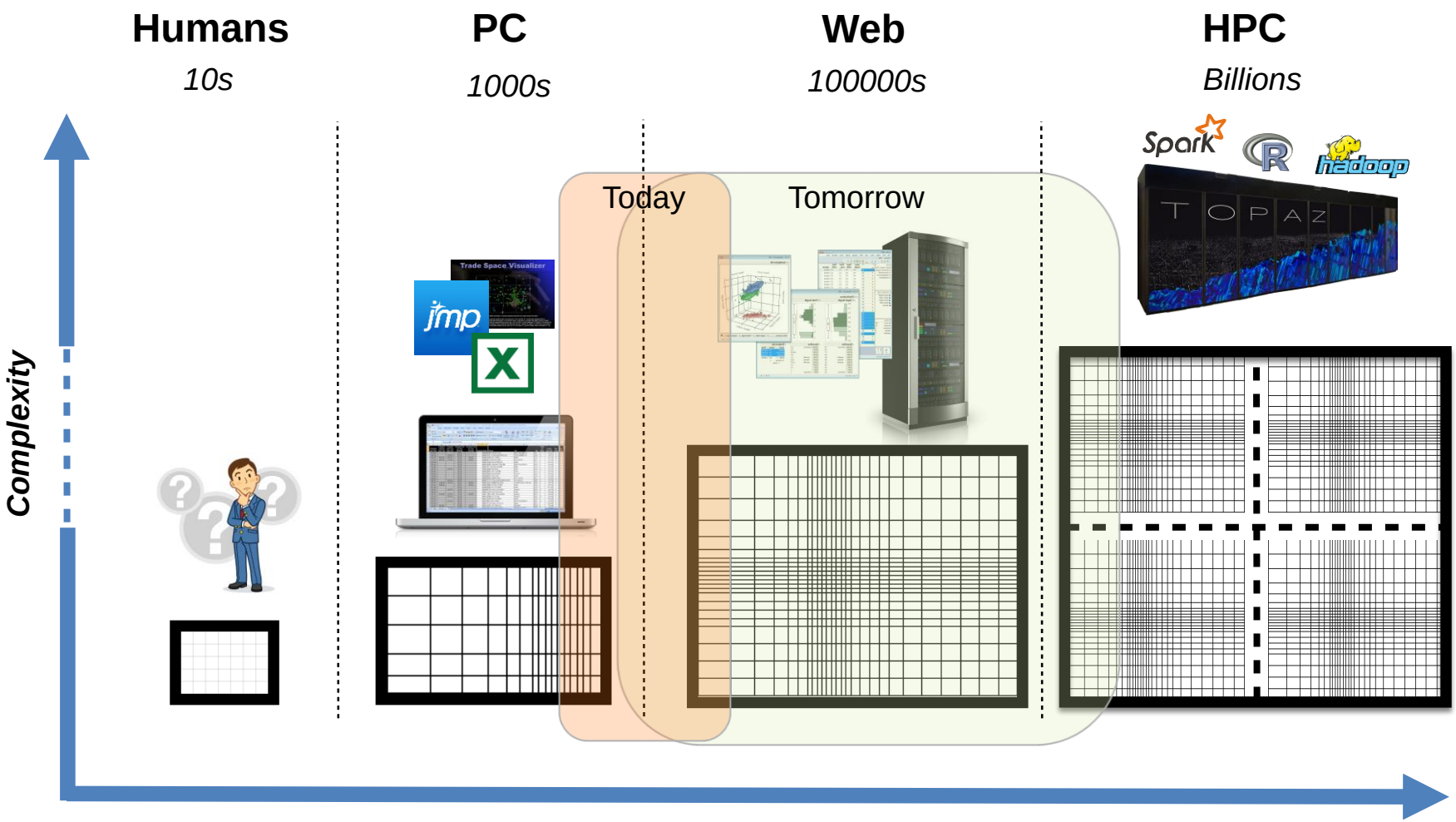
Ontology Models: Consistency in System Communication

Original system breakdowns by ontologies or SysML, along with requirements, are tied to the tradespace

- **Inserts greater accuracy and verification into the analytic processes**
- **Passing the metadata gives us insight into how to analyze the data**
- ***Direct mapping via SysML → WBS → MILSTD-881C (soon 881D) is an OSD-CAPE requirement***



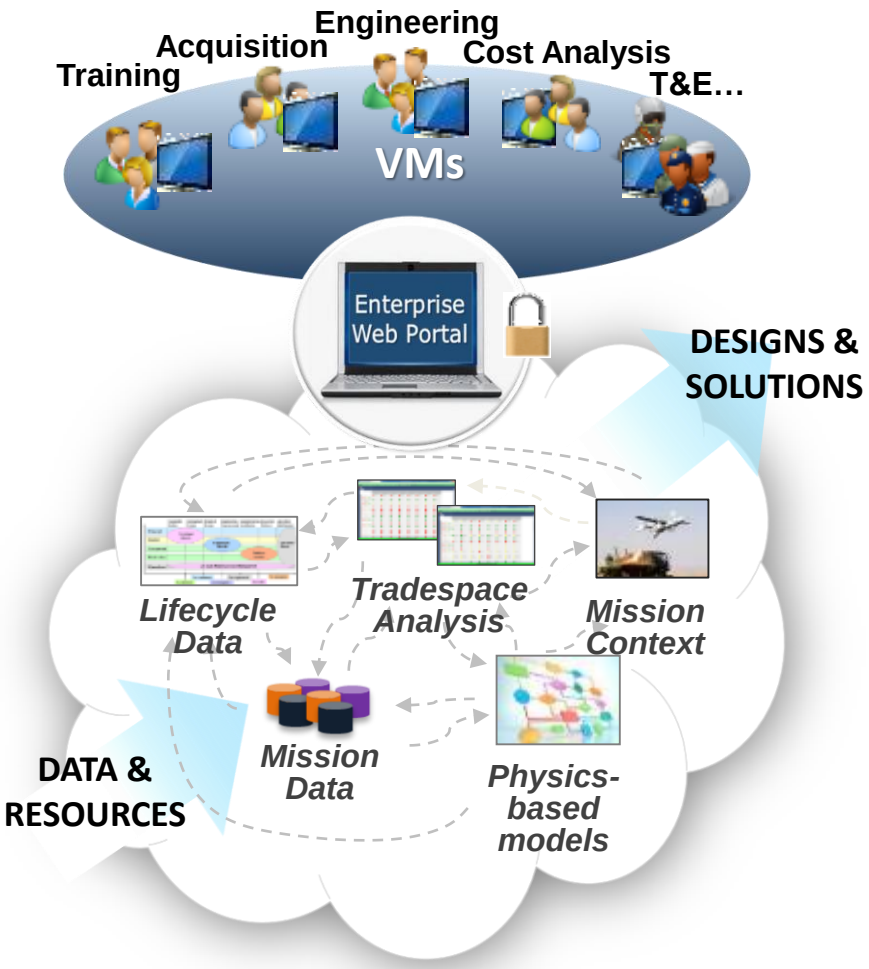
Data Metrics



Tradespace Analytics – Data Analysis and Visualization Tool

Beta-Release Status:

- **Supplied acquisition community a web-based environment for storing, visualizing and analyzing data**
- **Allowed for access and annotation by multiple parties for any given location;**
- **Provided the base for a collaborative decision support environment.**
  - Gaps in previous environments forced point-based design methodology.
- **Successfully supported MBSE and data filtering**
  - Previously available MBSE were expensive and resource heavy – requiring local resources and administrative personnel, required expensive licensing agreements.



Tradespace Analytics Beta Release Lessons Learned

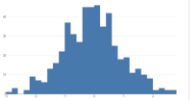
The FY17 Beta Release of TradeAnalyzer to a number of DoD Users resulted in important lessons and changes

- **Use of ParaView Web - generating interactive visualizations of large data-sets and annotation capabilities**
- **Role Based Access Control (RBAC) needed to execute R-Scripts in a secured environment; implementation in a complex collaborative environment is challenging.**
- **Working on secure authentication mechanisms that couple with customers local access control policies is an ongoing and important DoD issue.**

ERS Tradespace development is now focusing on the user-oriented approach in preparation for DoD-wide implementation and adoption

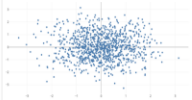
Tradespace Analytics and Visualizations

Available Plotting Options



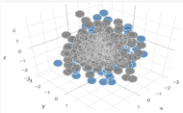
Histogram

A diagram consisting of rectangles whose area is proportional to the frequency of a variable and whose width is equal to the class interval



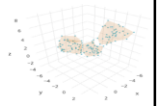
Scatter Plot 2d

A graph in which the values of two variables are plotted along two axes, the pattern of the resulting points revealing any correlation present



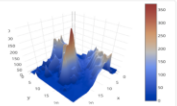
Scatter Plot 3d

A graph in which the values of three variables are plotted along three axes, the pattern of the resulting points revealing any correlation present



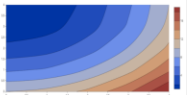
Clustering 3d

A graph in which the values of three variables are plotted alon three axes, with a mesh alpha clustering overlay



Surface Plot 3d

Surface plots are diagrams of three-dimensional data. Rather than showing the individual data points, surface plots show a functional relationship between a designated dependent variable (Y), and two independent variables (X and Z).



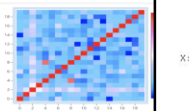
Contour

A contour plot is a graphical technique for representing a 3-dimensional surface by plotting constant z slices, called contours, on a 2-dimensional format.



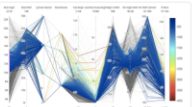
Heatmap

Graphical representation of data where the individual values contained in a matrix are represented as colors.



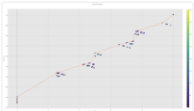
Correlation Matrix

Graphical representation showing the correlation coefficients betweensets of variables.



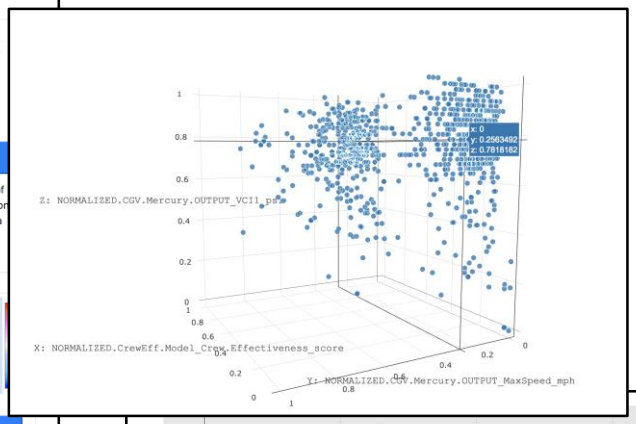
Parallel Coordinates

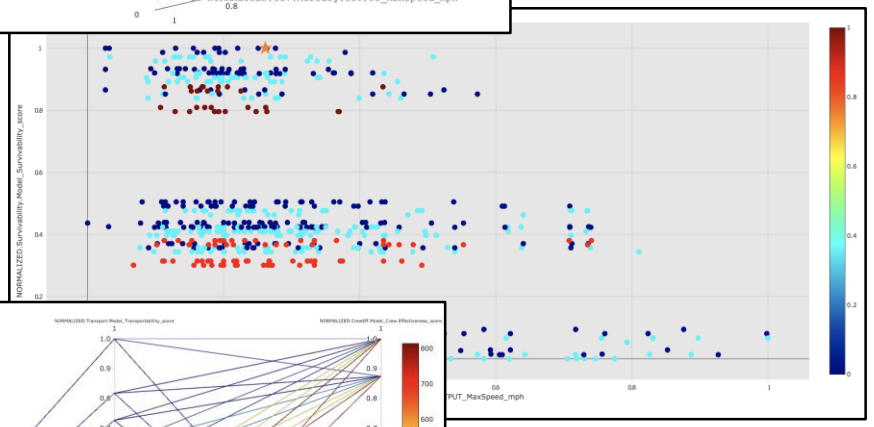
A common way of visualizing high-dimensional geometry and analyzing multivariate data.

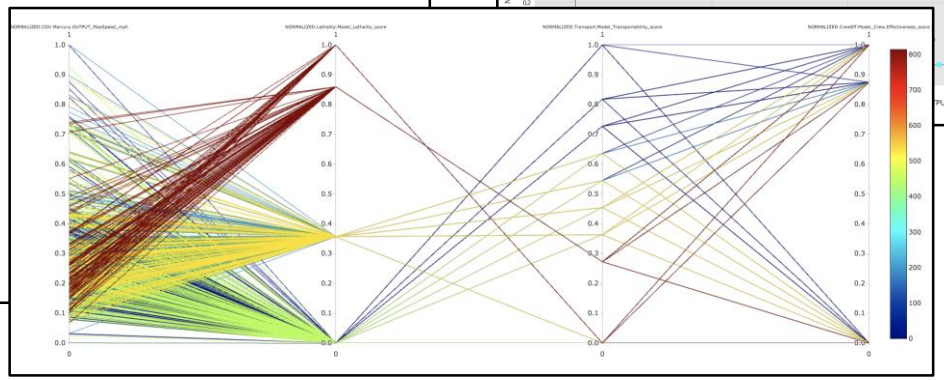


Pareto Front

A framework for partially evaluating a set of "actions" with multi-dimensional outputs assuming a very weak "desirability" partial ordering which only applies only when one processes is better (or at least as good) for all the outputs. It is useful for reducing a set of candidates prior to further analysis.







plotly JS

python

Updates to Architecture

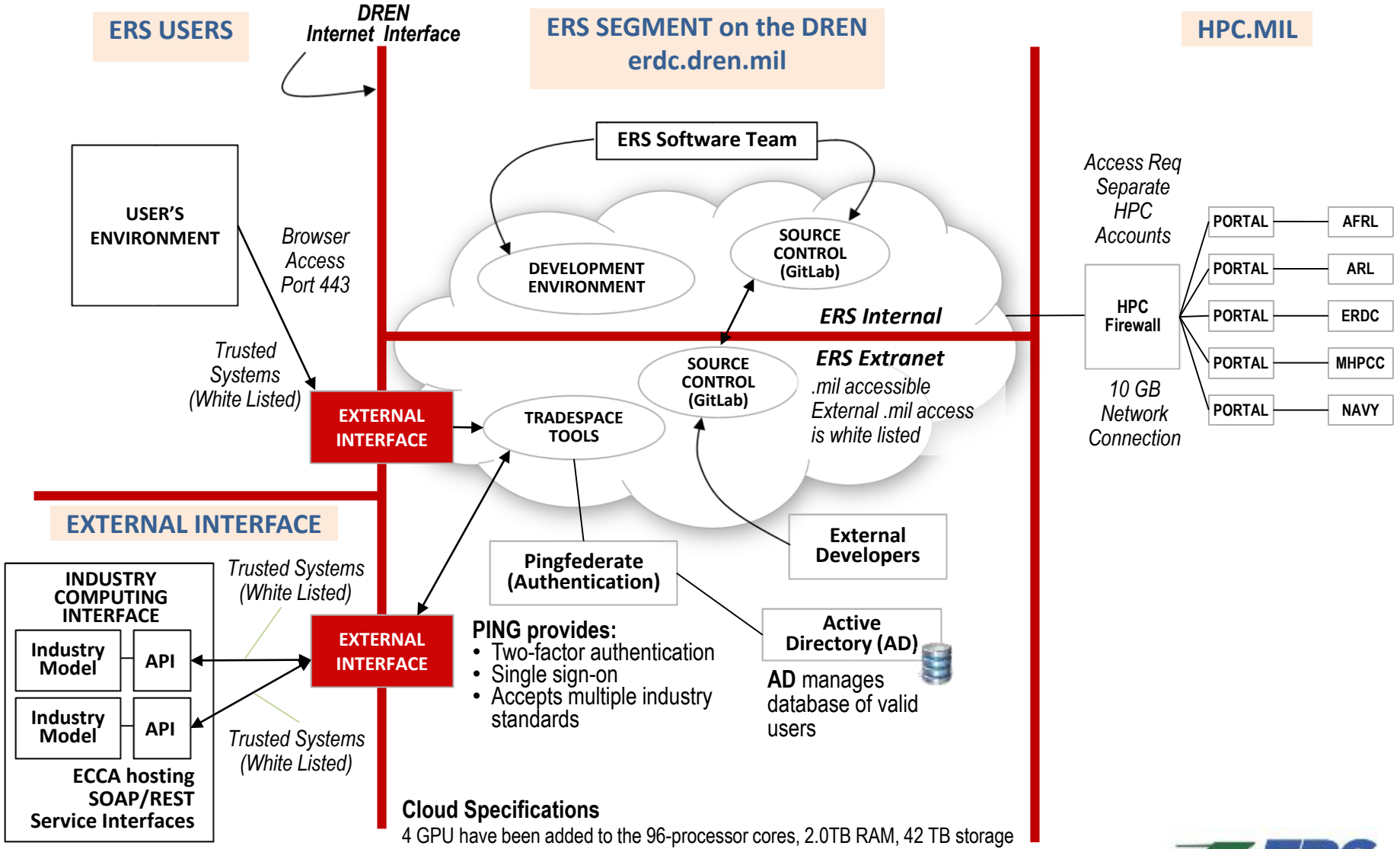
- ***Web Hosted***
- ***Access Control***
- ***Collaboration***
  - ***Shared Notebooks***
  - ***Shared Data***
- ***Versioning***
- ***Analytic Packages***
- ***Scalable***
- ***Portable***
- ***Reproducible***
- ***Distributed***
  - ***Spark***
  - ***Hadoop***



Relevant ERS NDIA Talk

10:40 - Resilient Tools: Building an Agile Framework for the Analysis of Environmental Impacts on Military Systems
Dharhas Pothina, PhD - ERDC

Network Access

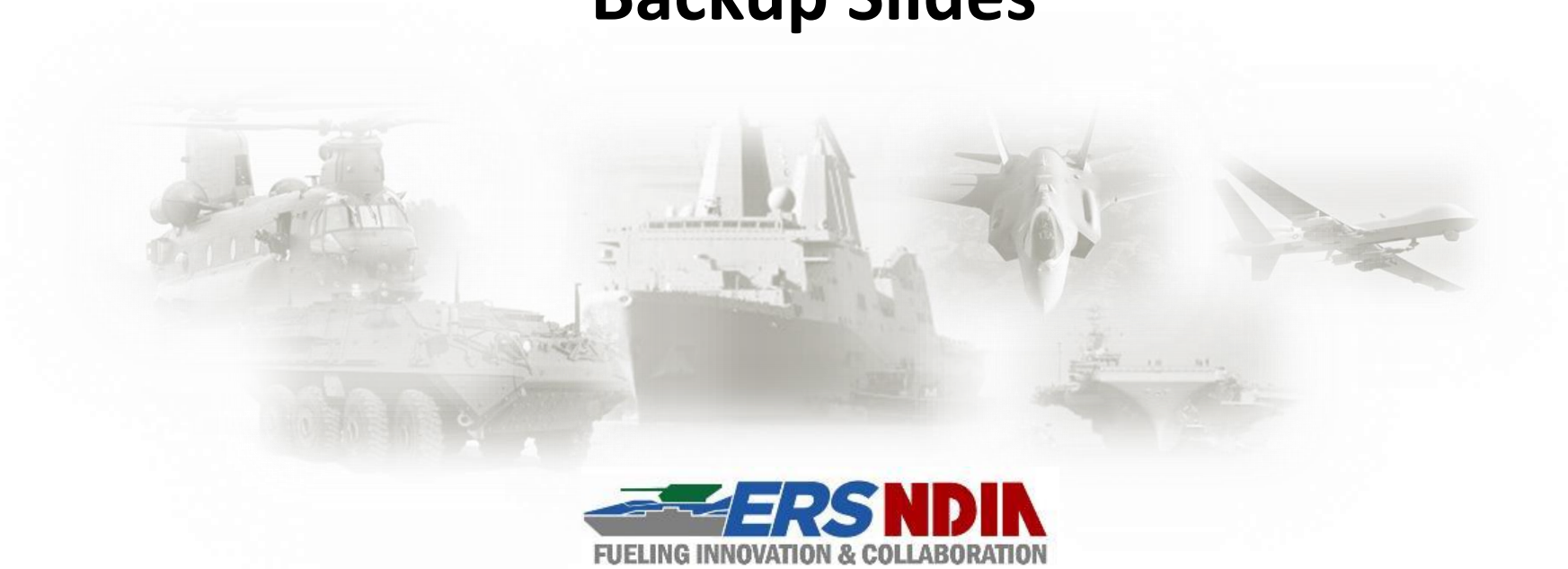


Questions



ERS NDIA
FUELING INNOVATION & COLLABORATION

Backup Slides



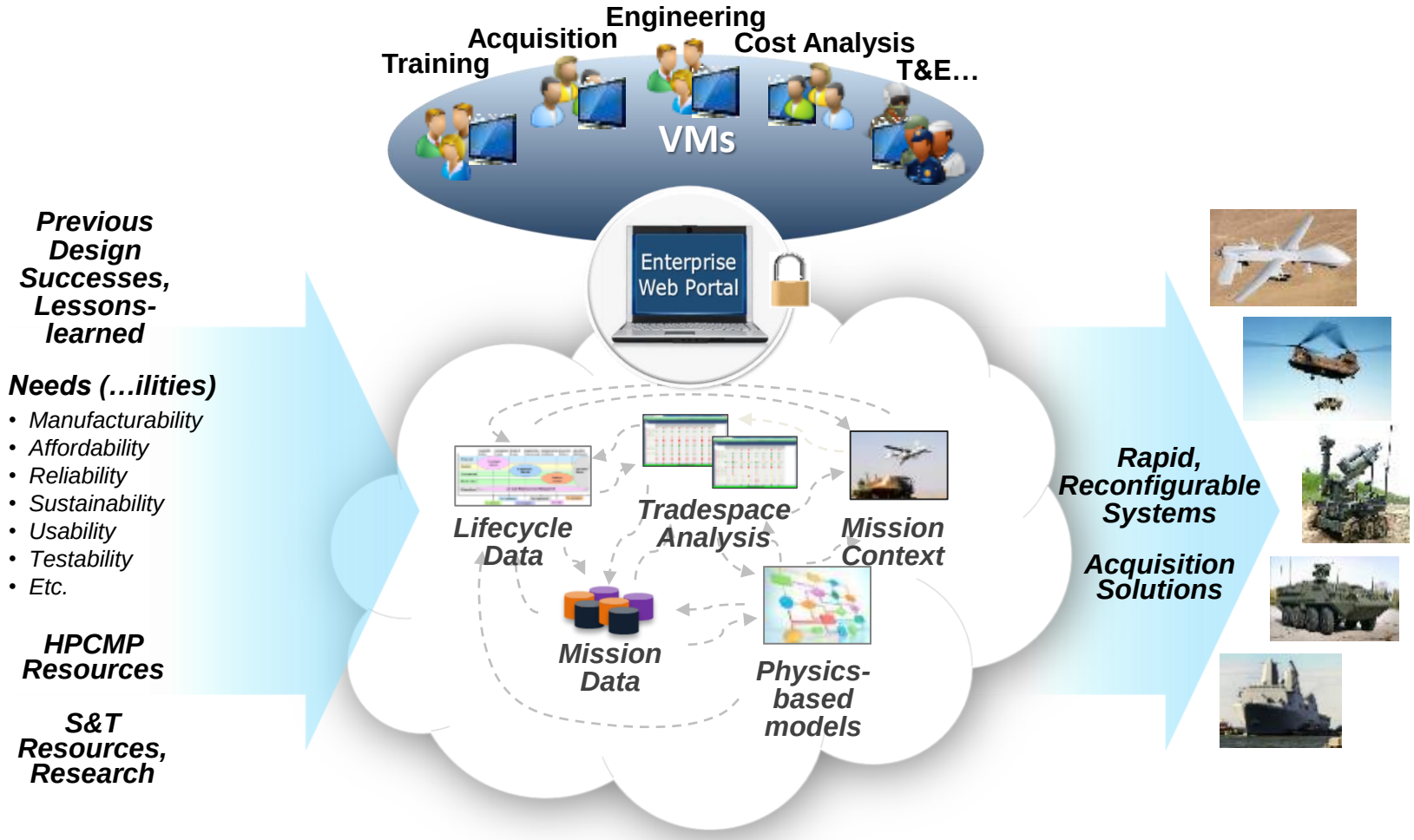
ERS NDIA
FUELING INNOVATION & COLLABORATION

What is a Tradespace

- **Tradespace is the space spanned by completely enumerated design variables. It is the potential solution space.**
- **Tradespace can also be defined as the set of processes, program and system parameters, attributes, and characteristics required to satisfy mission profile.**
- **The enumeration of a large tradespace helps prevent designers from starting with point designs while allowing them to investigate more thorough design solutions sets.**

System-Supported Collaboration Supports Data-Driven Decision-Making

ERS Tradespace Analytics support Collaborative Processes





Introducing Lifecycle Cost to Early Conceptual Tradespace Exploration

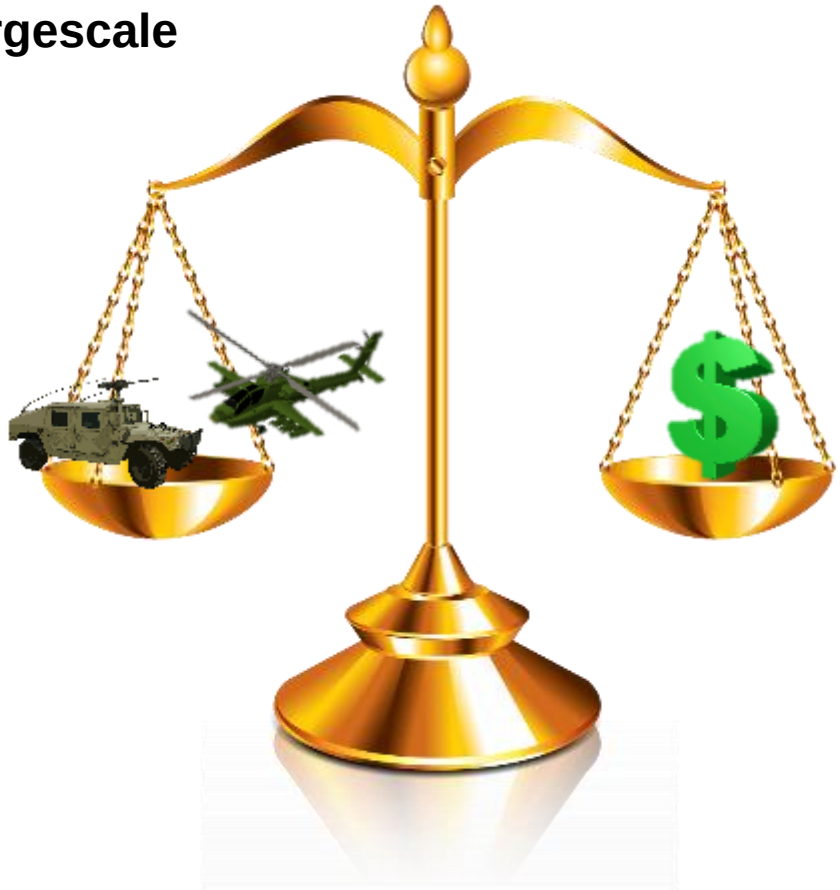
20th Annual NDIA Systems Engineering Conference
October 26, 2017

E. Alex Baylot, Research Industrial Engineer
James "Jed" Richards, Operations Research Analyst
US Army ERDC

Objective and Outline

Provide ERS Lifecycle Cost (LCC) development plan and methods for linking cost models to performance models for generating largescale tradespaces

- Objective
- Background
- Cost Estimating Techniques
- Cost Analysis Use Case
- Surrogate Model Creation Method
- Low-Cost Attritable Aircraft Use Case
- ERS Cost Model Development Plan
- Summary
- Questions

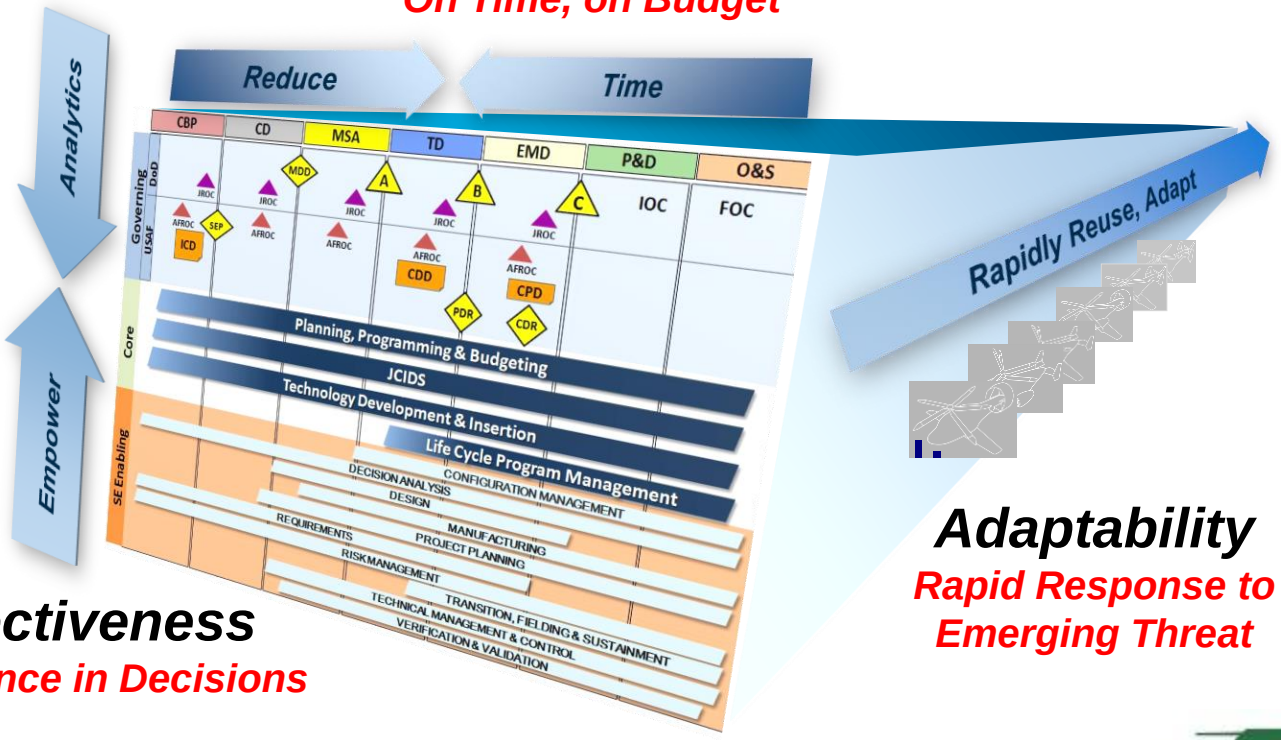


Background

A goal of the Engineered Resilient Systems (ERS) Program is to create a capability for linking cost and performance models for early concept exploration of design alternatives

Affordability

On Time, on Budget



Effectiveness

Confidence in Decisions

Adaptability

Rapid Response to Emerging Threat

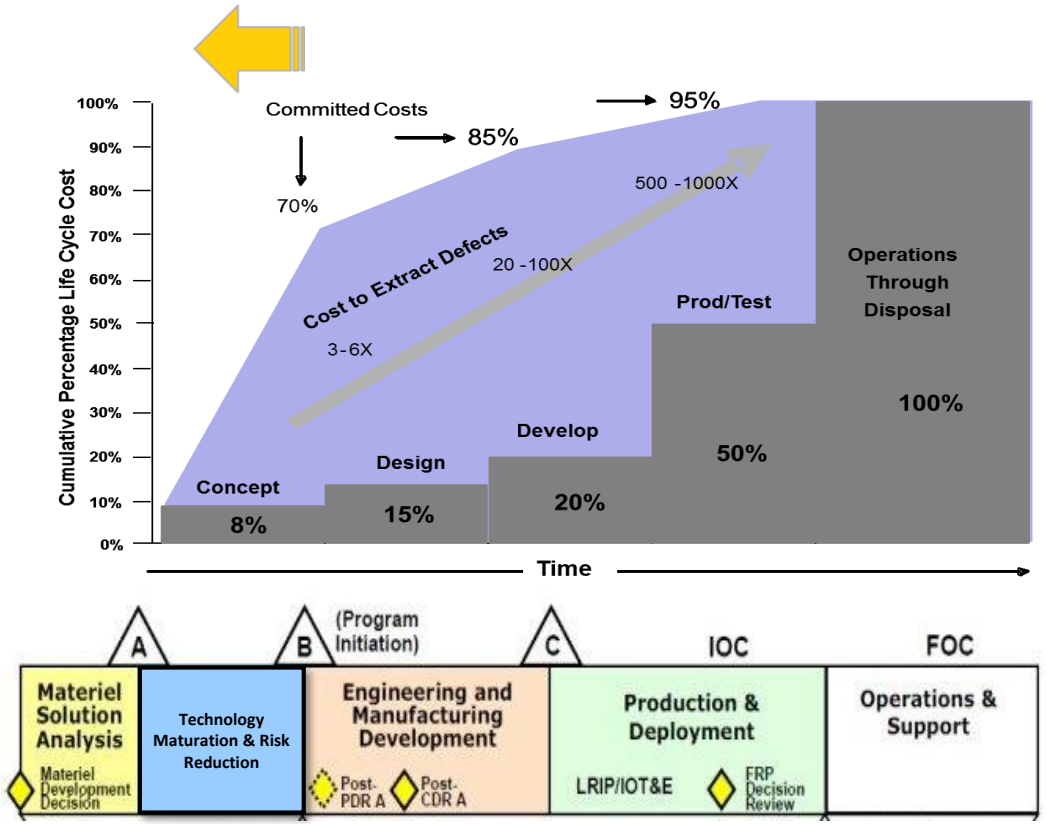
Distribution A: Approved for Public Release

Background

Affordability Analysis (Pre-Milestone A/B)

- Determine Affordability Goals/Caps
- Estimate Program Lifecycle Cost
- Establish Cost Targets
- Analyze Cost/Performance Trades

Committed Lifecycle Cost



Reference DoDI 5000.02 Defense Acquisition Life Cycle Compliance Baseline

Distribution A: Approved for Public Release

Cost Estimating Techniques

Analogy

- Quick, inexpensive, easy-to-change
- Subjective, not precise, poor comparison between new and old systems
- Typically used pre-Milestone A through Milestone A

Parametric

- Cost estimating relationships, inexpensive, easy to do “what-if” drills
- Moderately subjective, precision only as good as databases
- Typically used pre-Milestone A through Milestone B

Engineering

- Very accurate in later stages of EMD, limited subjectivity, uses WBS
- Very expensive, very time consuming, “what-ifs” are difficult
- Typically used Milestone B through post-Milestone C

Actual Costs

- Limited subjectivity, very accurate
- Limited actual cost data, very expensive, very time consuming, “what-ifs” are difficult
- Typically used Milestone C through post-Milestone C

DAU ACQ 101

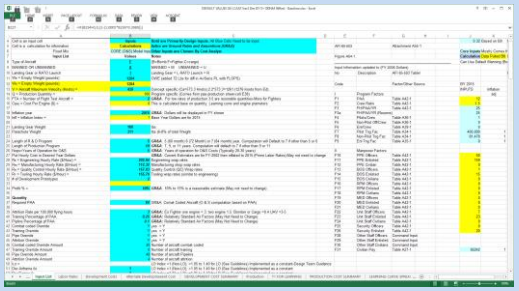
Cost Analysis Use Cases

	Use Cases	ERS Partner
Create/Adapt Cost Model	1 – Manual CER: User manually enters Cost Estimating Relationships (CER) to build a cost model	UAS (NCCA, UAS Handbook)
	2 – Existing Menu: User choses an existing cost constraint component and adjusts (calibrates) for specific cost generation	Helicopter (GTRI, Commercial rotorcraft cost model)
	3 – Historic Cost Data: cost model from user provided historic cost data	Ground Vehicle (TACOM, CADE data)
Link Existing Cost Model	4 – Existing Model Surrogate: Allows user to provide an existing cost data set derived from any source to generate meta model for cost domain tradespace generation (surrogate cost modeling)	Surface Ship (NSWC Carderock, Surface Combatant Performance Based Cost Model)
	5 – Excel Cost Model: Allows user to provide an existing excel based cost model to link to tradespace generation	Un-Manned Aircraft (AFRL – LCAAT)
	6 – COTS Cost Model: User provides a COTS integrated tools model	[development pending]

Distribution A: Approved for Public Release

Surrogate Model Creation Method

Connecting cost models to other tradespace models



Python Wrapper/Parser

Use existing spreadsheet cost model

I/O Combinations

+100K

Use Monte-Carlo techniques



Surrogate Model

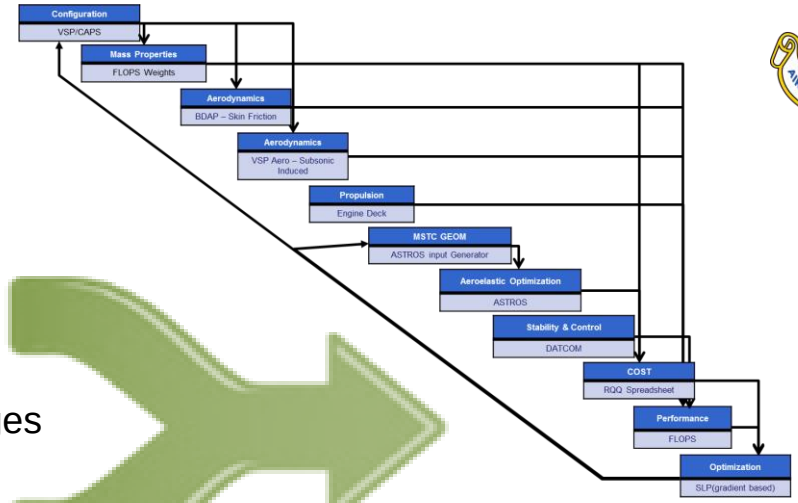
Generate surrogate-regression model

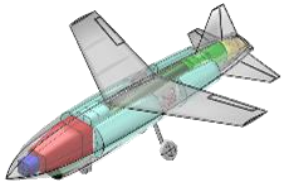
Low-Cost Attritable Aircraft Use Case

Current Method*

Computer-language cost model derived from spreadsheet to MATLAB or Python

- 4 months development
- Slow response to changes





- ❑ **Aeroelasticity**
- ❑ **Structural sizing**
- ❑ **Cost**
- ❑ **Stability & Control**
- ❑ **Multi-Fidelity**
- ❑ **Parametric Analysis Optimization**

Surrogate Method



100X reduction in cost model integration period

- 24 hours development
- Quick response to changes

Model Execution

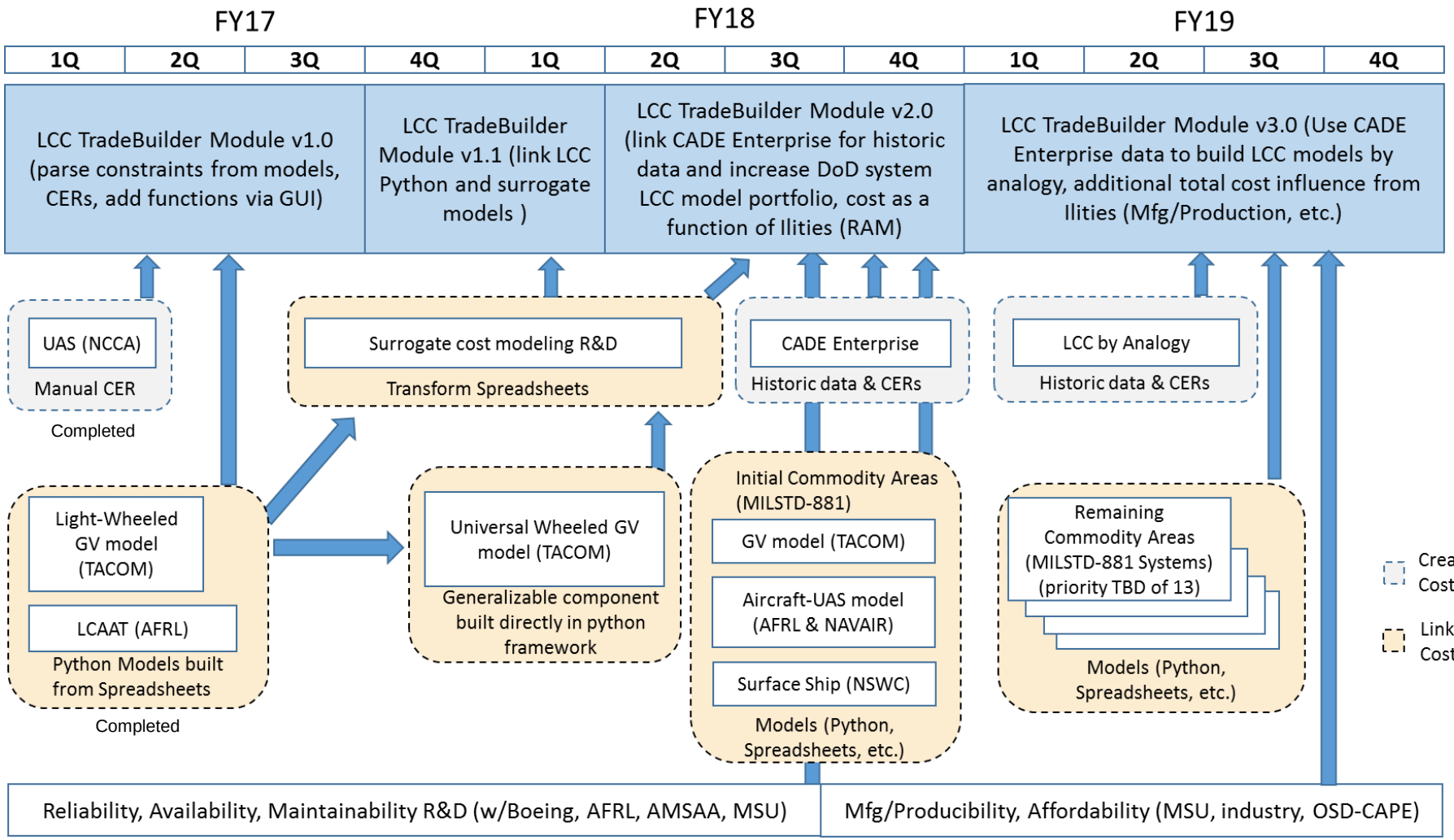




*Not typical

Distribution A: Approved for Public Release

ERS Cost Model Development Plan

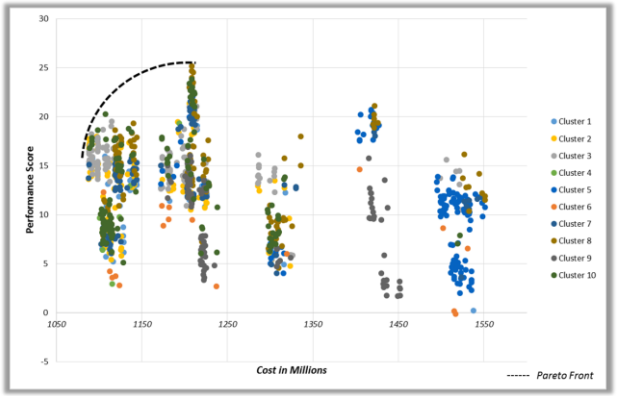


Distribution A: Approved for Public Release

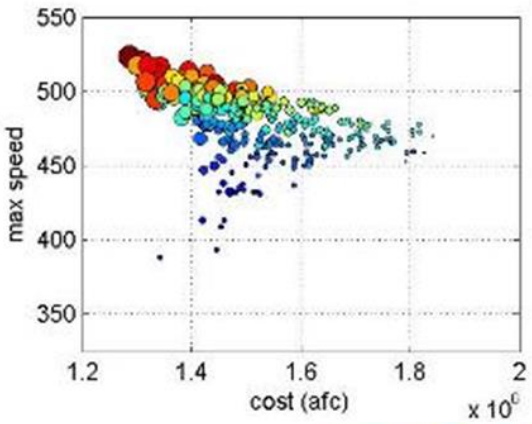
Summary

- DoDI 5000.02 identifies the requirement at Milestone (MS) A for an Affordability analysis in addition to a cost analysis and is driving more accurate cost analysis to the left
- ERS is developing methods to better integrate cost models into conceptual tradespace exploration using existing models or surrogate models
- Surrogate modeling methods show promise to greatly accelerate the integration process into tradespace exploration for pre-MS A & at MS A
- The ERS cost model development plan strives to provide a capability for all system commodities supporting all Services and OSD-CAPE

Ground Vehicle



UAS



Distribution A: Approved for Public Release

Questions

Mr. E. Alex Baylot, US Army ERDC
Alex.Baylot@usace.army.mil

Mr. James “Jed” Richards, US Army ERDC
James.E.Richards@erdc.dren.mil

Digital Engineering and Engineered Resilient Systems (ERS)

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 26, 2017

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

History

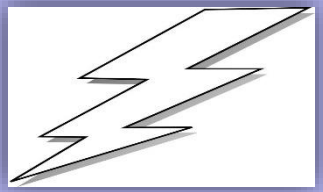
1st Industrial Revolution



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)

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

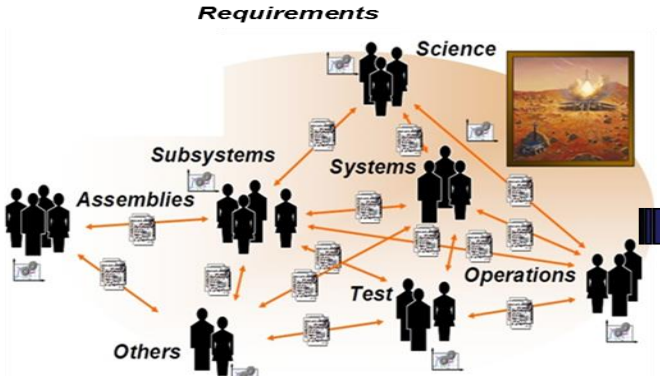
Digital Engineering: MBSE approach for DoD

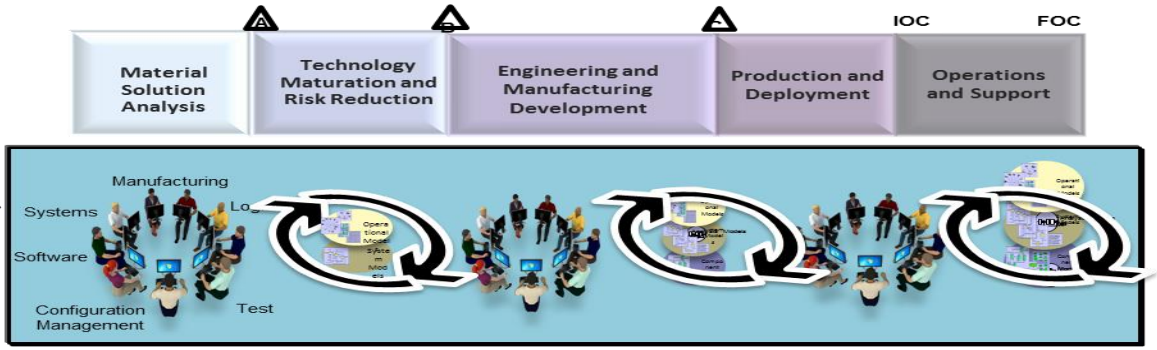
Current State

- 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 static disconnected 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, **and/or** 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

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

ERS 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

ERS

- **Engineered Resilient Systems (ERS) combines advanced engineering techniques with high-performance computing to develop concepts and tools that significantly amplify design options examined**
- **Develop/Integrate advanced engineering tools for efficient, integrated design and development across the full range of the product lifecycle**

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Digital Engineering Relationships

Digital Engineering Ecosystem

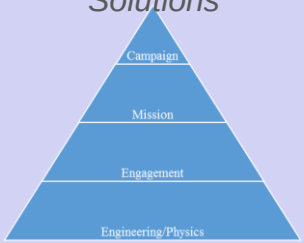
Digital Engineering Strategy

User selected and integrated based on outcome needed

Supporting tools: (Large Tradespace Analytics datasets, Analysis of Alternatives, Virtual Prototyping Evaluation, etc.)

ERS ENGINEERED RESILIENT SYSTEMS

Traditional Mod/Sim Solutions

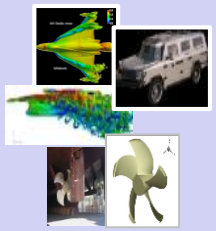


(DoD) Modeling and Simulation Coordination Office (DMSCO)

Other Initiatives

Physics-based / Engineering Design Tools

CREATE



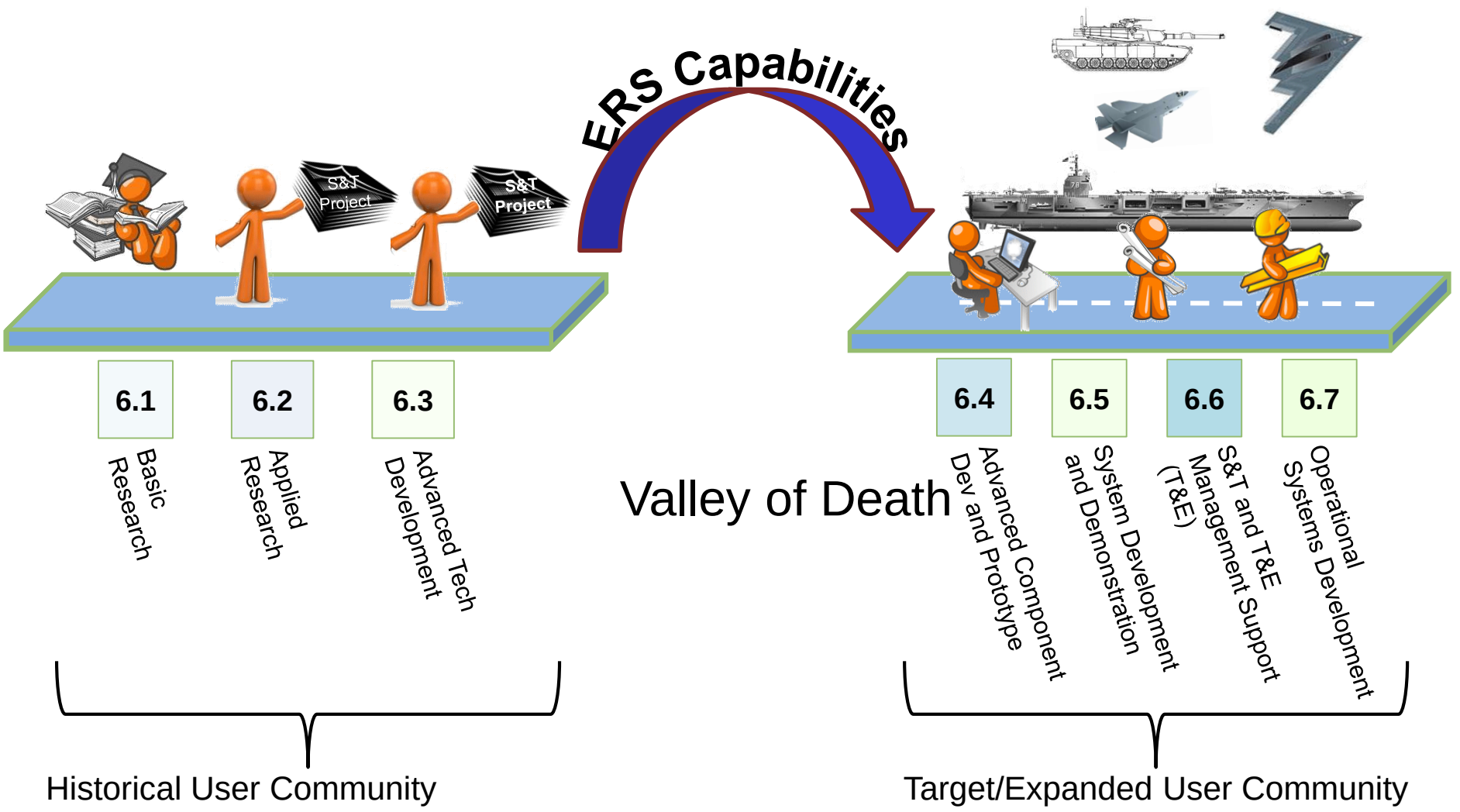
Computational Research and Engineering Acquisition Tools and Environments (CREATE)

World-class Computational Resources (High Performance Computing), Software, Networking

DOD HPC MODERNIZATION PROGRAM

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Transitioning S&T to Engineering & Acquisition

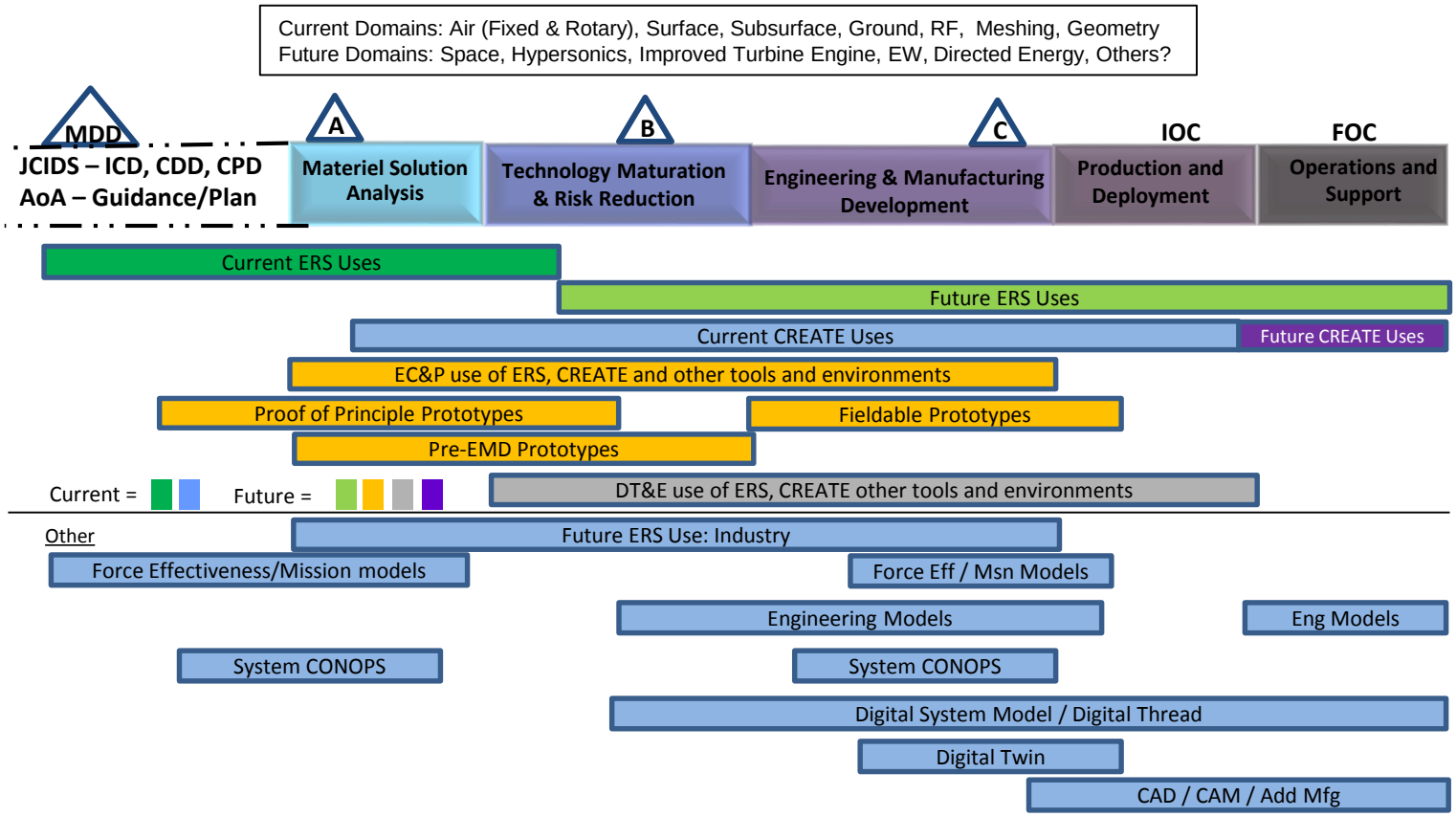


Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

DRAFT Vision for ERS, CREATE, et al (crossing the Valley of Death)

DRAFT

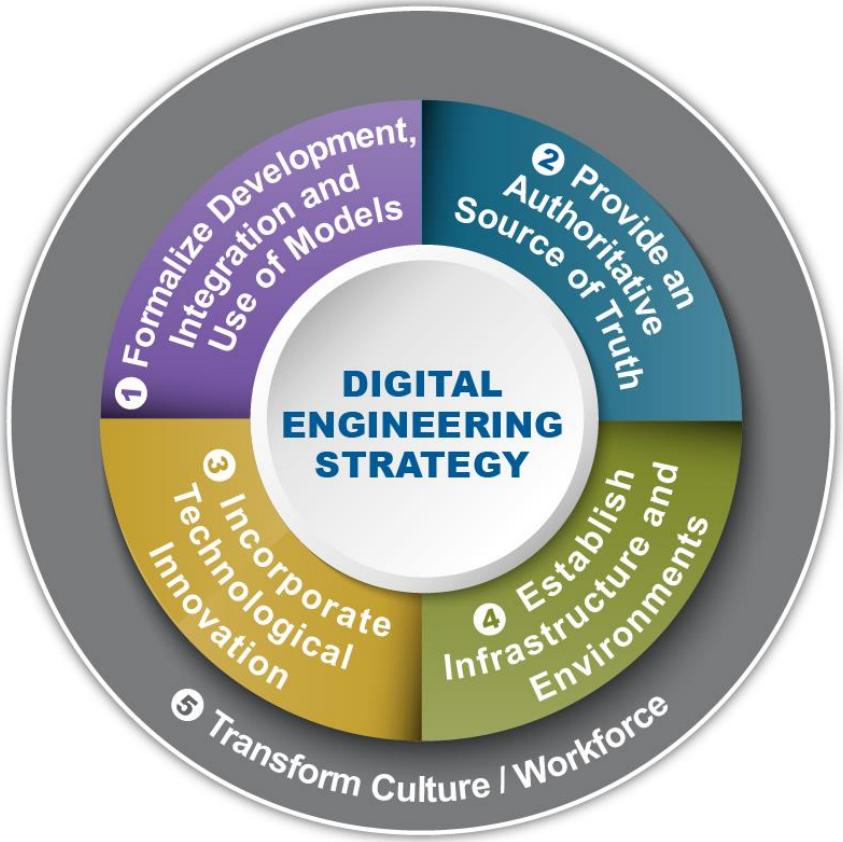
DRAFT



Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

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

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Goal #1: Formalize Development, Integration & Use of Models



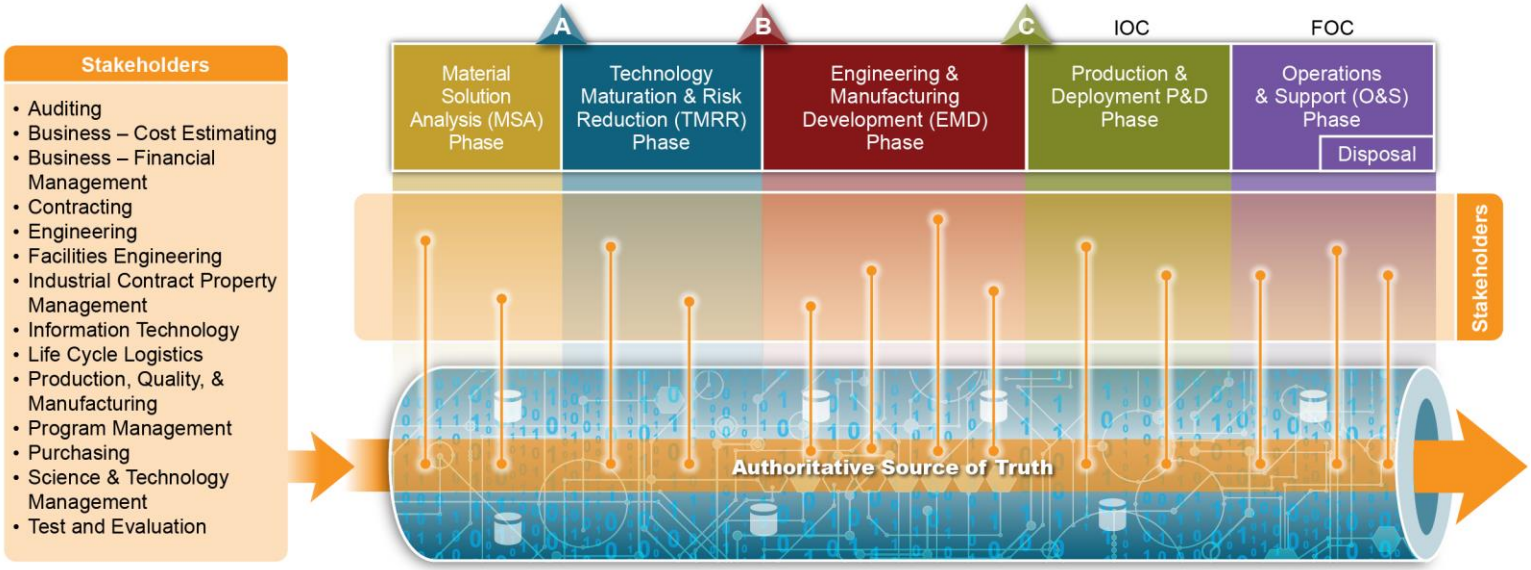
ERS in DE Goal 1:

- Use of models to replace the sequential, fixed requirement approach to design
- Use of models will enable prototyping, experimenting and testing of solutions virtually before physical prototypes and full scale systems are available
- Use of evolving models will allow analysis of design options to be shifted left in the lifecycle
- Understand how to defeat a concept through inverse modeling

Models as the cohesive element across a system's lifecycle

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Goal #2: Provide an Authoritative Source of Truth



ERS in DE Goal 2:

- Models are inherently more adaptable across mission sets and environments
- The authoritative sources of truth means ground truth
- ERS is fast and accurate enough to understand and mitigate risk in large, complex, and integrated data set

Right information, right people, right uses, right time

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Goal #3: Incorporate Technological Innovation



- ❖ **Big Data and Analytics**
- ❖ **Cognitive Technologies**
- ❖ **Computing Technologies**
- ❖ **Digital-to-Physical Fusion Technologies**

ERS in DE Goal 3:

- Explore new concepts to integrated advanced engineering models
- Replace intensive manual processes to stitch data and artifacts together with workflow automation
- Explore new decision analytics that generate real alternatives that reflect the entire lifecycle demanded by increased digital engineering use
- Utilize machine learning to analyze massive and complex datasets containing a variety of data types from a multitude of sources
- Architecturally integrated with knowledge management

Harness technology, new approaches, and human-machine collaboration to enable an end-to-end digital enterprise

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Goal #4: Establish Infrastructure & Environments



ERS in DE Goal 4:

- Architect an overall data ecosystem on HPCs
- Build generalized and reusable workflow engine
- Build enterprise-level web portal
- Organize software tools around the data
- Create visualization techniques that support decision makers

Foundational support for Digital Engineering environments

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Goals #5: Transform Culture and Workforce



ERS in DE Goal 5:

- Understand that migrating to a digital ecosystem does not remove the responsibility from the users to select, manage, govern and use the tools appropriately
- Gain confidence in performing activities in a collaborative, integrated, digital model-based environment
- Learn to articulate the problem, workflow, and model boundary conditions to a third party
- Build understanding in how to appropriately reduce reliance on physical experimentation

Institutionalize Digital Engineering across the acquisition enterprise

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

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

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

For Additional Information

Mr. Robert Gold

ODASD, Systems Engineering

703-695-3155

robert.a.gold4.civ@mail.mil

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Digital Engineering Overview

- **Background**
  - Dynamic operational and threat environments
  - Growth in system complexity and risks
  - Linear acquisition process that lacks agility and resiliency
  - 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

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.

Digital Models Have Incredible Potential

DoD needs:

- **Flexible designs that adapt and are resilient to unknown missions and threats**
- **Cost and affordability as quantifiable attributes of the trade space**
- **Systems of Systems, and Enterprise, contexts in order to respond to multiple stakeholders**
- **A balance between agility in acquisition and rigorous analysis and data**
- **Critical information appropriately protected while designing for interoperability**
- **Support in significantly diverse domains**

Balancing these axioms is challenging.
It drives the need for, and use of digital models to:

- **Maintain consistency about the system**
- **Integrate technical and non-technical drivers**
- **Understand the various perspectives on the system under development**

Models are advancing the STATE OF PRACTICE of SE

Distribution Statement A – Approved for public release by DOPSR 10/03/2017. Case # 18-S-0008 applies. Distribution is unlimited.



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

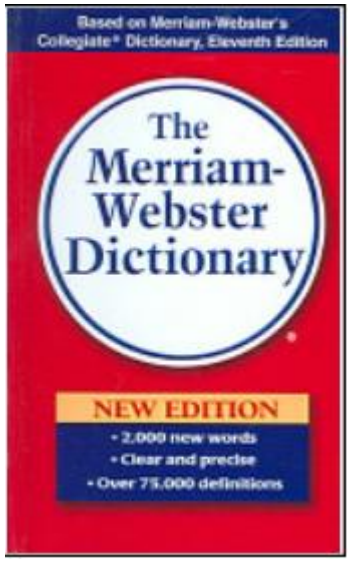
Copyright © 2017 Raytheon Company. All rights reserved.

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

Copyright © 2017 Raytheon Company. All rights reserved.

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

Copyright © 2017 Raytheon Company. All rights reserved.

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***

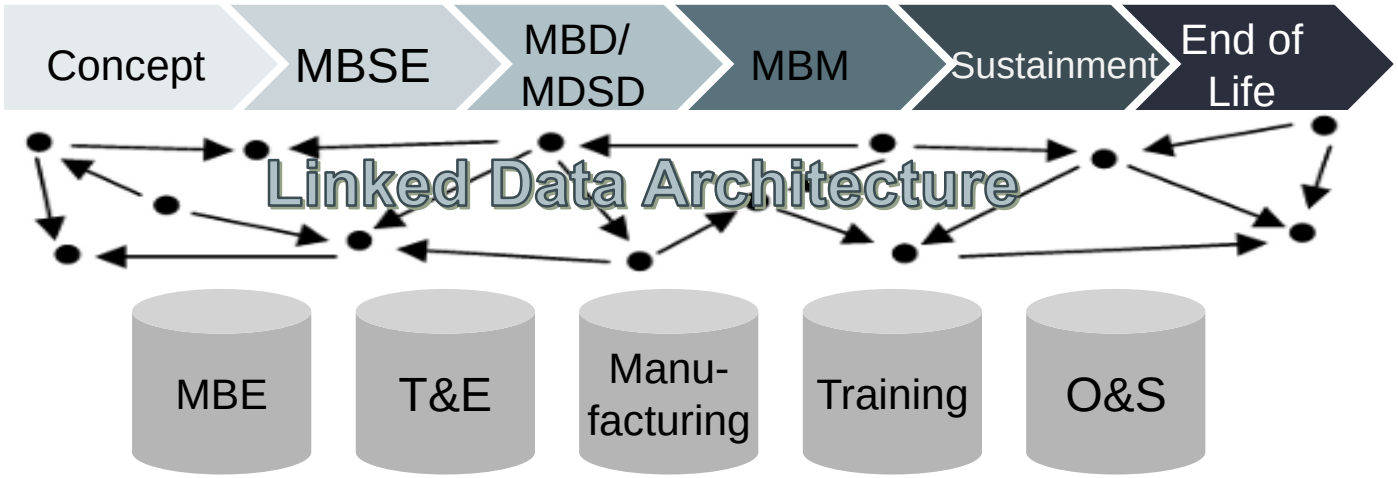
- Our model data is then turned in to **actionable information** as part of the overall design processes
- Our models become the source of information for deliverable documents which are **produced automatically**
- **Design decisions** are then **linked** and **consistent** across the solution space

The Models are the Master

Copyright © 2017 Raytheon Company. All rights reserved.

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

Copyright © 2017 Raytheon Company. All rights reserved.

Raytheon

System Digital Thread

Inputs

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

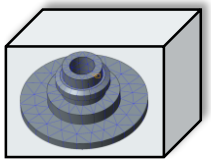
Tools and Techniques

System Design

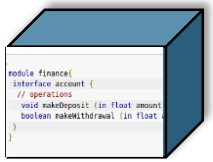
- Requirements Allocation and Flowdown
- SysML, UML Models
- Modeling Environment (Rhapsody, Magic Draw, etc.)
- Performance Analysis (Matlab)
- Architecture Frameworks (DODAF, etc)
- Collaborative Environment
- Automation (modeling, reporting, etc.)

Outputs

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



Hardware Design



Software Design



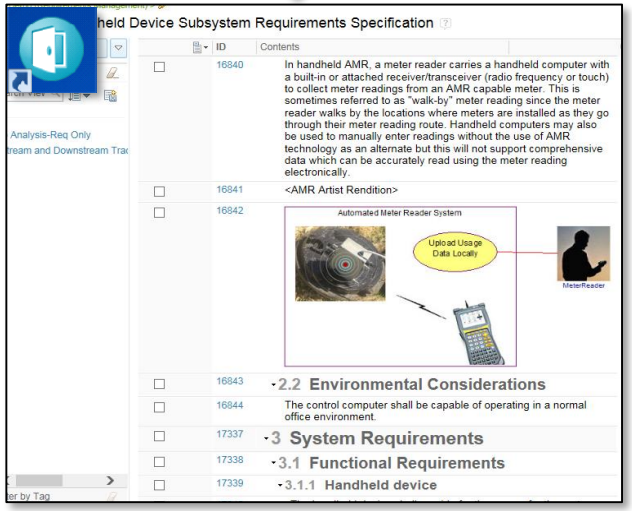
System Test

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

Copyright © 2017 Raytheon Company. All rights reserved.

Creating the System Digital Thread

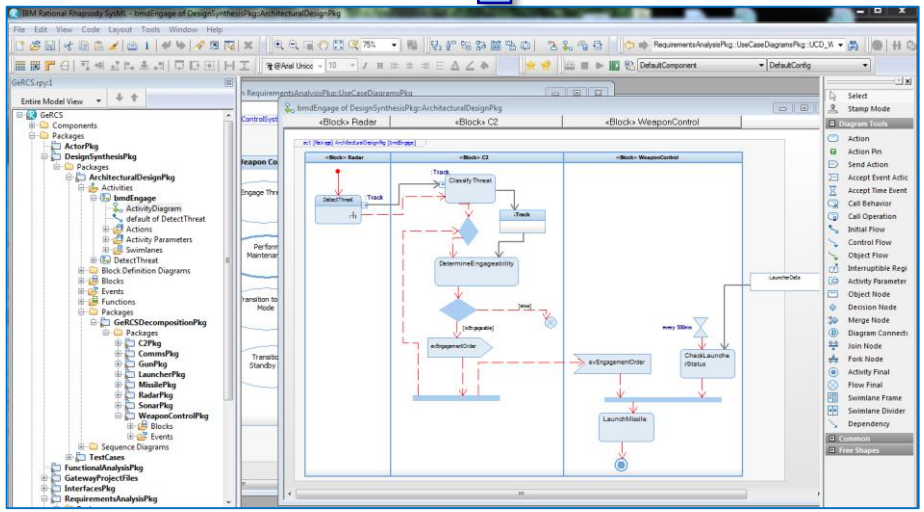
Requirements



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

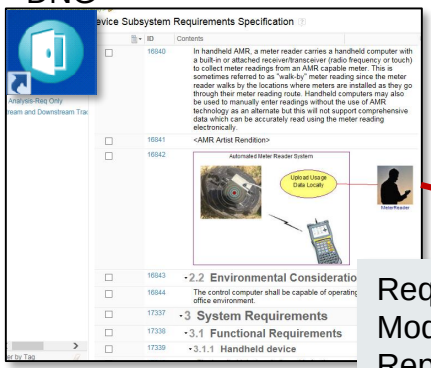
- System Use Cases
- Behaviors
- Interfaces
- Functions

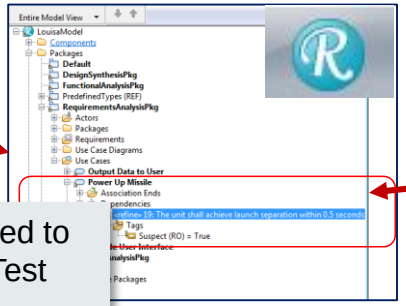
Copyright © 2017 Raytheon Company. All rights reserved.

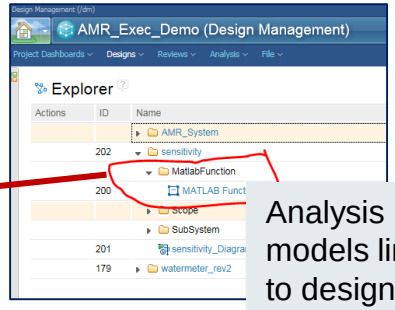
Creating the System Digital Thread

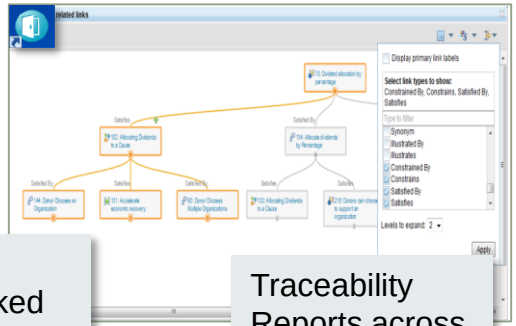
Requirements → System Models → Performance Analysis → Automated Digital Thread Reporting

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

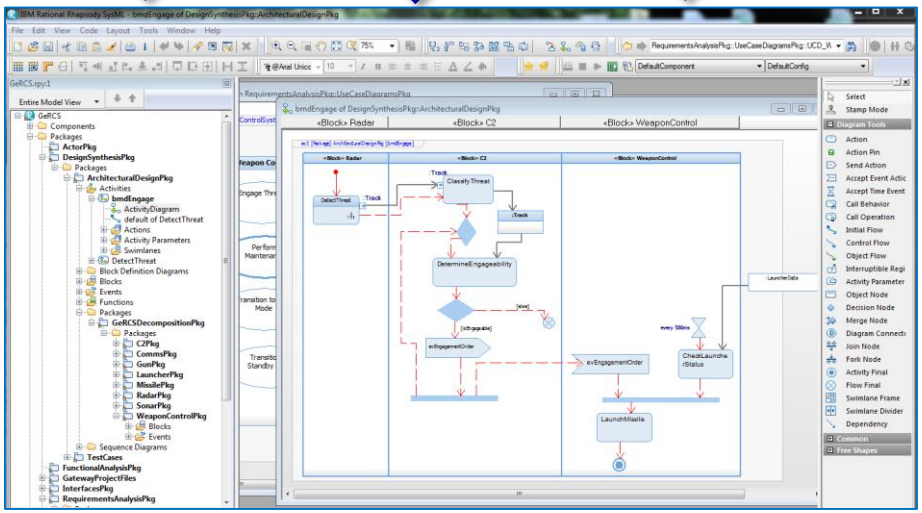
Copyright © 2017 Raytheon Company. All rights reserved.

Creating the System Digital Thread

SysML Model

Requirements Links

Performance Analysis Links

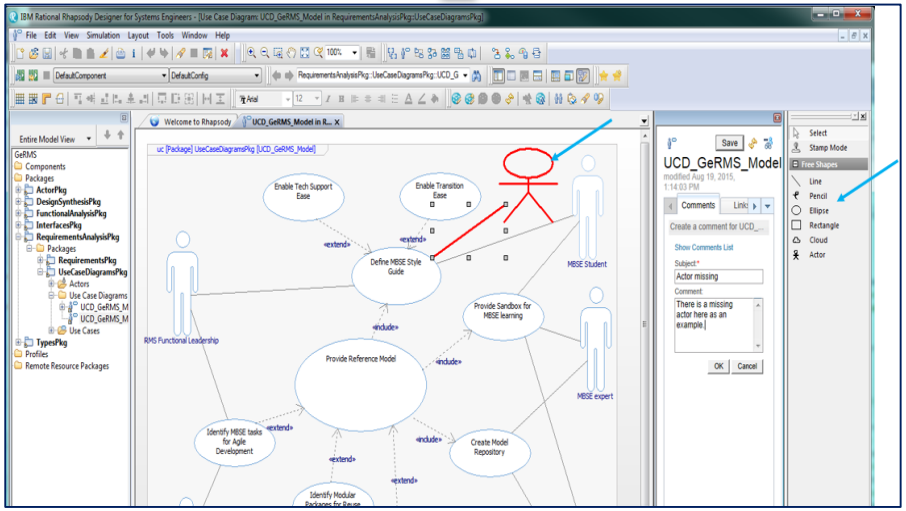


Generate Integrated SysML Model - typically in Rhapsody or MagicDraw. Power Point and Visio SysML diagrams **do not** count

- System Use Cases
- Behaviors
- Interfaces
- Functions

Team Reviews

Reviewed Models and Digital Thread



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

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

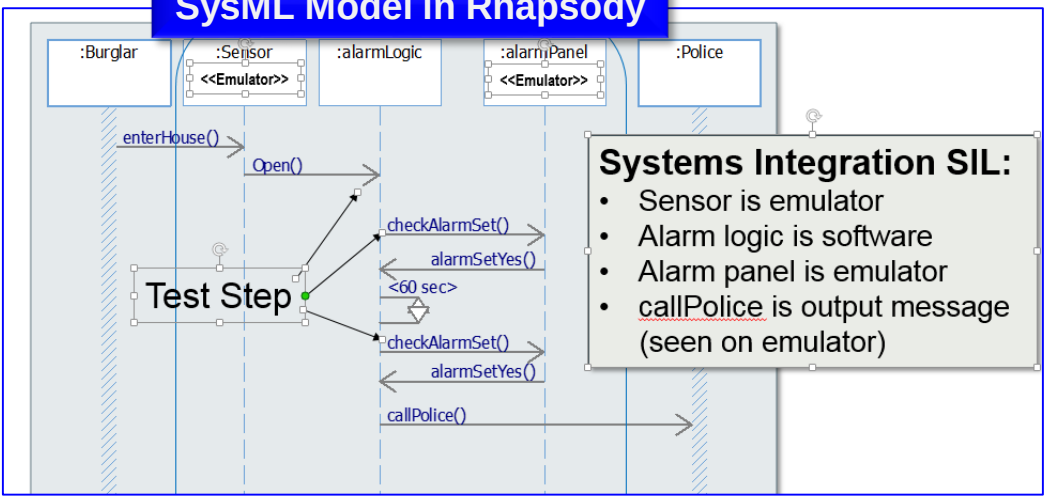
Copyright © 2017 Raytheon Company. All rights reserved.

Creating the System Digital Thread

System Models

Requirements (DNG/DOORS)

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)

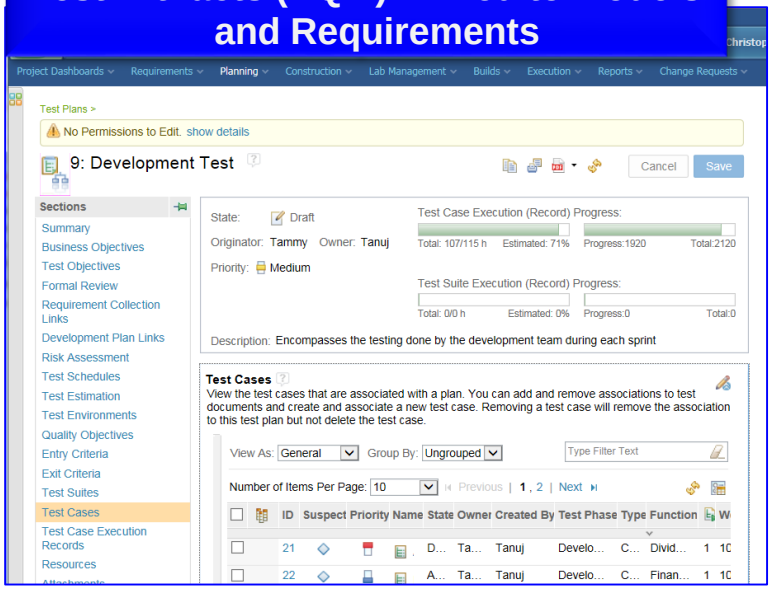
Model Driven Testing - Test Sequences, Vectors and Stimulators defined in models. Test artifacts (e.g., cases, plans, procedures) link to the model(s) to define the scope and interactions required for each test event.

Test Artifact Development

Test Plans and Procedures

Test Result Reports and Metrics

Test Artifacts (RQM) Linked to Models and Requirements



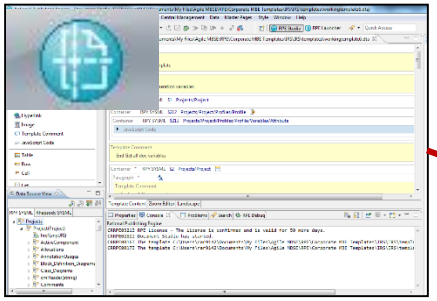
Test Defintion- Test artifacts (e.g., cases, plans, procedures) linked requirements and model. Documents and reports automatically generated

Copyright © 2017 Raytheon Company. All rights reserved.

Maintaining the System Digital Thread

Requirements | System Models | Test Artifacts

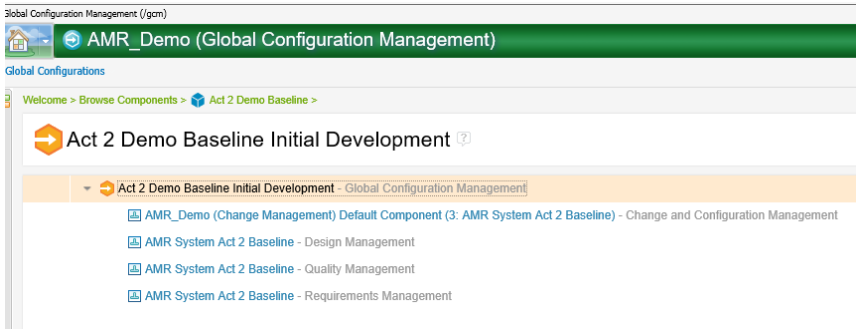
RPE





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

Requirements Baseline | System Models Baseline | Test Artifacts Baseline



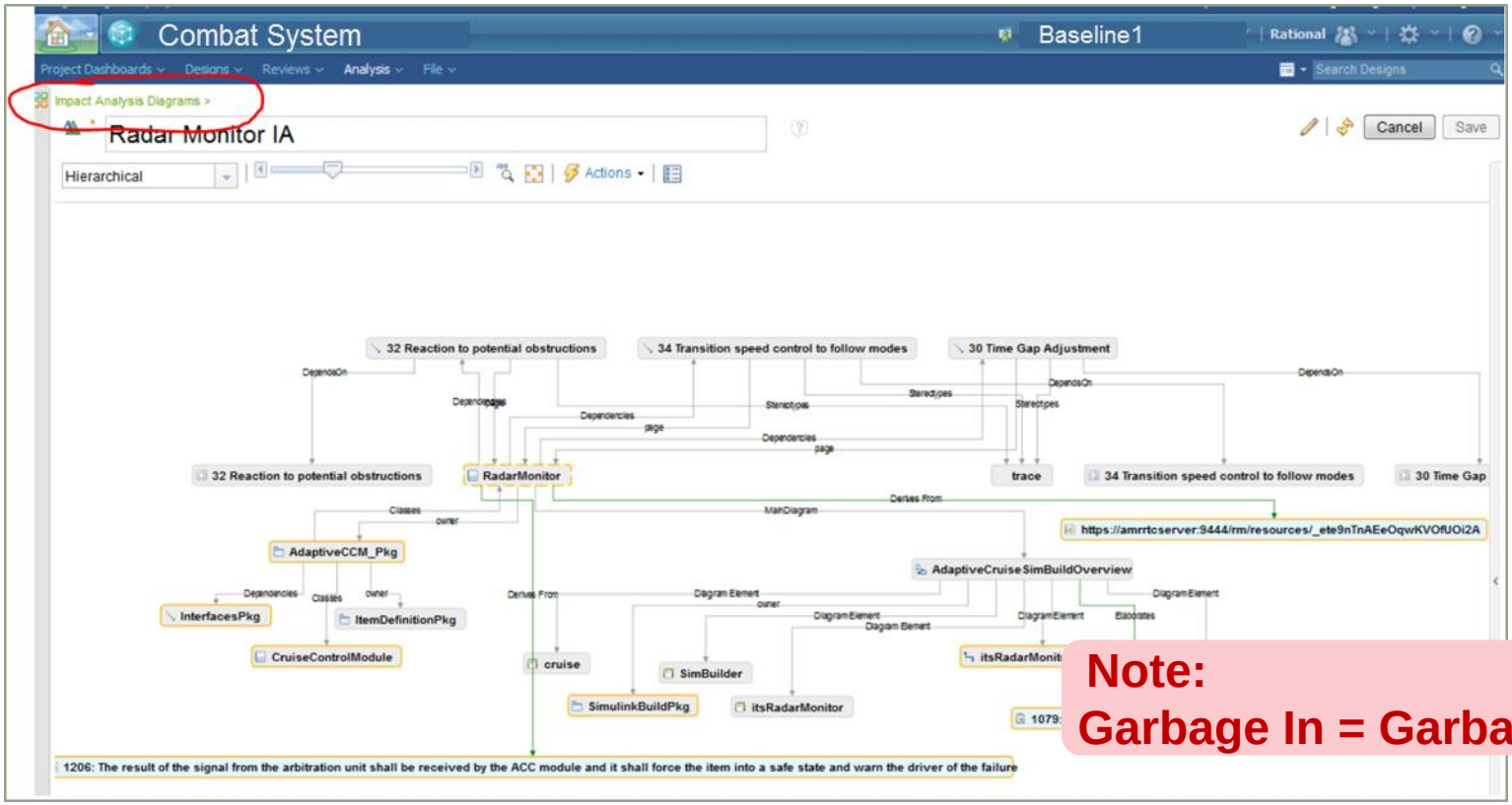
CM of Models – Configures baselines across multiple contributing applications forming a "configuration of configurations"

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

Copyright © 2017 Raytheon Company. All rights reserved.

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.

Copyright © 2017 Raytheon Company. All rights reserved.

Software Digital Thread

Inputs

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

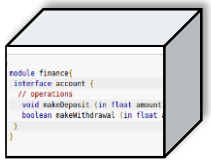
Software Design

Tools and Techniques

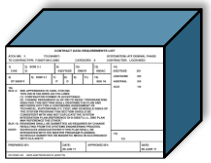
- Software Requirements Flowdown
- UML Models
- Software Modeling Environment (Rhapsody, Magic Draw, Eclipse, etc.)
- Code Generation
- Continuous Integration and Test
- Automation (Code, CDRLs, Reports, etc.)

Outputs

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



Generated Software



Generated CDRLs



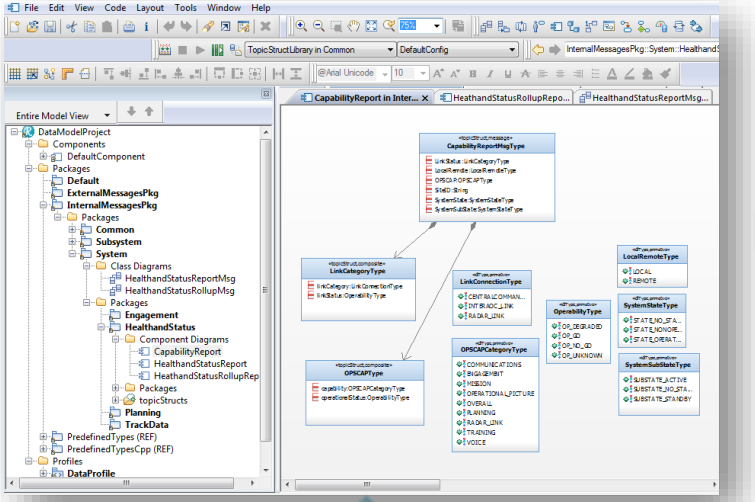
Automated Tests

Connecting the Digital Thread across engineering functions further enhances design consistency

Copyright © 2017 Raytheon Company. All rights reserved.

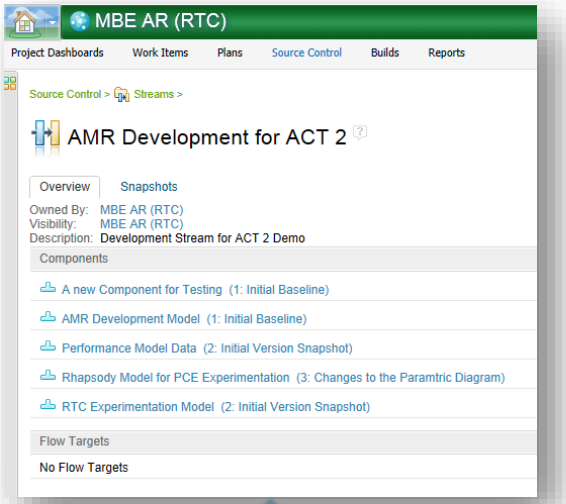
Pulling the Digital Thread through Software

Create Software & Data Model in Rhapsody/RDM



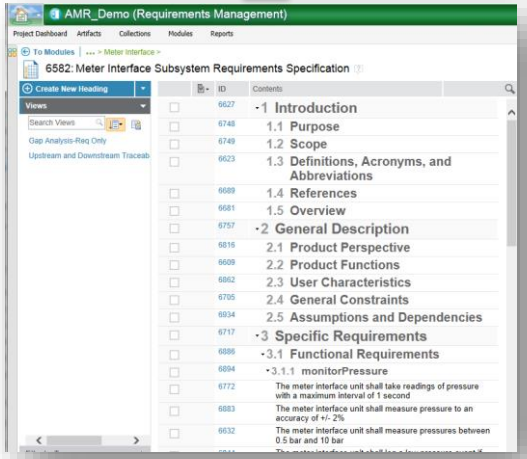
Code Generated from Model

Manage/Track Changes in RTC

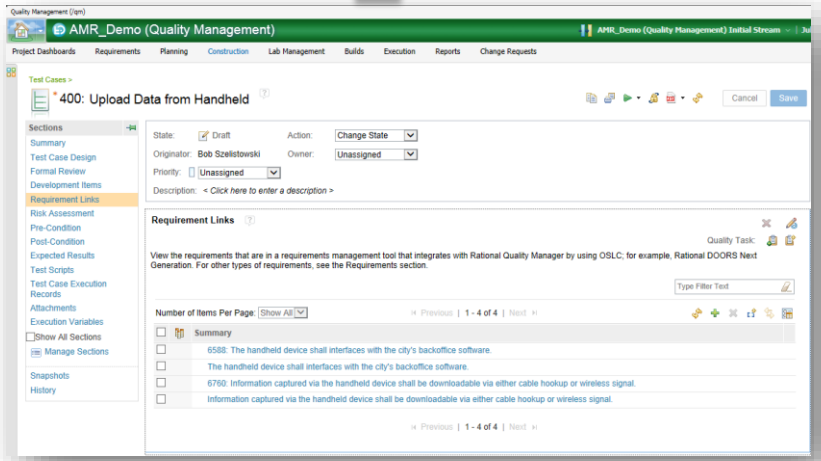


Trace to Model

Continuous IV&V



Validated by Test Case



Requirements in DNG

Test Cases & Execution Results in RQM

Copyright © 2017 Raytheon Company. All rights reserved.

HW Digital Thread

Inputs

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

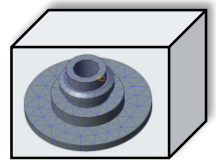
Hardware Design

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



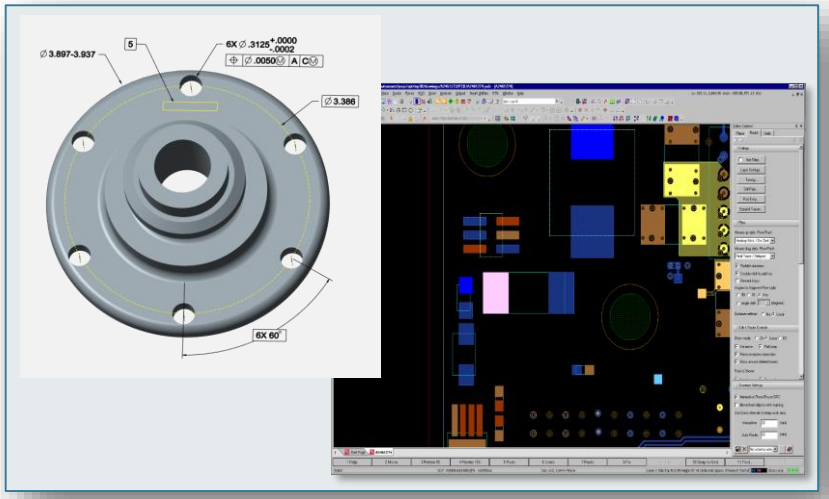
Digital Twin Artifacts

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

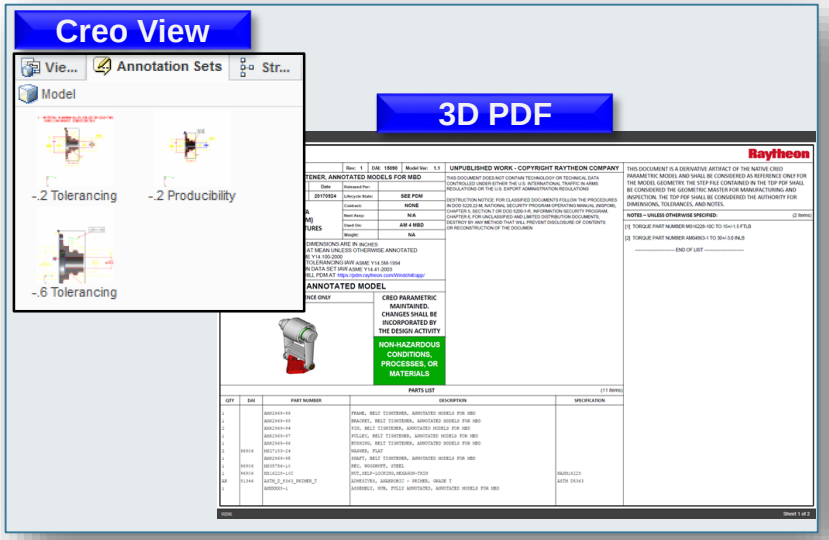
Copyright © 2017 Raytheon Company. All rights reserved.

Pulling the Digital Thread through HW

Create ME/EE Design Models



Model Based Peer Reviews

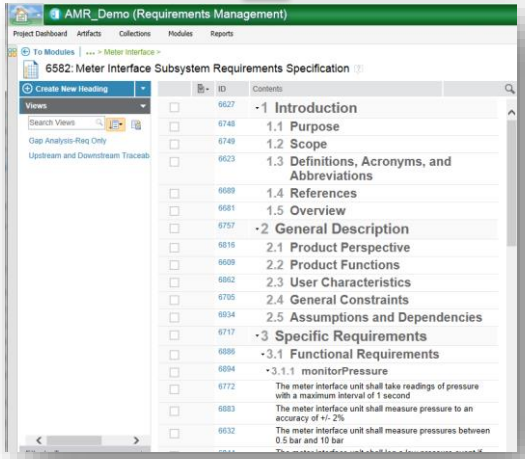


Derivative Artifacts Generated from Model

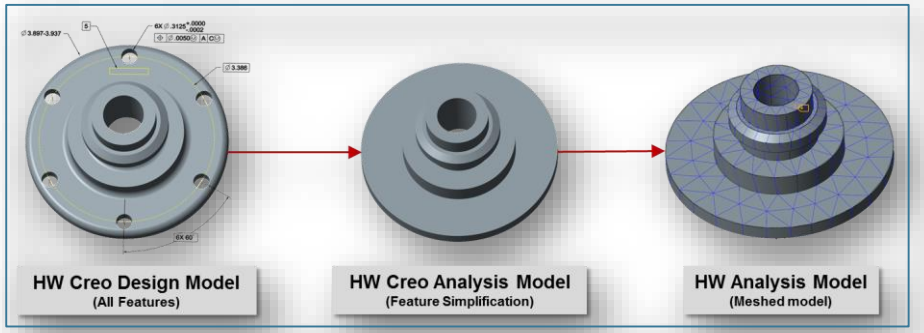
Trace to Model

Design Analysis and Optimization

Validated by Test Case



HW Requirements in DNG



Analysis Models Linked and Sourced to Design Model

Copyright © 2017 Raytheon Company. All rights reserved.

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.

Copyright © 2017 Raytheon Company. All rights reserved.

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



Copyright © 2017 Raytheon Company. All rights reserved.

Tradespace Analysis and Exploration incorporating Reliability, Availability, Maintainability, and Cost

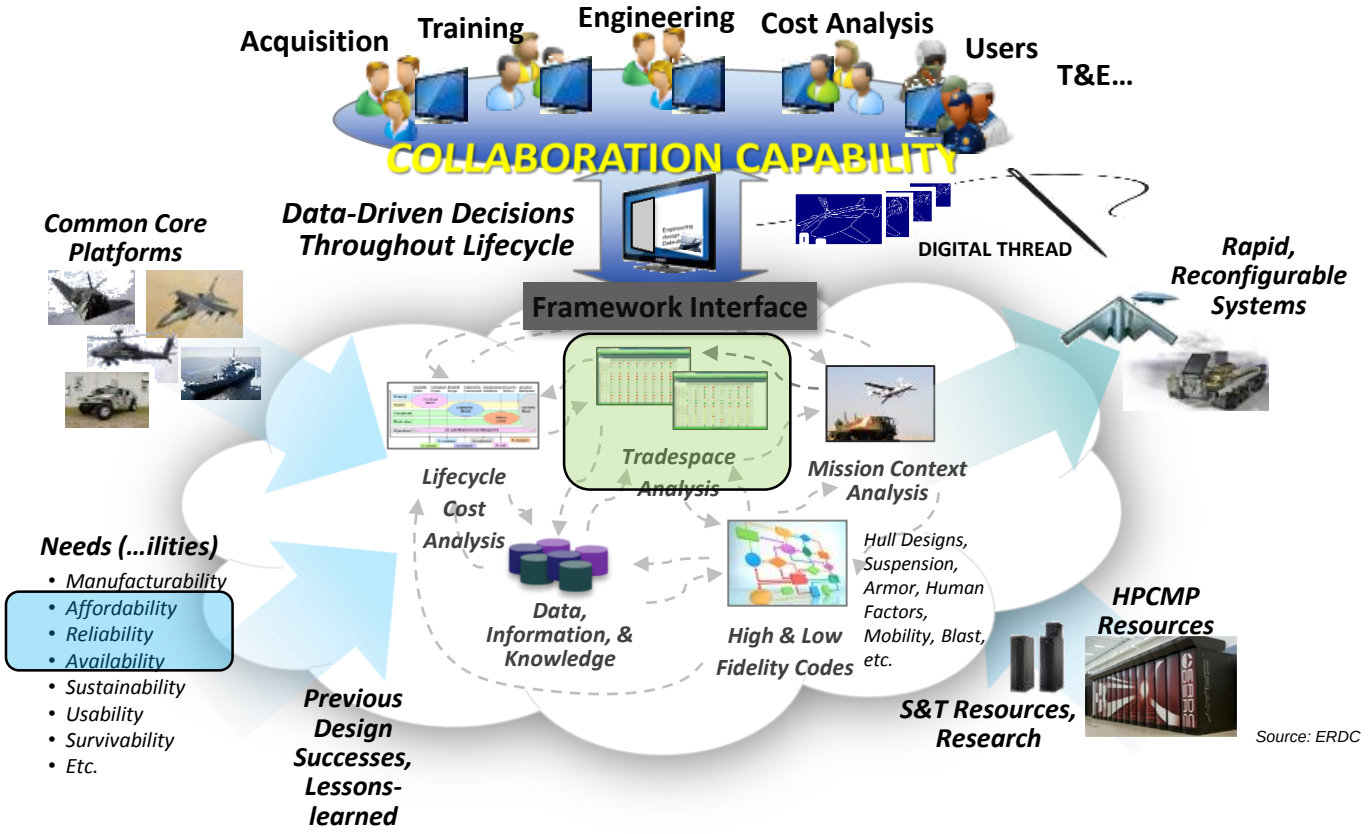
Saikath Bhattacharya[1], Vidhyashree Nagaraju[1], Lance Fiondella[1], Eric Spero[2], and Anindya Ghoshal[2]

[1]University of Massachusetts, Dartmouth, MA

[2]US Army Research Laboratory, Aberdeen Proving Ground, MD

Background

- DOD Engineered Resilient Systems framework



Background (2)

- Tradespace exploration processes and accompanying tools
  - Provide intuitive environment to explore alternatives
  - Assess designs for feasibility in multiple contexts
  - Promising methodology to
    - Facilitate effective designer/stakeholder communication
    - Ensure final product with mutually agreed set of capabilities
    - Support systems engineering tradeoffs during acquisition lifecycle

Background (3)

- Majority of TSE research emphasizes tradeoffs between functional requirements
- Nonfunctional requirements such as reliability, availability, and maintainability which impact operation and support costs (O&S) considered less frequently
- Proposed strategy incorporates reliability engineering into tradespace exploration (TSE)
  - Develop subsystem-level reliability investment model to
    - Achieve savings over system lifecycle
    - Explore tradeoff between fleet size and average procurement unit cost (APUC)

Reliability Modeling

Cost & Availability Modeling

- Crow AMSAA model

  - Strategy to achieve desired level of reliability growth over series of developmental test cycles

  – Variety of failures discovered

    - Not all of equal severity or importance
    - Simplest method divides into two categories
      - A-mode – no corrective action taken
      - B-mode – corrective action taken

Model Assumptions

- B-mode failures
  - K – total number of failures (large unknown constant)
  - Each failure occurrence leads to system failure
    - Equivalent to series system
  - Failures discovered prior to end of testing cycle (T) subject to fix attempt by T

System failure rate and failure intensity

- As $K \to \infty$, expected failure intensity

$$\rho(T) = \lambda_A + \lambda_B \left((1 - \mu_d) + \frac{\mu_d}{1 + T} \right)$$

  - μ_d – Average success rate of corrective actions
  - λ_A – Rate of A-mode failures
  - $\sum_{i=1}^{K} (1 - d_i)\lambda_i$ – B-mode failure rate after corrective action
    - d_i – Fix effectiveness of i^{th} B-mode
  - $(\lambda_B - \sum_{i=1}^{K} \lambda_i)$ – unobserved B-mode failures

Reliability Investment

- Essential function failures (EFF) prevent fully mission capable (FMC) system

$$FMC = \prod_{i=1}^{n}(1 - EFF_i)$$

  - Similar to Crow's model of B-mode failures
- MTBEFF:= 1/expected failure intensity

$$M(T) := \rho(T)^{-1}$$

Cost vs. Time

- Cost and time required to achieve MTBEFF

$$\gamma(T) = \frac{1}{CV^2}(C_0 T + \mu_b \ln(1+T))$$

  - CV – Coefficient of variation in B-mode failures
  - C_0 – Cost to operate test, analyze, and fix (TAAF)
  - μ_b – Average value of cost increments incurred by corrective action

Subsystem MTBEFF as function of reliability investment

- Solving cost equation for time T_i and composing with MTBEFF provides direct relationship

$$M_i(T_i) = \lambda_{A,i} + \lambda_{B,i}\left(1 - \mu_{d,i} + \frac{C_{0,i}\mu_{d,i}}{\mu_{b,i}F^{-1}\left[\frac{C_{o,i}e^{\left(\frac{C_{0,i}+CV_i^2\gamma_i}{\mu_{b,i}}\right)}}{\mu_{b,i}}\right]}\right)^{-1}$$

  - $F(W) = We^W$ - Lambert W-function

Maximizing availability through reliability investment

- Steady state availability of subsystem i

$$A_i(T_i) = \frac{M_i(T_i)}{M_i(T_i) + \text{MTTR}_i}$$

  - MTTR_i - mean time to repair subsystem i
  - Treated as estimate of system or subsystem reliability

Availability and fleet size

- Average number of subsystem replacement over system lifecycle

$$P_i = \left\lfloor \frac{L}{M_i(T_i)} - \varepsilon \right\rfloor$$

- Average cost of initial subsystem i and replacements over system lifecycle

$$C_i = c_i * (1 + P_i)$$

- Average cost of n subsystem over system lifecycle

$$C_s = \sum_{i=1}^{n} C_i$$

Availability and fleet size (2)

- Number of systems that can be purchased and supported with budget B

$$\eta(\mathbf{T}) = \left\lfloor \frac{B - \sum_{i=1}^{n} \gamma_i(T_i)}{C_s} \right\rfloor$$

  - **T** - Vector of subsystem reliability investments
  - B - Total budget
  - C_s - Cost of n subsystem over system lifecycle

Average Procurement Unit Cost

- Simple subsystem level optimization model considering investment in reliability improvement

$$\min APUC(\mathbf{T}) = \min\left[\frac{\eta(\mathbf{T}) * C_s + \sum_{i=1}^{n} \gamma_i(T_i)}{\eta(\mathbf{T})}\right]$$

$$\text{such that } T_i > 0$$

  - Total cost = $\eta(\mathbf{T}) \times APUC$

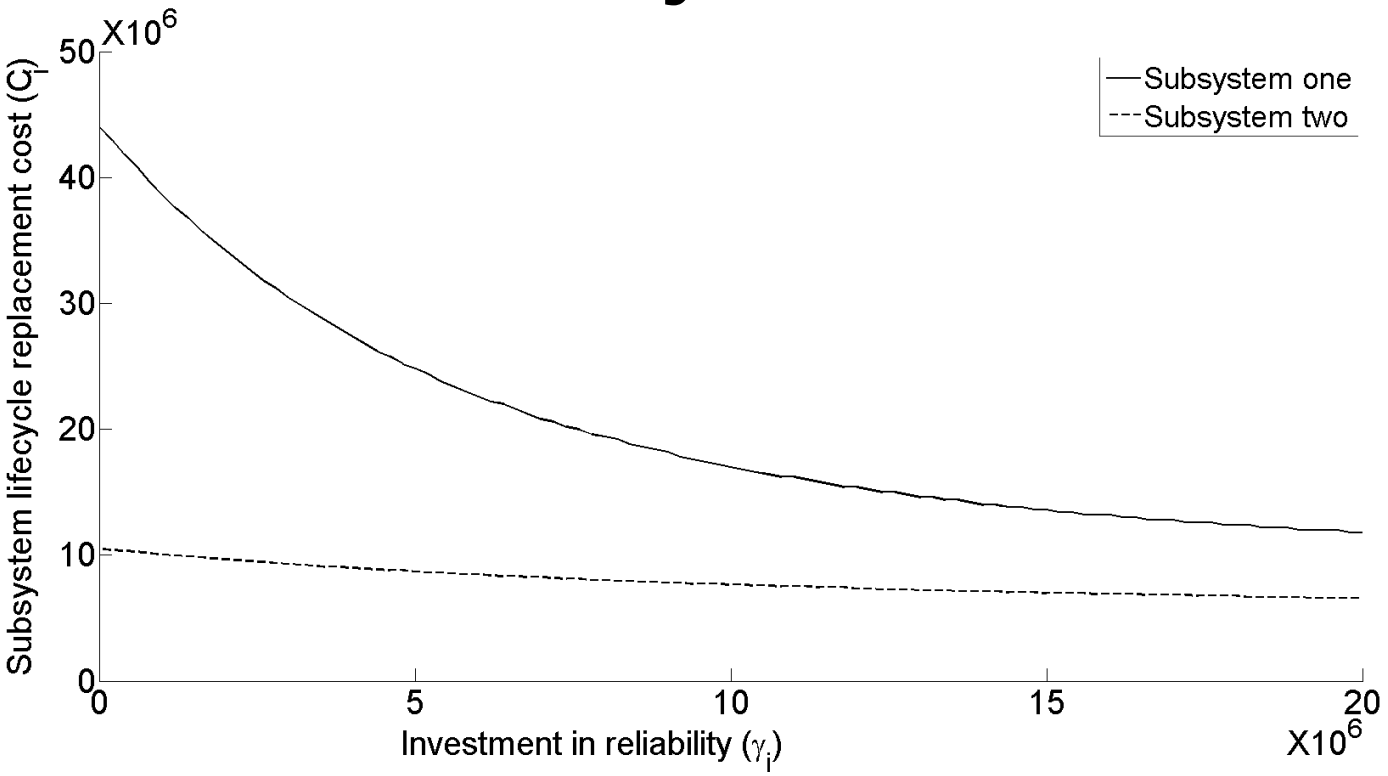
Illustrations

Subsystem Parameters

- $n = 2$ subsystems
- $B = \$1{,}000{,}000{,}000$
- $L = 20{,}000$ flight hours per vehicle

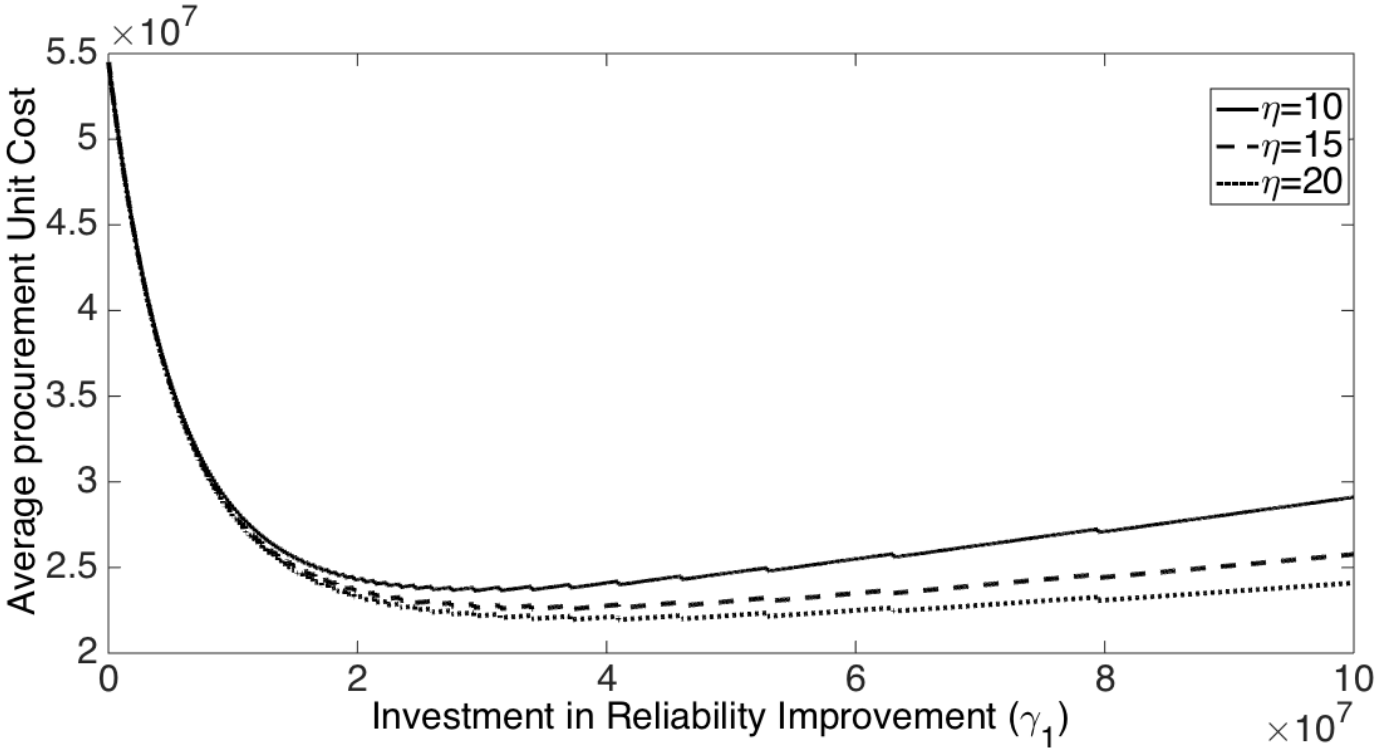
Parameters	**Subsystem** $i = 1$	**Subsystem** $i = 2$
$M_{A,i}$ (initial A-mode failure MTBEFF)	1,000 Hours	500 Hours
$M_{B,i}$ (initial B-mode failure MTBEFF)	100 Hours	200 Hours
$C_{0,i}$ (Cost of operating TAAF)	$1,000,000	$8000,000
$\mu_{b,i}$ (Cost of corrective action during TAAF)	$5,000,000	$4,000,000
$\mu_{d,i}$ (B-mode fix effectiveness factor)	0.9	0.8
c_i (Subsystem replacement cost)	$200,000	$75,000
$MTTR_i$ (Mean time to repair)	24 Hours	36 Hours

Impact of reliability investment on lifecycle cost



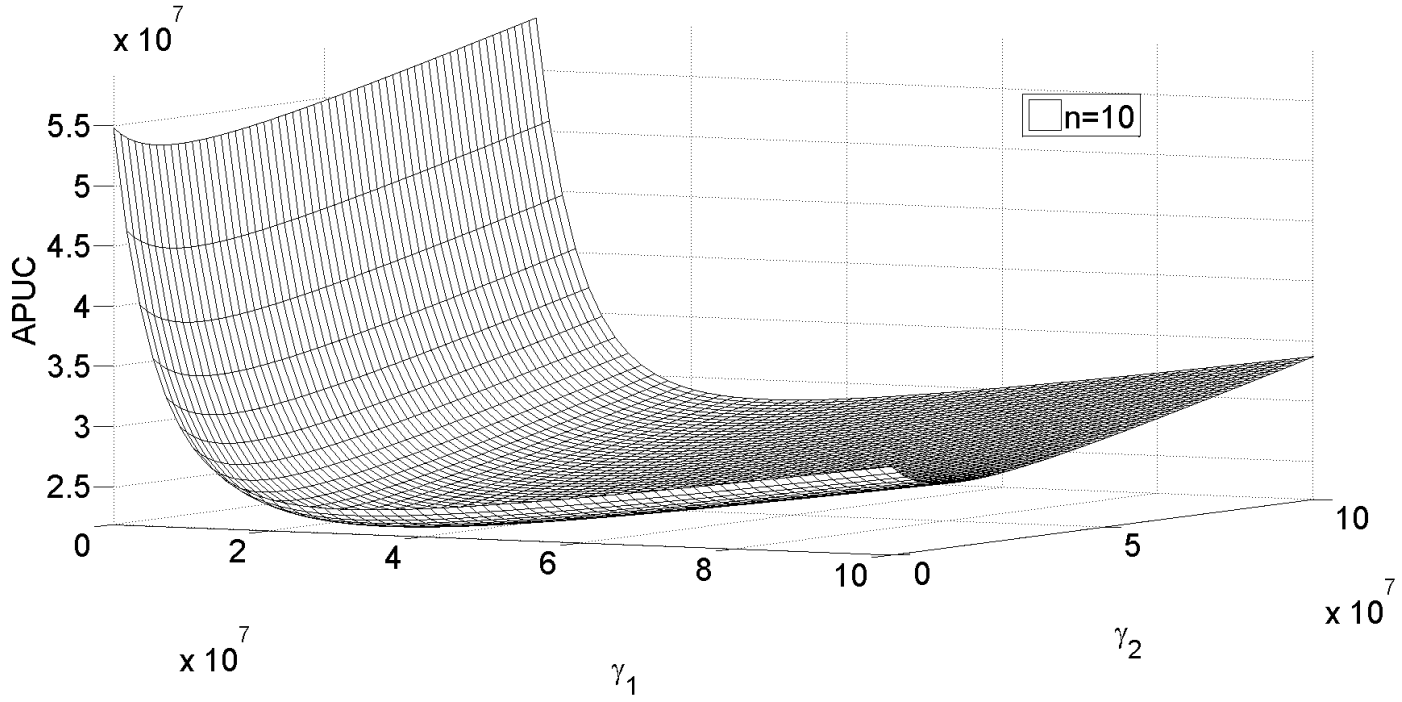
Investment in subsystem one could achieve greater part replacement cost savings over system lifecycle

Sensitivity of APUC to reliability investment



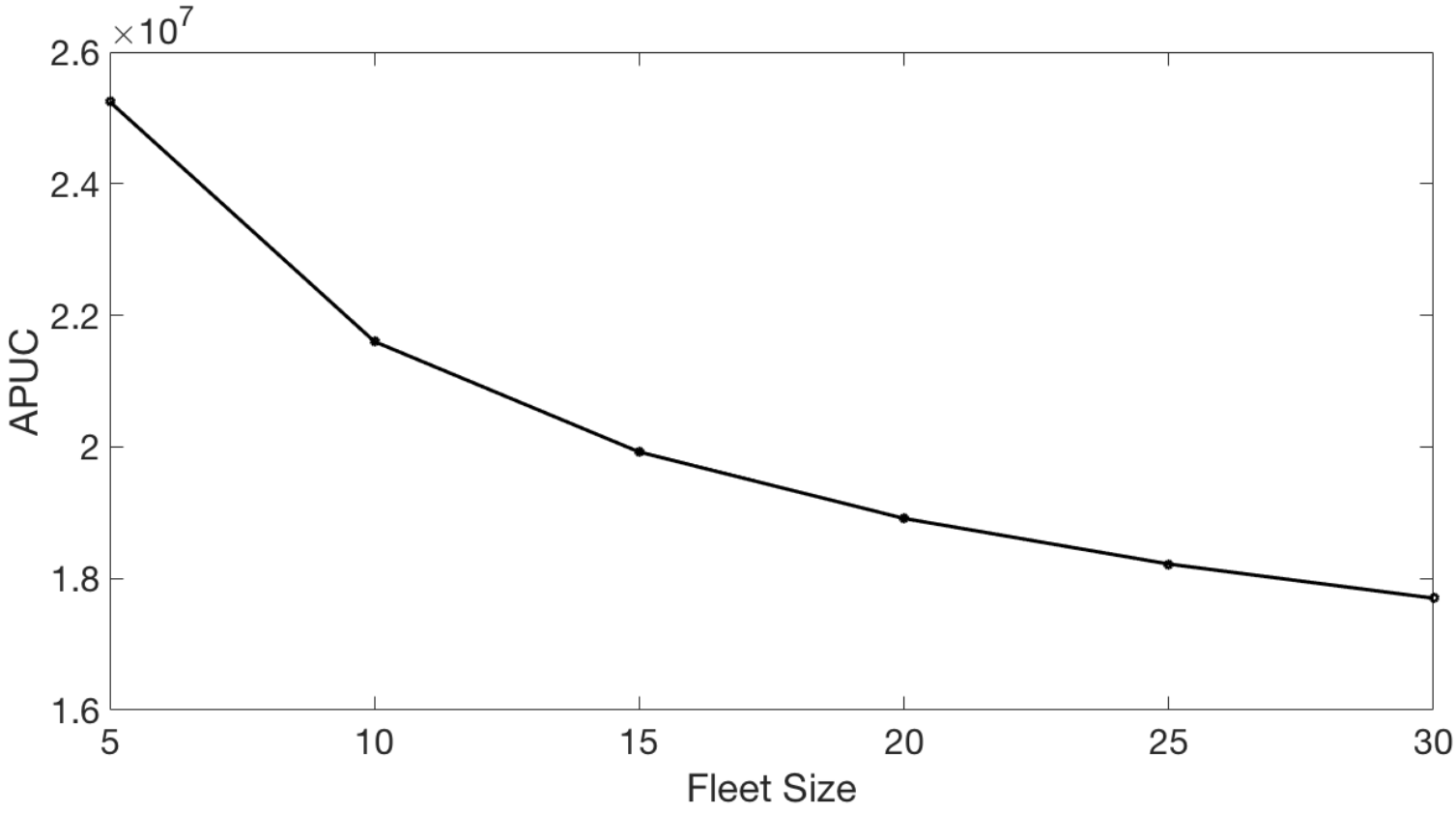
APUC decreases initially, but gradually increases as larger investments leads to little reduction in subsystem lifecycle cost

Impact of subsystem reliability investment on APUC



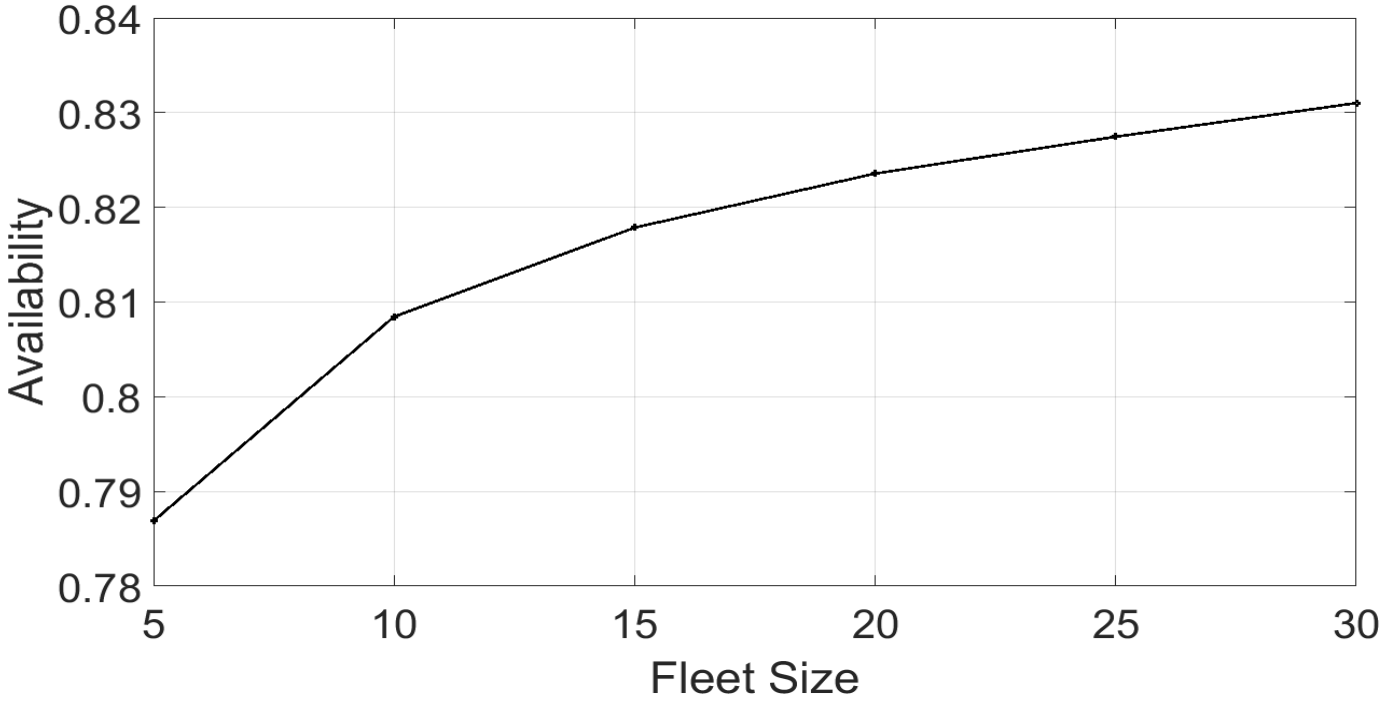
Optimal subsystem reliability investment strategy possesses unique minimum

Impact of fleet size on optimal APUC



Economy of scale decreases APUC as fleet size increases

Impact of fleet size on optimal availability



Increasing fleet size increases reliability investment and subsequently availability

Impact of fleet size on various parameters

η	APUC (10^6)	γ_1 (10^6)	γ_2 (10^6)	Unit cost (10^6)	Total Cost(10^6)	Availability
5	25.25	22.35	8.13	19.15	126.23	0.7869
10	21.60	29.34	15.66	17.10	216.00	0.8084
15	19.92	33.98	21.11	16.25	298.84	0.8179
20	18.91	40.95	24.81	15.63	378.26	0.8236
25	18.22	40.95	29.54	15.40	455.49	0.8275
30	17.71	46.00	33.52	15.05	531.02	0.8310
100	15.62	46.00	48.49	14.68	1562.00	0.8376
1000	13.79	79.45	93.15	13.63	1379.76	0.8422

Increasing fleet size decreases APUC and unit cost but increases reliability investment and total cost

Summary, Conclusions, Future research, and Acknowledgement

Summary and Conclusions

- Combine reliability engineering and TSE
  - Strategy to consider investment over long term
- Studies linking reliability investment and APUC could promote
  - Compromise between performance and non-functional reliability and affordability attributes
  - Reduce lifecycle cost and enhance affordability
  - Improve fleet availability
  - Identify trade off between fleet size, availability, and cost

Future Research

- Greater realism in cost modeling
- Validation through application to rotary wing aircraft in government databases
- Combine methodology with CATE and NDARC to enable rotorcraft TSE considering reliability and availability

Acknowledgement

- This research was supported by the US Army Research Laboratory (ARL) through the National Institute of Aerospace (NIA) under Grant award number C15-2A00-UMASS, sub award activity number 2A69-UMASS.



Analysis of Environmental Impacts on Military Systems

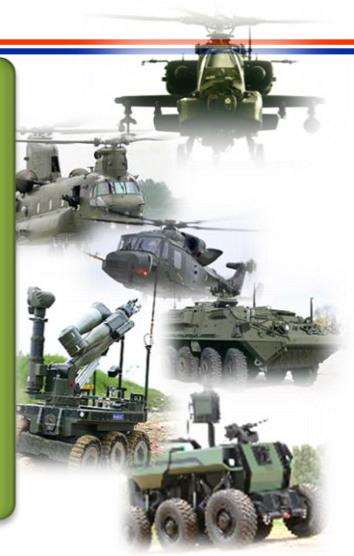
20th Annual NDIA Systems Engineering Conference
October 26, 2017

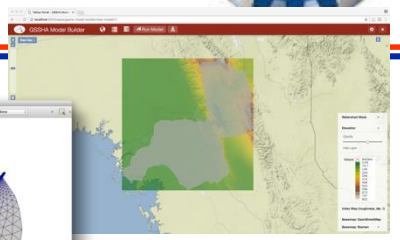
Dr. Dharhas Pothina
Associate Technical Director
US Army Engineer Research and Development Center

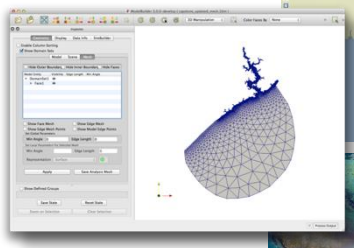
Environmental Simulation

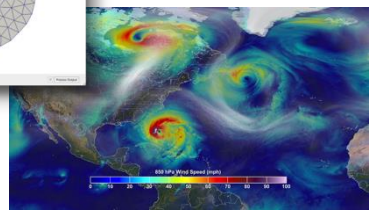
- Data Access/Archival
- Hi Fidelity Physics
- Tradespace Analytics
- Advance Computing Infrastructure

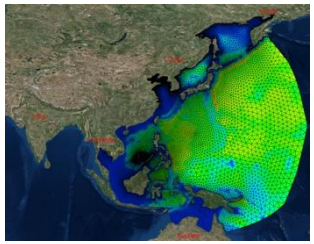
MILITARY SYSTEMS

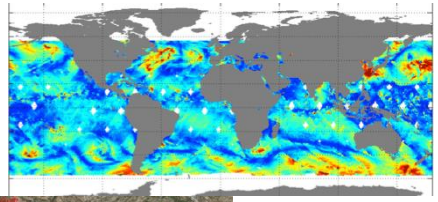


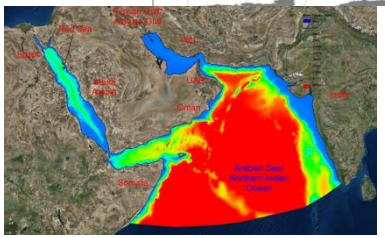




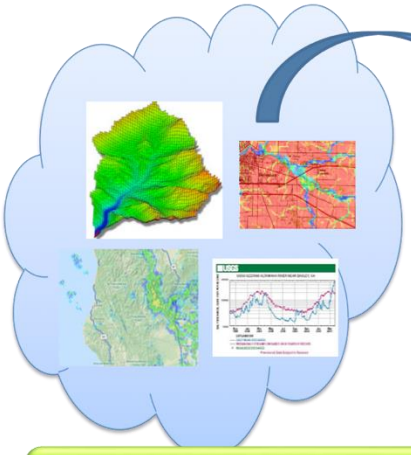




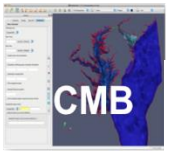




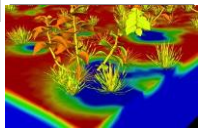
Met Office



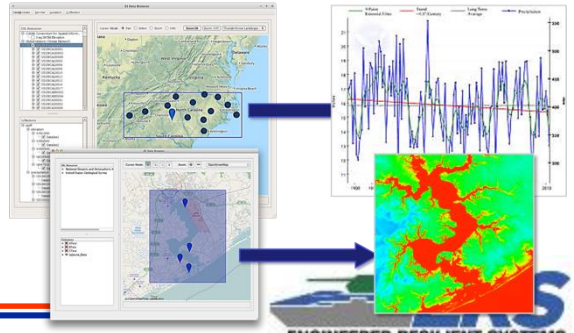










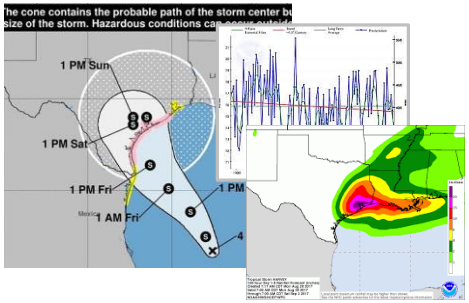


High Resolution Global Capability with Rapid Turn Around

Why

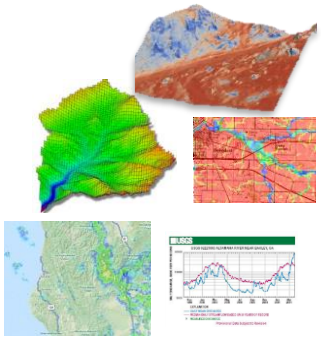
- **Gaps:**
  - DoD has an explosion of environmental data but access and retrieval is difficult
  - Demand within DoD for data has expanded but it is challenging to efficiently utilize
  - DoD lacks capability to produce high-fidelity, predictive, environmental physics for the entire globe to support operations and acquisitions
  - Data sources within the DoD have a scale and parameter mismatch (weather, terrain, etc.) for many classes of problems (operational, in-depth analyses, …)
- **ERS Approach:**
  - Develop a modular HPC enabled framework to discover, simulate, and retrieve environmental data
  - Develop high-fidelity scene generation and environmental simulation tools
  - Demonstrate modeling of environmental scenes worldwide
- **Leverage:**
  - DoD, federal, international, geospatial data, and environmental-modeling frameworks
  - Army ERS program
  - Studies directed by Army MSCoE, NVESD, PEO IEW&S, and others

Motivating Example: Hurricane Flooding

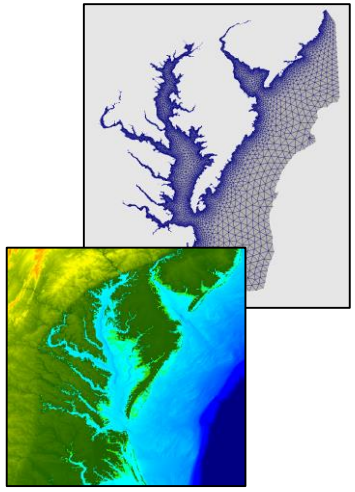


FORECAST SCENARIOS

Rapidly evaluate many forecast scenarios anywhere across the globe



ENVIRONMENTAL DATA



COMPUTATIONAL GEOMETRY



PHYSICS BASED SIMULATION ENGINES

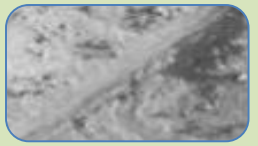
Temperatures

Soil Moisture

Inundation

Velocities & Depths

Use Cases



Sensors



Mobility



Fluid Structure Interaction

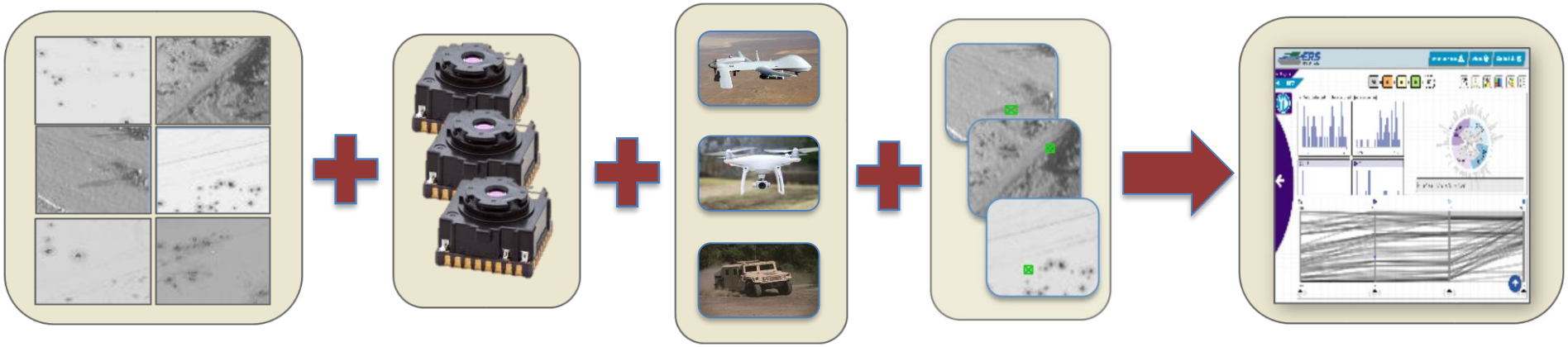
VIZUALIZATION & ANALYSIS

6 Months → Hours

Motivating Example: Sensor Virtual Proving Ground Workflow

Analyze Environmental Impacts

- Access **validated** geotypical simulations and real imagery
- Bring in notional Sensor / Automatic Target Recognition (ATR) Models
- Mount on arbitrary platforms
- Test existing sensors for probability of detection (PD) and false alarm rates (FAR) in new or different environments



VALIDATED ENVIRONMENTS | **SENSORS** | **PLATFORMS** | **TARGET RECOGNITION MODELS** | **TRADESPACE ANALYTICS**

Evaluate thousands of sensor/platform/environment combinations with validated physics

Desired Capability

A New Approach

Integrated Product

Powerful but heavyweight and inflexible, making it **hard** to:

- Adapt to new tasks
- Make use of available computing hardware
- Automate repetitive steps like parameter sweeping
- Create novel visualizations
- Add support for data larger than previously expected

Ad-Hoc Scientific Python

- Flexible by design
- Glue components together to make a workflow
- Components can be substituted/modified at will
- Flexible support for scaling up and out (Numba, Dask)
- Simple visualization via web browsers for local or remote sessions
- Solutions for big data viewed in browsers (Datashader)
- Emerging support for deploying notebooks as apps, dashboards

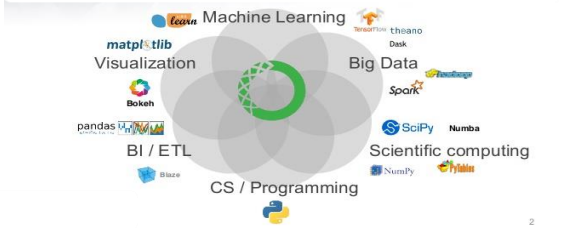
Can require excessive setup and programming and be complicated to deploy

Designing for Resiliency

- Modular Python wrapped components
- Flexible workflows
- Front end agnostic
- Scale to multiple architectures
- Enhance existing open tools when possible
- Utilize existing enterprise capabilities when available
- Use standards when possible/feasible but value simplicity over compliance

Notional Architecture

Open Data Science Ecosystem



ANACONDA ENTERPRISE

Rapid Application Development

python

ERS Quest

Stellar Science Galaxy

DASK

Stellar Science Galaxy

Spark



Scale

Workflow Automation

Enterprise Security
Secure Collaboration
Containerized Deployment

Frontends

jupyter



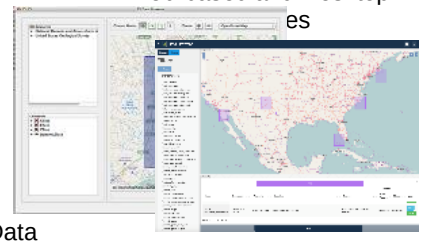
CMB

ERS Quest

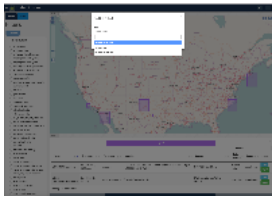
Search, download, and transform environmental data needed to set up high-fidelity, physics based models

- Extensible Plugin Architecture
- Python API
- Abstraction Layer
- Multiple Frontends
- Geospatial/Geotypical Search
- Data Catalog/Retrieval/Archival
- Data Transformation

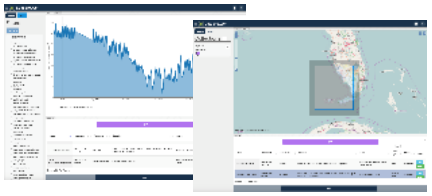
Web-based and Desktop

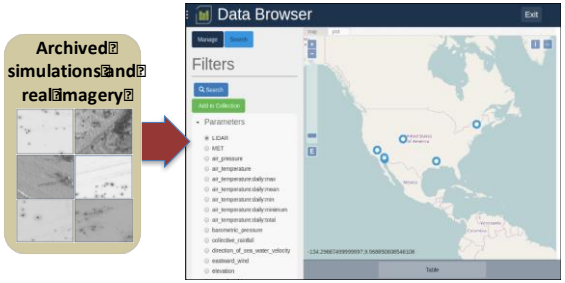


Transform Data



Visualize Time Series and Raster





Demo





ERS Quest



Collaborators

Environmental Simulator Team:

Kevin Winters
Scott Christensen
Aaron Valorosa
Gaurav Savant

ERDC Collaborators:

Integrated Simulation Environment Phenomenology (ISEP) Program

Industry Collaborators:

Anaconda Incorporated
Kitware Incorporated
Aquaveo

Questions



ERS NDIA
FUELING INNOVATION & COLLABORATION



Raytheon

The Language of Complexity: Ontology in Systems Design and Engineering

Raytheon Missile Systems

Abe Wu, Dr. George Ball, Dr. Kit Runge, Randy Ramsey, Nick Barrett, Todd Schneider, Dr. Cary Butler, Martin Kittrell

Oct 24, 2017

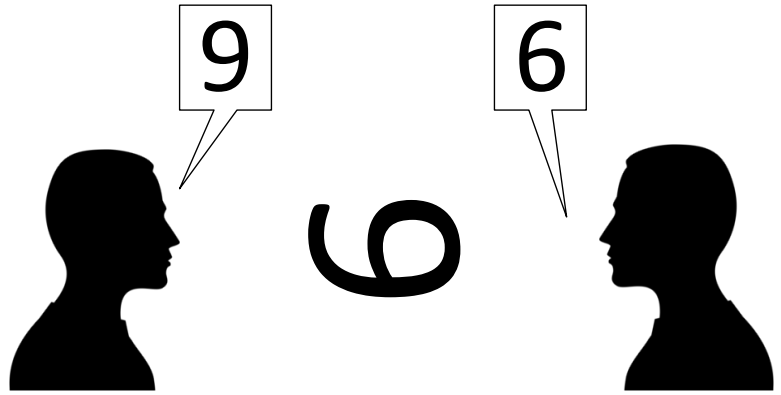
Copyright © 2017 Raytheon Company. All rights reserved.

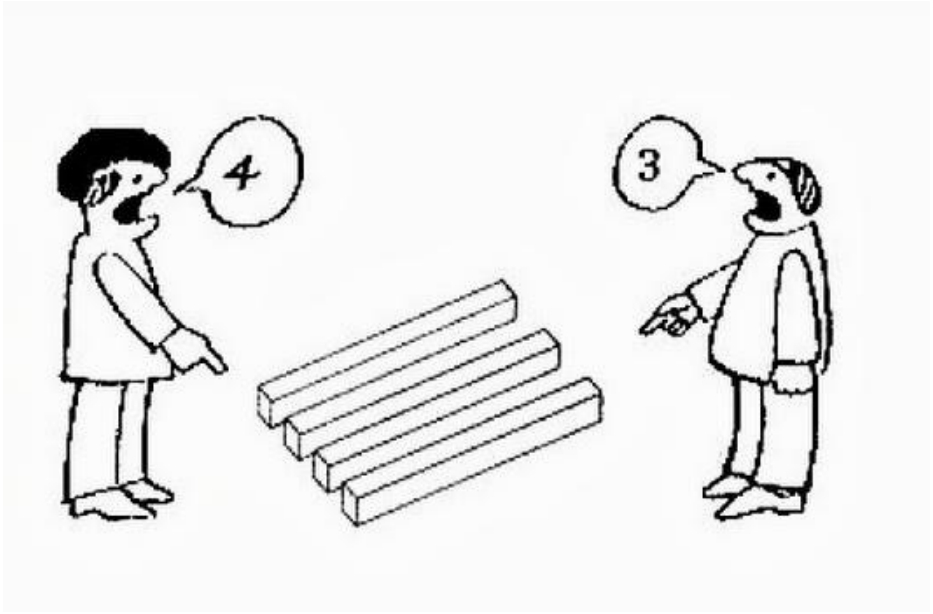
The Problem

Raytheon
Missile Systems

Toilet Out of Order

Use Floor Below



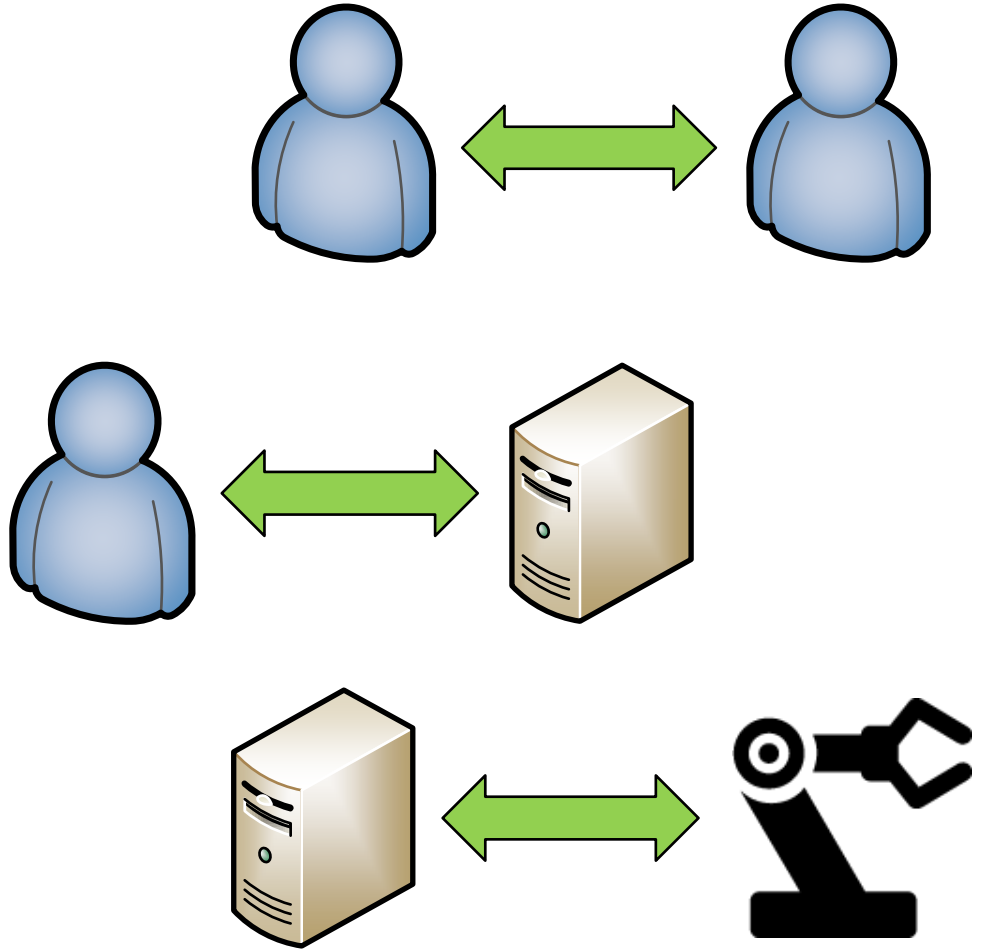


The Problem (cont'd)

Raytheon
Missile Systems

During Systems Development, how do we ensure we **consistently communicate** the **correct meaning** in language used between:

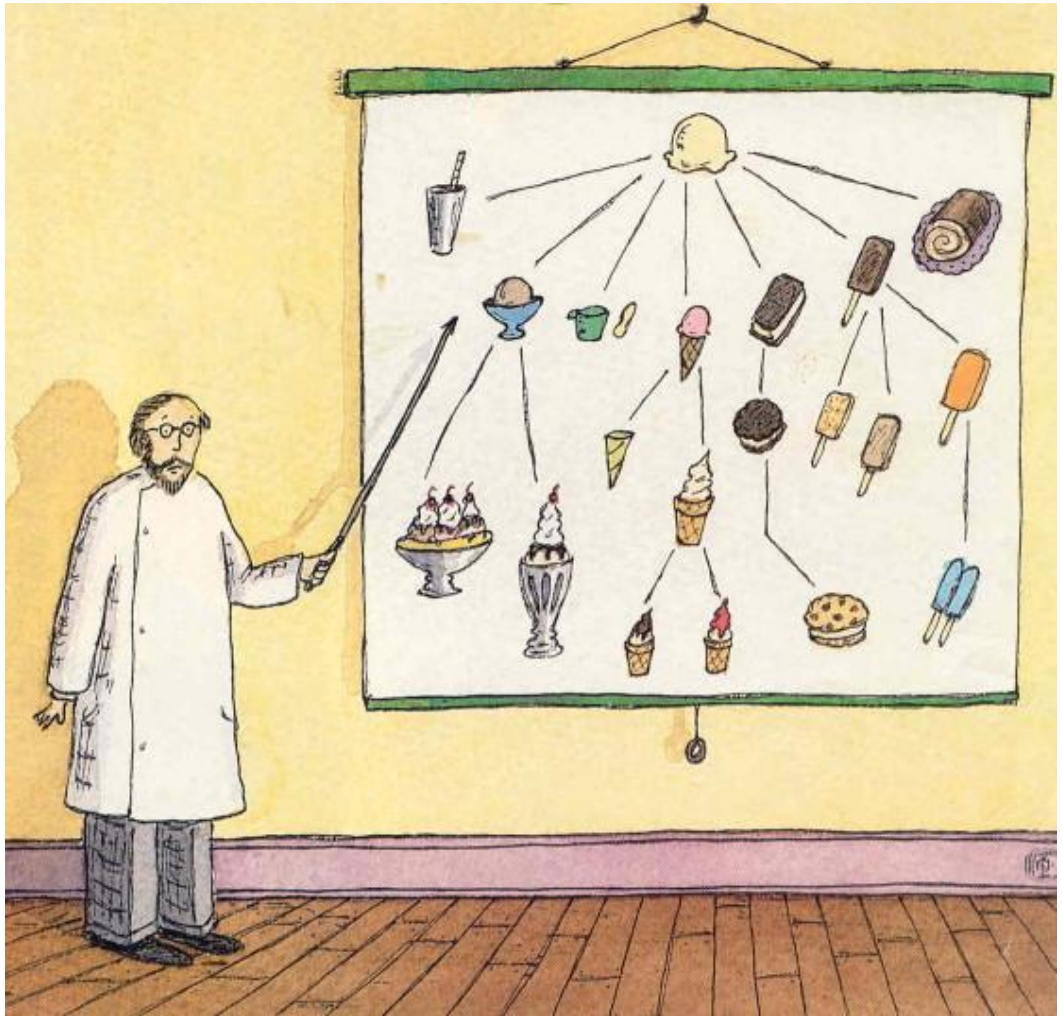
- humans & humans
  - across domains / disciplines
- humans & machines
- machines & machines



Without clear communication, we get cost overruns, delays, and rework.

What is an Ontology?

Raytheon
Missile Systems



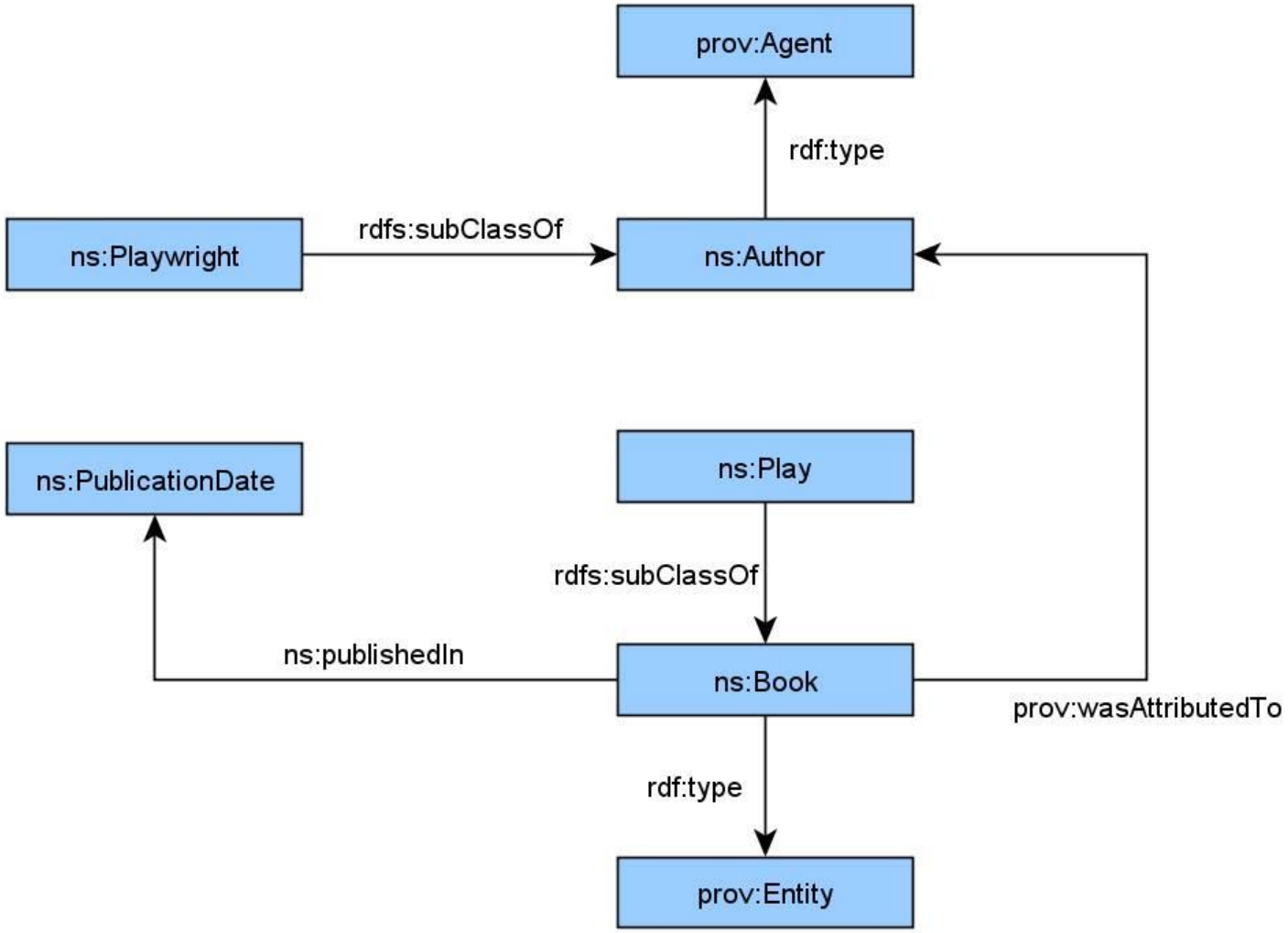
A formal specification of things, concepts, and the relationships between them, within some knowledge domain.

Describes:

- classes: abstractions of things
- individuals: the actual things themselves
- properties: relationships between individuals
  - includes constraints / restrictions on relationships

Written Works Ontology

Raytheon
Missile Systems



Why Ontologies?

Raytheon
Missile Systems

- Language disambiguation
- Well established technology
- Can model any system
- Formal relationships between objects
- Machine and human readable
- Reasoning / Inferencing engines
- Complex queries
- Information model to complement physics-based models







US Army Corps of Engineers®



















Industry Application

Raytheon
Missile Systems

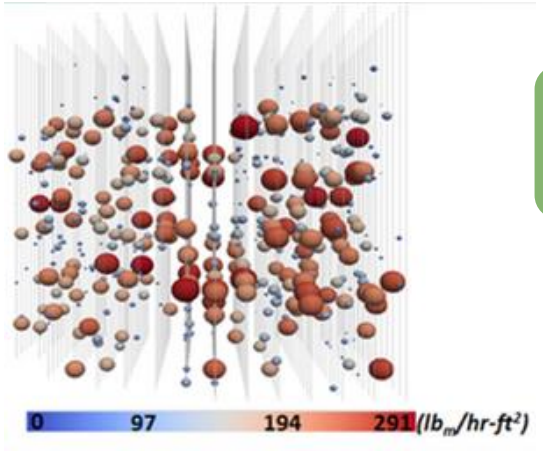


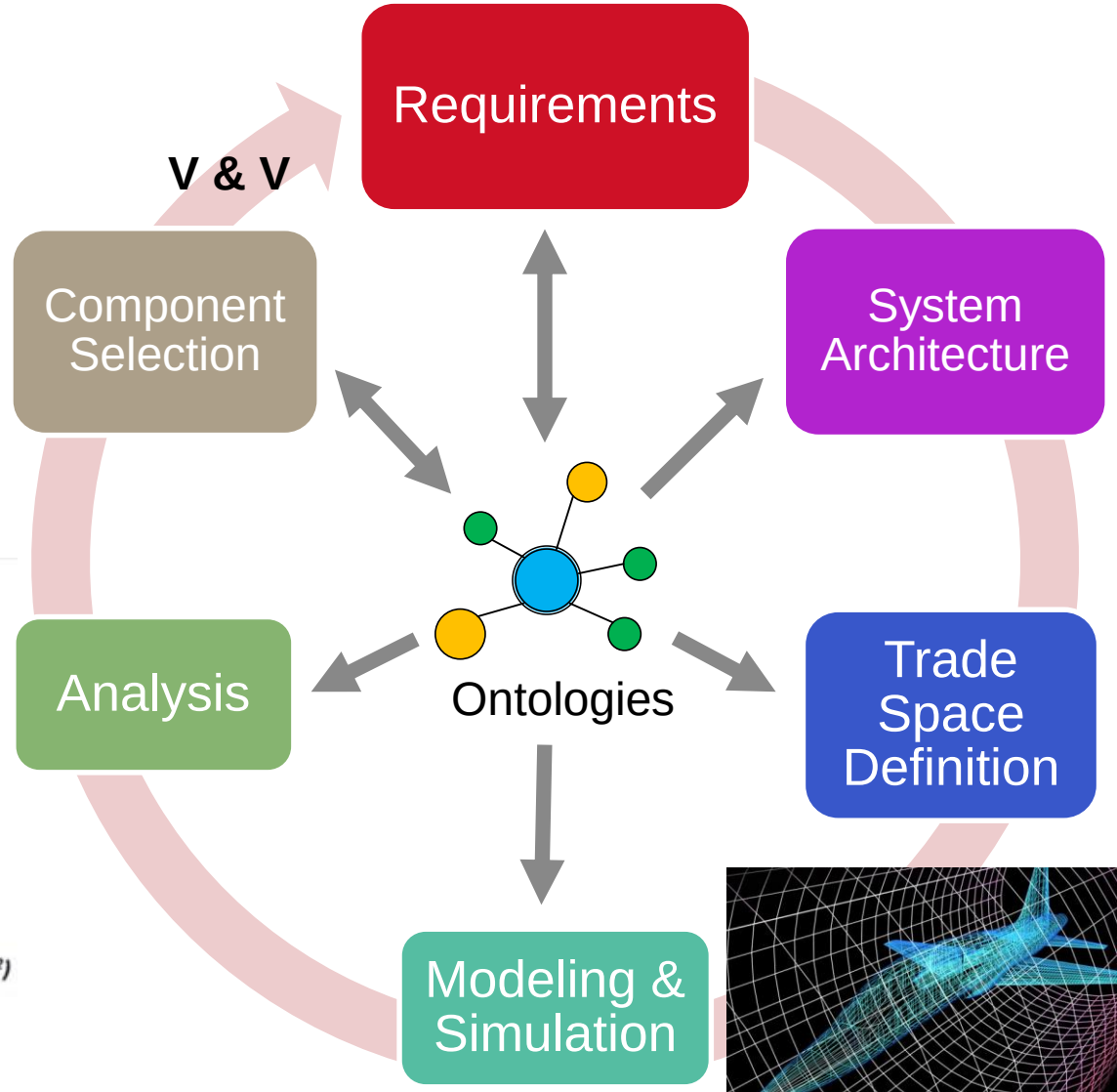
- Ford
  - Started developing ontologies to capture their manufacturing process in 1989 (Rychtyckyj, 1999)[3]
  - Digitized and standardized “process sheets”: vehicle assembly work instructions
  - Improved labor time estimation accuracy
  - Invested effort to rewrite ontology in a newer language, even with impact to production (Rychtyckyj, 2016)[4]

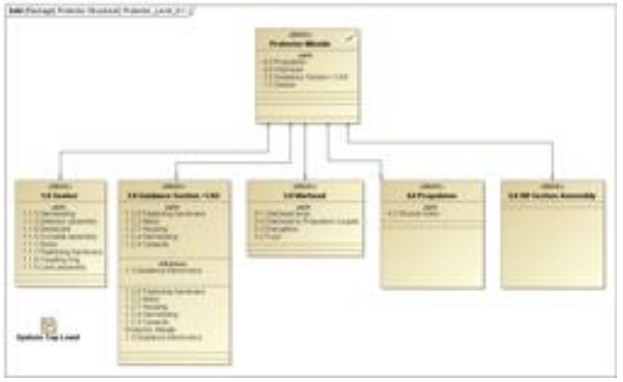
Design Process with Ontologies

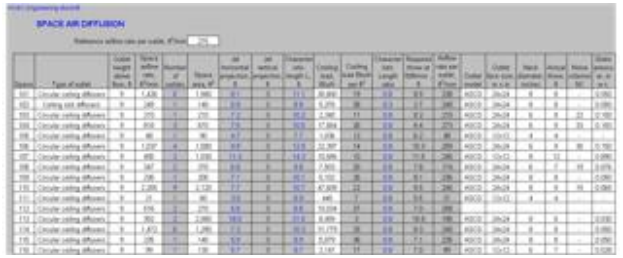
Raytheon
Missile Systems

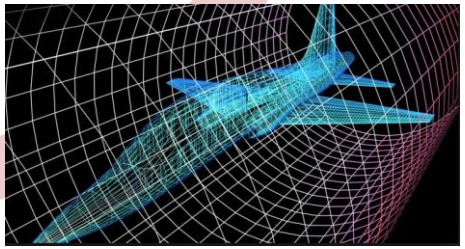






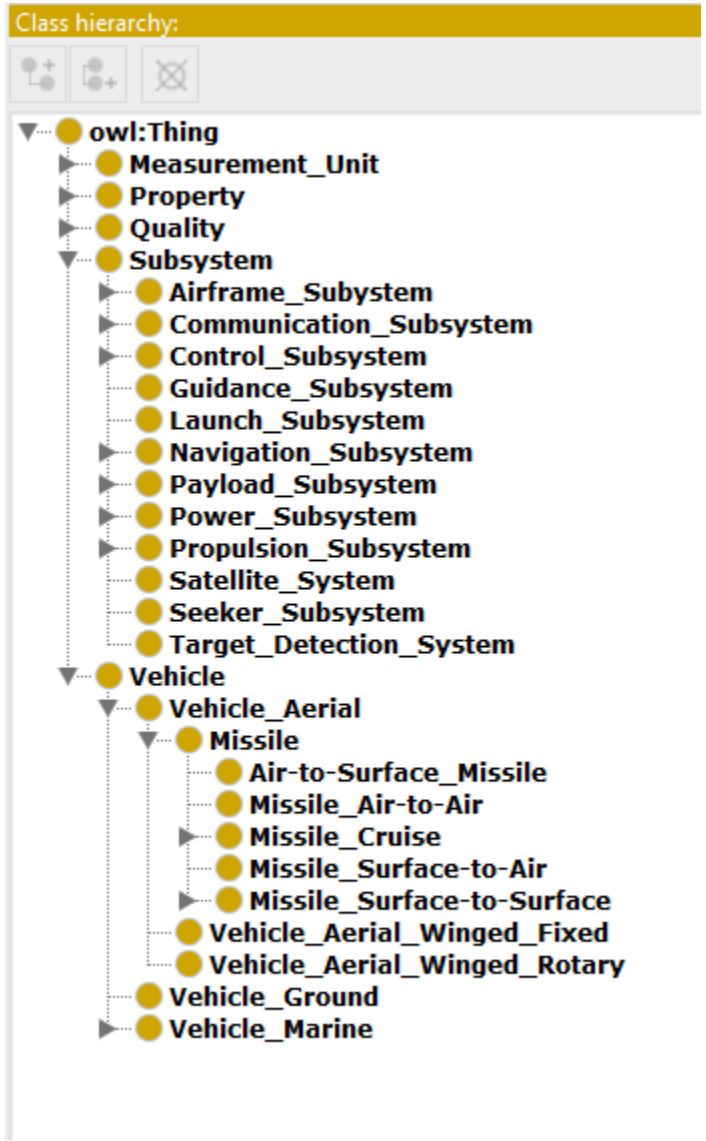


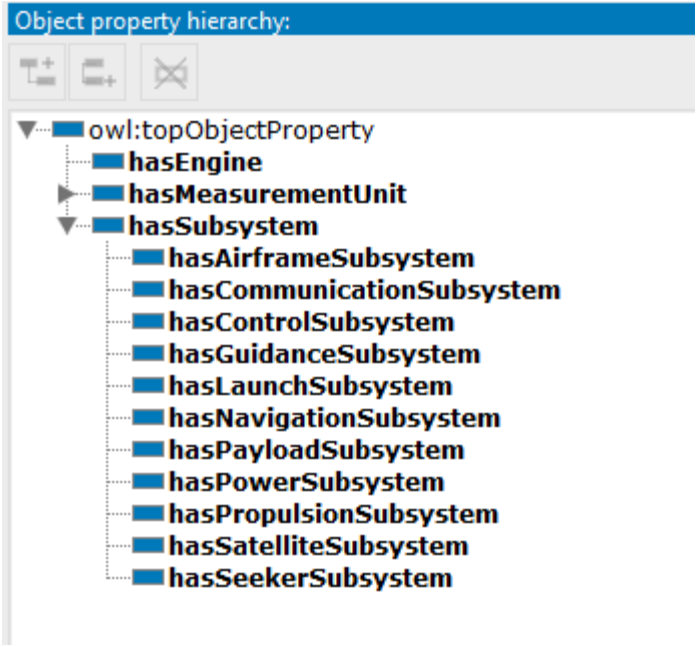


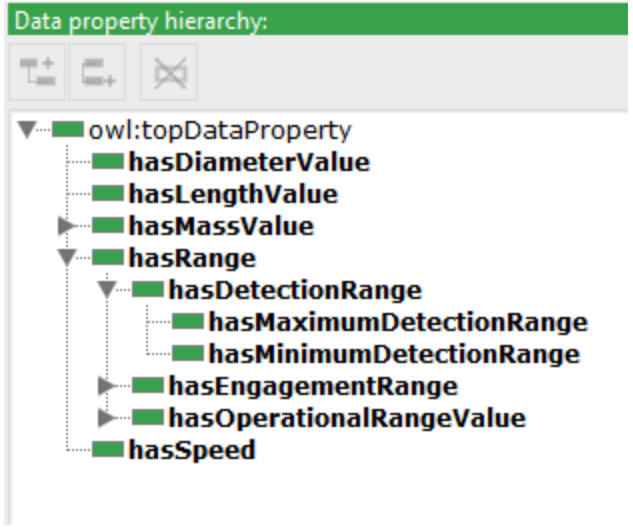


Domain Ontology

Raytheon
Missile Systems







Value Proposition to the DoD

Raytheon Missile Systems

- Improve acquisition process
  - Design products faster (Better Buying Power[5]).
  - Improve ability to compare competitive product proposals.
  - Evaluate a broader assessment of alternatives.
- Consistency among stakeholders
  - Ensure that the DoD's interpretation of requirements equals manufacturer's interpretation.
- Traceability
  - Allow for traceability of design decisions back to the requirements



Questions?

Raytheon
Missile Systems

References

1. Roz Chast, http://rozchast.com/cartoons_newyorker.shtml.
2. IBM developerWorks, 2012, Reification and Trust: Ontology-driven NLP.
3. Rychtyckyj, N. 1999. DLMS: Ten Years of AI for Vehicle, Assembly Process Planning. In *Proc. of AAAI'99/IAAI'99*, 821–828.
4. Rychtyckyj, N. 2016. Ontology Re-Engineering: A Case Study from the Automotive Industry. In *Proc. of AAAI'16/IAAI'16*, 3974-3981.
5. Better Buying Power

Contact Info

Raytheon Missile Systems

Abraham Wu

Raytheon Missile Systems

abraham.wu@raytheon.com

(520) 545-6544

Developing Standards for Systems of Systems (SoS) Engineering
IS0/IEC/IEEE 21839: SoS Considerations through the Lifecycle of a System

Dr. Judith Dahmann
The MITRE Corporation
jdahmann@mitre.org

Garry Roedler
Lockheed Martin
garry.j.roedler@lmco.com



Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Introduction

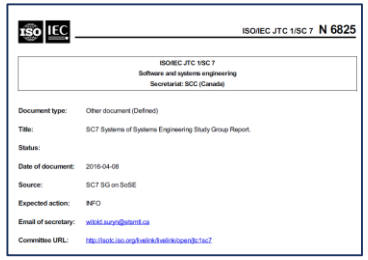
- Systems of systems engineering (SoSE) practice is maturing to the point that the International Organization for Standardization (ISO) has initiated the development of a set of SoSE Standards
- Following the recommendations of a 2016 Special Study Group on SoS Standards, three new work item proposals for SoS standards were approved and work has begun
- This presentation presents
  - The background on the new SoS standards development
  - Describes the new standards in development including the content and conclusions of the ISO Special Study Group report which provided the basis for the proposed new standards for SoSE
  - Discusses the three development activities particularly ISO/IEC/IEEE 21839

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

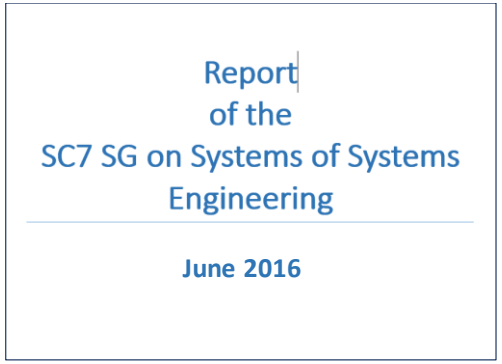
2016 Special Study Group on SoS Standards




ISO/IEC JTC 1/SC 7 N 6825

ISO/IEC JTC 1/SC 7
Software and systems engineering
Secretariat: SCC (Canada)

Document type: Other document (Defined)
Title: SC7 Systems of Systems Engineering Study Group Report.
Status:
Date of document: 2016-04-08
Source: SC7 SG on SoSE
Expected action: INFO
Email of secretary:
Committee URL:


Report
of the
SC7 SG on Systems of Systems Engineering

June 2016

- Study Group was chartered at SC7 Plenary in 2015
- Focused on
  - SoSE State of the Practice
  - SoS Applications
  - Current Standards
  - Recommendations for SoSE standards development
- Report was issued in June 2016

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Three SoSE Standard Developments

- ISO/IEC/IEEE 21839

  Systems and software engineering -- System of systems considerations in life cycle stages of a system

- ISO/IEC 21841

  Taxonomies of SoS Types

  - Elaboration of ISO/IEC 15288 Annex G)
  - Initial CD now complete and out for review

- ISO/IEC 21840

  Application of SE Processes for SoSE across the life cycle

  - Elaboration of ISO/IEC 15288 Annex G
  - Working draft out for review

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

ISO/IEC/IEEE 21839: Systems and Software engineering – SoS considerations through the lifecycle of a system

- Jointly developed with the IEEE Computer Society
- Based on work done as part of The Technical Cooperation Program (TTCP)
  - Technical Panel of Systems Engineering for Modernization which produced a guide to SoS Considerations for Engineering Systems.
  - This group is largely focused on defense systems but the guide has broad applicability
- Progress
  - June 2016: Working draft based on TTCP guide was circulated as part of the new work item proposal
  - September 2016: Kickoff of standard development
  - March 2017: Committee draft release for comment
    - Based on lifecycle stages in ISO 24748 – Systems and software engineering lifecycle management, part 1
    - Generalized beyond defense
  - September 2017: Updated CD released for comment

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Scope

- Provides a set of critical considerations to be addressed for systems created by humans
  - Concerns those systems that are man-made and are configured with one or more of the following: hardware, software, humans, procedures and facilities
  - Wide variety of systems in terms of their purpose, domain of application, complexity, size, novelty, adaptability, quantities, locations, life spans and evolution.
  - Applies to one-of-a-kind systems, mass produced systems, or customized, adaptable systems
- Addresses system of systems (SoS) considerations that apply to systems at each stage in the life cycle of a system
  - Aligned with ISO/IEC/IEEE 15288 and the ISO/IEC/IEEE 24748 framework for system life cycle stages and associated terminology
  - Selected subsets of these considerations may be applied throughout the life of systems
  - Accomplished through the involvement of all stakeholders
- This document does not detail
  - The approach to addressing system of systems considerations in terms of methods or procedures
  - The described documentation in terms of name, format, explicit content, and recording media of documentation.



Ultimate goal to achieve user satisfaction by ensuring that when delivered, the system will operate effectively in the operational or business environment which will typically be characterized as one or more SoS

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Key Definitions

system of systems

set of systems that interact to provide a unique capability that none of the constituent systems can accomplish on its own.

Note 1 to entry: Each constituent system is a useful system by itself, having its own management, goals, and resources, but coordinates within the SoS to provide the unique capability of the SoS.

[Source: ISO/IEC/IEEE 12070]

system life cycle

evolution with time of the system from conception through to disposal

[Source: ISO/IEC/IEEE 24748-1]

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Life Cycle Stages from ISO/IEC 24748 - Part 1

Concept	Development	Production	Utilization	Support	Retirement

Figure 1 -- Life cycle stages
(From ISO/IEC/IEEE 24748-1, Figure 5 – Representative life cycle model, page 15)

Table 1 – Life cycle stages, their purposes and decisions
(From ISO/IEC/IEEE 24748 -1, Table 1 An example of stages, their purposes and major decision gates)

LIFE CYCLE STAGES	PURPOSE	DECISION OPTIONS
CONCEPT	Identify stakeholders' needs Explore concepts Propose viable solutions	- Begin subsequent stage or stages - Continue this stage - Go to or restart a preceding stage - Hold project activity - Terminate project
DEVELOPMENT	Refine system requirements Create solution description Build system Verify and validate system	
PRODUCTION	Produce systems Inspect and test	
UTILIZATION	Operate system to satisfy users' needs	
SUPPORT	Provide sustained system capability	
RETIREMENT	Store, archive or dispose of system	

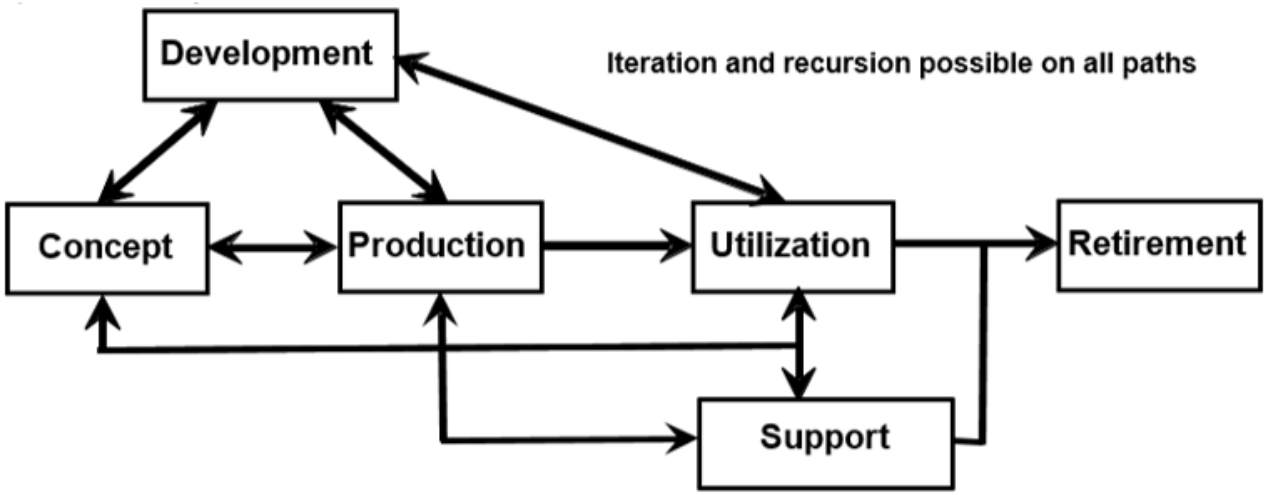


Figure 2 – Possible progress of life cycle stages
(From ISO/IEC/IEEE 24748-1, Figure 6 – Life cycle model with some of the possible progressions)

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Focus of 21839

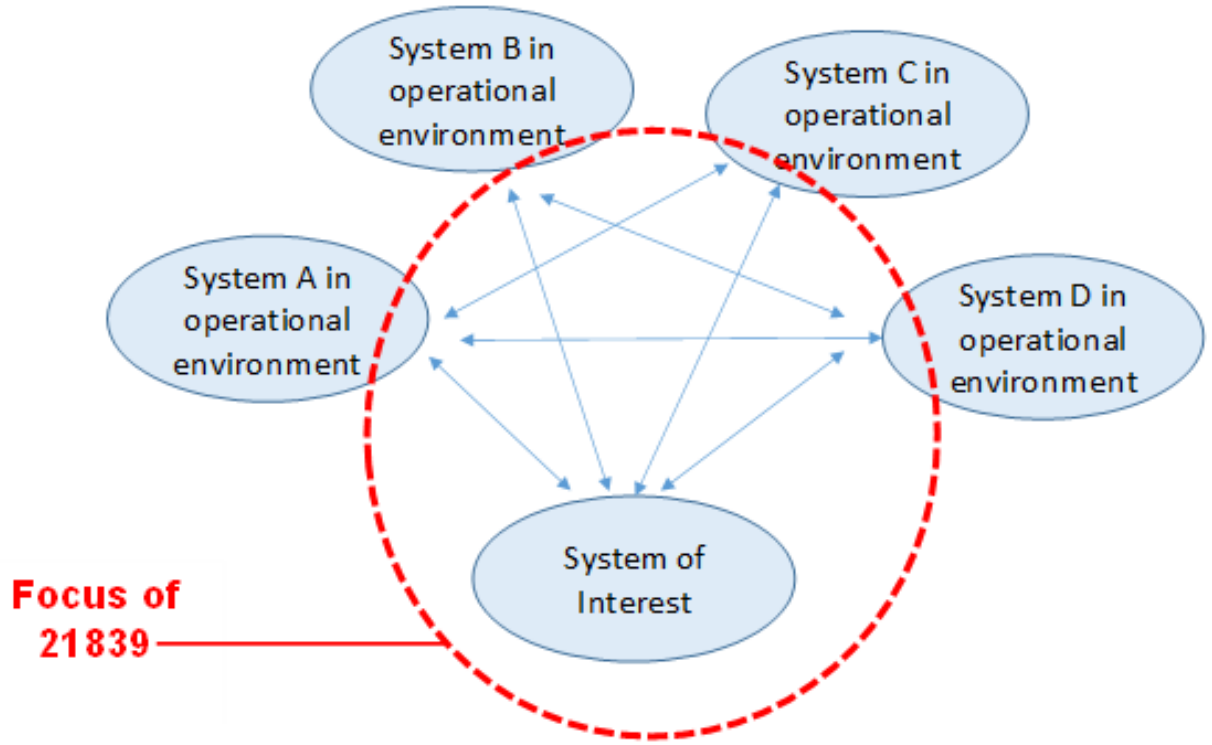


Figure 3: Focus of the document is on the constiuent system in an SoS

Focus is on constituent systems and their relationship to other systems in the one or more SoS where they will be deployed

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Three areas of SoS Considerations for Systems
Capability Considerations

- Capability refers to the ability to achieve user objectives in a mission or business context
- User capabilities are often based on the
  - Collective effects of multiple systems ('material') as well as other
  - Factors beyond the systems themselves (training, procedures, etc. or 'non-material')
- Typically, the development of a system begins with a user need based on a gap in needed capability and a proposed system focuses on filling that capability gap
- Consequently, right from the earliest point in a system life cycle, need a description of
  - Role of a new system in supporting the needed user capability
  - How the system is envisioned to function in the operational or business context
    - Including the constraints that context places on the system and the relationships, interfaces and dependencies with other systems supporting the capability.

Approved for public release. Distribution unlimited 17-3712-14
© 2017 The MITRE Corporation. All rights reserved.

Three areas of SoS Considerations for Systems
Technical Considerations

- To assess alternative approaches to address a needed user capability -- consider technical impacts on external stakeholders or systems affected by the proposed system, includes both
  - Systems/services on which the new or upgraded system depends and
  - Systems/services that depend on the new or upgraded system
- Once these have been identified, assess the ability to influence resource changes in associated systems, infrastructure, or nonmaterial factors
  - Constraints on the system are imposed by its SoS context -- consider these in selecting the system solution.
  - As the system moves into requirements definition and design, the technical considerations play a larger role

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Three areas of SoS Considerations for Systems Management Considerations

- Consider management issues when dependencies resulting from interactions need to be negotiated with other systems involved
  - Such as interfaces, new or changed functionality in other systems
- If there is an entity with some type of responsibility that spans an SoS, establish management arrangements with that entity
- SoS related cost and schedule considerations need to be addressed
  - Includes identifying costs and schedules associated with external systems
- Mechanisms should be in place to monitor progress in the areas of cross-system dependencies for prompt identification of any changes or delays which could mean added cost and time
  - Plans need to be formulated to accommodate these if necessary

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Document Structure

- Sections for each of the stages with considerations in each area as they apply to the stage

5 Recommended practices

5.1 SoS considerations in the concept stage

5.1.1 General

5.1.2 Capability considerations

5.1.3 Technical considerations

5.1.4 Management considerations

5.2 Addressing SoS considerations in the development stage

5.2.1 General

5.2.2 Capability considerations

5.2.3 Technical considerations

5.2.4 Management considerations

5.3 Addressing SoS considerations during production stage

5.4 Addressing SoS considerations during utilisation and support stages

5.4.1 General

5.4.2 Capability consideration

5.4.3 Technical considerations

5.4.4 Management considerations

5.5 Addressing SoS considerations in retirement stage

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Excerpt from Concept Stage Capability Considerations

Prior to entry into the **Concept Stage**, all available information should be evaluated to help ensure the understanding of the situation and identify any missing information . In particular, the following questions concerning the **capability being sought** and **the context of that capability** need should be addressed:

- Has the operational or business **context** of the capability gap (user need) been described?
- Has the **existing capability** been described, including the **systems that currently support** that capability?
- Have operational or business context constraints on potential solutions been identified?
- How would any new system which might address the gap **fit into current operations** or business processes?
- If a new system were to be considered, have **interfaces with or required changes to current systems or systems which are planned or in development been identified**?

An early description of the SoS context and its potential impact on system requirements and dependencies will provide a **solid basis for development of a system that will meet user needs, including quality characteristics. Identifying and addressing constraints are key to effective solutions**. Early identification of potential changes in interfaces or to other systems allow for **organizational negotiations** and agreements to be put in place as well **as multi-lateral trade-off analysis** of whether changes should be implemented and where changes can best be implemented. **Identifying these factors early** can contribute to a sound solution selection, including an understanding of risks. This is particularly important for any long lead items.

Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

Summary and Next Steps

- The second Committee Draft ISO 21839 is now in review
- Comments are due in early November
- Next step will be comment review and update

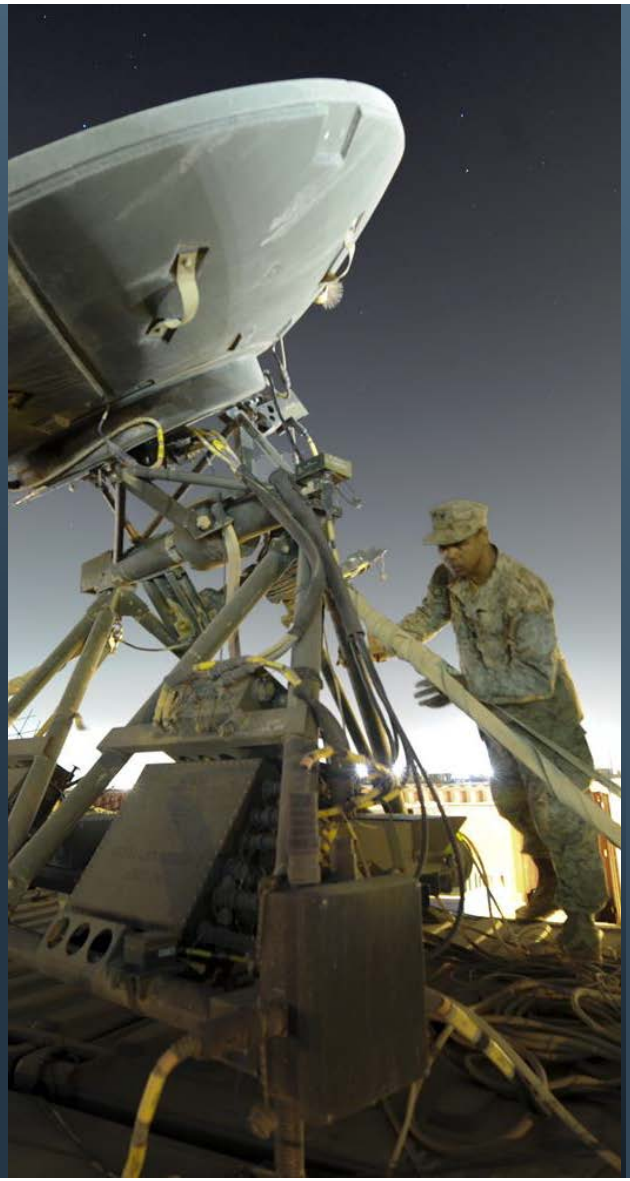


Approved for public release. Distribution unlimited 17-3712-14

© 2017 The MITRE Corporation. All rights reserved.

UNCLASSIFIED: Distribution Statement A. Approved for public release; distribution is unlimited.

Booz | Allen | Hamilton



A PRAGMATIC APPROACH TO SYSTEM MODELING FOR HAZARD IDENTIFICATION AND RISK MANAGEMENT

Michael J. Vinarcik, ESEP-Acq, OCSMP-Model Builder Advanced

2017 National Defense Industrial Association

Systems Engineering Conference

OCTOBER 26, 2017

UNCLASSIFIED: Distribution Statement A. Approved for public release; distribution is unlimited.

CONTACT INFORMATION

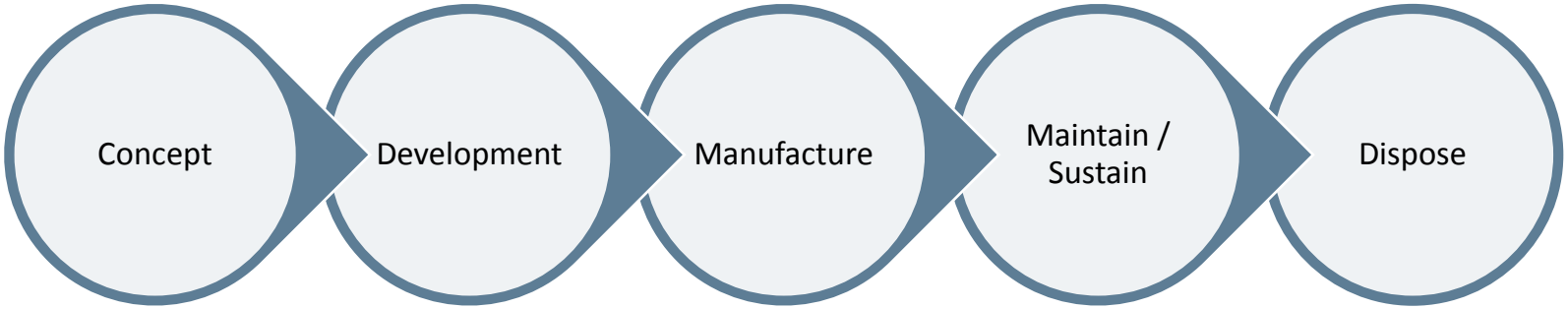
Michael J. Vinarcik

248-227-1659

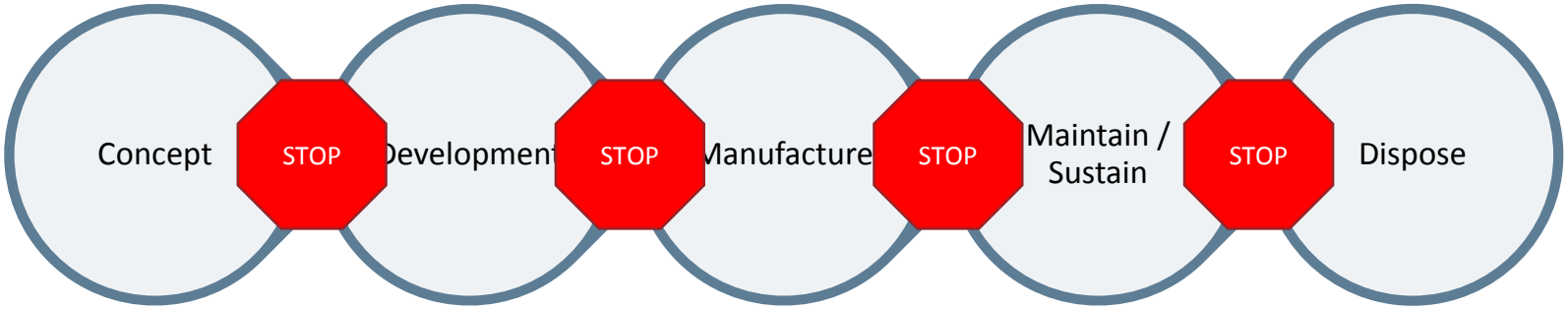
Booz Allen Hamilton

vinarcik_michael@bah.com

AN ABSTRACT VIEW OF PRODUCT DEVELOPMENT



AIR GAPS



Fidelity and momentum is lost every time there is a handoff; this is caused by the “air gaps.”

INDUSTRIAL AGE VS. INFORMATION AGE

"Our current defense acquisition system applies industrial age processes to solve information age problems."

- LtGen Robert D. McMurray, AFLCMC/CC
  Keynote address
  2017 Wright Dialogue With Industry Conference,
  Dayton OH, 18 July 2017

YOU HEAR THAT, MR. ANDERSON? … THAT IS THE SOUND OF INEVITABILITY…

Agent Smith, *The Matrix*

DIGITAL ENGINEERING

- The Department of Defense is developing a strategy to transform its end-to-end acquisition process.
- It is expected to be released for use by 2019.
- This presentation will focus on methods that ESOH professionals can use to smoothly integrate their efforts with digital engineering.
- The following four slides are extracted from another presentation here at the NDIA SE Conference; please seek out Ms. Philomena Zimmerman or her team for more information.
- I have indicated where this presentation supports the strategy.



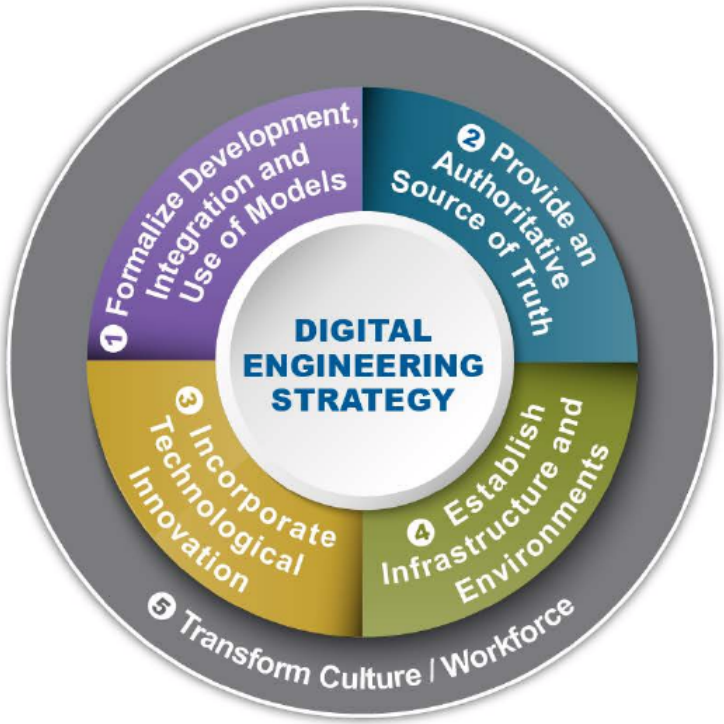
DoD Digital Engineering Strategy

Ms. Philomena Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense
for Systems Engineering

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited..

Digital Engineering Strategy: Five Goals

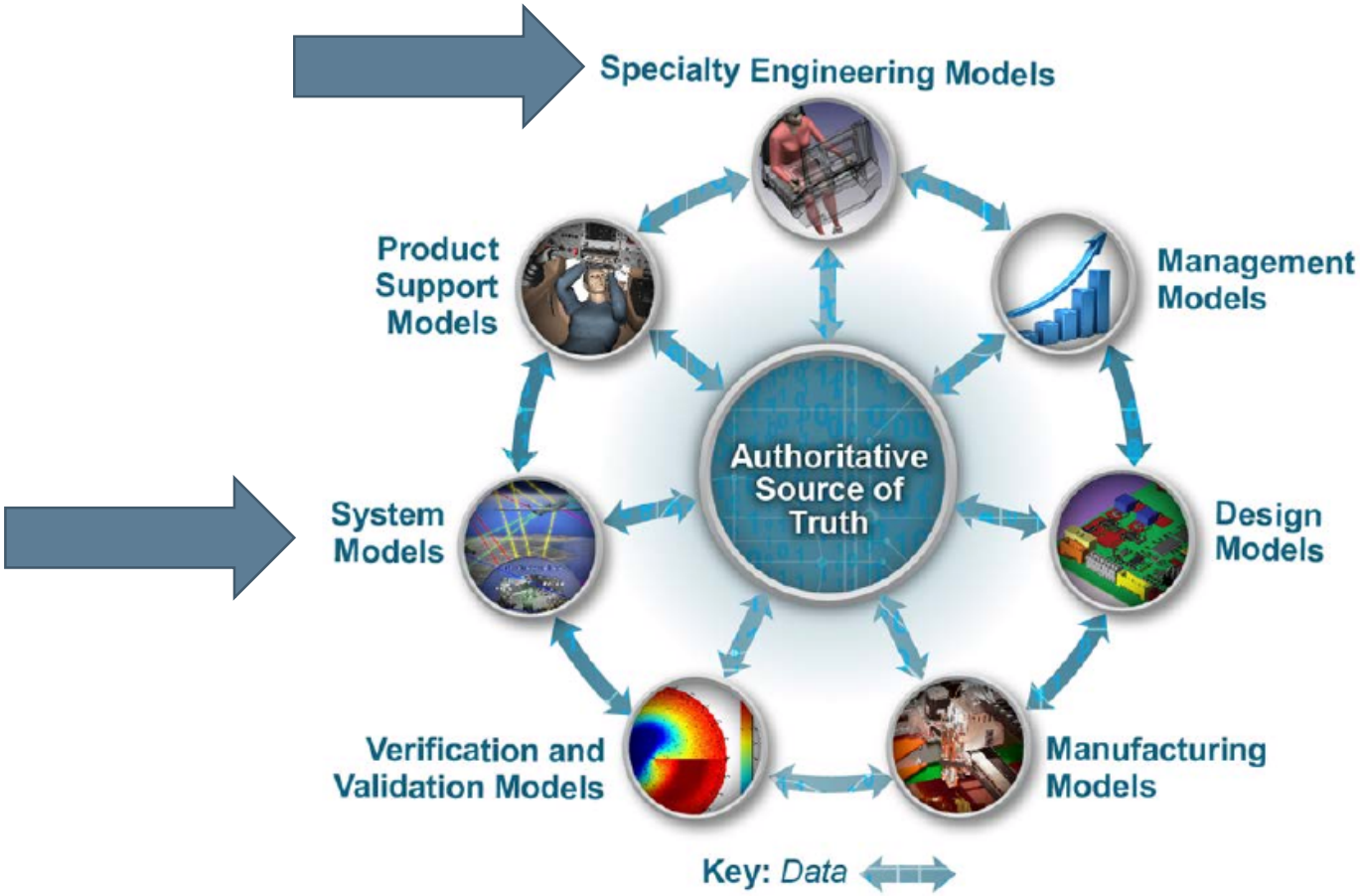
1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** 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

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

Goal #1: Formalize Development, Integration & Use of Models



Models as the cohesive element across a system's lifecycle

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

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

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

SYSTEM MODELING

- System modeling is emerging as a way to manage the inherent complexity of modern systems by providing a mechanism to store, manage, and associate information about a system under development.
- This information can then be extracted and presented to stakeholders in formats relevant to them.

Models grow organically as detail is added with no loss of fidelity.

from *Modeling Safety and CyberSecurity Controls in SysML,* 2016 NDIA Systems Engineering Conference, Vinarcik

SYSML: THE SYSTEMS MODELING LANGUAGE

- SysML is the most widely-adopted modeling language and has a thriving tool ecosystem.
- A well-constructed system model unambiguously represents a system's behavior, structure, and interrelationships between elements.
- Its flexibility allows integration of other discipline-specific analyses
  - Reliability
  - Safety

BENEFITS OF INTEGRATION

- Eliminating other tools from the analysis chain pays dividends:
  - Reduction in license costs
  - Elimination of interface/integration
  - Improved visibility to all stakeholders
  - Common language and understanding

Reduce lag and drag!

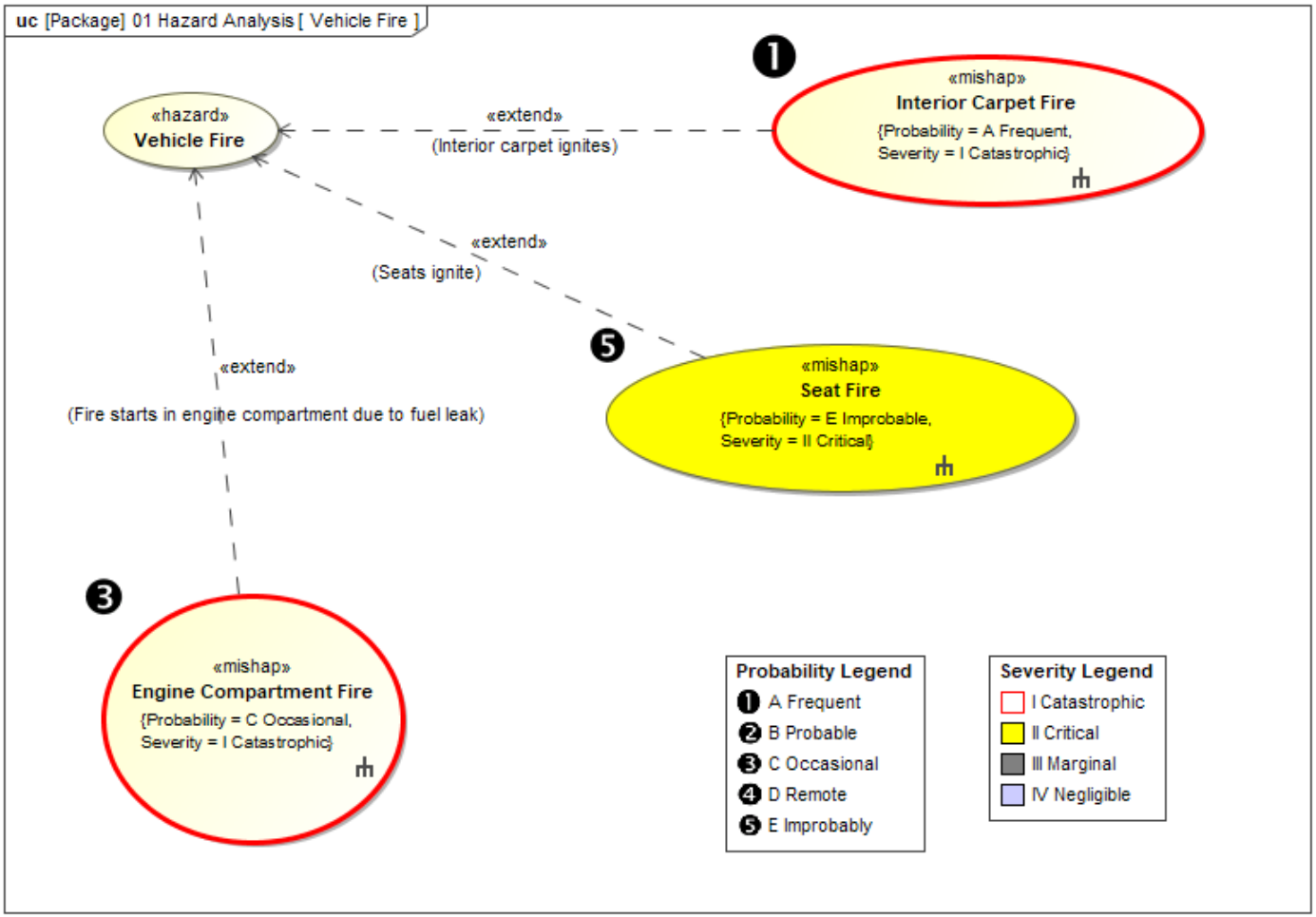
AN EXAMPLE: NOTIONAL PASSENGER AUTOMOBILE

- An unclassified, non-DoD example was needed for this presentation.
- A notional automobile is used as the basis for this example, which uses “fire” as the hazard.
- Note: I am not an ESOH professional and this is provided as an example of one approach to integrate ESOH into an evolving system model.

A REQUIRED MINDSET SHIFT

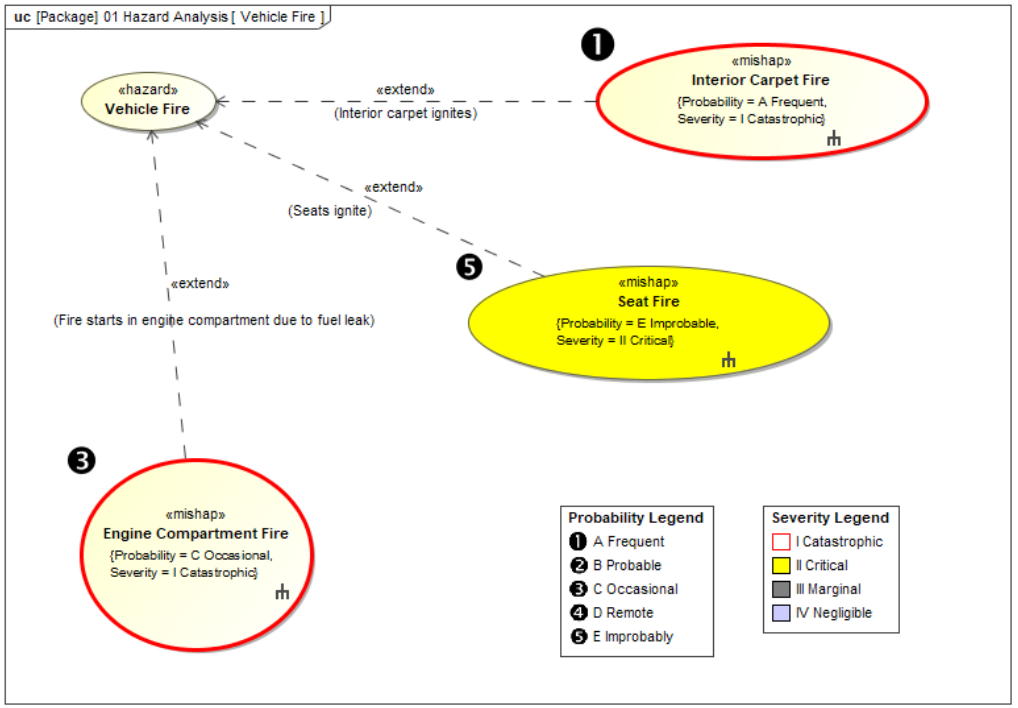
- To successfully leverage SysML, any user must understand that it is not “about” the diagrams.
- What is truly important is:
  - Elements and their properties
  - Relationships, their properties, and what they connect
- Once you see analyses in these terms, representing them in a system model is much easier.
- The collection of elements (including logic/branching elements) permits a rich description of system behavior, structure, interfaces, and parametrics.

NOTIONAL HAZARD ANALYSIS



HAZARD ANALYSIS: ELEMENTS USED

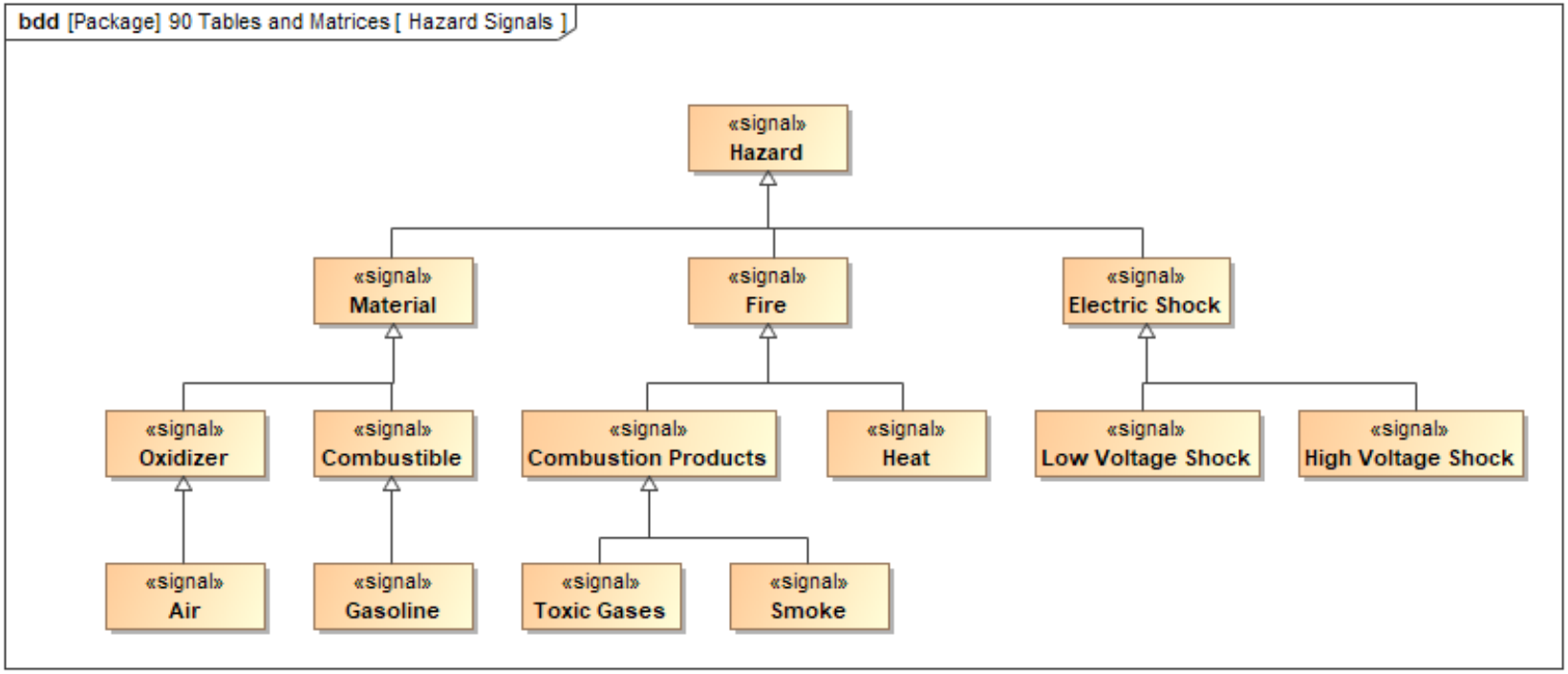
- *Use cases* with <<hazard>> and <<mishap>> stereotypes
- *Extension points* as causal factors
- <<extend>> relationships between mishaps and hazard
- Dynamic legends (color, fill, and icons based on properties of the elements)



WHY USE CASES?

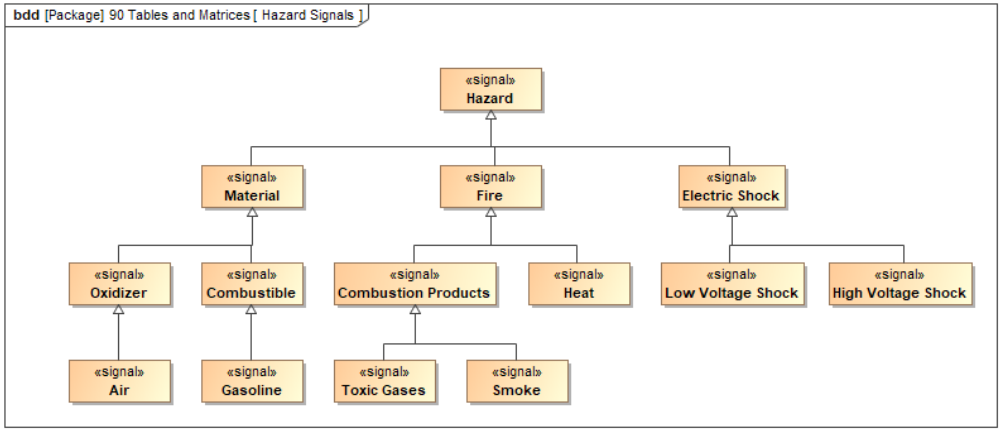
- *Use cases* are convenient SysML representations of behavior. They include:
  - *<<extend>>* relationships for conditional triggering of alternate *use cases*
  - They may be decomposed by activity diagrams

HAZARD SIGNALS

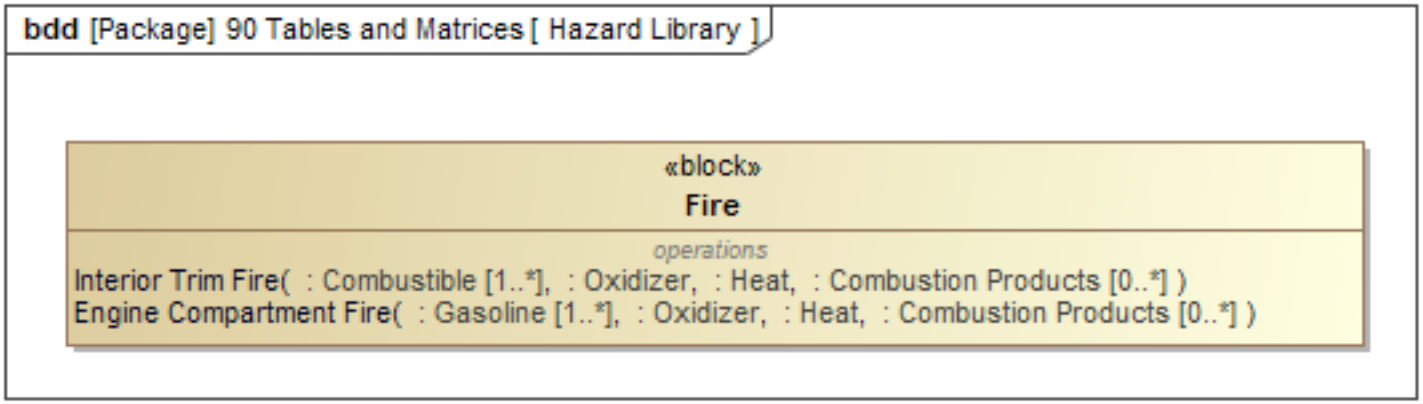


SIGNAL USAGE

- <<signals>> are used to type flow properties on interfaces, content conveyed on flows, and input/output parameters
- This hierarchy allows more specific signals to be used to satisfy more general input/output parameters

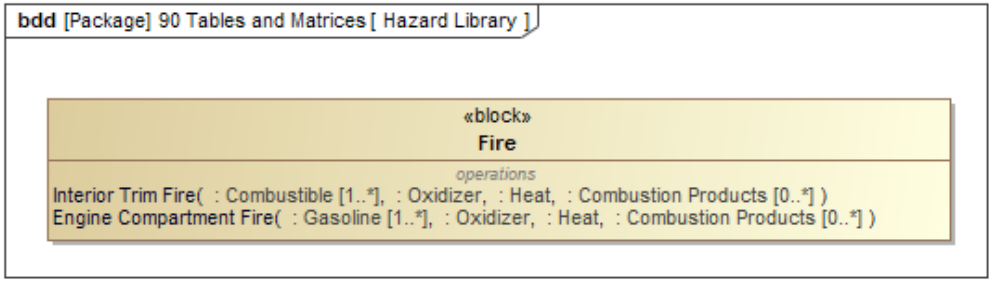


HAZARD BLOCK



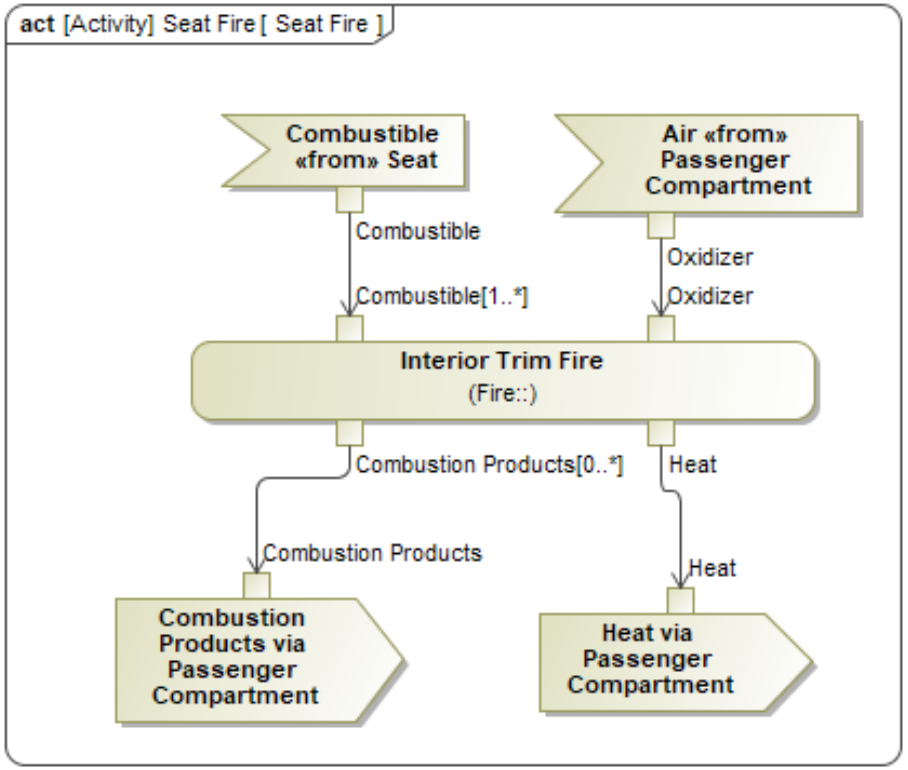
HAZARDS AS OPERATIONS

- <<operations>> own input/output *parameters*
- In this case, an Interior Trim Fire requires at least one combustible, an oxidizer, and generated heat and may generate combustion products (smoke, toxic gas, etc.)



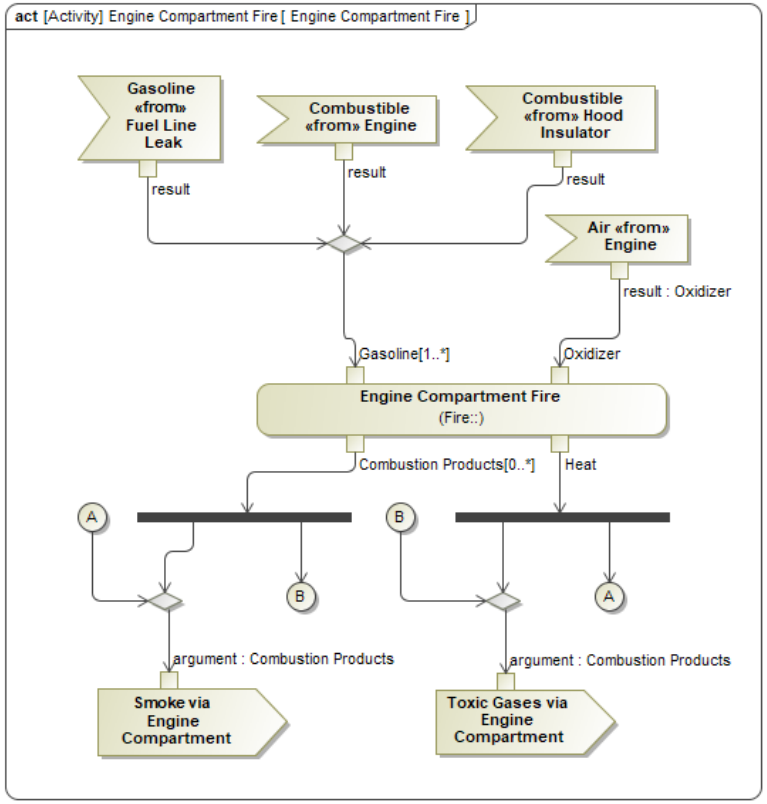
MISHAP DECOMPOSITION

- This activity diagram shows the operation an its input/output *parameters*.
- Each *pin* must be connected (no unconnected pins).
- This forces the analyst to identify the source and destination of all inputs and outputs.
- *Flow final* nodes may be used if there is no output of interest.



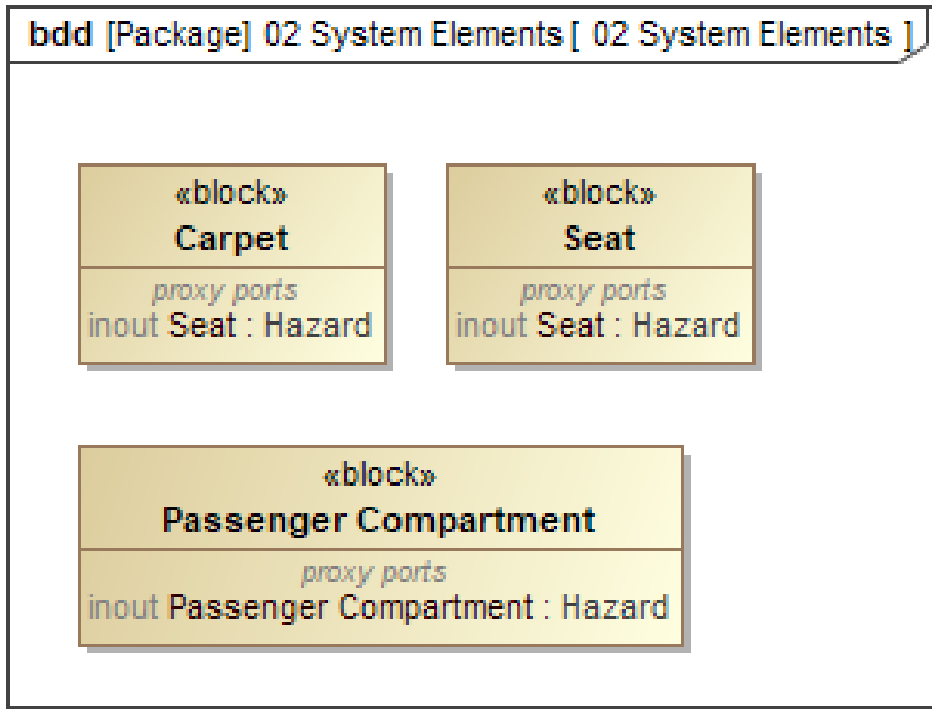
ENGINE COMPARTMENT FIRE

- Note the more complex logic and multiple sources for inputs.



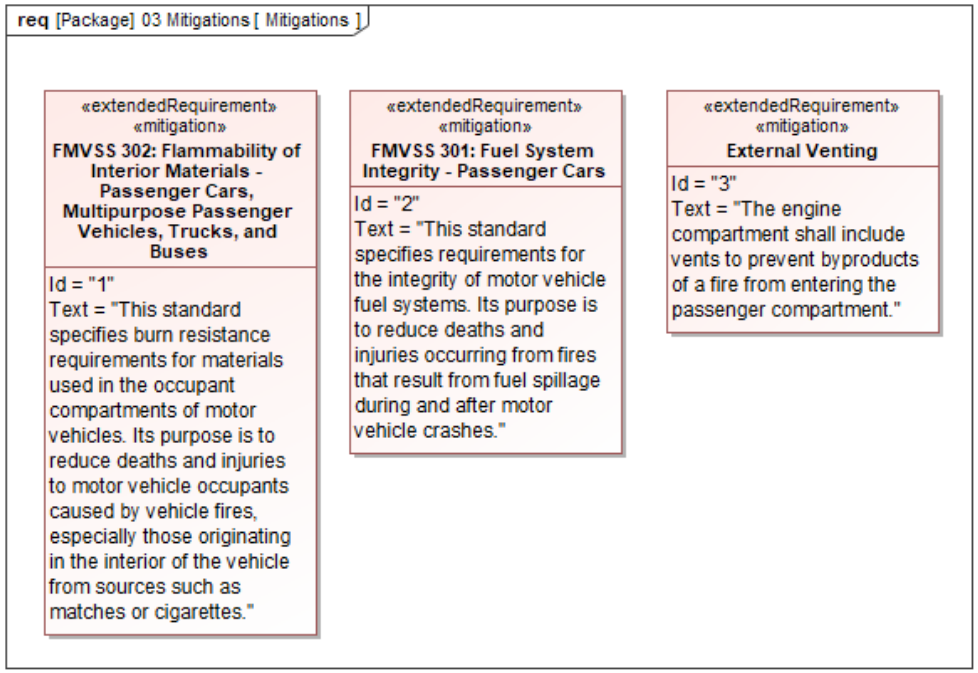
HAZARD PORTS

- The *send signal* and *accept event* elements may be assigned to *ports*.
- This allows the modeler to specify the source or destination of the flow.
- *Hazard ports* (which can legally flow hazard signals) are added to each system element to facilitate this.
- These ports would be hidden/excluded from normal architectural analysis.



MITIGATIONS

- Mitigations are requirements that have a <<mitigation>> *stereotype* applied.
- They may have body text and hyperlinks to the standard, design guidelines, or other relevant material.



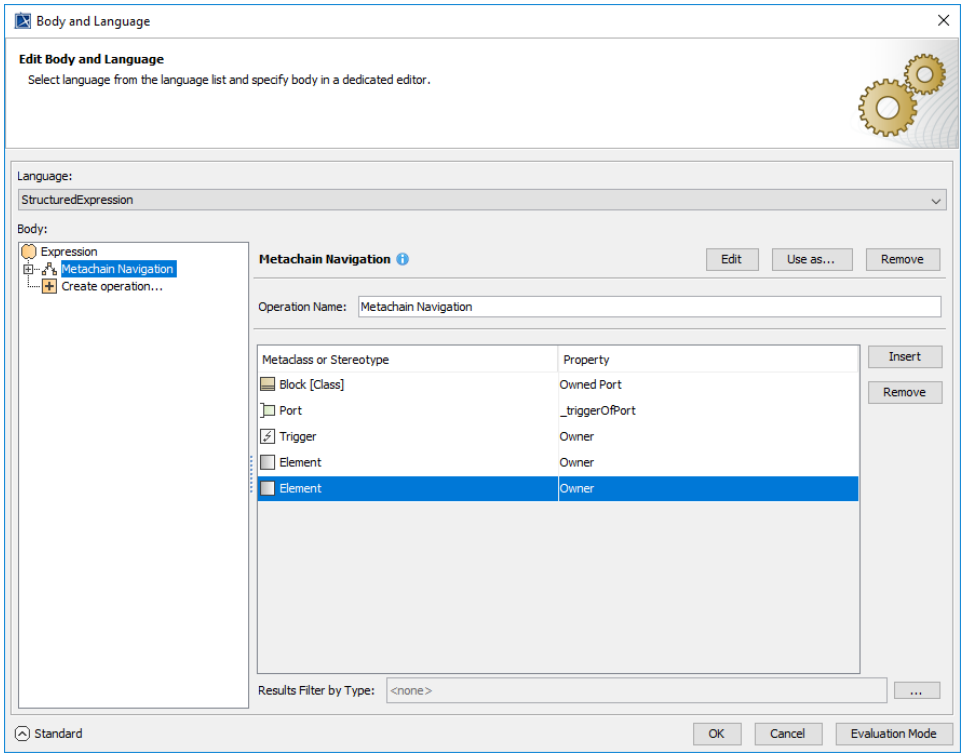
MISHAPS

#	Name	Documentation	Severity	Probability	Causal Factor	Related Hazard
1	Engine Compartment Fire	This mishap describes the outcome of a fire starting in the engine compartment due to a fuel leak.	I Catastrophic	C Occasional	Fire starts in engine compartment due to fuel leak	Vehicle Fire
2	Interior Carpet Fire	This mishap describes the outcome of an interior carpet fire.	I Catastrophic	A Frequent	Interior carpet ignites	Vehicle Fire
3	Seat Fire	This mishap describes the outcome of vehicle seats igniting.	II Critical	E Improbable	Seats ignite	Vehicle Fire

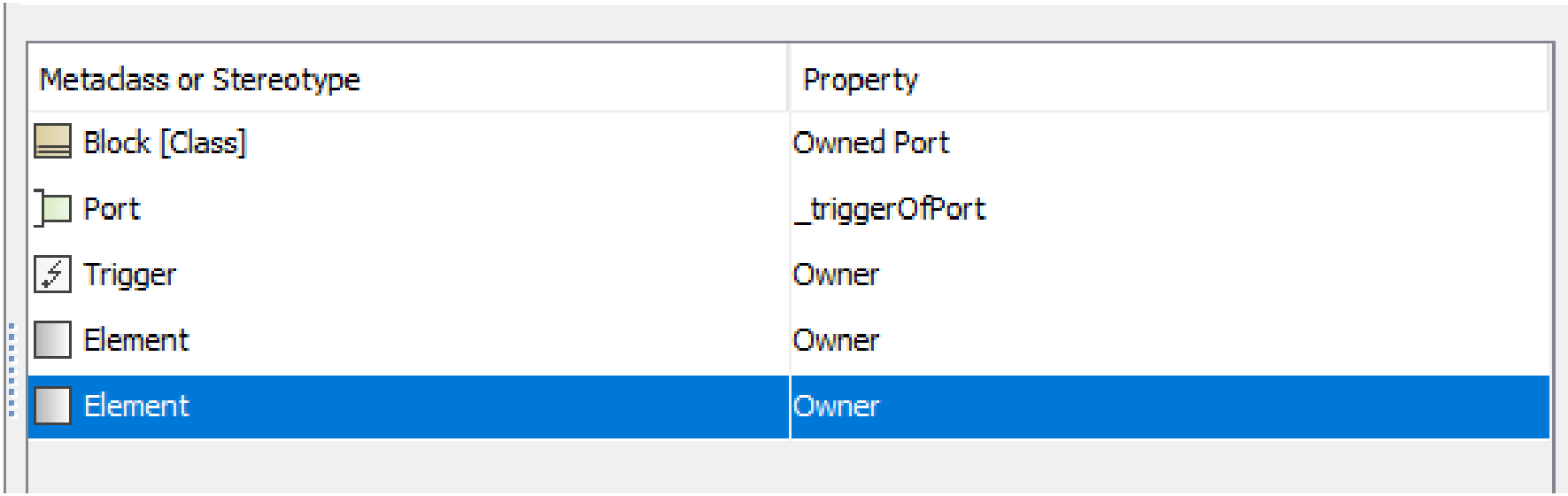
Note: All of these columns populate due to properties or querying the mishap analysis

METACHAIN NAVIGATION

- Metachain navigation uses structured expressions to navigate elements, relationships, and properties.
- It can also perform set-based operations (intersection, exclude, etc.), property tests, and mathematical operations.
- Metrics can also be developed (e.g., number of unconnected pins)



NOTIONAL METACHAIN: SYSTEM ELEMENT TO HAZARDS TO WHICH IT CONTRIBUTES



Metaclass or Stereotype	Property
Block [Class]	Owned Port
Port	_triggerOfPort
Trigger	Owner
Element	Owner
Element	Owner

SYSTEM ELEMENTS

#	Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations	Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability					
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting					
3	Engine Compartment					Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire									
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline						
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible						
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability	Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability				1 FMVSS 302: Flammability	

CONTRIBUTIONS AND MITIGATIONS

#	△ Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting
3	Engine Compartment				
4	Fire				
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline	
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible	
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability

RECEPTIONS, MITIGATIONS, AND ERRORS

Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
			1 FMVSS 302: Flammability	

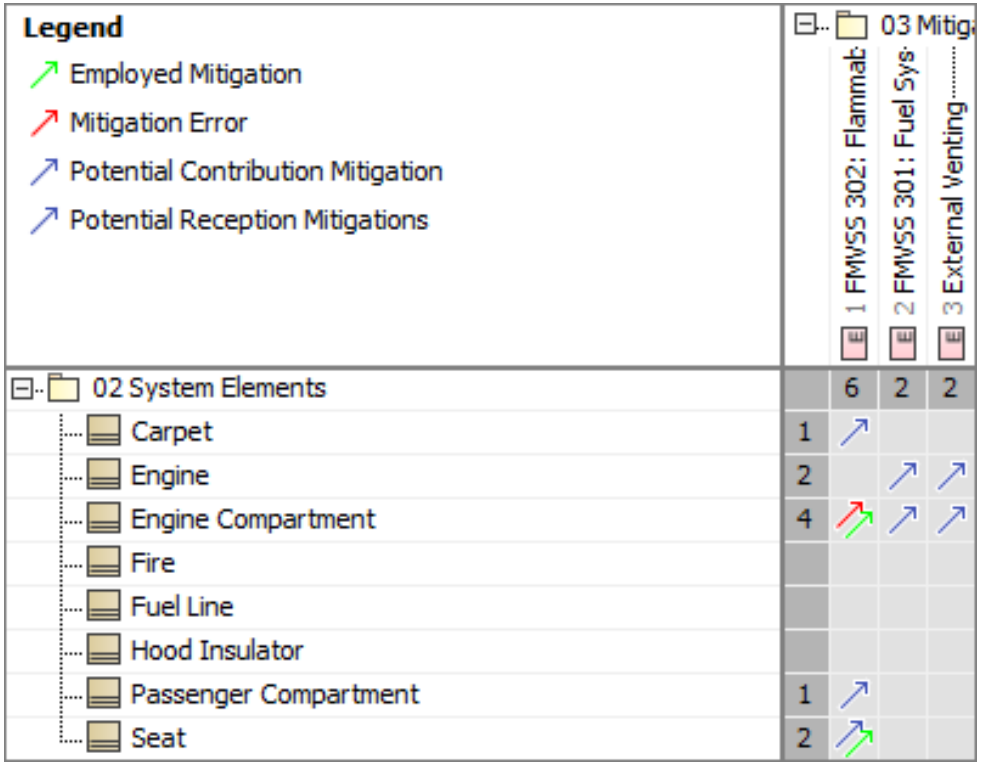
MITIGATION ERRORS

#	△ Name	Potential Contribution Mitigations	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	1 FMVSS 302: Flammability			
2	Engine	2 FMVSS 301: Fuel System 3 External Venting			
3	Engine Compartment		2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire				
5	Fuel Line				
6	Hood Insulator				
7	Passenger Compartment	1 FMVSS 302: Flammability			
8	Seat	1 FMVSS 302: Flammability		1 FMVSS 302: Flammability	

FMVSS 302 is neither a potential contribution nor a reception mitigation, so its employment is an error.

MITIGATION RELATIONSHIPS

- Relationships may also be displayed in a matrix using direct connections or custom metachains.
- Any relationship in a table may be shown in a matrix (and icons may be used in place of arrows).



ERROR CHECKING

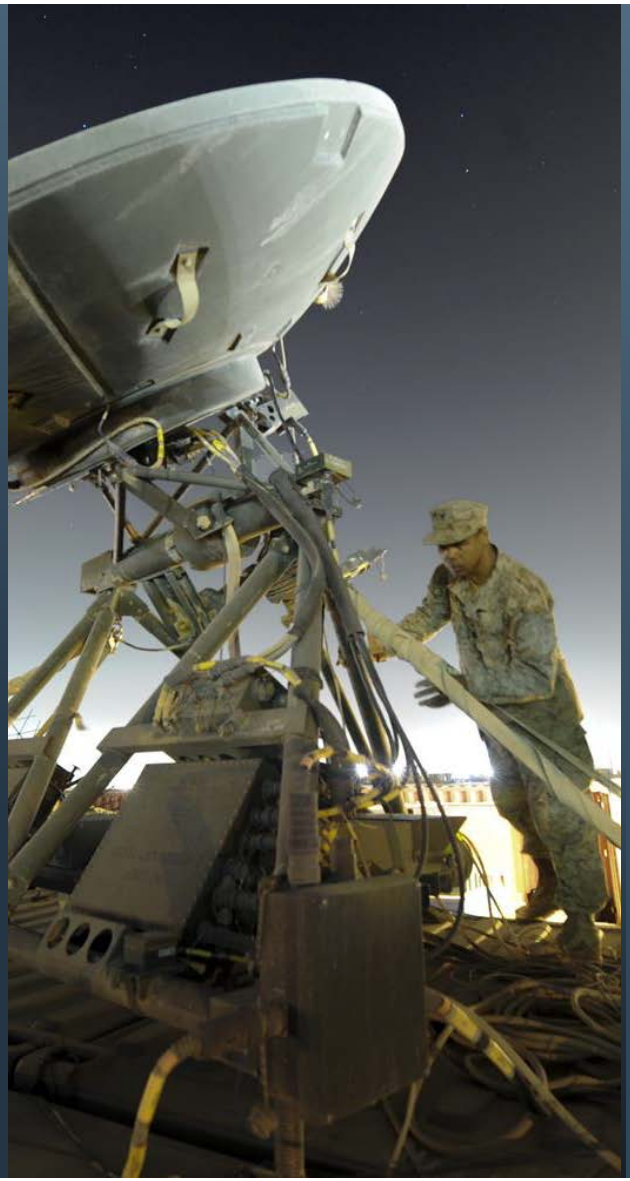
#	Name	Owner	Type	△ Incoming	Outgoing
1		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
2		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
3		Engine Compartment Fire	Combustion Products		Object Flow[Combustion Products[0..*] ->]
4		Interior Trim Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb
5		Interior Carpet Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb Object Flow[Combustion Products[0..*] -> Comb
6		Interior Carpet Fire	Heat		Object Flow[Heat -> Heat]
7		Interior Trim Fire	Heat		Object Flow[Heat -> Heat]
8		Engine Compartment Fire	Heat		Object Flow[Heat ->]
9		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
10		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
11		Combustible			Object Flow[->]
12		Combustible			Object Flow[->]
13		Gasoline	Gasoline		Object Flow[Gasoline ->]
14		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
15		Smoke	Combustion Products	Object Flow[-> Combustion Products]	
16		Toxic Gases	Combustion Products	Object Flow[-> Combustion Products]	
17		Engine Compartment Fire	Gasoline	Object Flow[-> Gasoline[1..*]]	
18		Interior Carpet Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
19		Interior Trim Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
20		Toxic Gases	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
21		Combustion Products	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
22		Smoke	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
23		Heat	Heat	Object Flow[Heat -> Heat]	
24		Heat	Heat	Object Flow[Heat -> Heat]	
25		Interior Carpet Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
26		Engine Compartment Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
27		Interior Trim Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	

CONCLUSIONS

- The use of a relatively small number of customizations can be used to enable the integration of ESOH analysis into the system model used in support of systems architecture and engineering.
- The error-checking and customized queries made possible by this approach allow maximum insight to be achieved with little incremental effort.
- Reuse, the elimination of adjacent tools and systems, and the reduction in lag between analysis and stakeholder visibility are all possible with this approach.

UNCLASSIFIED: Distribution Statement A. Approved for public release; distribution is unlimited.

Booz | Allen | Hamilton



A PRAGMATIC APPROACH TO SYSTEM MODELING FOR HAZARD IDENTIFICATION AND RISK MANAGEMENT

Michael J. Vinarcik, ESEP-Acq, OCSMP-Model Builder Advanced

2017 National Defense Industrial Association

Systems Engineering Conference

OCTOBER 26, 2017

UNCLASSIFIED: Distribution Statement A. Approved for public release; distribution is unlimited.

CONTACT INFORMATION

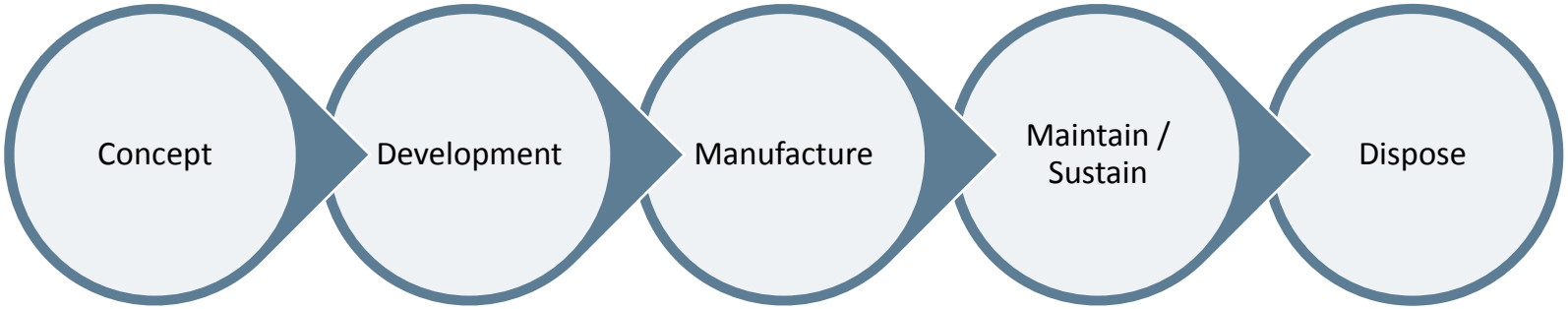
Michael J. Vinarcik

248-227-1659

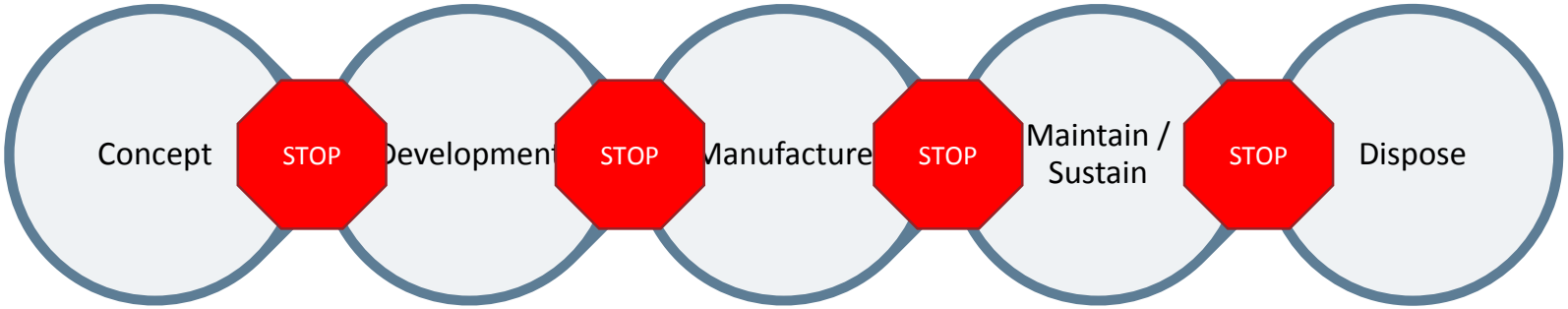
Booz Allen Hamilton

vinarcik_michael@bah.com

AN ABSTRACT VIEW OF PRODUCT DEVELOPMENT



AIR GAPS



Fidelity and momentum is lost every time there is a handoff; this is caused by the “air gaps.”

INDUSTRIAL AGE VS. INFORMATION AGE

"Our current defense acquisition system applies industrial age processes to solve information age problems."

- LtGen Robert D. McMurray, AFLCMC/CC
  Keynote address
  2017 Wright Dialogue With Industry Conference,
  Dayton OH, 18 July 2017

YOU HEAR THAT, MR. ANDERSON? … THAT IS THE SOUND OF INEVITABILITY…

Agent Smith, *The Matrix*

DIGITAL ENGINEERING

- The Department of Defense is developing a strategy to transform its end-to-end acquisition process.
- It is expected to be released for use by 2019.
- This presentation will focus on methods that ESOH professionals can use to smoothly integrate their efforts with digital engineering.
- The following four slides are extracted from another presentation here at the NDIA SE Conference; please seek out Ms. Philomena Zimmerman or her team for more information.
- I have indicated where this presentation supports the strategy.



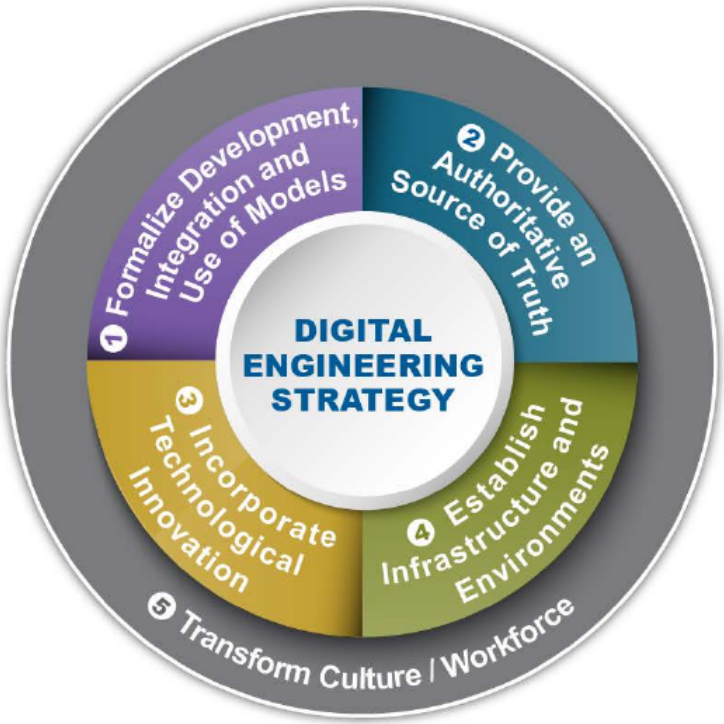
DoD Digital Engineering Strategy

Ms. Philomena Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense
for Systems Engineering

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited..

Digital Engineering Strategy: Five Goals

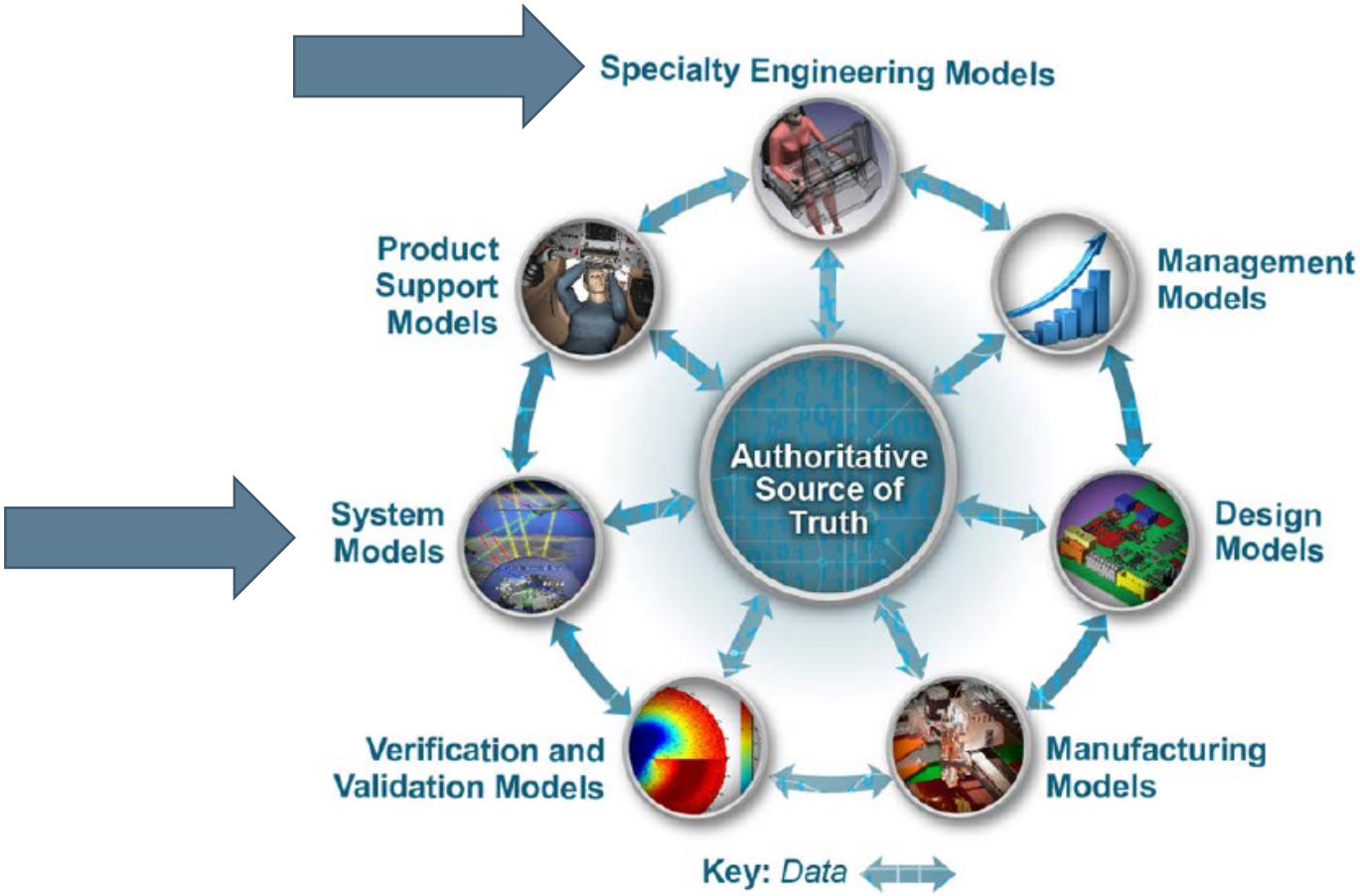
1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to improve the engineering practice
4. Establish supporting **infrastructure and environments** 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

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

Goal #1: Formalize Development, Integration & Use of Models



Models as the cohesive element across a system's lifecycle

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

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

Distribution Statement A – Approved for public release by DOPSR on MM/DD/2016, SR Case # 17-S-#### applies. Distribution is unlimited.

SYSTEM MODELING

- System modeling is emerging as a way to manage the inherent complexity of modern systems by providing a mechanism to store, manage, and associate information about a system under development.
- This information can then be extracted and presented to stakeholders in formats relevant to them.

Models grow organically as detail is added with no loss of fidelity.

from *Modeling Safety and CyberSecurity Controls in SysML,* 2016 NDIA Systems Engineering Conference, Vinarcik

SYSML: THE SYSTEMS MODELING LANGUAGE

- SysML is the most widely-adopted modeling language and has a thriving tool ecosystem.
- A well-constructed system model unambiguously represents a system's behavior, structure, and interrelationships between elements.
- Its flexibility allows integration of other discipline-specific analyses
  - Reliability
  - Safety

BENEFITS OF INTEGRATION

- Eliminating other tools from the analysis chain pays dividends:
  - Reduction in license costs
  - Elimination of interface/integration
  - Improved visibility to all stakeholders
  - Common language and understanding

Reduce lag and drag!

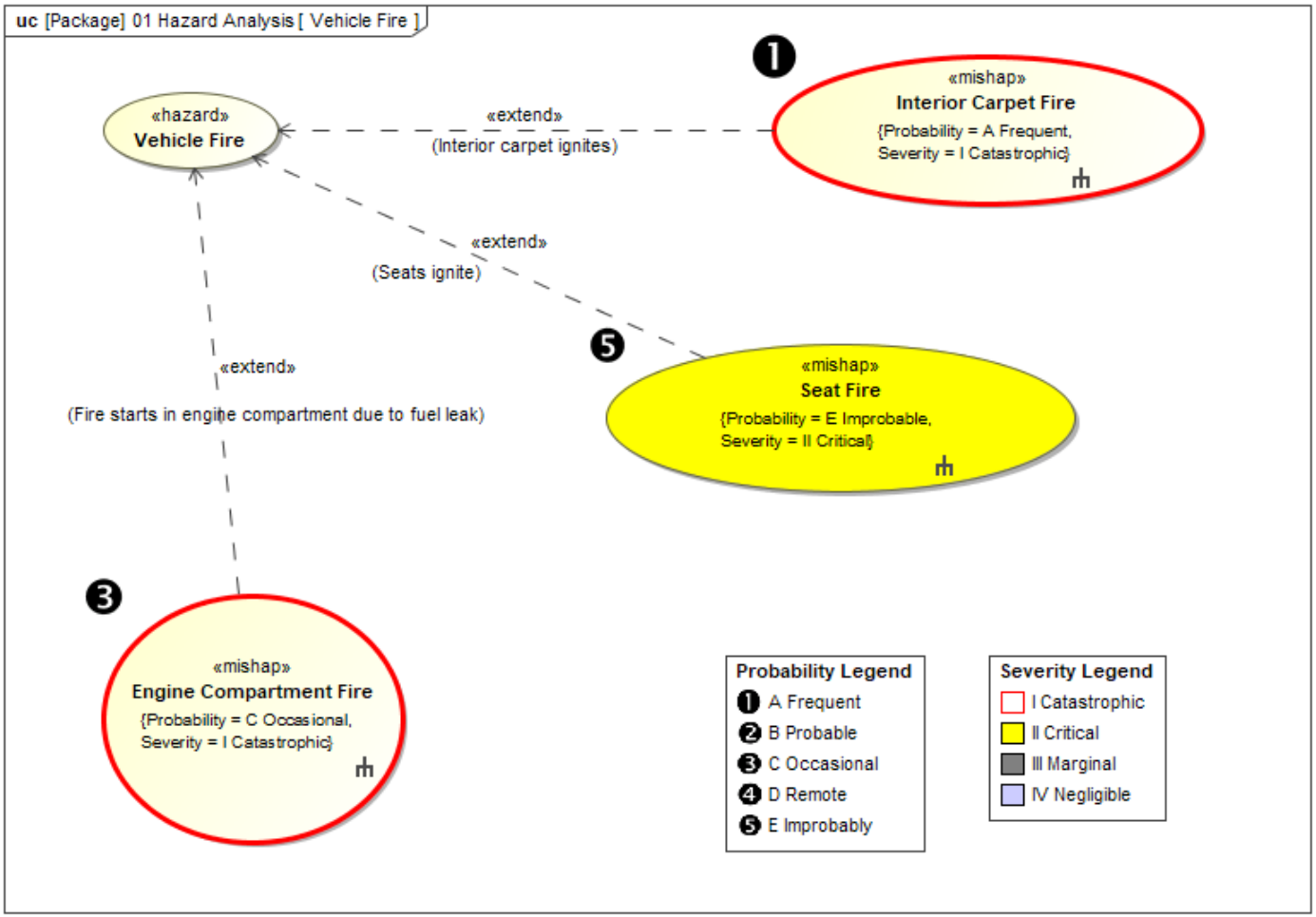
AN EXAMPLE: NOTIONAL PASSENGER AUTOMOBILE

- An unclassified, non-DoD example was needed for this presentation.
- A notional automobile is used as the basis for this example, which uses “fire” as the hazard.
- Note: I am not an ESOH professional and this is provided as an example of one approach to integrate ESOH into an evolving system model.

A REQUIRED MINDSET SHIFT

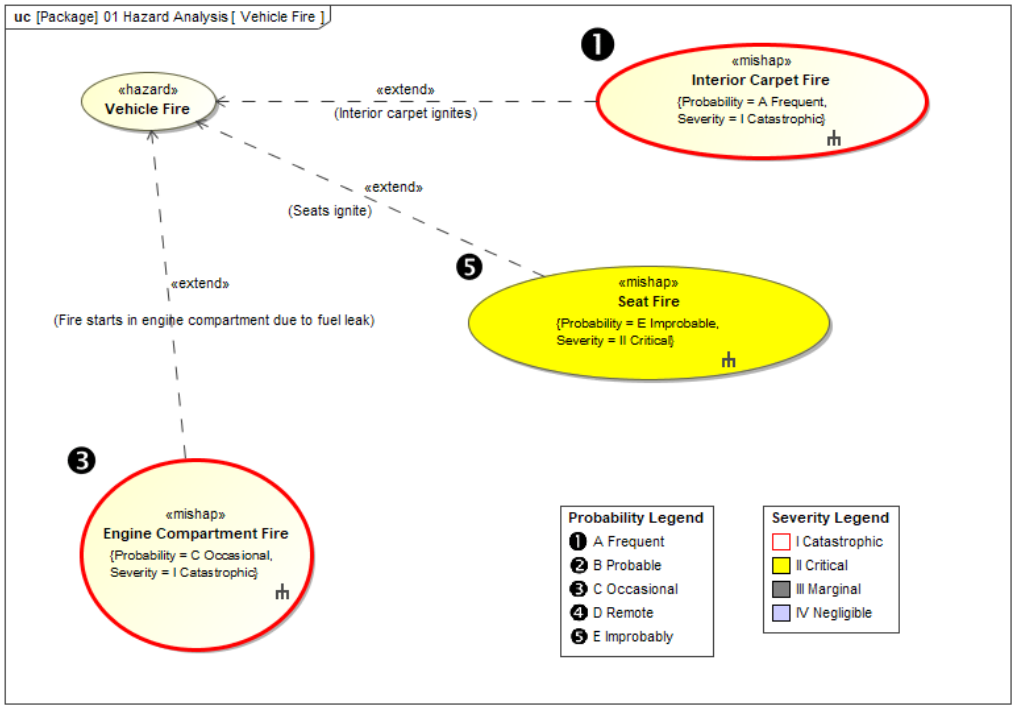
- To successfully leverage SysML, any user must understand that it is not “about” the diagrams.
- What is truly important is:
  - Elements and their properties
  - Relationships, their properties, and what they connect
- Once you see analyses in these terms, representing them in a system model is much easier.
- The collection of elements (including logic/branching elements) permits a rich description of system behavior, structure, interfaces, and parametrics.

NOTIONAL HAZARD ANALYSIS



HAZARD ANALYSIS: ELEMENTS USED

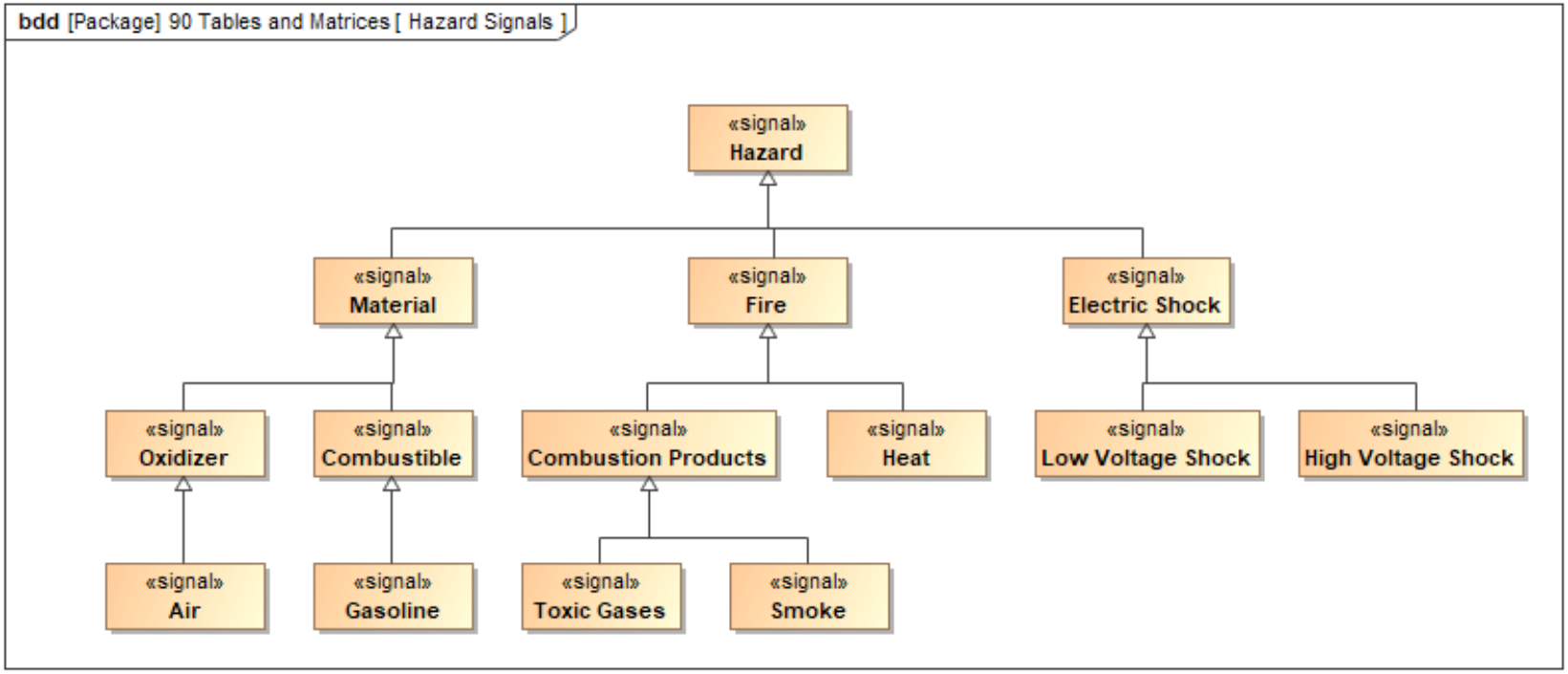
- *Use cases* with <<hazard>> and <<mishap>> stereotypes
- *Extension points* as causal factors
- <<extend>> relationships between mishaps and hazard
- Dynamic legends (color, fill, and icons based on properties of the elements)



WHY USE CASES?

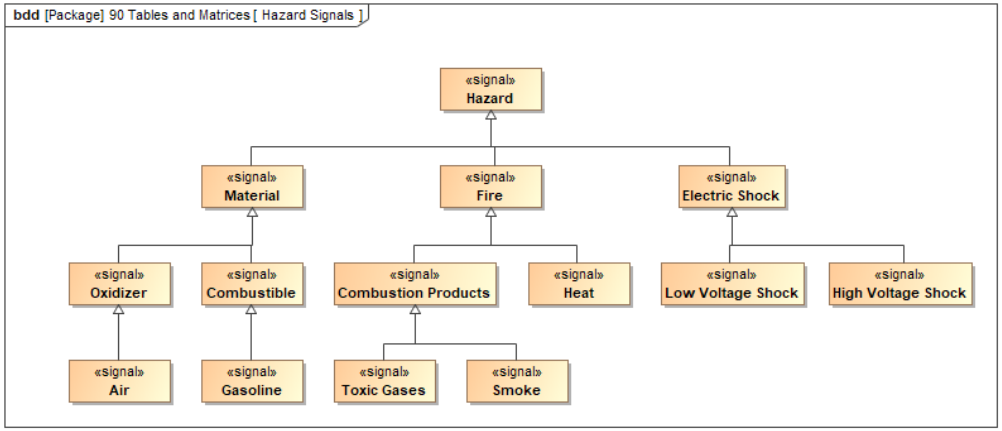
- *Use cases* are convenient SysML representations of behavior. They include:
  - *<<extend>>* relationships for conditional triggering of alternate *use cases*
  - They may be decomposed by activity diagrams

HAZARD SIGNALS

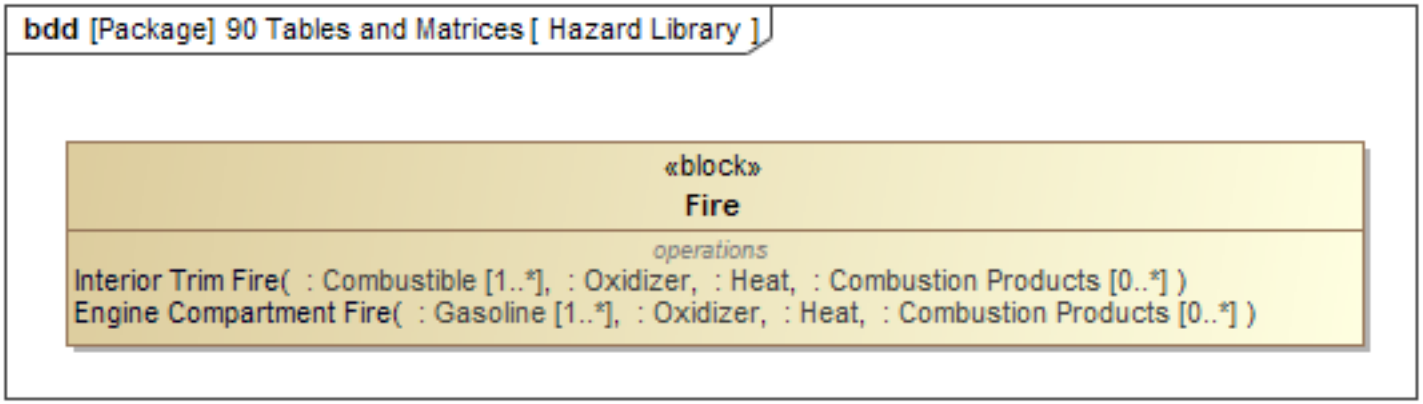


SIGNAL USAGE

- <<signals>> are used to type flow properties on interfaces, content conveyed on flows, and input/output parameters
- This hierarchy allows more specific signals to be used to satisfy more general input/output parameters

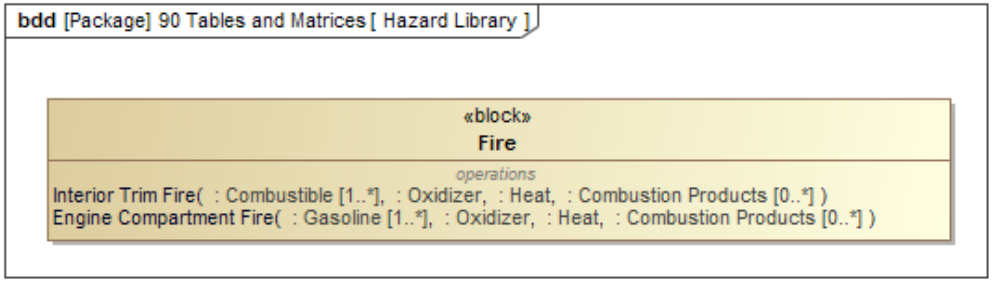


HAZARD BLOCK



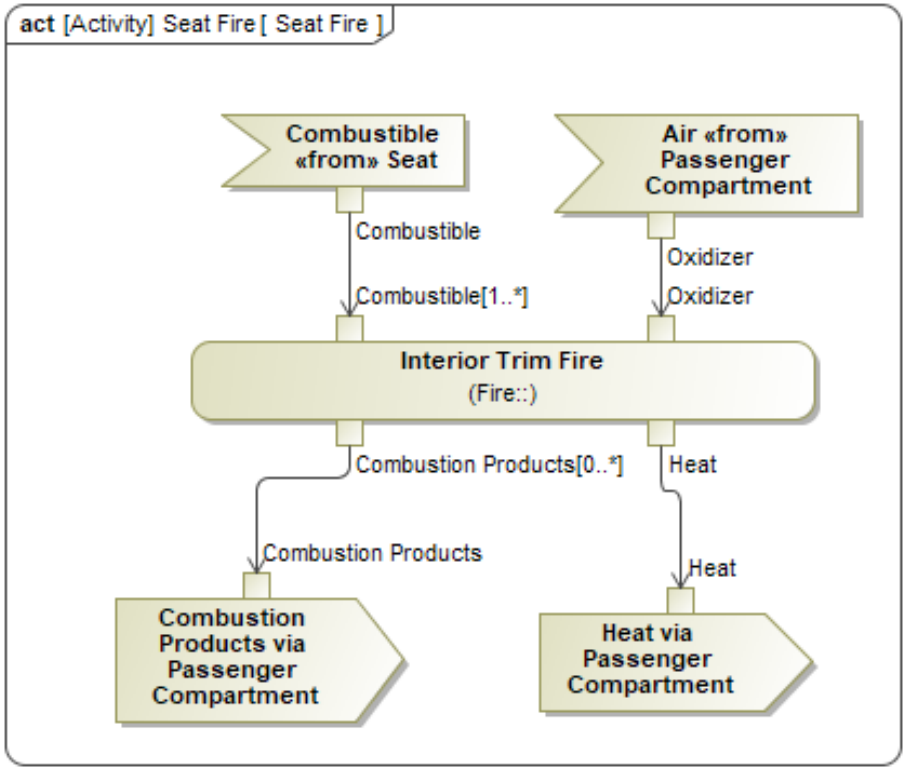
HAZARDS AS OPERATIONS

- <<operations>> own input/output *parameters*
- In this case, an Interior Trim Fire requires at least one combustible, an oxidizer, and generated heat and may generate combustion products (smoke, toxic gas, etc.)



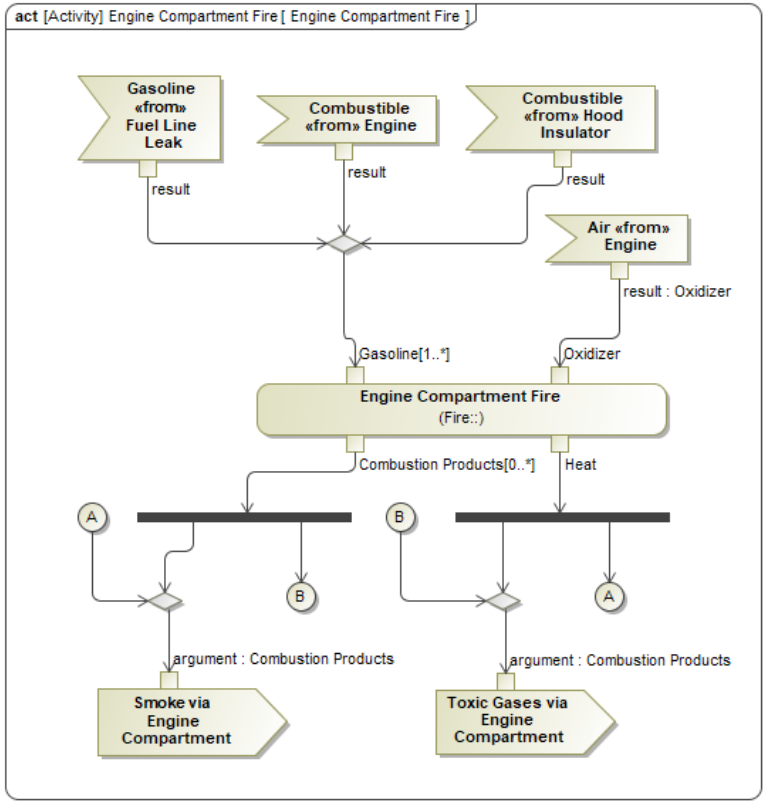
MISHAP DECOMPOSITION

- This activity diagram shows the operation an its input/output *parameters*.
- Each *pin* must be connected (no unconnected pins).
- This forces the analyst to identify the source and destination of all inputs and outputs.
- *Flow final* nodes may be used if there is no output of interest.



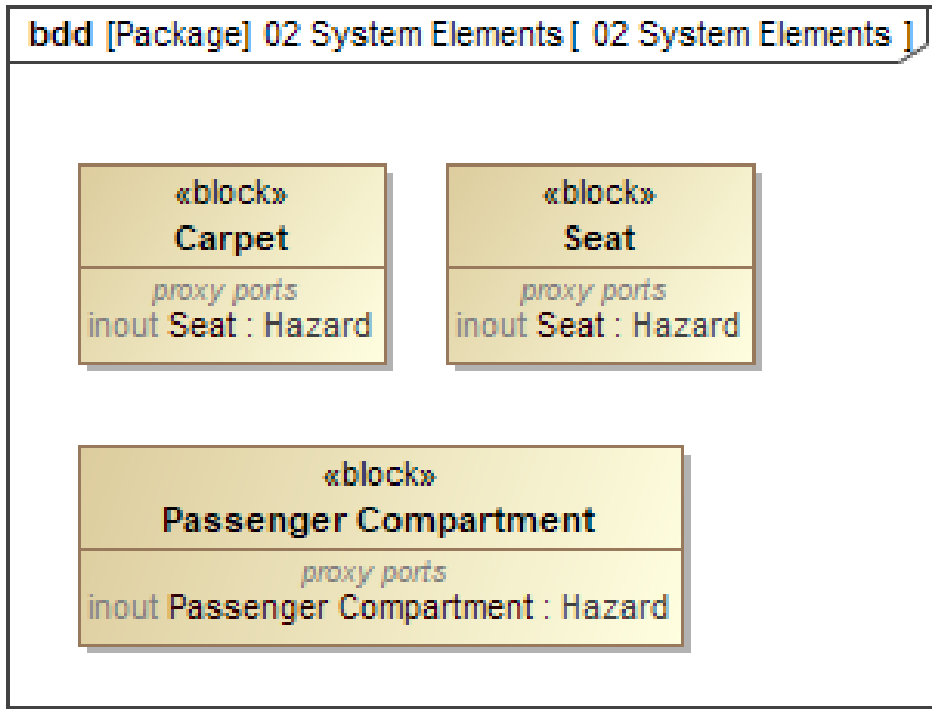
ENGINE COMPARTMENT FIRE

- Note the more complex logic and multiple sources for inputs.



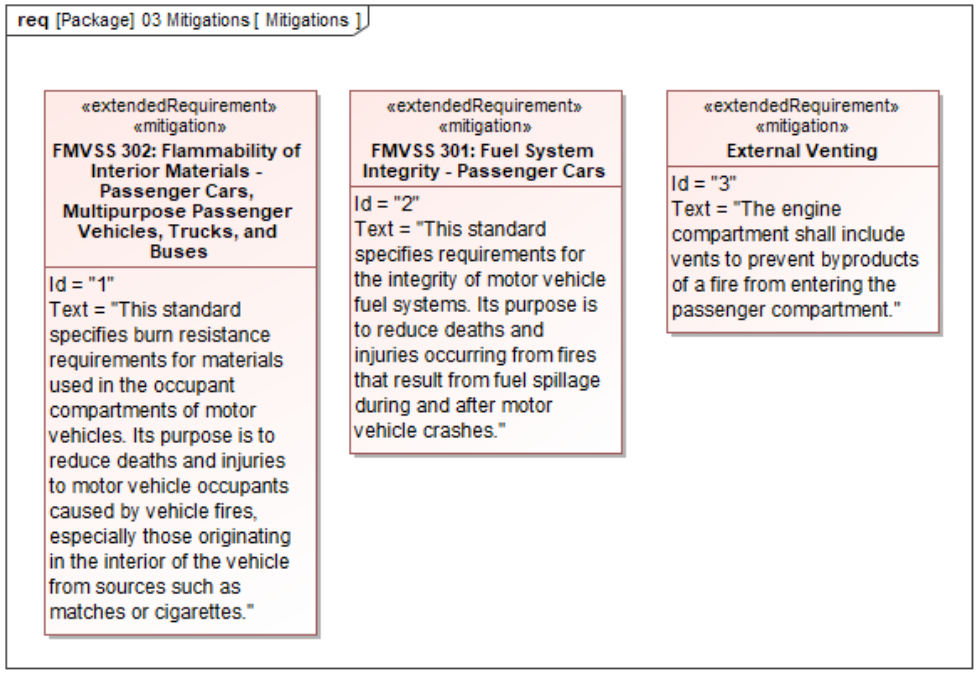
HAZARD PORTS

- The *send signal* and *accept event* elements may be assigned to *ports*.
- This allows the modeler to specify the source or destination of the flow.
- *Hazard ports* (which can legally flow hazard signals) are added to each system element to facilitate this.
- These ports would be hidden/excluded from normal architectural analysis.



MITIGATIONS

- Mitigations are requirements that have a <<mitigation>> *stereotype* applied.
- They may have body text and hyperlinks to the standard, design guidelines, or other relevant material.



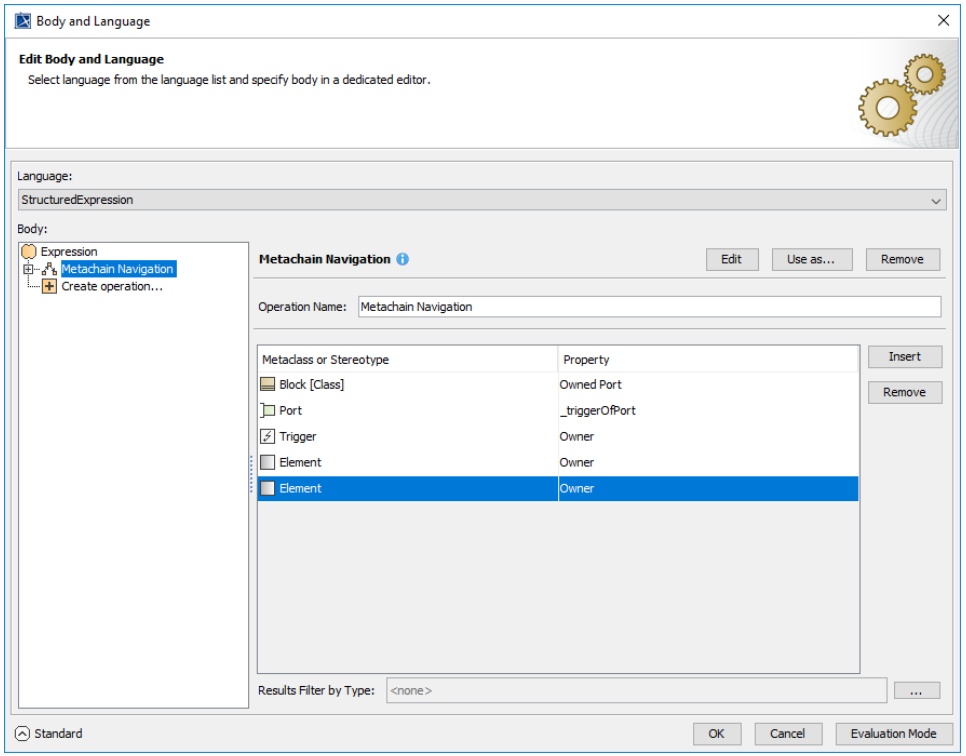
MISHAPS

#	Name	Documentation	Severity	Probability	Causal Factor	Related Hazard
1	Engine Compartment Fire	This mishap describes the outcome of a fire starting in the engine compartment due to a fuel leak.	I Catastrophic	C Occasional	Fire starts in engine compartment due to fuel leak	Vehicle Fire
2	Interior Carpet Fire	This mishap describes the outcome of an interior carpet fire.	I Catastrophic	A Frequent	Interior carpet ignites	Vehicle Fire
3	Seat Fire	This mishap describes the outcome of vehicle seats igniting.	II Critical	E Improbable	Seats ignite	Vehicle Fire

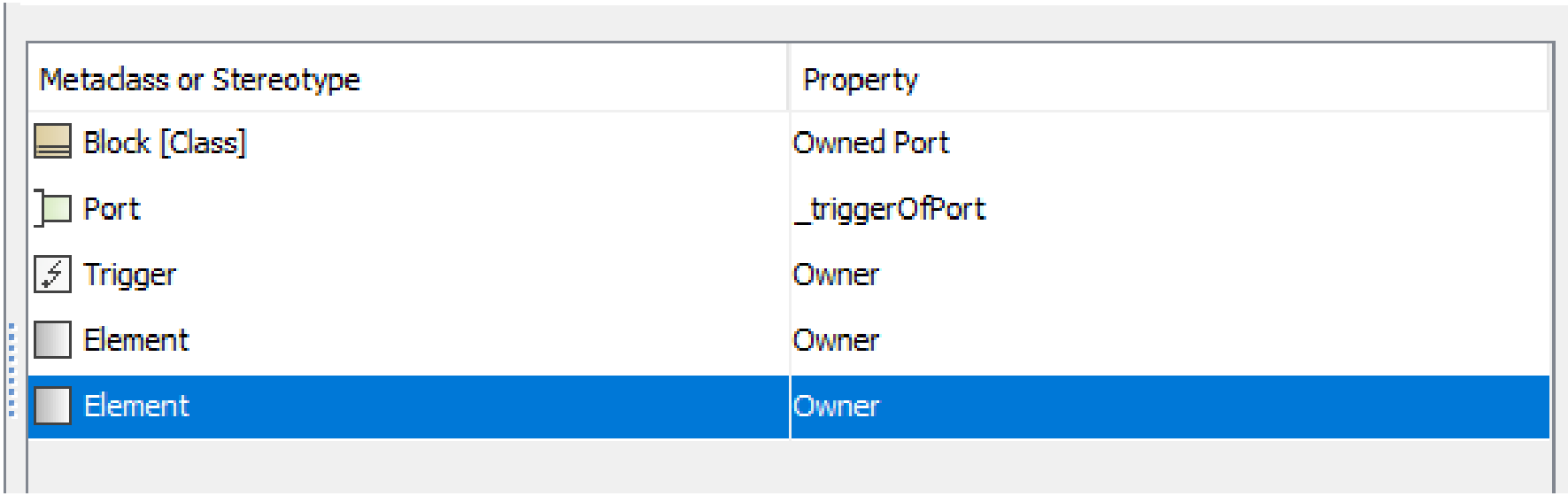
Note: All of these columns populate due to properties or querying the mishap analysis

METACHAIN NAVIGATION

- Metachain navigation uses structured expressions to navigate elements, relationships, and properties.
- It can also perform set-based operations (intersection, exclude, etc.), property tests, and mathematical operations.
- Metrics can also be developed (e.g., number of unconnected pins)



NOTIONAL METACHAIN: SYSTEM ELEMENT TO HAZARDS TO WHICH IT CONTRIBUTES



Metaclass or Stereotype	Property
Block [Class]	Owned Port
Port	_triggerOfPort
Trigger	Owner
Element	Owner
Element	Owner

SYSTEM ELEMENTS

#	Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations	Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability					
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting					
3	Engine Compartment					Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire									
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline						
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible						
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability	Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability				1 FMVSS 302: Flammability	

CONTRIBUTIONS AND MITIGATIONS

#	△ Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting
3	Engine Compartment				
4	Fire				
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline	
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible	
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability

RECEPTIONS, MITIGATIONS, AND ERRORS

Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
			1 FMVSS 302: Flammability	

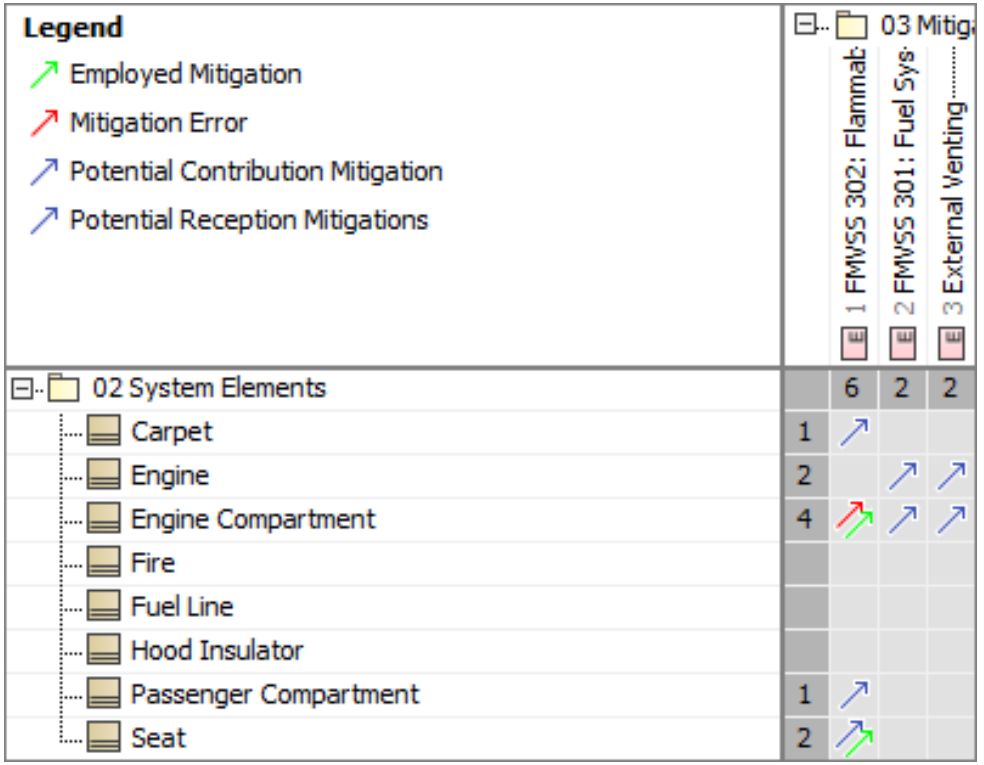
MITIGATION ERRORS

#	△ Name	Potential Contribution Mitigations	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	1 FMVSS 302: Flammability			
2	Engine	2 FMVSS 301: Fuel System 3 External Venting			
3	Engine Compartment		2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire				
5	Fuel Line				
6	Hood Insulator				
7	Passenger Compartment	1 FMVSS 302: Flammability			
8	Seat	1 FMVSS 302: Flammability		1 FMVSS 302: Flammability	

FMVSS 302 is neither a potential contribution nor a reception mitigation, so its employment is an error.

MITIGATION RELATIONSHIPS

- Relationships may also be displayed in a matrix using direct connections or custom metachains.
- Any relationship in a table may be shown in a matrix (and icons may be used in place of arrows).



ERROR CHECKING

#	Name	Owner	Type	△ Incoming	Outgoing
1		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
2		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
3		Engine Compartment Fire	Combustion Products		Object Flow[Combustion Products[0..*] ->]
4		Interior Trim Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb
5		Interior Carpet Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb Object Flow[Combustion Products[0..*] -> Comb
6		Interior Carpet Fire	Heat		Object Flow[Heat -> Heat]
7		Interior Trim Fire	Heat		Object Flow[Heat -> Heat]
8		Engine Compartment Fire	Heat		Object Flow[Heat ->]
9		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
10		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
11		Combustible			Object Flow[->]
12		Combustible			Object Flow[->]
13		Gasoline	Gasoline		Object Flow[Gasoline ->]
14		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
15		Smoke	Combustion Products	Object Flow[-> Combustion Products]	
16		Toxic Gases	Combustion Products	Object Flow[-> Combustion Products]	
17		Engine Compartment Fire	Gasoline	Object Flow[-> Gasoline[1..*]]	
18		Interior Carpet Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
19		Interior Trim Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
20		Toxic Gases	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
21		Combustion Products	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
22		Smoke	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
23		Heat	Heat	Object Flow[Heat -> Heat]	
24		Heat	Heat	Object Flow[Heat -> Heat]	
25		Interior Carpet Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
26		Engine Compartment Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
27		Interior Trim Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	

CONCLUSIONS

- The use of a relatively small number of customizations can be used to enable the integration of ESOH analysis into the system model used in support of systems architecture and engineering.
- The error-checking and customized queries made possible by this approach allow maximum insight to be achieved with little incremental effort.
- Reuse, the elimination of adjacent tools and systems, and the reduction in lag between analysis and stakeholder visibility are all possible with this approach.



LEVERAGING INTERNATIONAL AEROSPACE ENVIRONMENTAL GROUP'S DECLARATION PROCESS FOR CHEMICAL SUBSTANCES REPORTING

How the International Aerospace Environmental Group's (AIEG) Aerospace and Defense Declarable Substances List, "AD-DSL", can be leveraged by DoD Acquisition Programs

Karen Gill
Booz Allen Hamilton

OCTOBER 2017

NDIA SYSTEMS ENGINEERING CONFERENCE ABSTRACT # 19836

AGENDA

- HAZARDOUS MATERIALS MANAGEMENT IN DOD ACQUISITION
- IAEG CHEMICAL SUBSTANCES REPORTING PROCESS AND IPC DATA EXCHANGE STANDARD
- IAEG DECLARATION PROCESS VIDEO
- AEROSPACE INDUSTRIES DECLARABLE SUBSTANCES LIST
- DEPARTMENT OF DEFENSE (DOD) - INDUSTRY COLLABORATION TO IMPROVE HAZMAT MANAGEMENT IN DOD ACQUISITION
- BENEFITS OF GOVERNMENT-INDUSTRY COLLABORATION
- HAZMAT INFORMATION FLOW ALONG THE SUPPLY CHAIN
- LOGISTICS PRODUCT DATA REPORTS UPDATE
- LOOKING AHEAD
- SUMMARY

ACKNOWLEDGEMENTS

Special Thanks for their invaluable contributions to this presentation:

Tim Sheehan

Yvonne Pierce

Mary Hammerer

Margaret Proul

HAZARDOUS MATERIALS MANAGEMENT IN DOD ACQUISITION

- DoD acquisition policy for Hazardous Materials (HAZMAT) management:
  - Identify HAZMAT associated with the system and used for operation and support of the system; and, plan for their minimization and/or safe disposal in accordance with all regulatory requirements.
  - Use the system safety methodology in Military-Standard-(MIL-STD)-882E, *DoD Standard Practice System Safety*, to eliminate hazards where possible and manage Environment, Safety, and Occupational Health (ESOH) risks where hazards cannot be eliminated.
- Industry has two main components of HAZMAT management for DoD customers:
  - Reporting – Understand and communicate materials present in military hardware products and HAZMAT needed to support the hardware/system
    - "Materials and Substances Declaration"
  - Selection – Select the material that meets the need(s) of the system while minimizing risks throughout the product life cycle
    - Government approval for use of HAZMAT categorized as "Prohibited"

INTERNATIONAL AEROSPACE ENVIRONMENTAL GROUP'S MATERIALS DECLARATION PROCESS FOR CHEMICAL SUBSTANCES REPORTING

IAEG
INTERNATIONAL AEROSPACE ENVIRONMENTAL GROUP®

- International Aerospace Environmental Group (IAEG ®) developed a declaration process for chemical substances for the Aerospace and Defense (AD) industries to obtain information about the chemical substance content of its products from the industry's global supply chain.
- The process consists of several tools used to enhance industry substance compliance processes and address chemical substance-related supply risks.
  - **Aerospace and Defense Declarable Substances List (AD-DSL) -** a list of regulated substances of concern to the AD industry and its customers; used for substance declarations.
  - **Aerospace and Defense Substance Reporting Template (AD-SRT)** – an interim Excel form used to request and obtain chemical substance information from AD suppliers consistent with IPC 1754 data fields and rules.
  - **IAEG® Supplier Training** – Training to provide chemical substance data consistent with the IAEG® declaration process.

Adapted from: http://www.iaeg.com

INDUSTRY ASSOCIATIONS COLLABORATE ON DECLARATION PROCESS DATA EXCHANGE STANDARD

- IPC is the global trade association serving the printed board and electronics assembly industries, their customers, and suppliers.
- The **IPC-1754 Standard**, "*Materials and Substances Declaration for Aerospace and Defense, Heavy Equipment and Other Industries*" allows industries to communicate chemical information within the supply chain in a consistent and structured manner, based on an agreed-upon set of rules.
  - IPC-1754 **identifies data elements and supports the electronic data exchange** of declaration information using XML.
  - The Standard is currently in draft, and is expected to be published in December 2017.

One format for common suppliers offers significant advantages.
The Standard can be used by any hardware-producing industry.

Adapted from: http://www.ipc.com

WHY A STANDARD ON SUBSTANCE REPORTING?

- Industry standard versus company specific solutions
- Standardized industry requirements and format for substance data exchange provides:
  - Improved supply chain awareness and buy-in
  - Ecosystem to support development of tools and processes that support data exchange and management
  - Enhanced efficiencies obtaining necessary data and developing declarations
  - Reduced turnaround time for declarations
  - Improved quality of data (vs. custom data request)
  - Reduced cost versus custom information technology tools development and training

Adapted from Rick Shanks presentation "Materials Declaration Initiatives in the A&D Industry", March 2017

IAEG DECLARATION PROCESS FOR CHEMICAL SUBSTANCES REPORTING (4 MINUTE VIDEO)



AEROSPACE AND DEFENSE DECLARABLE SUBSTANCES LIST



IAEG
INTERNATIONAL AEROSPACE ENVIRONMENTAL GROUP®

- The AD-DSL includes substances that:
  - Are product related and
  - Have regulatory-based restrictions and/or reporting requirements of industry interest
- Latest version – Developmental Version 2 (August 14, 2017)
- Two types of data reporting possible, depending on need:
  - Chemicals in the product – mandatory when AD-DSL chemicals are present
  - Chemicals required to manufacture or support products – optional
- Forward-looking – "what is and what is likely to be regulated…"
- Aerospace and defense companies use the data acquired to:
  - Identify and comply with compliance liabilities – regulatory/contractual
  - Identify dependence/materials obsolescence risks in the supply chain
  - Report product related hazardous chemicals to customers

DOD-INDUSTRY COLLABORATE TO IMPROVE HAZMAT MANAGEMENT

- 2012 - DoD **MIL-STD-882E** published
  - Includes a new optional Task 108, *Hazardous Materials Management Plan*
- DoD-Aerospace Industries Association(AIA) NAS411 Workgroup Collaborative Projects
  - Harmonize NAS411 and MIL-STD-882E Task 108
  - 2013 - **NAS411, *Hazardous Materials Management Program*** Rev 3 published
    - Adopted for use by DoD in 1994, renewed 2017
  - 2013 - **NAS411-1, *Hazardous Material Target List (HMTL)* Rev New** published
    - List of HAZMAT to be actively managed and tracked
  - 2016 - **NAS411-1 Rev 1** published
    - Added discrete Chemical Abstract Service (CAS) numbers for all chemicals
    - Added “tracked” chemicals
    - Adopted for use by DoD in 2017



BENEFITS OF GOVERNMENT-INDUSTRY COLLABORATION

- NAS411 and 411-1:
  - Provide a common framework to avoid trying to manage all known HAZMAT and focus on highest priority HAZMAT
  - Requires program offices and their contractors to agree on a finite list of HAZMAT to be actively managed for the system
    - Both documents contain tailorable content that can be modified to meet customer and supplier needs and supplier capabilities
  - Eliminates the need for multiple different HAZMAT lists from the various DoD Component organizations

	HAZMAT Categories		
Requirement	**Prohibited**	**Restricted**	**Tracked**
Program Office must approve usage	X		
Eliminate or minimize HAZMAT	X	X	
Report HAZMAT locations and amounts (in articles or used in operation/support)	X	X	X

Reduces cost and increases relevance of HAZMAT information.

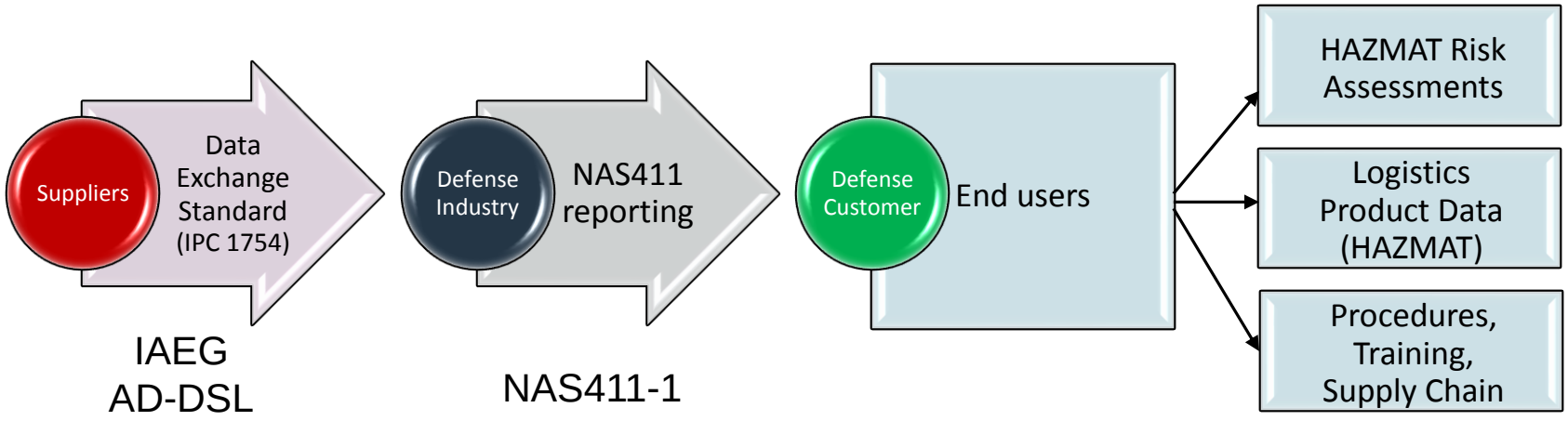
DOD & AIA WORKING TO HARMONIZE THE AD-DSL AND NAS411-1 LISTS

- There is significant overlap of chemical listed on the two lists.

List Attributes	IAEG AD-DSL	NAS411-1 HMTL
Discrete list of chemicals	X	X
Product-related regulated hazardous chemicals	X	X
Hazardous chemicals identified in the supply chain	X	X
Hazardous chemicals identified in delivered hardware and used in operation/support	X	X
Hazardous chemicals identified in manufacturing processes	X	

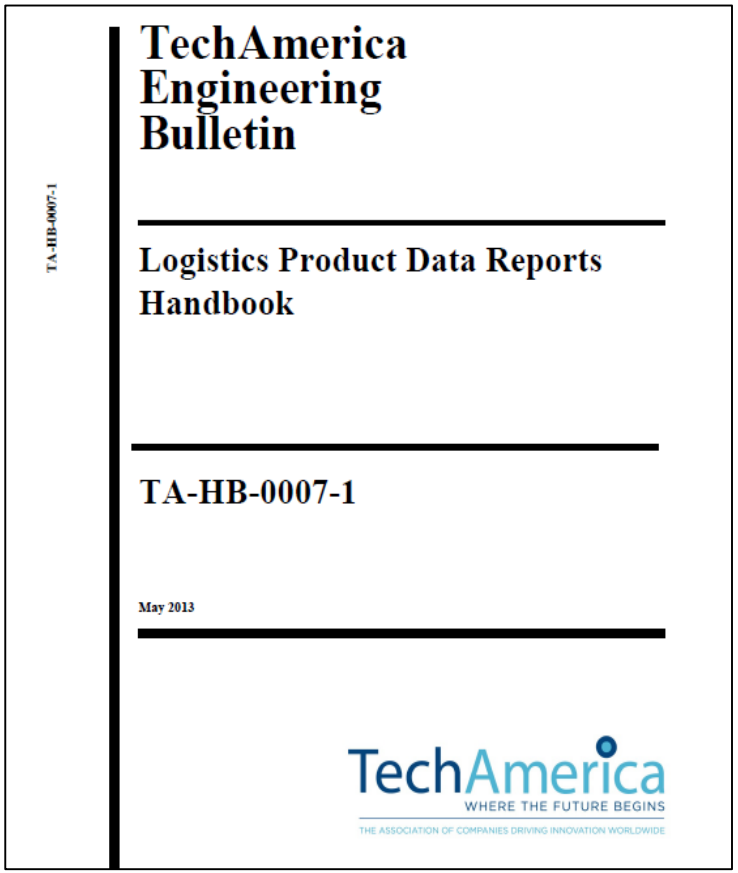
Consistency between lists promotes supply chain efficiency and risk management support.

HAZMAT INFORMATION FLOW ALONG THE DEFENSE SUPPLY CHAIN



The hope is DoD acquisition programs will take advantage of the increased capabilities of the defense industry by using NAS411 and NAS411-1 on contracts.

LOGISTICS PRODUCT DATA REPORT UPDATE LEVERAGES NAS411 AND NAS411-1



- Life Cycle Logistics Supportability Committee is updating LSA-078 Report
- New report does a better job of identifying all HAZMAT associated with a system
- Good News – Most programs are already buying most of these data elements for other Logistics Product Data (LPD) reports – provisioning, maintenance planning, etc.

Accurate HAZMAT data reported via LPD with improved ESOH risk coordination.

Adapted from Mary Hammerer presentation "Logistics Product Data for Hazardous Materials Tracking", October 2016

LOGISTICS PRODUCT DATA REPORT UPDATES LEVERAGES NAS411 AND NAS411-1, CONT.

- New “HAZ” Entity in next update to LSA-078 Report
- Improves collection of HAZMAT in articles, end items, and maintenance tasks
- Provides traceability between NAS411 required data and “HAZ” Entity

LPD ELEMENT	DEFINITION
Substance Name	Name of the hazardous substance
Substance Identification	Chemical Abstracts Service Registry Number
Substance Mass Minimum	This field identifies the inclusive lower limit of the hazardous substance in the part when mass is expressed as a range
Substance Mass Maximum	This field identifies the inclusive upper limit of the hazardous substance in the part when mass is expressed as a range
Substance Mass Nominal	This field identifies the nominal mass of the hazardous substance in the part which is a defined value that may not correspond exactly to the actual value because manufacturing processes result in small variations
Substance Mass Unit of Measure	This field identifies the unit of measure for the substance mass: milligrams, grams, or kilograms
Substance Mass Percent	Calculated Value
Chemical Category	Chemicals with shared chemical and toxicological properties which are grouped into categories. E.g. "cyanide compounds," "lead compounds", etc.
Hazardous Materials Target List Category	The hazardous material category of "Prohibited", "Restricted", or "Tracked", as identified in the contract

Adapted from Mary Hammerer presentation “Logistics Product Data for Hazardous Materials Tracking”, October 2016

LOOKING FORWARD

- The need to report on specific HAZMAT continues to evolve:
  - REACH, TSCA, OSHA, Canada CMP, etc.
  - The AD-DSL and NAS411-1 HMTL will be managed to reflect changing needs.
  - The NAS411 WG will work to increase inclusion of HAZMAT used to operate and support systems.
- Planned updates include:
  - AIA feedback loop to obtain input from users of NAS411-1“
  - Semi-annual reviews of the NAS411-1 HMTL
    - Comparison and adjustment between the two lists (AD-DSL & NAS411-1)
    - Resolve scope differences between the two lists
- LPD elements and reports improvements to leverage the materials declaration process using NAS411 and 411-1

SUMMARY

- The IAEG Materials Declaration Process allows industries to communicate chemical information within the supply chain in a consistent and structured manner, based on an agreed-upon set of rules.
- Leveraging the AD-DSL and Materials Declaration Process is a win-win for industry and DoD
  - Harmonizes NAS411 & AD-DSL to the greatest extent possible
  - Supports both industry and DoD needs
  - Helps support ESOH risk management in acquisition
    - Improves supply chain management and sustainability
    - Helps with predictive material obsolescence (know where HAZMAT is used)
    - Addresses global regulatory compliance
    - Provides content/format standardization (reliable data and efficiencies)
    - Increases visibility to material presence, concentration, source

Use of industry materials declaration processes to obtain supplier product information expected to provide cost avoidance savings to program offices.



Karen Gill
Senior Lead Technologist

Booz | Allen | Hamilton

Booz Allen Hamilton
1550 Crystal Dr, Suite 1100
Arlington, VA 22202
Tel (703) 412-7436
gill_karen@bah.com

LIFE CYCLE ASSESSMENT: A TOOL FOR PROTECTING DEFENSE ASSETS

Kelly Scanlon, DrPH, CIH

Chemical & Material Risk Management Program

Office of the Assistant Secretary of Defense

(Energy, Installations, and Environment)

20th Annual Systems Engineering Conference

October 26, 2017

AGENDA

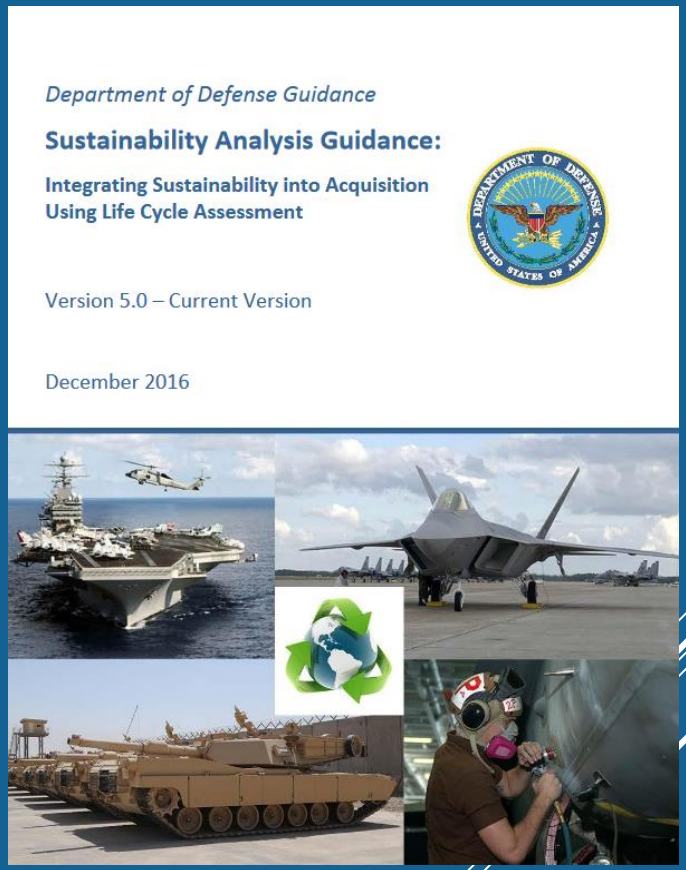
- Policy
  - Sustainability Analysis Guidance
- People
  - DoD Community of Interest
  - Federal LCA Commons
- Practice
  - Pilot Projects

SUSTAINABILITY ANALYSIS GUIDANCE

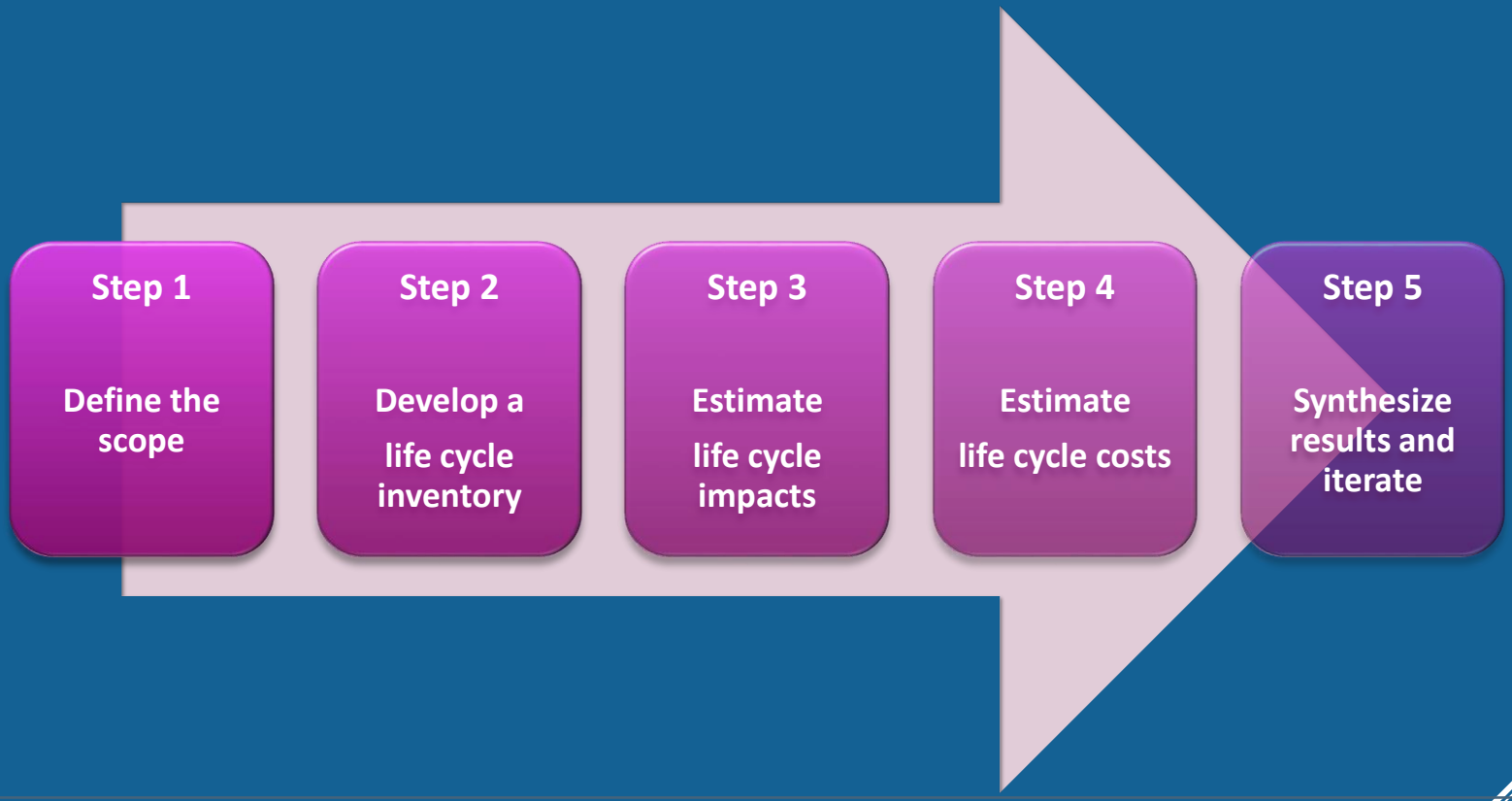
INTEGRATING SUSTAINABILITY INTO ACQUISITION USING LIFE CYCLE ASSESSMENT

Sustainability Analysis = LCA + LCC

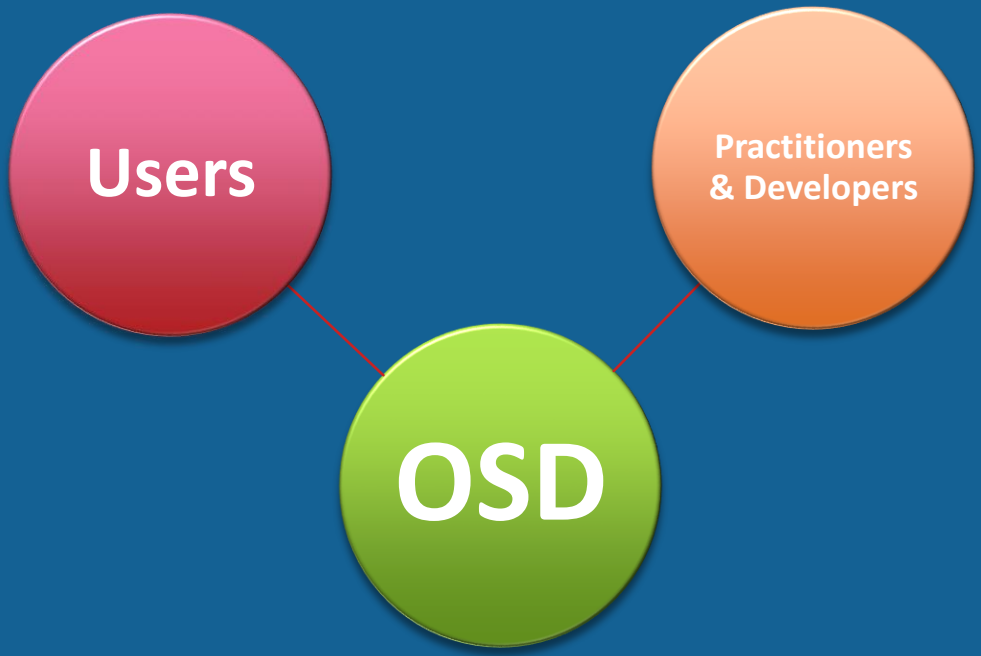
- Consistent, practical, flexible methodology
- Identifies most sustainable alternative among those that meet performance requirements
- Uncovers previously hidden human health and environmental impacts and their associated life cycle costs
- http://www.denix.osd.mil/esohacq/home/



SUSTAINABILITY ANALYSIS METHODOLOGY



SUSTAINABILITY ANALYSIS COMMUNITY OF INTEREST



Current Examples

ESOH
SERDP-ESTCP
Systems Engineering
AFLCMC
FRCSE
GE
ERDC
Lockheed Martin

FEDERAL LCA COMMONS















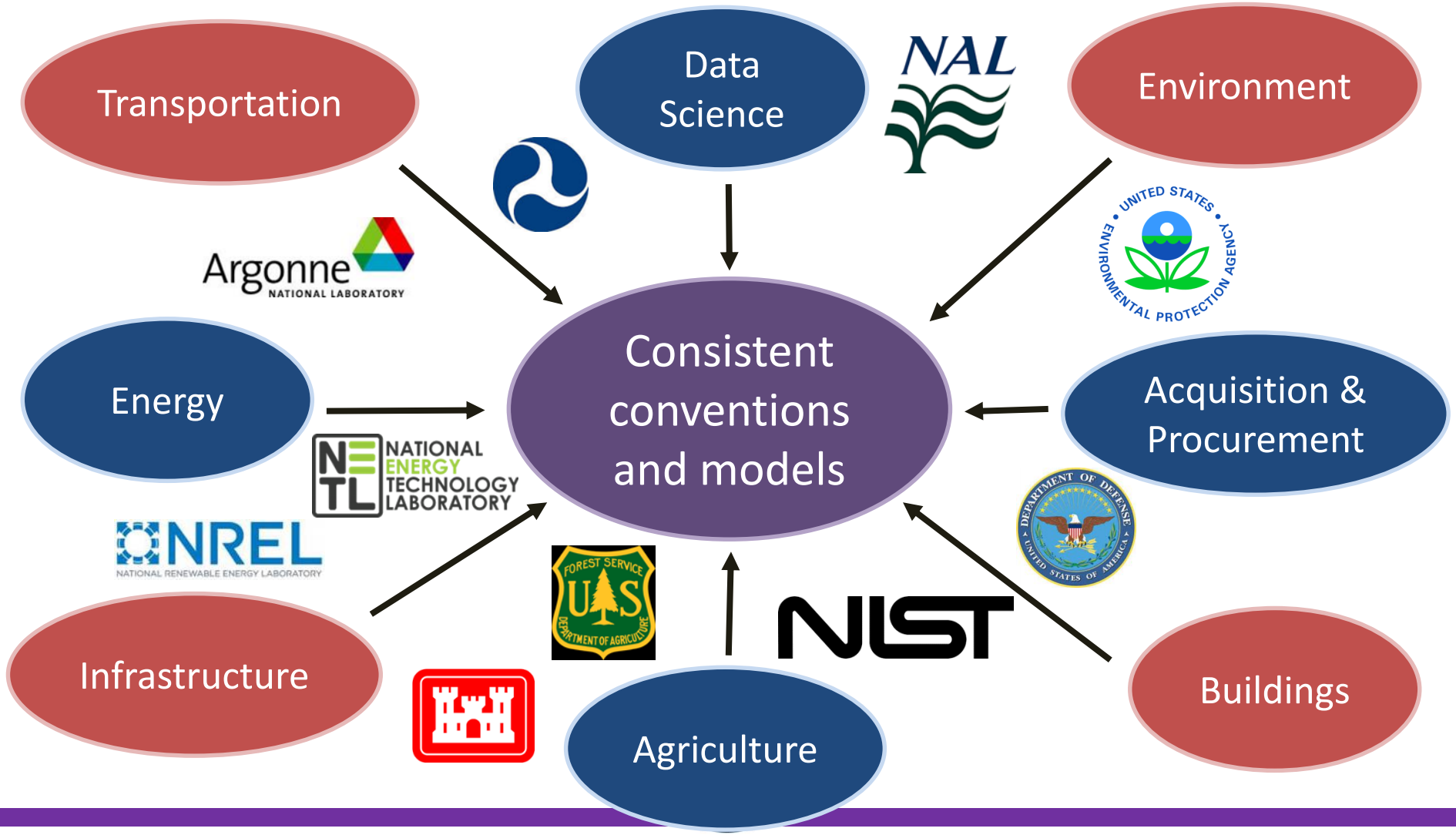






How We Collaborate

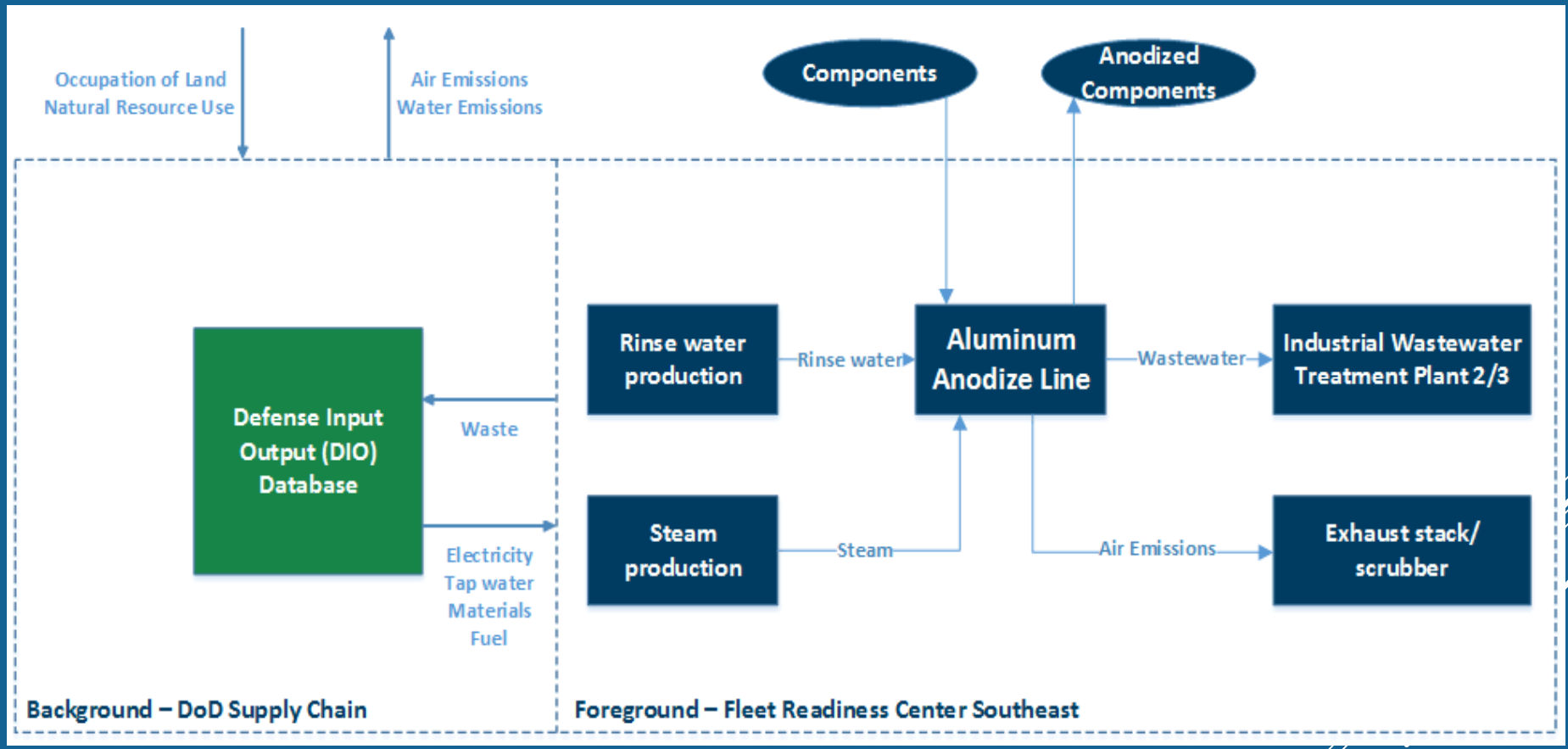
Interagency **Community-of-Practice** around LCA



PILOT PROJECT

NAVAL AIR SYSTEMS COMMAND
FLEET READINESS CENTER SOUTHEAST (FRCSE)

SCOPE


Occupation of Land
Natural Resource Use
Air Emissions
Water Emissions
Components
Anodized Components
Defense Input Output (DIO) Database
Waste
Electricity
Tap water
Materials
Fuel
Rinse water production
Rinse water
Aluminum Anodize Line
Wastewater
Industrial Wastewater Treatment Plant 2/3
Steam production
Steam
Air Emissions
Exhaust stack/ scrubber
Background – DoD Supply Chain
Foreground – Fleet Readiness Center Southeast

LIFE CYCLE INVENTORY

OLD/RAISED ANODIZE LINE (UNIT PROCESS)

Material inputs (old/raised line) Tape, brite pads, and other supporting materials are outside the scope of this study

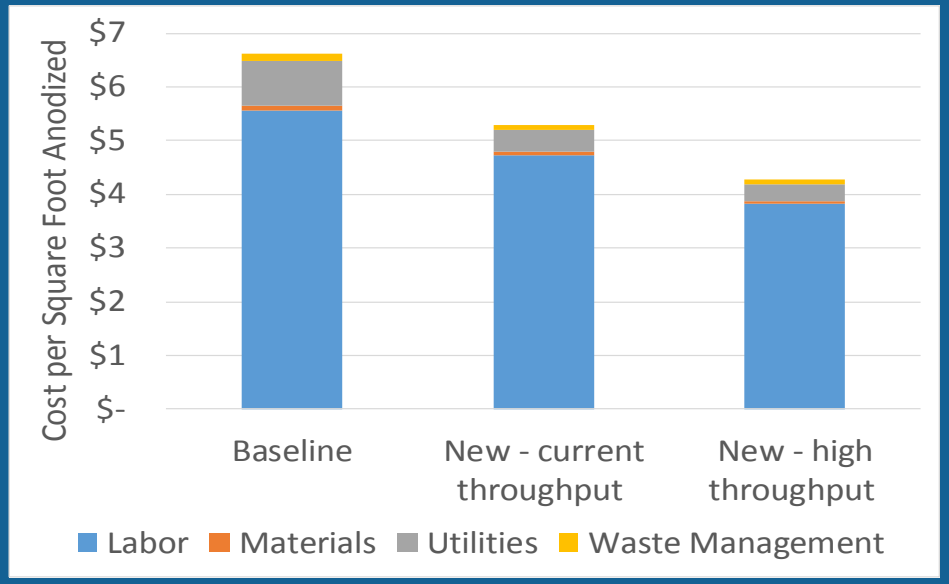
Description	Usage	Units	Annual Usage		Cost	Units	Cost per Year	NAICS	Data Source(s)
Sodium dichromate	70	lbs/year	70.000	$	326.74	$/100 lbs	$ 228.72	325180 Other Basic Inorganic Chemical Manufacturing	FRCSE consumable records
Aluminum ball cathodes	0.67	cathode/year	0.67		$1,000.00	$/cathode	$ 666.67	332812 Metal Coating, Engraving (except Jewelry and Silverware), and Allied Services to	FRCSE Metalast ROI/CBA
Sulfuric acid	201.33	gal/year	201.33	$	210.00	$/6.5 gal	$ 6,504.62	325180 Sulfuric acid manufacturing	FRCSE consumable records
Aluminum sulfate	80.58	lbs/year	80.58	$	22.75	$/50 lbs	$ 36.67	325180 aluminum sulfate manufacturing	FRCSE consumable records

Amount used in a year

Annual cost

Link to DIO (supply chain)

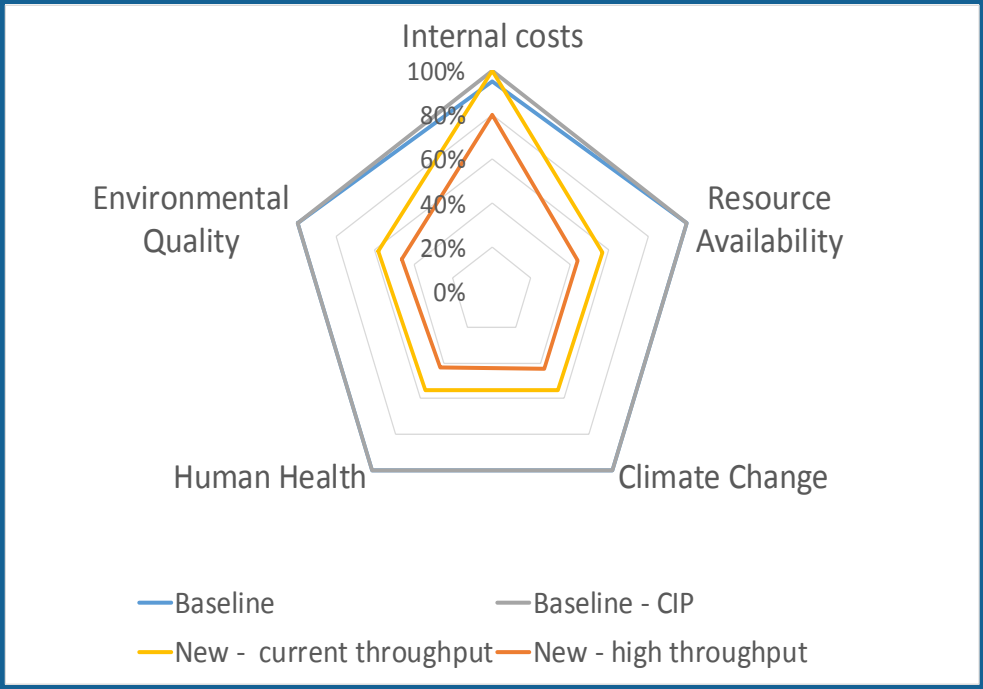
LIFE CYCLE COSTING



	Baseline	Baseline – with CI	New – current throughput	New – high throughput
Initial Costs (occur in year 0)				
Equipment & Materials	$-	$1.51	$23.38	$17.99
Labor	$-	$0.84	$-	$-
Annual Costs (recurring)				
Labor	$5.56	$5.56	$4.72	$3.81

	Baseline	Baseline – with CI	New – current throughput	New – high throughput
Materials	$0.09	$0.09	$0.07	$0.05
Utilities	$0.84	$0.84	$0.41	$0.32
Waste Management	$0.13	$0.13	$0.09	$0.09
Net Present Value	**$91.01**	**$95.65**	**$96.19**	**$76.80**

INTEGRATED IMPACT & COST RESULTS



Alternative	Internal costs	Resource Availability	Climate Change	Human Health	Environmental Quality
Units	*USD*	*MJ extra*	*kg CO2-eq*	*DALY*	*PDF*m2*yr*
Baseline	1.1E+2	1.5E+6	8.5E+5	5.1E-1	8.2E+3
Baseline - CIP	1.2E+2	1.5E+6	8.5E+5	5.1E-1	8.2E+3
New - current throughput	1.2E+2	8.4E+5	4.7E+5	2.8E-1	4.8E+3
New - high throughput	9.6E+1	6.5E+5	3.7E+5	2.2E-1	3.8E+3

THANK YOU



Check it out!

SERDP-ESTCP Symposium, Washington, DC

Short Course: Sustainability Analysis - Capturing Life Cycle Impacts and Costs in Defense Systems

November 30, 2017

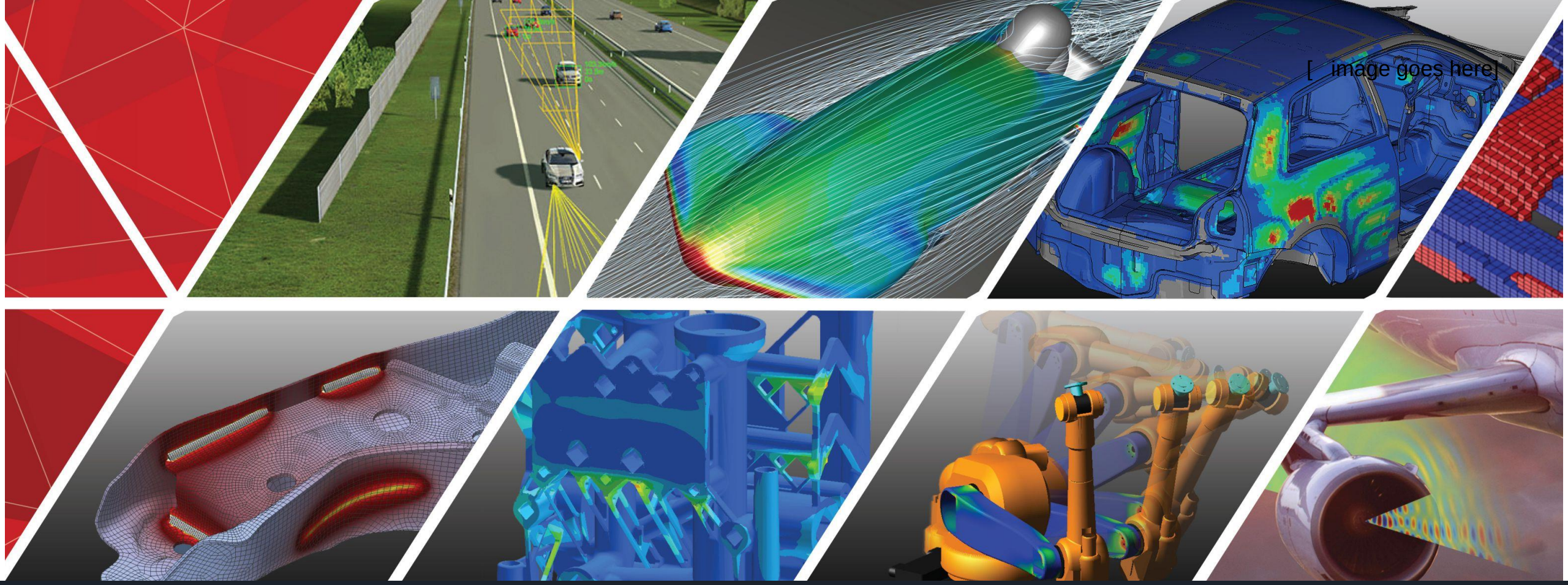
Kelly Scanlon

Chemical & Material Risk Management Program

Office of the Assistant Secretary of Defense (Energy, Installations, and Environment)

kelly.a.scanlon4.civ@mail.mil

703-571-9073



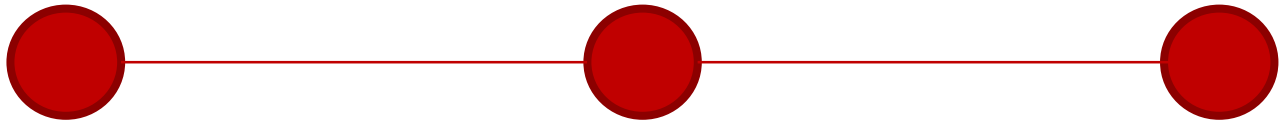
MSC Software

Model Based Systems Engineering (MBSE) Considerations for ESOH

Leo Kilfoy, General Manager
Engineering Lifecycle Management Business Unit
Oct 26, 2017

PART OF HEXAGON

Agenda

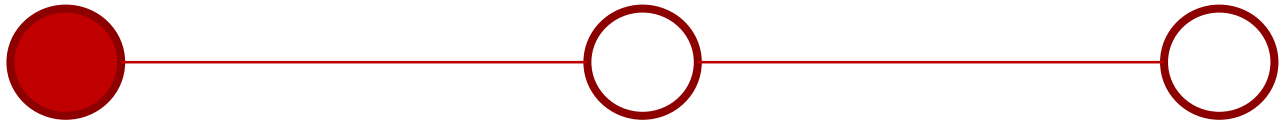


Brief Intro to MSC & ELM

ELM & MBSE Use Cases

MBSE for ESOH

Brief Intro to MSC & ELM



Brief Intro to MSC & ELM

ELM & MBSE Use Cases

MBSE for ESOH

MSC Software Company at a Glance

Company Overview

- Leading provider of computer aided engineering (“CAE”) software solutions
  - ✓ Mission critical simulation & analysis (”S&A”) products enabling engineers and analysts to validate and optimize their designs
  - ✓ Complement and / or replace the traditional physical prototype-based “build-and-test” product design process
- **Value proposition:** Improve quality, accelerate time-to-market and save costs associated with design and test of manufactured products
- Recently acquired by Hexagon Manufacturing Intelligence

Strong Core Business

- Virtually every auto, aero & heavy machinery OEM is a customer
- 25+ year relationship with the top 50 customers
- Broad core product portfolio (built over 40+ years) complemented by investments in new in-house extensions and complementary acquisitions
- Acquisitions – Best in class acoustics (FFT), multi-phase material modeling (e-Xstream engineering) and mechanical joining and welding (Simufact)

Game Changing CAE Platform: “Apex”

- Game changing CAE platform
  - ✓ Complements and significantly extends the core simulation solutions
  - ✓ 19 patents filed so far, 5 awarded to date
  - ✓ Award winning

GOLDEN MOUSETRAP AWARDS 2015 WINNER

TECH BRIEFS 2014 Product of the Year Finalist

INNOVATIONSPREIS-IT BEST OF 2015 initiative mittelstand INDUSTRIE & LOGISTIK

THE INTERNATIONAL BUSINESS AWARDS℠

THE AMERICAN BUSINESS AWARDS™

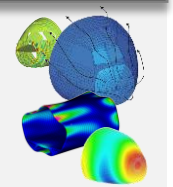
Key Highlights



- ***Founded:*** 1963
- ***HQ:*** Newport Beach, CA
- ***Total Offices:*** 27

MSC’s Value Proposition

AIRBUS AN EADS COMPANY



Airbus Leverages MSC to Reduce Aircraft Noise

Noise Reduction

Key Results: Understand the effects of various parameters such as the excitation type, the presence of the floor, and the variable thickness on the interior noise levels

BUGATTI



MSC Helps Bugatti Build The World’s Fastest Cars

Vehicle Dynamics

Key Results: Successfully develop chassis and driveline performance prior to building first prototype

NISSAN INFINITI.



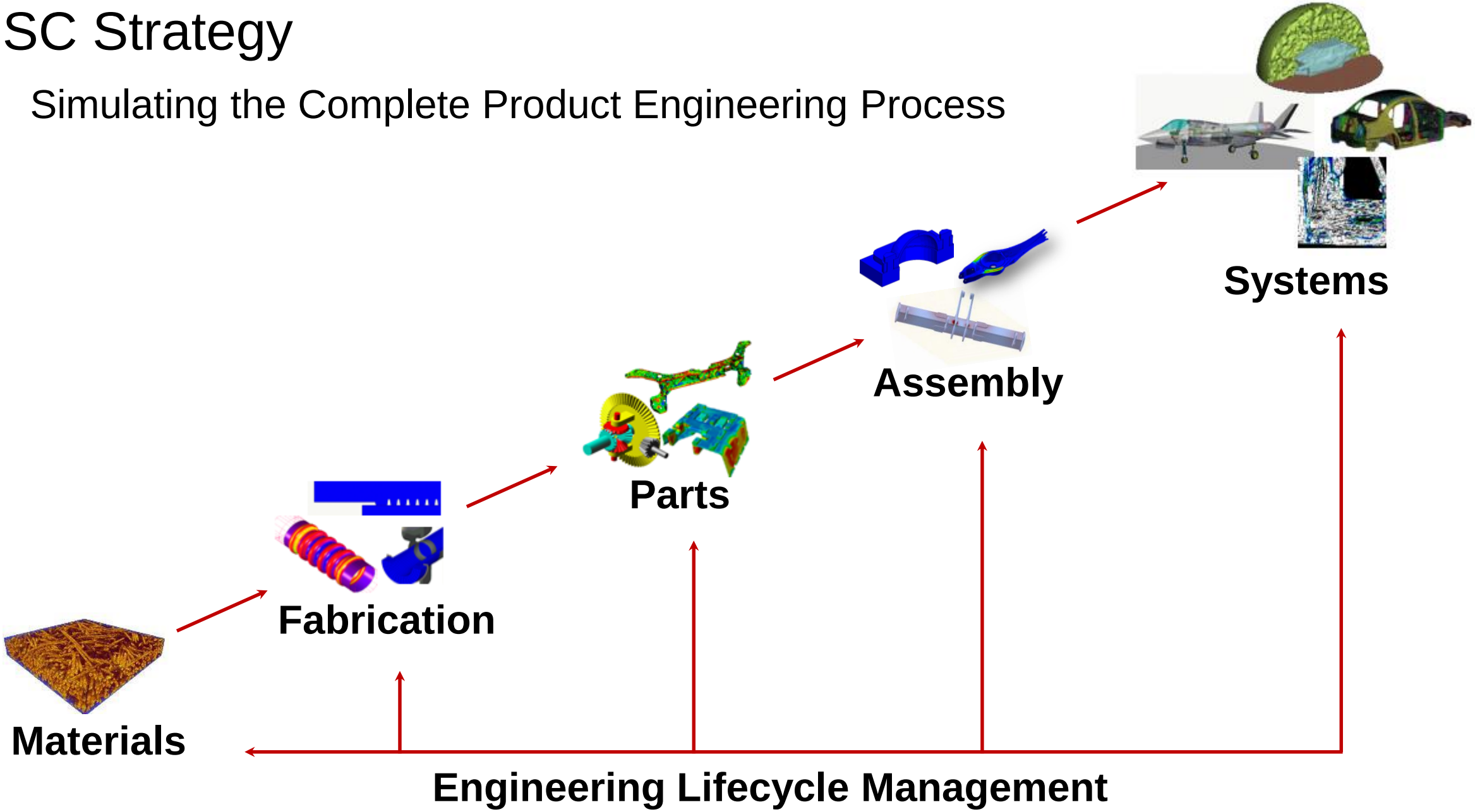
Nissan Uses MSC To Design Quieter Cars

Noise Vibration and Harshness (NVH)

Key Results: Improvement of the fidelity of numerical models thanks to the accurate representation of trim components

MSC Strategy

Simulating the Complete Product Engineering Process



ELM = Engineering Lifecycle Management

- ELM manages **process & data** for engineering related domains across the product lifecycle
  - Engineering information includes **environment, simulation, materials and test**
- ELM integrates to the Enterprise
  - ***Relation to PLM:*** ELM directly integrates across all phases (Concept, Design, Realize and Support) of Product Lifecycle Management (PLM)
  - ***Relation to MBSE:*** ELM Tools supports MBSE by managing engineering information in engineering domain specific models
    - Allows teams to build products and address problems in **domain context**
    - Integrated Domain Modeling and Analysis supports **Engineering Decision**



- MSC's ELM Enterprise Tool Suite
  - **SimManager** is the ***Engineering Model Factory*** for MBSE
  - **Material**Center is a ***Materials Lifecycle Management*** system for the enterprise

Who Uses ELM?





- Target Company Profile
  - **Distributed** geographically & organizational engineering teams
  - Need for iteration to **optimize** performance
  - **Regulatory** environment / **Liability**
  - Unfilled **headcounts**
  - Useful for **Complex Design** Environments
    - Products (cars, planes, rockets, etc.)
    - Duty cycles (100s of load cases)
    - Multi-stage, multi-discipline simulations
- Benefits
  - Drives quality, consistency, and collaboration
  - Managing engineering information across the **Product Lifecycle**
  - Increased **productivity**
  - **Throughput**

SimManager: Delivering the Digital Thread to Industry

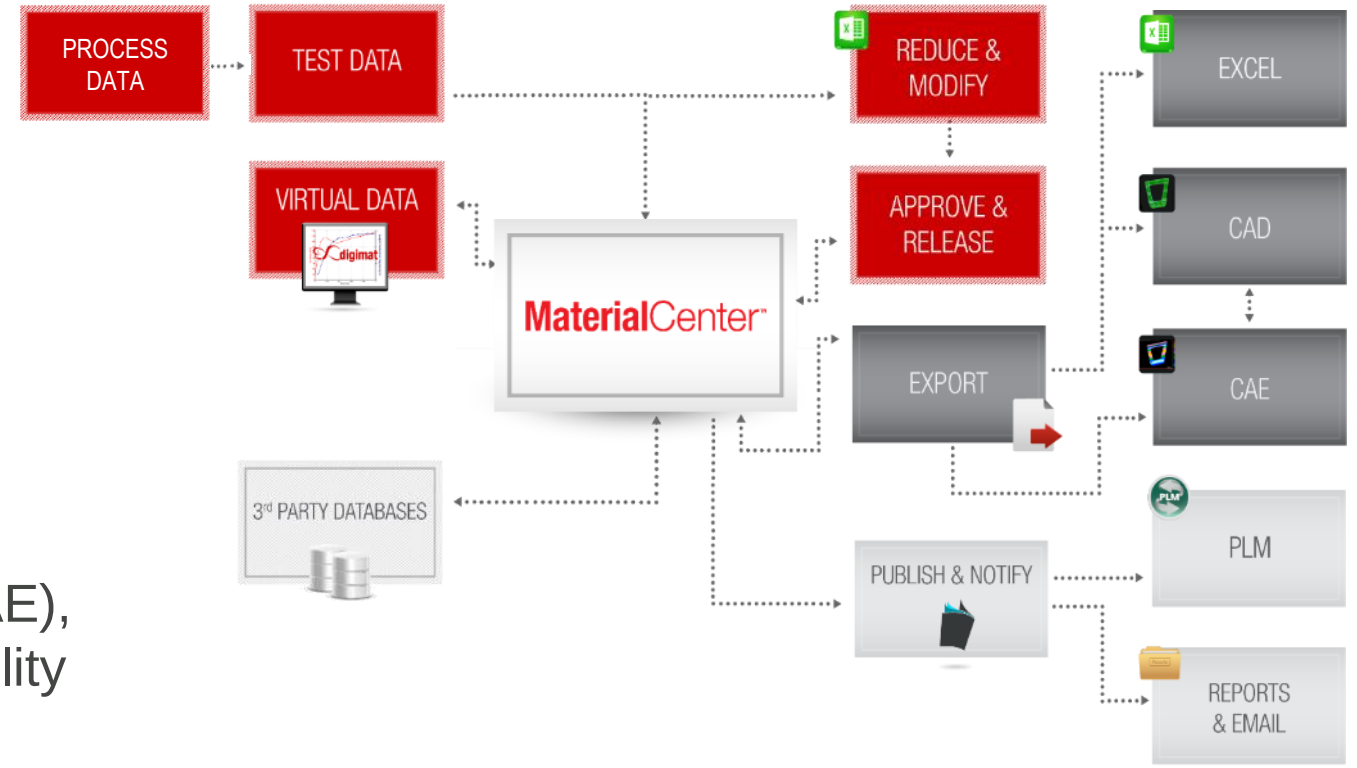


- **Automotive**
  - Managing Vehicle Level Simulation & Teaming
  - Developed across 17 years of Simulation Process & Data Management experience
  - Covering a broad set of disciplines (Strength, Crash & Safety, CFD, Durability, MBD, NVH, etc)
  - Global teaming at OEM and Tier 1 levels
    - Audi, BMW, PSA, Daimler, VW, Ashok Leyland, Brilliance, FAW, FAW Car, ChangAn Auto, Scania, ZF, GKN Driveline, Dicastal, etc.

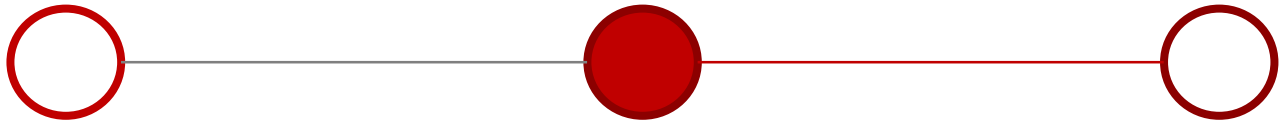
- **Aerospace & Defense**
  - Delivering consistent solutions faster across product lifecycle
  - Managing
    - Global/Internal Loads
    - Test-to-Virtual Comparisons/Management
    - Detailed Analysis/Sizing
    - Sustaining fleet in service repair analysis (Digital Twin)
    - etc.
  - Broad customer base
    - Airbus, Boeing, Leonardo, UTAS, Embraer, St. Gobain, Oshkosh Defense, Cobham, etc

MaterialCenter: Managing Materials Lifecycle

- MaterialCenter is a Material Lifecycle Management (MLM) system
- Scope:
  - Manufacturing & Process Data
  - Physical & Virtual Test
  - Materials Discipline
  - Engineering: CAD, CAE, PDM/PLM
- Integrates across all PLM Lifecycle phases
- Supports MBSE by managing multiple material models (Test, Design, CAD, CAE), material revision history and full traceability



ELM & MBSE



Brief Intro to MSC & ELM

ELM & MBSE Use Cases

MBSE for ESOH

MBSE: Model Based Systems Engineering

- MBSE
  - is a Systems Engineering methodology focused on using **domain models** as opposed to documents for engineering
  - includes behavioral, systems architecture, requirements, performance, simulation, test, etc.
  - lowers risk and improves system understanding **across the product lifecycle**
- MSC ELM
  - is broadly focused on MBSE, specifically **Simulation, Materials & Test domains**
  - supports MBSE providing system behavior, performance & risk to facilitate **decision making process**

ELM Solution in the PLM

Interaction with PLM components of the Development Process

Addresses a Range of Questions

Can I build it?

Is it durable?

Will it fail?

Is it safe?

Can I test it?



Will it perform?

Is it crashworthy?

Why did it fail?

Can it be lighter?

Is it too loud?

ELM Solution in the PLM

Interaction with PLM components of the Development Process



Product Requirements
& Objectives

Question

PDM

Product Definition

Environment for Simulation

Can I build it?

Is it durable?

Will it fail?

Is it safe?

Can I test it?



Will it perform?

Is it crashworthy?

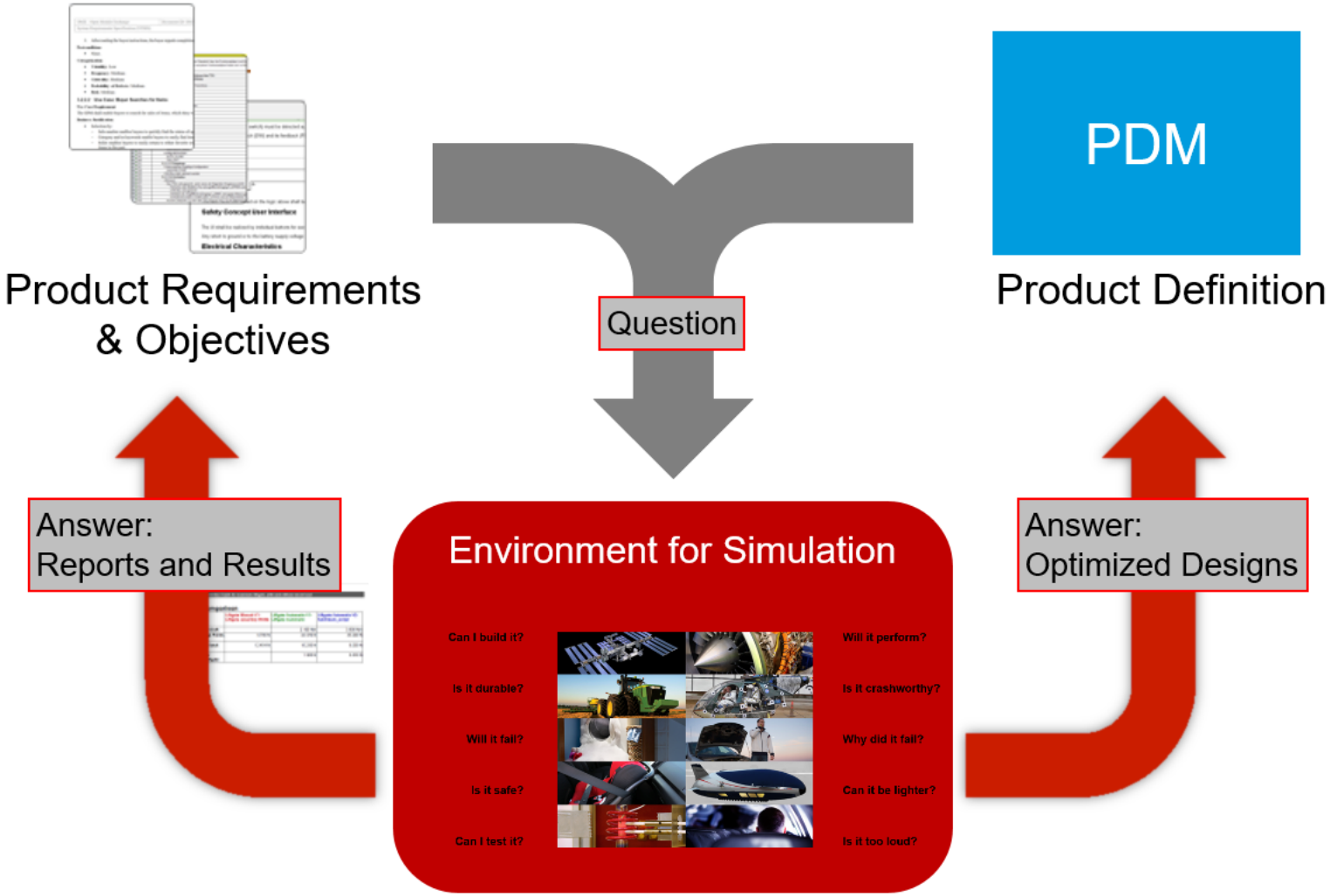
Why did it fail?

Can it be lighter?

Is it too loud?

ELM Solution in the PLM

Interaction with PLM components of the Development Process



ELM Solution in the PLM

SimManager: Building the required Simulation Environment



Product Requirements & Objectives

PDM

Product Definition

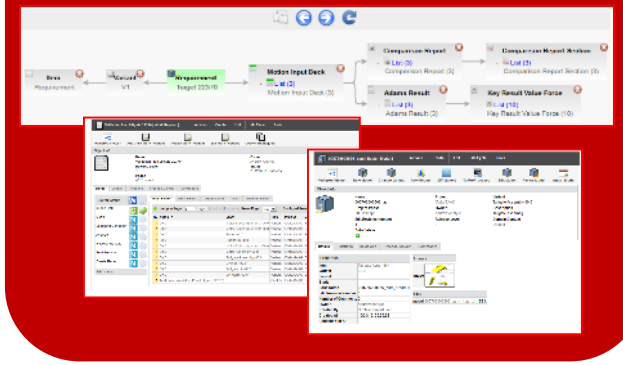
Question



Answer: Reports and Results



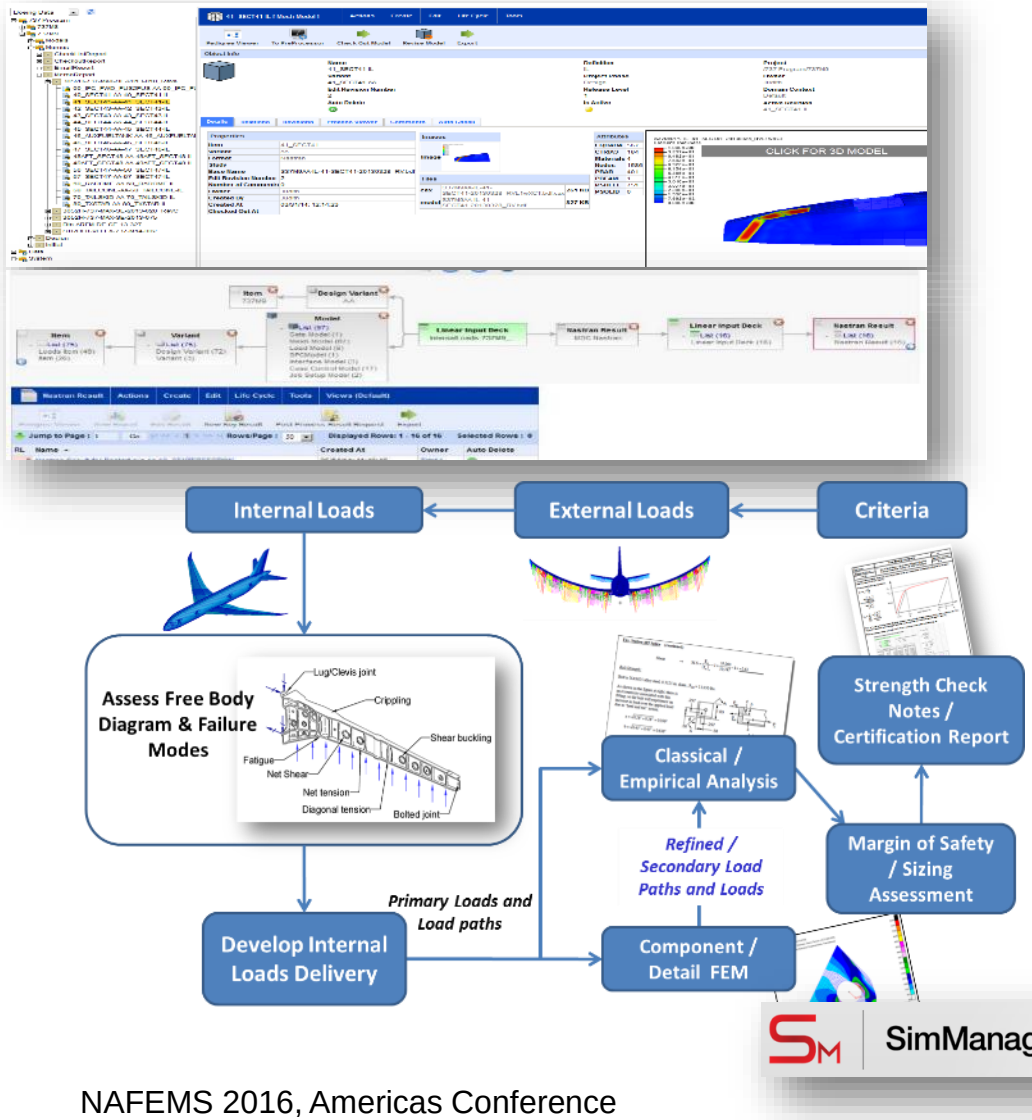
SimManager



Answer: Optimized Designs

Boeing Internal Loads

- Internal Loads…
  - are **critical** in the airplane design process
  - revisions have **significant impact** on engineering activities
  - derive from an **assembly** of subsection component models
  - must be consistent and authored through a **controlled release process**
- Needs
  - Support management across a **long product lifecycles** (30-50 years)
  - Managing **precise version control** & pedigree of inputs/outputs
  - Drive better performance & **throughput**
- Project Status
  - Production on 737 MAX project
  - Rolling out other aircraft programs

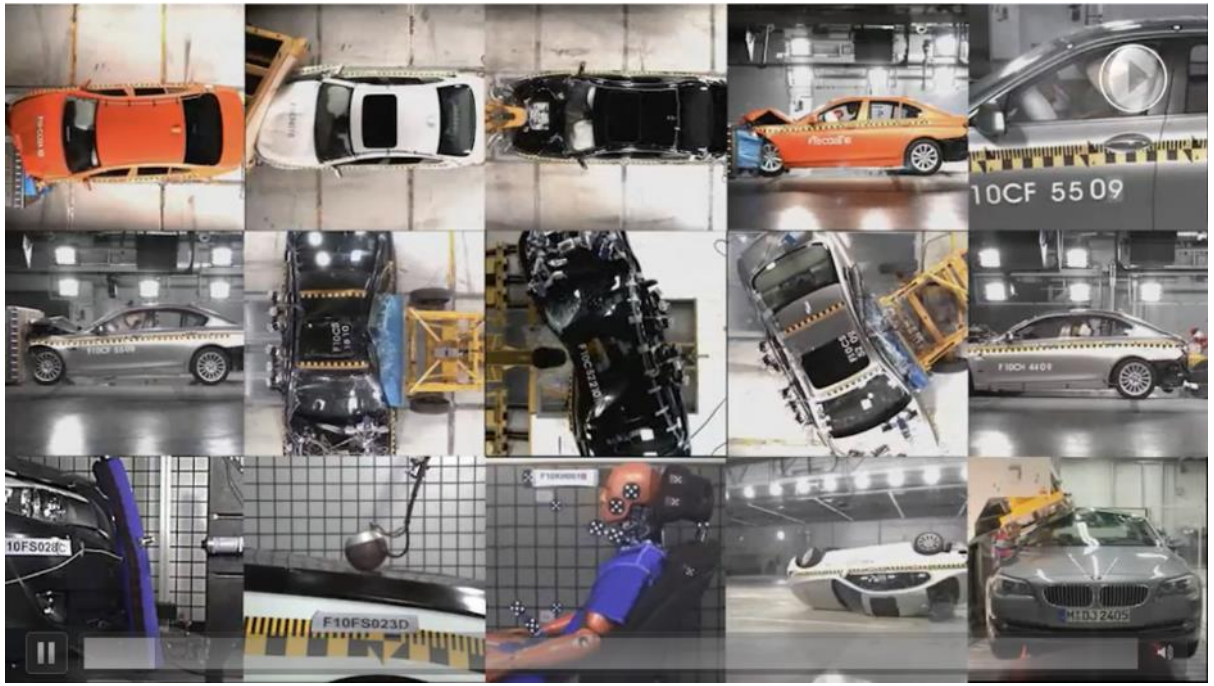


BMW

- Need
  - Build safer, more reliable product
  - **Innovate** product quicker
  - Improve engineering **throughput**
  - Drive **consistent, repeatable analysis** from engineer to engineer
- SimManager manages…
  - all Occupant Safety, Head Impact, Pedestrian Safety, Crash, NVH, Forming, Interior, Exterior, Driveline, MBD, CFD disciplines **for all vehicle programs**
  - a global simulation team **across 4 continents**
  - **all organizations** in BMW including car, engine, sport & motorcycle
  - **Scale** - 1000's simulations, 100's of users… every day… producing Pb's of data every year



Physical Test
Example: BMW 5 Series Crash Tests

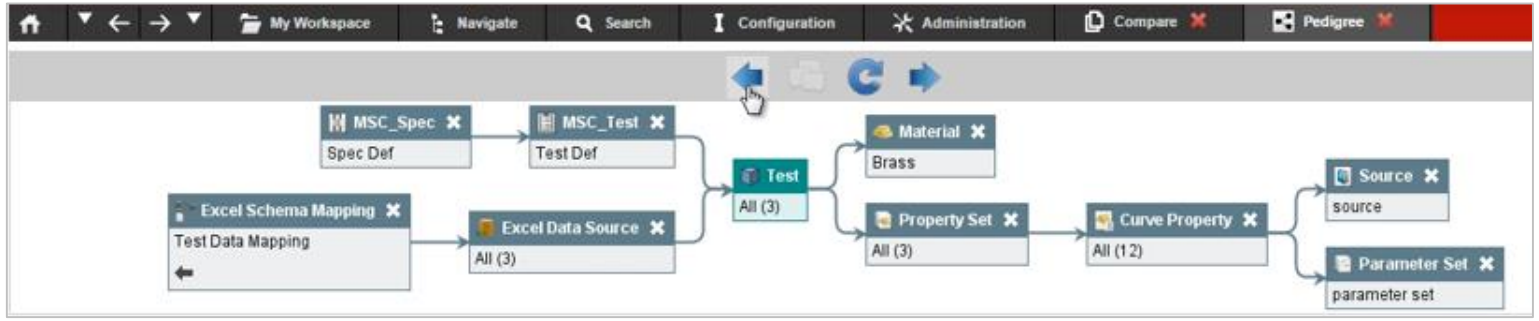




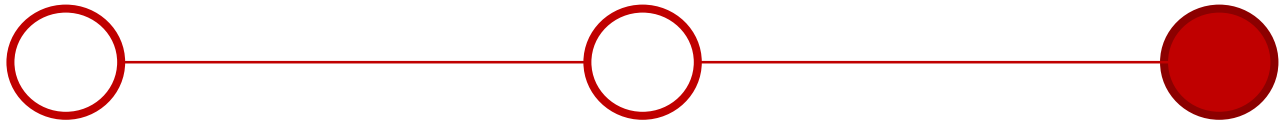
Managing Test & Design Data in Aerospace

UTC Aerospace Systems

- Customer Need
  - Integration of multiple business units to manage **multiple material models** (composites, metals, plastics, etc.) for **multiple material disciplines** (Test, Design, CAD, CAE)
- MaterialCenter Solution
  - **Precise tracing** the who, what, where, when, and why for Aerospace material management.
  - ITAR and EAR compliant **security** methods.
- Value
  - Enabling **collaboration** of engineers from various geographical locations.
  - Robust **material object model** for managing data from various sources and test standards supporting multiple disciplines (Test, Materials Engineering, CAD, CAE)



MBSE for ESOH



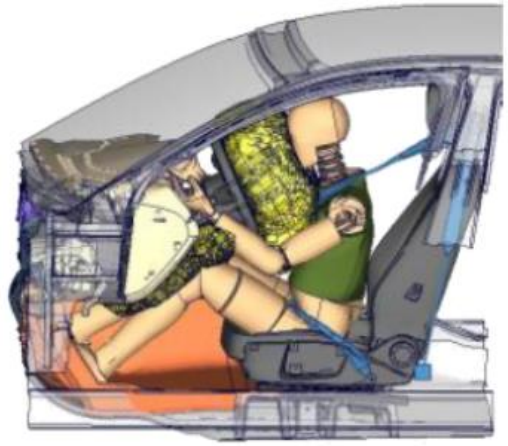
Brief Intro to MSC & ELM

ELM & MBSE Use Cases

MBSE for ESOH

MBSE – ESOH: Safety Simulation

- Simulation of Models across various disciplines provides **evaluation of system safety and performance**
- Simulations can represent **complex events of complex systems** involving human interaction, such as occupant safety or pedestrian protection
- **Traceability** across simulations is critical to relate outputs (results/reports) to specific revisable inputs and events (pedigree finger print)
- **Simulation automation** provides for faster evaluation supporting
  - **Consistent, repeatable** evaluation
  - Potential **changes in requirements** from theater
- MBSE simulation frameworks must support **multiple representations** (CAD, FEA, CFD, 1D, etc)





MBSE – ESOH: Chemical Compliance

- Over 100 different organizations are defining governance for chemical compliance & safety globally
  - Common examples include REACH, RoHS, etc
- Chemical compliance involves evaluation of
  - Base material and composition
  - Regulatory requirements, source & identification (CAS)
  - Quantification & Usage (areas, volumes, etc)
  - Processing information
- Data comes from multiple sources
  - Geometry (CAD/PDM), Supplier (ERP), Material (MLM)
- MBSE Models must include Material, Supplier(s), Geometry, Processing Information, Regulations
  - All Parts must have traceable material composition
  - Models should reference regulatory information to support evaluations
  - Data must be tracked across product lifecycle as regulations are continuously updated
- MBSE models can provide history of past evaluations & provide fast evaluation against future regulations





Questions



Thank you

Cybersecurity and Modular Open Systems Approach

October 26, 2017

Bill Decker
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35806
724-612-0999
For further info: tim.denman@dau.mil

Approved for Public Release

Ground rules

- This is a discussion, not a lecture
- Your opinions and viewpoints are welcomed
- There are no right/wrong answers

Agenda

- Introduction
- Modular Open Systems Approach
  - What is it?
  - Why do we want (or have) to do it?
  - What does it mean to the SE?
- Cybersecurity
  - Critical requirement, often not clearly stated
- Discussion
  - How can we serve both masters?
- Conclusion

Introduction

- Assumptions (remember what they do)
  - MOSA – open means publically available technical data and software
  - Cybersecurity means no vulnerability to cyber attack

FY17 NDAA MOSA Definition
Sec. 805, §2446a (b)(1) p.253

- Congressional MOSA Definition – FY17 Legislation

- An integrated business and technical strategy that:
  - (A) Employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms;
  - (B) Is subjected to verification to ensure major system interfaces comply with, if available and suitable, widely supported and consensus-based standards;
  - (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 system;
  - (D) complies with the technical data rights set forth in Sec 2320, title 10.

MOSA Community Definitions

- Current MOSA Terminology – OSA Contract Guidebook
  - "Modular Open Systems Approach or MOSA" is the DoD's implementation of Open Systems. Within the MOSA context, programs should design their system based on adherence to the following five MOSA principles: Establish an Enabling Environment., Employ Modular Design, Designate Key Interfaces, Use Open Standards, Certify Conformance. *[A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF]*
  - "Open Systems Approach" means an integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industry standards organization. [*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*]

SE activities

- Identify modules in the system
  - May be hardware or software or combination
  - DoDAF architectural artifacts may be used
  - Internal to system, as well as system to system
- Identify key interfaces
  - Specify standards to be employed
- Work with PM to identify and ensure delivery of needed technical data/software
- Manage technical risk for PM

Cybersecurity Implementation into Acquisition Programs – 3 Sub-processes

- **Requirements Generation**
  - The PM team and requirements developers must be cognizant of the mandatory System Survivability KPP, which includes cyber survivability requirements
  - PMs will need to deliver systems that are able to operate and complete their missions in cyber-contested environments.

- **Acquisition and Program Management**
  - PMs must address cybersecurity in program reviews, including Deep Dives, In-Process Reviews, and Overarching Integrated Product Team (OIPT) meetings
  - The PM needs to build an IPT structure that includes cybersecurity expertise.

- **Systems Engineering and Test and Evaluation**
  - Implementation of a disciplined systems engineering process that includes cybersecurity is required from requirements analysis through design, test and evaluation, fielding, sustainment, and decommissioning.
  - The PM must develop a cybersecurity Test and Evaluation (T&E) strategy, allocate resources for cybersecurity T&E, and ensure they are described in the TEMP.

SE Role in Cybersecurity

- Cybersecurity strategy
  - Identify cyber risks
  - Work with IPTs to determine controls that are appropriate
  - Implement controls/reporting
  - Integration with Program Protection Plan (PPP)
  - A multi-disciplined Systems Security Engineering (SSE) WG can provide an integrated PPP that includes the Risk Management Framework (RMF), Supply Chain Risk Management (SCRM) and protection of Critical Program Information (CPI).
- Work with internal/external cyber assets
  - DoD and Service CIOs, NSA, DISA, etc.
  - Authorizing Officials (AO) and Security Control Assessors (SCA)

Discussion

- Pros vs Cons of public interfaces

Pros	Cons
Identified early	Identified early
Controls applied from start	Exploitation has more time
Benefits of MOSA	One exploit approach works for many applications
More open evaluation of the interfaces	Monocultures: Same vulnerabilities
??	

Conclusion

- Challenge is to implement MOSA without compromising security
  - Must be planned from start
  - Shortcuts lead to risk
- PMs should be intimately involved

MOSA Considerations Throughout the Systems Engineering Lifecycle - Implementation Guidance

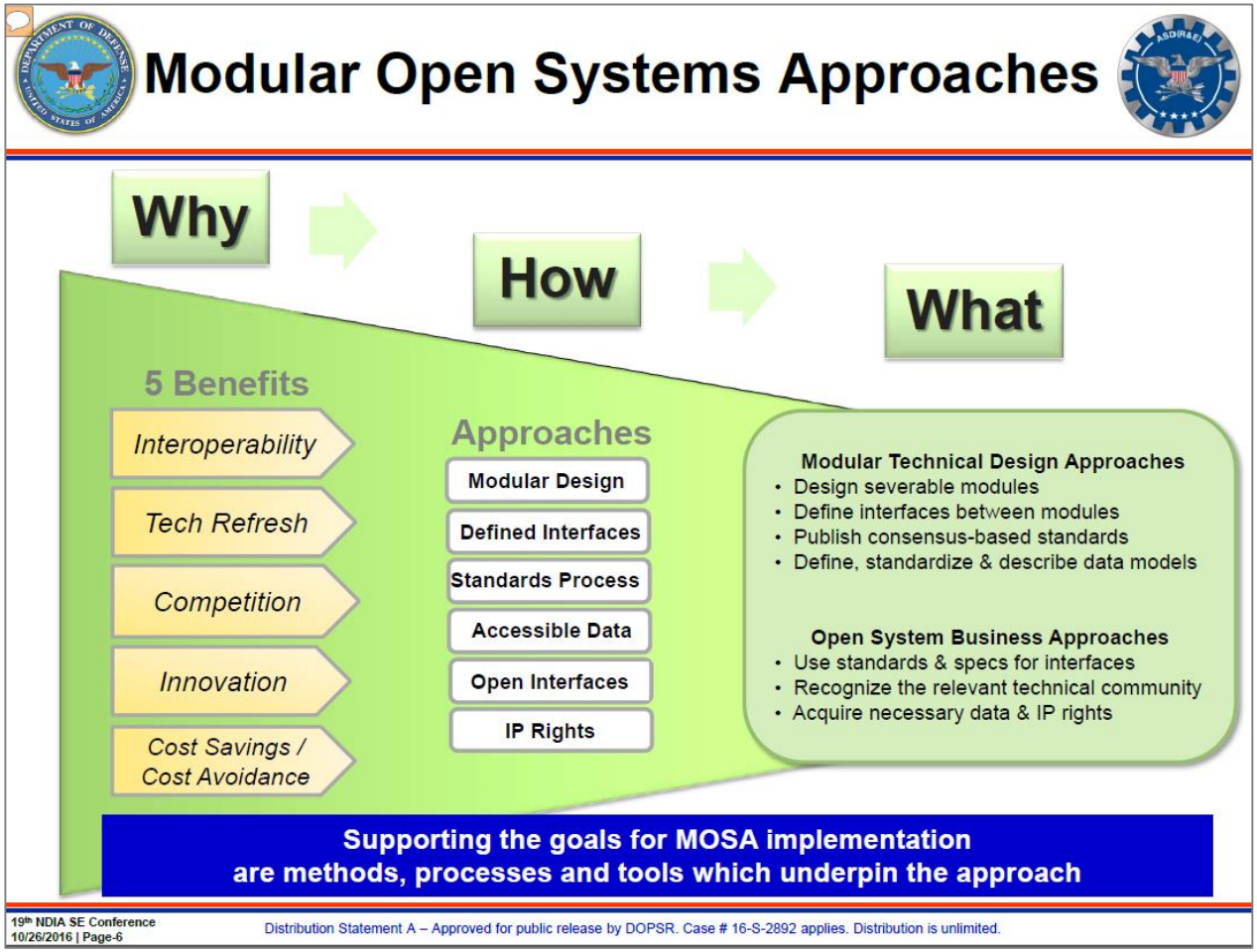
Philomena Zimmerman
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Judith Dahmann, Mimi Hailegiorghis, George Rebovich, Peter Korfiatis, Brian Soeder
The MITRE Corporation

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

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Benefits and Approaches



Challenge:

How do we translate this into practical MOSA considerations incorporated into systems engineering activities at each acquisition stage?

Enabling security has been identified as an added MOSA benefit

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

Assumptions

- **Implementation of modularity and open systems in a system development or upgrade can provide particular benefits to each system**
- **To achieve these benefits for a system it is important to**
  - Understand the objectives and drivers for a new system or system upgrade early and assess how modularity and open systems can be used to achieve these objectives
  - Address MOSA considerations at each stage in development as they apply to the desired benefits for the particular system
- **This needs to be done as an integral part of the systems engineering for the system with relevant MOSA considerations in trades at each stage of development**
  - AoA, preferred solution, requirements, design, development and test
- **…. and relevant MOSA considerations need to be reflected in acquisition, systems engineering and test planning**

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

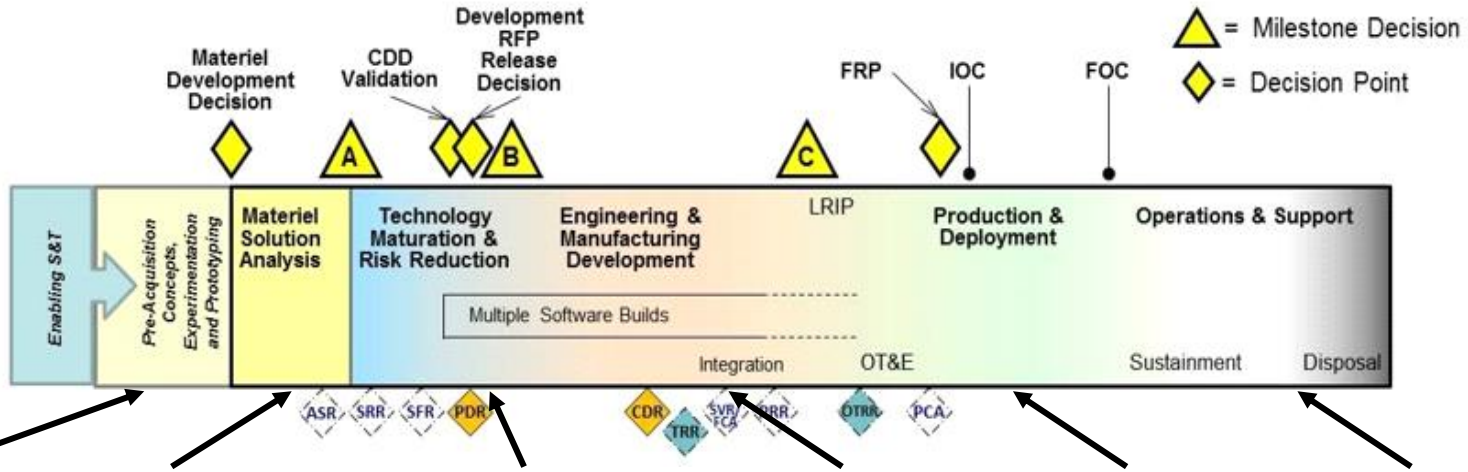
The Basic Concept

- **To effectively implement modularity and open systems through SE to achieve system objectives ….**
  - Identify where MOSA can benefit the system as envisioned and factor this into **actions throughout the entire lifecycle**
  - Begin with assessing the o**bjectives and drivers of the future deployed system** with a MOSA perspective at the earliest point
- **Key points**
  - **Tailor** use of MOSA to the situation of the **particular system**
  - Identify **opportunities for MOSA** benefits at the **inception** of the system development
  - Implement **engineering follow-though** at each stage to ensure these MOSA benefits are explicitly addressed in the engineering decisions **as part of the systems engineering process**

Develop a set of MOSA considerations and related questions to be addressed at each stage of development

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations At Each Stage



Pre-MDD: What are the drivers for this system and how can MOSA support these? Are these addressed in AoA guidance?

MSA: Does the preferred solution provide opportunity to employ MOSA to achieve system objectives?

TMRR: Are the factors to achieve desired MOSA benefits included in acquisition strategy, SE Plan, and T&E strategy, lifecycle support strategy, RFP and preliminary design?

EMDD: Does the detailed design and developmental test incorporate MOSA considerations, to assure design and development will achieve expected benefits?

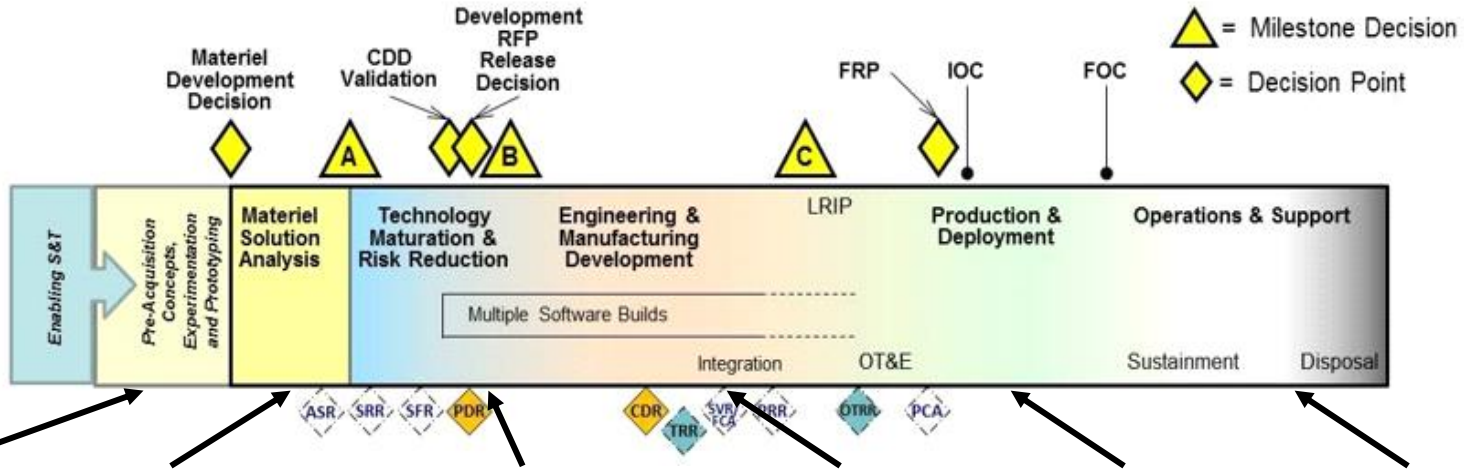
P&D: Does the plan include continued review, testing and evaluation to ensure the product baseline modularity and openness?

O&S: How is support of the system structured to take advantage of the MOSA characteristics expected to benefit the systems?

Planning for P&D and O&S needs to be done early

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

Questions to Be Addressed Though Life Cycle Stages



Pre-MDD: What are the drivers for this system and how can MOSA support these? Are these addressed in AoA guidance?

MSA: Does the preferred solution provide opportunity to employ MOSA to achieve system objectives?

TMRR: Are the factors to achieve desired MOSA benefits included in acquisition strategy, SE Plan, and T&E strategy, lifecycle support strategy, RFP and preliminary design?

EMDD: Does the detailed design and developmental test incorporate MOSA considerations, to assure design and development will achieve expected benefits?

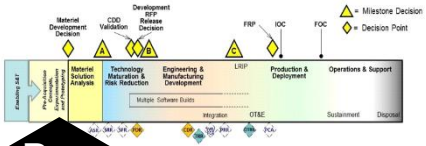
P&D: Does the plan include continued review, testing and evaluation to ensure the product baseline modularity and openness?

O&S: How is support of the system structured to take advantage of the MOSA characteristics expected to benefit the systems?

Planning for P&D and O&S needs to be done early

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Pre-Materiel Development Decision



- **Questions to assess how each of the 5 benefits might apply to the system being considered**
- **Identify the *specific system components* for modularity and open systems.**

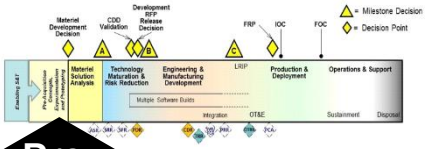
Interoperability | **Tech Refresh** | **Innovation** | **Cost Savings/Cost Avoidance**

Enhanced Competition			
Rationale	**Pre-MDD**	**Questions**	**Actions**
Modularity and open systems enable **enhanced competition** by allowing for acquisition of components of the system at the outset and over time **to be offered and obtained from all providers**, allowing for more competition selection of best match, **regardless of previous provider, on a component level**.	To make this feasible, those components of a prospective system which may be **amenable to independent procurement**, need to be identified and there needs to be **analysis to determine that there are multiple prospective suppliers**. Once identified, it is important identify system solutions which allow for making these components as separable modules in the system design with clear definition of functionality and interfaces. While these specifications will not be defined until later phases of the development, at this stage, it is important to ensure that the **alternatives being considered do not preclude such a design**, and that the **considerations in the Analysis of Alternatives (AoA)** address the ability to modularize the design to enable enhanced competition for these particular components of this prospective system.	• Given the alternatives being considered, **are there components or types of components which could benefit from enhanced competition? What are these components?** • Is there a large **performer base** for ..... types of systems considered in the alternatives**? Commercial availability and variety**? Commercial maturity? Market availability? • Do the **alternatives being considered allow for modularity and open systems** approaches which would support enhanced competition .....? • Does the **AoA guidance** call for consideration of potential of modularity and open systems to .....? • Does the AoA guidance include **business considerations, relative to data rights** for components and performers, that will enhance competition? Specific products to consider include reference architecture, technical standards ..... •	The need to apply MOSA to enable enhanced competition for specific components (or component types) should be included **in an initial version of the modularity and open system plans** for this acquisition and in **early system requirements and design considerations**. In particular, the plan should identify the **specific type of components which benefit from MOSA** for enhanced completion and the **supporting business case**, including evidence of available suppliers of the particular components. At this stage, the most useful .... **focus on functional architectures and logical grouping of functions that would enable MOSA implementation later**. *[Example: Sensor on a weapons platform]*

Snapshot example – comparable tables for other benefits

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Pre-Materiel Development Decision



- **Questions to assess how each of the 5 benefits might apply to the system being considered**
- **Identify the *specific system components* for modularity and open systems.**

Example questions

- Given the alternatives being considered, are there components or **types of components which could benefit from enhanced competition**? What are these components?
- Is there a **large performer base** for some or all of the elements in the types of systems considered in the alternatives? Commercial availability and variety? Commercial maturity? **Market availability**?
- Do the alternatives being considered allow for modularity and open systems approaches which would support enhanced competition for these components?

What are the drivers for this system and how can MOSA support them?

Sets the basis for considerations through life cycle stages

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

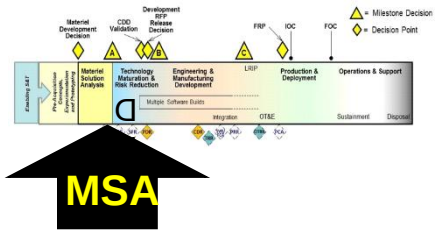
Describe Where System Can Benefit From Modularity or Open Systems

- **Based on the review of the Pre-MDD MOSA considerations for the system**
  - **Describe which components of the system can benefit, *identifying* the benefit, describing the *rationale* and pointing to a program *documentation* reference**
- **This information is carried through to subsequent stages as the basis for assuring follow-through in engineering trades and decisions**
- **May be revised based on new information or engineering decision**
  - **Key point is to assure that identified MOSA benefits are explicitly considered**

Component/Interface	MOSA Benefit	Rationale	Reported in …..
Name of component or interface identified as benefiting from modularity or open systems/ standards	Which of the MOSA benefits apply to this component/interface: Enhanced competition • Technology refresh • Incorporate innovation • Cost savings/cost avoidance • Interoperability	What is the rationale for applying MOSA to this component or interface?	How has this been documented? (e.g. reflected in the AoA Guidance, included in the AoA plan, other….)
Repeat for each component	Repeat for each component	Repeat for each component	Repeat for each component
Repeat for each component	Repeat for each component	Repeat for each component	Repeat for each component

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Materiel Solution Analysis



- **Questions on how the *system concept* supports achievement of the specific benefits anticipated for each specific system component identified for modularity and open systems**

Key activities during MSA

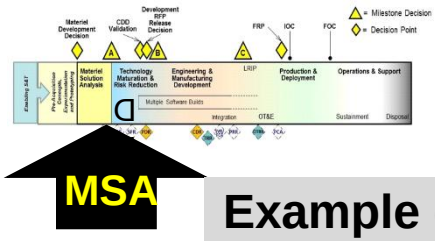
Enhanced Competition	
MSA Activity	**Questions**
Conduct AoA. Includes all activities and analyses conducted by the AoA Study team under the direction of the Senior Advisory Group/Executive Steering Committee (SAG/ESC) and CAPE, or Service equivalent. Concludes with a final SAG/ESC and AoA Report. Systems Engineers should support this activity.	• Where appropriate, does the AoA incorporate assessment criteria for promoting enhanced competition? o In particular, does the AoA analysis and results consider the **impact of alternatives on the ability of the system to independently procure** the <identified component>? (e.g. Does the solution provide the ability for the government to **replace/divest** the specific component?)
Perform Analysis to Support Selection of a Preferred Materiel Solution. Includes all engineering activities and technical analysis performed to support Service selection of the preferred materiel solution by balancing cost, performance, schedule and risk.	• Does the preferred solution allow for modularity and open standards which would be needed to independently procure the <identified component>? o That is, does the preferred solution allow for the <identified component> to **be a separable module with clear definition of functionality and interfaces amenable to independent procurement**? • **If not, have the consequences** of not being able to benefit from enhanced competition for the identified component **been explicitly factored** into the selection of the preferred solution?

Questions to help ensure MOSA considerations are addressed

Snapshot example: comparable tables for other benefits

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Materiel Solution Analysis



- **Questions on how the *system concept* supports achievement of the specific benefits anticipated for each specific system component identified for**

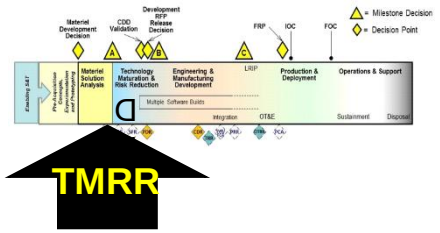
Example questions

- Where appropriate, does the AoA incorporate assessment criteria for promoting enhanced competition?
- Does the preferred solution allow for modularity and open standards which would be needed to independently procure the <*identified component*>?
- If not have the consequences of not being able to benefit from enhanced competition for the identified component been explicitly factored into the selection of the preferred solution?
- Does the market research address and do the results reinforce the expectation that there are multiple potential sources of the <*identified component*>?

Ensure that decisions about the preferred solution explicitly consider the potential benefits of MOSA identified for the system

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Tech Maturation and Risk Reduction



- **Questions about the preliminary design to assess the extent to which it supports *key design considerations* for the specific components identified for modularity and openness**

Key activities during TMRR

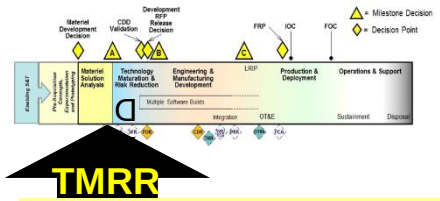
TMRR Activity	Questions
Perform Technology Maturation. The AS identifies technologies requiring further maturation before they can be implemented within a solution. Technology maturation involves design, development, integration and testing., ……	• Can the technologies addressed in the technologies **affect the modularity or open interfaces** of <**specific component(s)**>? o If so, are the modularity/interfaces of the <specific component(s)> considered in the technology maturation activities? o If not, what are the risks to the ability to achieve the expected benefits of MOSA for the <specific component(s)>?
Perform Prototyping. Prototyping is an engineering technique employed for several reasons: to reduce risk, inform requirements and encourage competition.	• Does the TMRR prototyping address **the modularity/interfaces** include MOSA (e.g., modularity and open system/standard interfaces of components and loose coupling of components), particularly the <**specific component(s)**> identified for the system? • Does the TMRR prototyping demonstrate the suitability of having "frameworks" and protocols for modularity, and the performance of those frameworks/protocols? o ….. • If **competition, innovation, or cost savings are among the prototyping goals**, are **MOSA elements explicitly** included in the prototype evaluation criteria? o ……
Perform System Trade Analysis. The Systems Engineer assesses alternatives with respect to performance, cost, schedule and risk, and makes a recommendation to the PM. The SE assessment should consider the full range of relevant factors, ……	• Do trade factors include MOSA elements such as interfaces or modularity particularly as related to the <**specific component**(s)> identified for **modularity/open interfaces** for this system? o …… • Do trade factors include **affordability, technology refresh, or interoperability**? How are the <specific component(s)> identified for modularity/open interfaces addressed in these trade studies?
Develop System Architecture.	• To what extent does the system's architecture identify functional allocation, functional dependency, distinct functional grouping of components that allows for loose coupling, and reflect the modularity/open systems for the <specific component(s)> identified for this system?

Questions to help ensure MOSA considerations are addressed

Snapshot example: Address these questions for each opportunity to benefit from MOSA

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Tech Maturation and Risk Reduction



- **Questions about the preliminary design to assess the extent to which it supports *key design considerations* for the specific components identified for modularity**

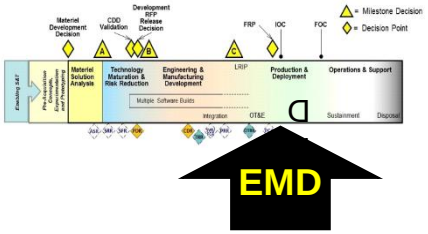
Example Questions

- Do the **architecture/preliminary specification** of the system include requirements for modularity and open systems approaches to allow for incorporation of new or improved capabilities without necessitating large changes to other elements of the system over the system lifecycle, particularly as this applies to the <*identified component*>?
- Do **prototyping** recommendations address MOSA-related requirements or solutions for enhanced competition, including areas of uncertainty or risk, feasibility of high-level conceptual designs, or the discovery or refinement of requirements?
- Do the **acquisition strategy, the systems engineering plan, the life cycle support plan and the testing strategy** address the need for modularity for the <*identified component*> to achieve enhanced competitiveness?

Are the factors to achieve desired MOSA benefits included in acquisition strategy, SE Plan and T&E strategy, lifecycle support strategy, RFP and preliminary design?

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Engineering, Manufacturing and Development



- **Questions about how the plans for the *detailed design and developmental test* incorporate MOSA considerations for the specific components identified for modularity and openness to assure *design and development* will achieve expected benefits**

Key activities during TMRR

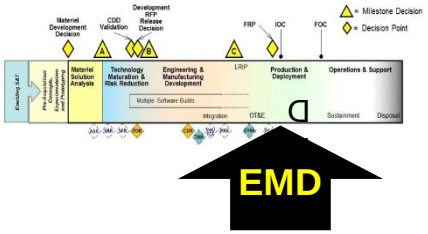
EMD Responsibility/Activity	MOSA Questions
Responsibility	
• Managing the system design to satisfy the **operational requirements**, within the constraints of cost and schedule, and to evaluate the system design, identify deficiencies and make recommendations for corrective action.	• Is due consideration given to the **modularity and open interfaces** of <**specific component**(s)> of the system as the system design is being refined to satisfy the operational requirements within cost and schedule constraints? • Have **the implications of the design changes to the MOSA objectives** for the <specific component(s)> of the systems been assessed? • Have alternative design approaches been considered that preserve MOSA objectives and requirements when modularity and openness of a <specific component(s)>been eliminated due to programmatic or other constraints?
• Conducting or supporting the technical evaluation in support of **source selection** for the EMD contract award.	• Do the **source selection technical evaluation criteria include modularity and open interfaces** for the <specific component(s)> ? • Do the source selection criteria include consideration of the proposers' capability to meet the system's MOSA objectives and requirements for the <specific component(s)> of the system?
• Maintaining **requirements traceability** and linkage to the initial product baseline.	• Are all **requirements for modularity and open interfaces** for the <specific component(s)> **traceable** and linked to the initial product baseline?
• Tracking and reporting initial product baseline changes after CDR and recommend the path forward in accordance with the **Configuration Management (CM)** process, ...	• Is attention paid to tracking and reporting of initial product baseline changes that **impact for modularity and open interfaces** for the <specific component(s)>? • Have the implications of the design changes on the for modularity and open interfaces for the <specific component(s)> been assessed?

Questions to help ensure MOSA considerations are addressed

Snapshot example: Address these questions for each opportunity to benefit from MOSA

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

MOSA Considerations: Engineering, Manufacturing and Development



- **Questions about how the plans for the *detailed design and developmental test* incorporate MOSA considerations for the specific components identified for modularity and openness to assure *design and development* will achieve expected benefits**

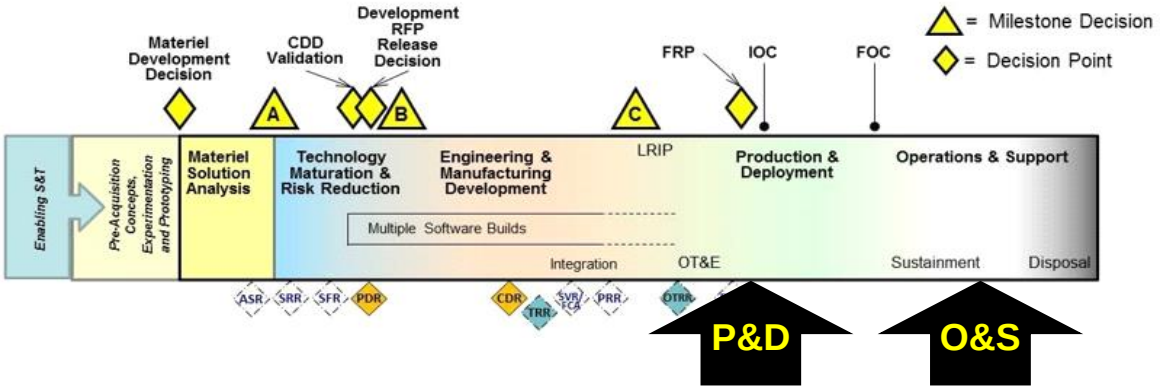
Example Questions

- Have alternative design approaches been considered that preserve MOSA objectives and requirements when modularity and openness of a <specific component(s)>been eliminated due to programmatic or other constraints?
- Do the source selection technical evaluation criteria include modularity and open interfaces for the <specific component(s)> identify for this system?
- Are all requirements for modularity and open interfaces for the <specific component(s)> traceable and linked to the initial product baseline?
- Have the implications of the design changes on the for modularity and open interfaces for the <specific component(s)> been assessed?

Does the detailed design & developmental test incorporate MOSA considerations, to assure design and development will achieve expected benefits?

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

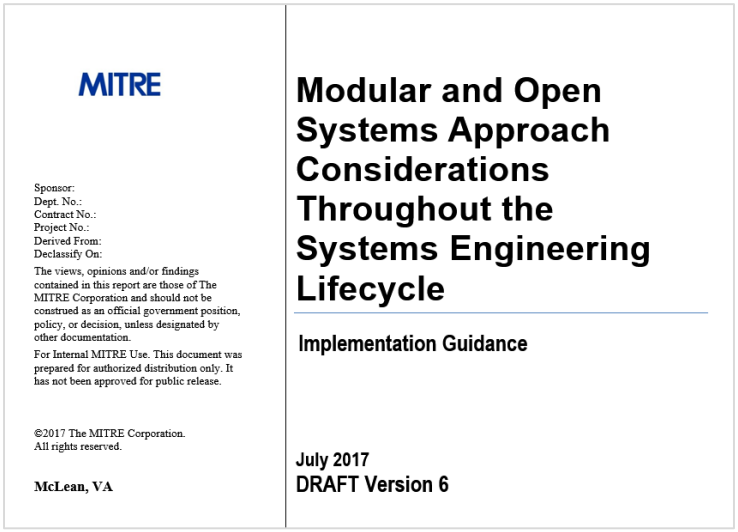
Considerations Continue Through the Full Life Cycle



- **Similar tables of considerations are included for Production & Deployment and Operations & Support stages**
  - **P&D: Does production include continued review, testing and evaluation to ensure the product as produced implements the modularity and openness as designed?**
  - **O&S: How is support and evolutional adaption of the system structured to take advantage of the MOSA characteristics expected to benefit the system?**

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

Summary


MITRE

Sponsor:
Dept. No.:
Contract No.:
Project No.:
Derived From:
Declassify On:

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

For Internal MITRE Use. This document was prepared for authorized distribution only. It has not been approved for public release.

©2017 The MITRE Corporation.
All rights reserved.

McLean, VA

Modular and Open Systems Approach Considerations Throughout the Systems Engineering Lifecycle

Implementation Guidance

July 2017
DRAFT Version 6

- **MOSA is recognized as having benefit for defense systems**
- **Application of MOSA should be focused on achieving benefits which specifically apply to the system under development**
- **Addressing MOSA as an integral part of systems engineering throughout the system life cycle ensures MOSA considerations are explicitly addressed in critical decisions**

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

For Additional Information

Philomena Zimmerman

ODASD, Systems Engineering

571.372.6695 | philomena.m.zimmerman.civ@mail.mil

Judith Dahmann, Mimi Hailegiorghis, George Rebovich, Peter Korfiatis, Brian Soeder

The MITRE Corporation

jdahmann@mitre.org, hailegik@mitre.org, grebovic@mitre.org, pkorfiatis@mitre.org, bsoeder@mitre.org

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0003 applies. Distribution is unlimited.

Implementing a Modular Open Systems Approach (MOSA) to Achieve Acquisition Agility in Defense Acquisition Programs

Philomena Zimmerman

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference

Springfield, VA | October 26, 2017

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

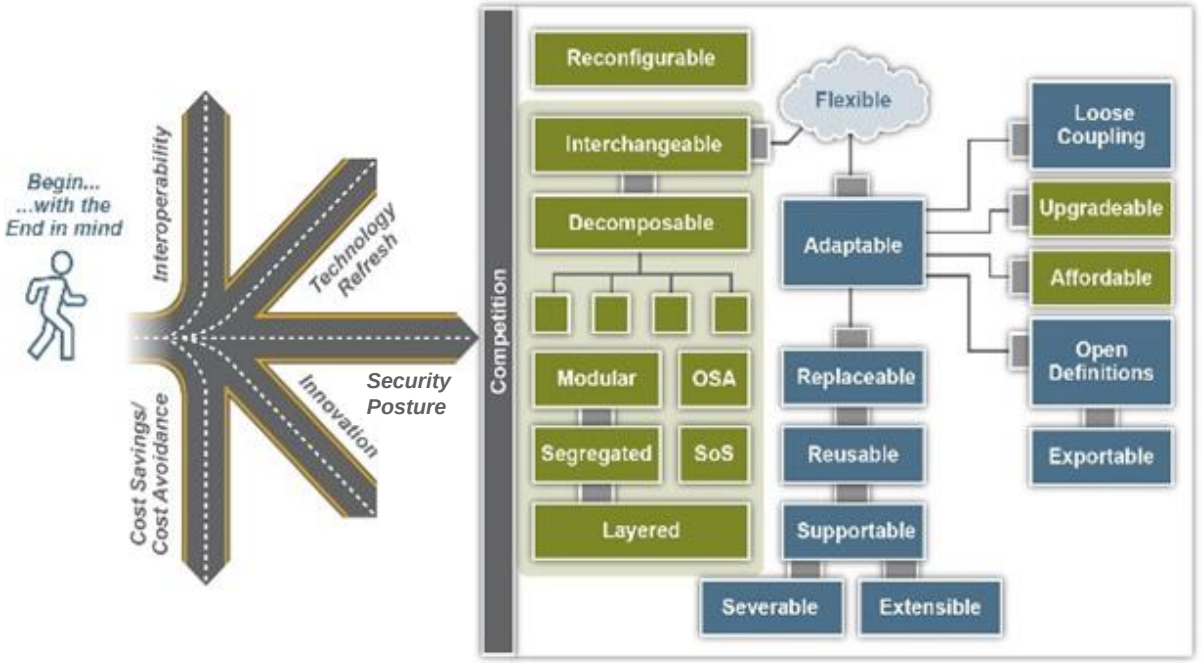
Contents

- **Modular Open Systems Approach**
- **National Defense Authorization Act for Fiscal Year 2017 (NDAA FY17) Acquisition Agility Act, Sec. 805 - 809**
- **Interfaces, Standards and Tech Data Rights**

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Design Choices

- **Begin with the End in Mind**
  - There is no single, magic bullet for implementing MOSA
    - There are multiple pathways for MOSA
  - Determine expected outcomes up front



Implementing MOSA is about trades

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

MOSA Stakeholder Communities

- **Open Collaboration**
  - Successful MOSA implementation should foster open collaboration across DoD communities and seek to unify MOSA efforts
    - There are elements from multiple communities that must collaborate for successful MOSA implementation



Multiple communities must align to enable MOSA

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Balancing Business and Technical Drivers

- **MOSA is intended to:**
  - Balance business objectives with technical methods
  - Serve as the acquisition program's foundational design and architecture structure to facilitate modernization, threat response, mission integration, competition, resource savings and security enablement
  - Enable system components and platforms to be separated, competed, and independently evolved throughout the lifecycle
    - Support using common, reusable hardware and software components that can be more readily adapted and refreshed allowing the DoD to deploy and support the latest technologies.
    - Provide the ability for competition of replacement elements, when properly supported by appropriate data rights/intellectual property access.

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Modular Open Systems Approaches

WHY	HOW	WHAT
Interoperability Tech Refresh Competition Innovation Cost Savings	Modular Design Defined Interface Standards Process Accessible Data Open Interfaces IP Rights	**Modular Technical Design Approaches** ▪ Design severable modules ▪ Define interfaces between modules ▪ Publish consensus-based standards ▪ Define, standardize & describe data models **Open System Business Approaches** ▪ Use standards & specs for interfaces ▪ Recognize the relevant technical community ▪ Acquire necessary data & IP rights

MOSA implementation consists of various methods, processes, and tools which underpin the approach.

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

NDAA FY17 MOSA Definition Sec. 805, §2446a (b)(1) p.253

- **An integrated business and technical strategy that:**
  - (A) Employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms;
  - (B) Is subjected to verification to ensure major system interfaces comply with, if available and suitable, widely supported and consensus-based standards;
  - (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 system;
  - (D) complies with the technical data rights set forth in Sec 2320, title 10.

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Defining MOSA

From Better Buying Power (BBP) 3.0 MOSA Initiative

- **Interpretation of law - recommended DoD definition:**
  - The Department of Defense defines a Modular Open Systems Approach (MOSA) as an integrated business and technical strategy for competitive and affordable acquisition and sustainment of a new or legacy system, or a component within a new or legacy system, over the entire system life cycle.
  - The approach uses a modular open systems architecture that defines key interfaces based on widely supported consensus-based standards for which conformance can be verified

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Acquisition Agility

- **The goal of the NDAA FY17 Acquisition Agility Act (Sec 805-809) is to improve our ability to evolve weapon systems**
  - (AAA) DoD Acquisition programs will be required to identify, develop and sustain major system interfaces, which comply with, if available and suitable, widely supported and consensus-based standards
  - (AAA WG) Military Services will establish prototyping investments targeted, in large part, to maturing technologies suited to meet MDAP evolution needs
  - Programs will determine the value proposition of MOSA by linking the design, interface, and standards definitions directly to the benefits they aim to achieve, including evolving operational requirements

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Emerging Technology and Evolving Threats

- **Responding to projected threats and changing technology**
  - (Sec 2446(b)) Address emerging threats, evolving technology, as well as component obsolescence when acquiring defense systems
  - (AAA WG) Anticipate evolution of technologies - forecast – for possible tech insertion, and interoperability through the use of technology maturation/prototyping and MOSA

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Program Planning and Requirements Development

- **Delivering agile technical solutions to the Warfighter**
  - MDAPs will use MOSA, where practicable, to enable incremental development, enhance competition, increase innovation and interoperability (Sec 2446B)
    - **Milestone B approval** includes use of MOSA at system interfaces, which are consistent with consensus-based standards, and appropriate data rights
    - **Program Acquisition strategies** describe MOSA across the system architecture, evolution of major system components, or addition of new or likely to change components, intellectual property (IP), tech data deliverables associated with the use of MOSA, describe the approach planned for systems integration and systems-level configuration management to ensure mission and information assurance.
    - **Request for Proposal (RFP)** for development and production phases describes MOSA of major system components in the design
    - **Program Capability Document** identifies capabilities likely to evolve because of changing threats, or potential interoperability needs
    - **Analysis of Alternatives (AoA) study plan** addresses applicability of MOSA, prototyping and evolutionary acquisition

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Support Acquisition Planning

- **Military Services will provide technical expertise and resources to support a modular open systems approach in requirements development and acquisition program planning (Sec 2446c)**
  - PEOs/PMs employ systems engineering and MOSA practices
  - Programs to address MOSA in product designs where feasible and cost-effective in architecture and engineering design documentation
  - Ensure MOSA training to requirements and acquisition workforce
- **Additional Milestone Reporting Requirements**
  - The DoD Community can structure technology investments, upgrades and innovation opportunities for insertion into programs at regular refresh cycles

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Technology Prototypes and System Components
(Sec 806)

- **Component prototyping using MOSA**
  - Prototyping and experimentation of major system components and other technologies will be overseen by the Military Services
    - including the identification and composition of the prototype oversight boards, as well as the services' procedures for selecting prototype projects
- **Integration of new components into acquisition programs**
  - Allowing for appropriate experimentation, risk reduction, and technology transition activities to be conducted
- **Prototype projects using MOSA**
  - Considering MOSA in development, weapon system component, and technology prototype projects

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Interfaces, Standards and Conformance Testing
(Sec 2446c)

- **System and component interfaces, along with supporting standards will be identified, developed, and sustained**
  - Allow interfacing components to evolve independently from the internal elements of a system
  - Enable efficient logistics and maintenance strategies. allowing interfacing components to evolve independently from the internal elements of a system
    - Development and sustainment of system interfaces will be coordinated and maintained through rigorous system configuration, configuration management and design disclosure
      - Other major systems interfaces will be maintained across the Services and DoD as necessary
    - Services will identify and select standards pertinent to their unique systems. Where gaps exist, standards will be developed and sustained as necessary
      - Standards conformance testing to be conducted ensure consistent implementation
      - Defense Standardization Program activities will be used and queried for help

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Acquisition of Data Rights and Intellectual Property (IP)
(Sec 809)

- **Acquiring Data Rights and IP**
  - Program Acquisition Strategy assists programs to appropriately promote competition
    - Acquisition programs should create and sustain a competitive environment from program inception through sustainment.
    - Strategies should consider:
      - Competitive prototyping, dual sourcing, an open systems architecture that enables competition for upgrades, acquisition of complete technical data packages, and competition at the subsystem level.



- **IP considerations**
  - The Strategy for managing IP across enables competitive and affordable acquisition & sustainment
    - PMs should identify and manage the full spectrum of IP and related issues from program inception and throughout the lifecycle
      - Assess program technical data needs
      - Enable the development of competitive acquisition of deliverables of IP & associated license rights

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Strategic Considerations

- **MOSA is not an all or nothing proposition**
  - Must tailor approach to expected MOSA benefits; requires tradeoffs
  - Must be addressed in all aspects of acquisition
- **MOSA is more than just defining architectures and selecting standards**
  - MOSA requires technical community enablers and business relationship enablers
- **Governance and leadership matter**
  - Leadership, and guidance applies across multiple programs
- **Industry must be an able and willing partner**
  - Crossing the government/industry boundary: Intellectual Property/Data Rights (IP/DR) in design, documentation, specifications, tools, etc.

MOSA enables flexibility and longevity in our weapon systems

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition












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

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

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

For Additional Information



Ms. Philomena Zimmerman

ODASD, Systems Engineering

571.372.6695

philomena.m.zimmerman.civ.mail.mil

Ms. Monique Ofori

Engility

571.372.6676 | monique.f.ofori.ctr@mail.mil

Distribution Statement A – Approved for public release by DOPSR on 10/03/2017, SR Case # 18-S-0004 applies. Distribution is unlimited.

From Architecture to Operations

Using Your Architecture Work in Operations

STEVEN H. DAM, PH.D., ESEP
CHRIS RITTER
SPEC INNOVATIONS
STEVEN.DAM@SPECINNOVATIONS.COM



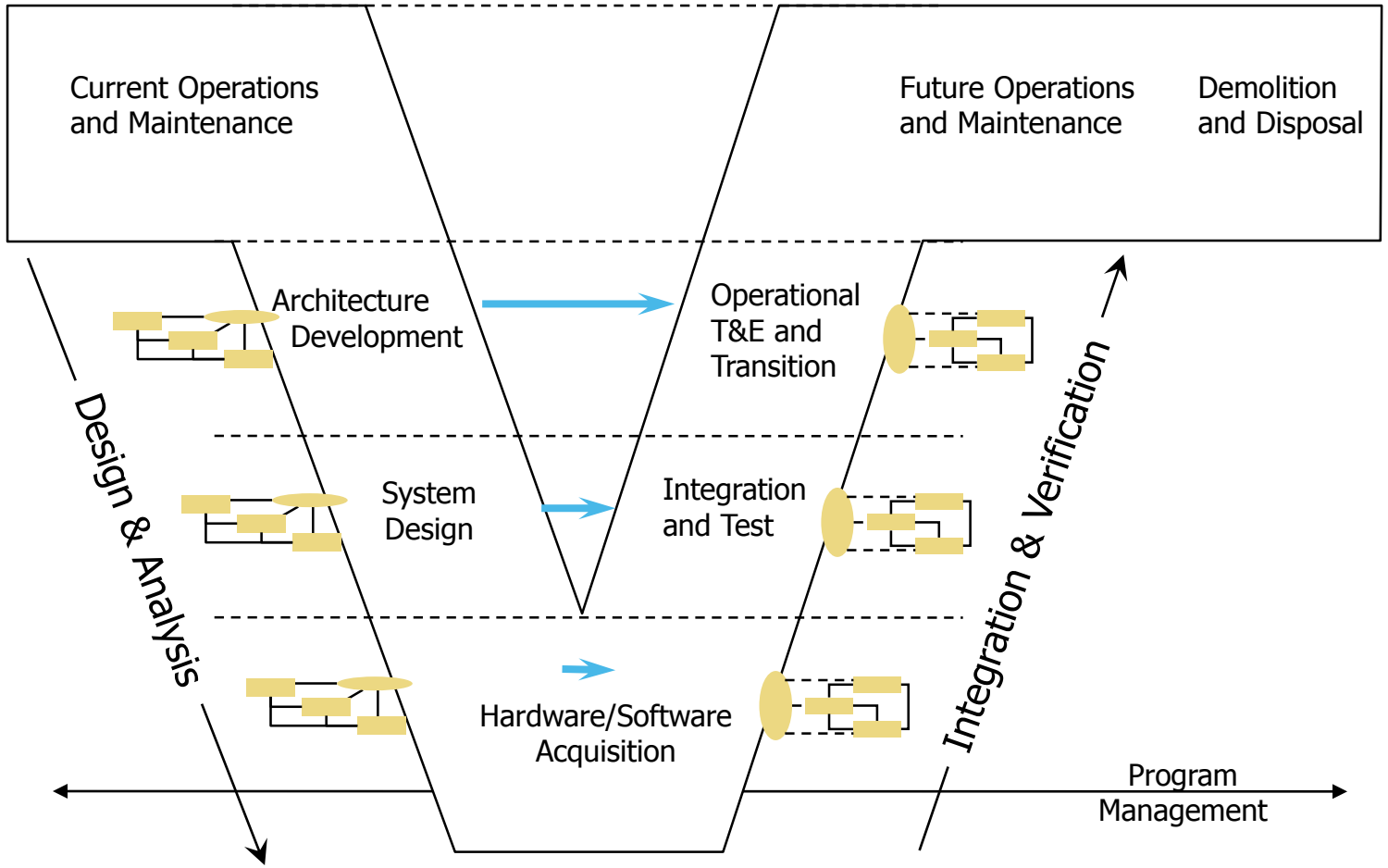
Outline

1. What Do We Do When We Develop Architectures?
2. How Is Architecture Useful to Operators?
3. How Can We Use Operational Information to Prepare for the Next Architecture?

1. WHAT DO WE DO WHEN WE DEVELOP ARCHITECTURES?



Product Lifecycle



Capturing As-Is Architecture Data

- Operational equipment
- Networks and other interfaces
- Operating processes and procedures
- Operating costs
- Operations personnel

We capture information that describes how current systems operate and where problems may occur

Developing To-Be Architecture Data

- Designs for new and modified equipment
- Designs of new and modified processes
- Plans for acquiring equipment
- Training needs

All this information will affect the operations of the as-is systems

When We Finish, What Do We Have?

- A complete database with all the information about the systems that operators (and maintainers) need to effectively and efficiently operate the systems

Why not put all that data to good use?

2. HOW IS ARCHITECTURE USEFUL TO OPERATORS?



How Can Architecture Be Useful

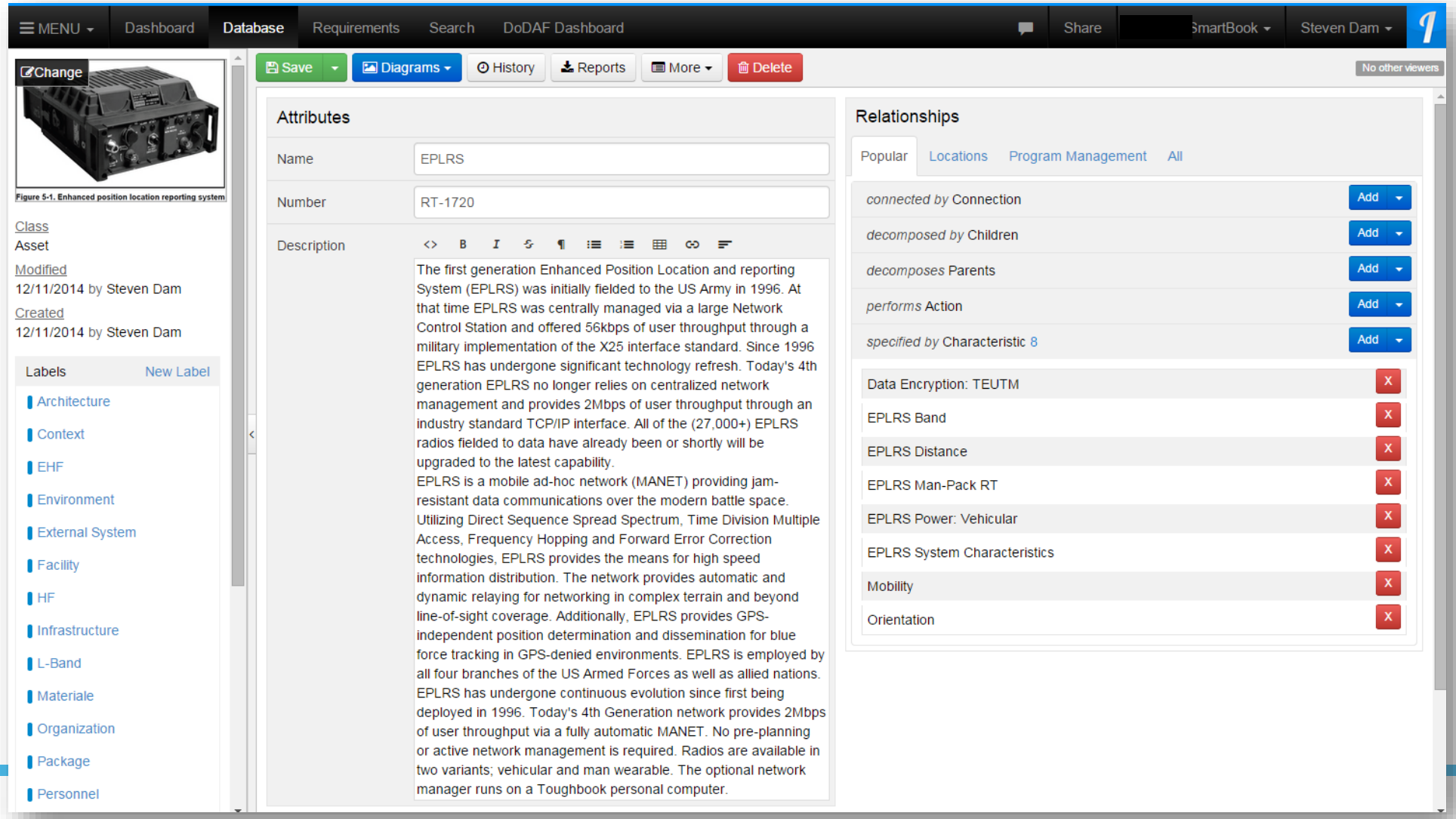
- For operators, architecture can provide the basis for understanding the limitations of and standard operating procedures (SOP) for using the components
- For maintainers, the architecture can provide a place to store critical information, such as reliability, availability, and maintenance procedure, for the components
- However, often this kind of information is either ignored by architects or occurs later in the lifecycle, after the architecture database has been ignored for years
- Too often architecture teams do not include the operational and maintenance perspectives

Capturing Operational Data

- Use cases, user stories, scenarios, threads, etc. are all ways to capture how a system is used or operated
- One way we capture this information is in a Concept of Operations (CONOPS)
  - However, most CONOPS are too high level and do not analyze the scenarios sufficiently to make sure they make any sense or even work in a realistic environment
  - An architecture-based CONOPS is then essential for this
  - Such a CONOPS can then form the basis for developing SOPs

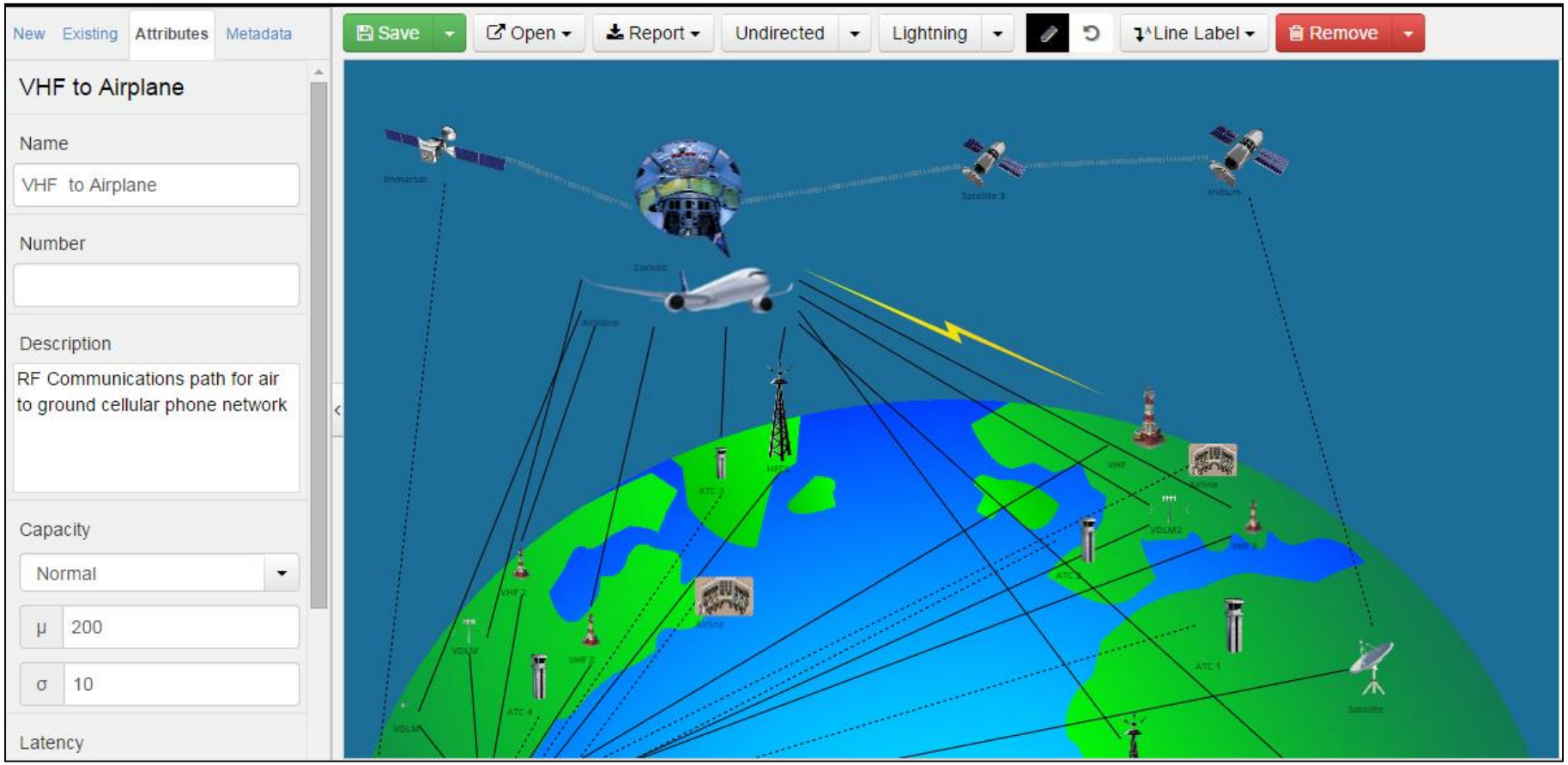


Information Capture Example



- MBSE tool provides means to capture and relate information about any asset
- This would provide a means to capture and share information about the systems and components

Visualizing the Comms Architecture Example

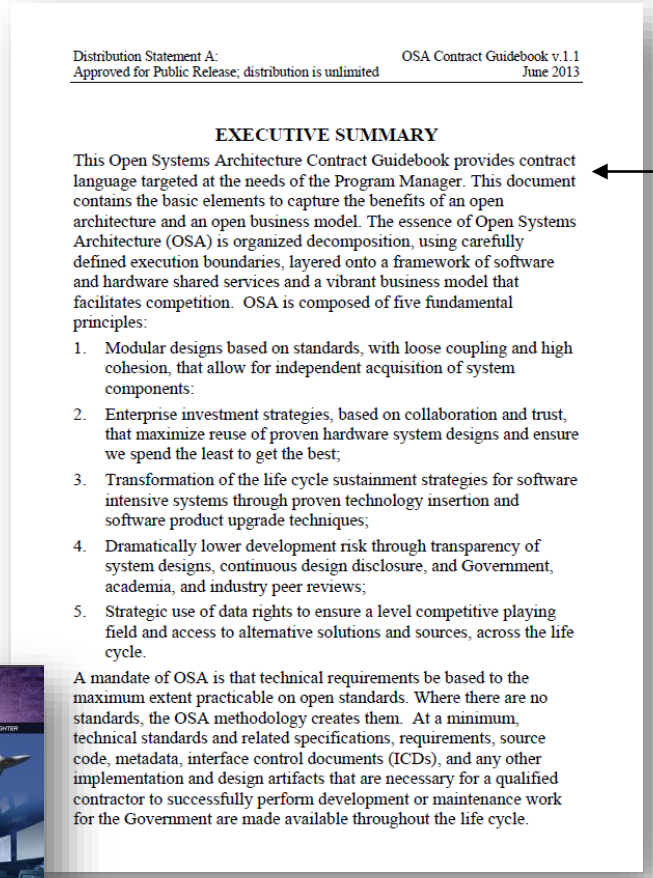


- Physical architecture captured in MBSE tool
- Provides constraints for functional modeling and simulation

Next Steps

- Similar information and documentation can support the maintainers
- However, we still need a database for the information that can then be reused for each perspective
- Most tools currently focus on only one lifecycle phase (e.g., architecture, operations, or maintenance), but the overlapping information clearly means that we could use a single database with multiple views
- Here is where the concept of MOSA helps us

Modular Open Systems Approach (MOSA)



Distribution Statement A:
Approved for Public Release; distribution is unlimited

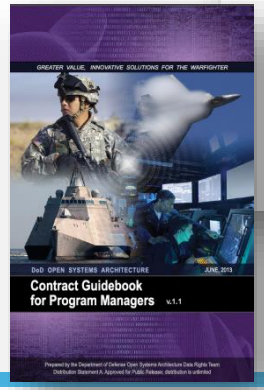
OSA Contract Guidebook v.1.1
June 2013

EXECUTIVE SUMMARY

This Open Systems Architecture Contract Guidebook provides contract language targeted at the needs of the Program Manager. This document contains the basic elements to capture the benefits of an open architecture and an open business model. The essence of Open Systems Architecture (OSA) is organized decomposition, using carefully defined execution boundaries, layered onto a framework of software and hardware shared services and a vibrant business model that facilitates competition. OSA is composed of five fundamental principles:

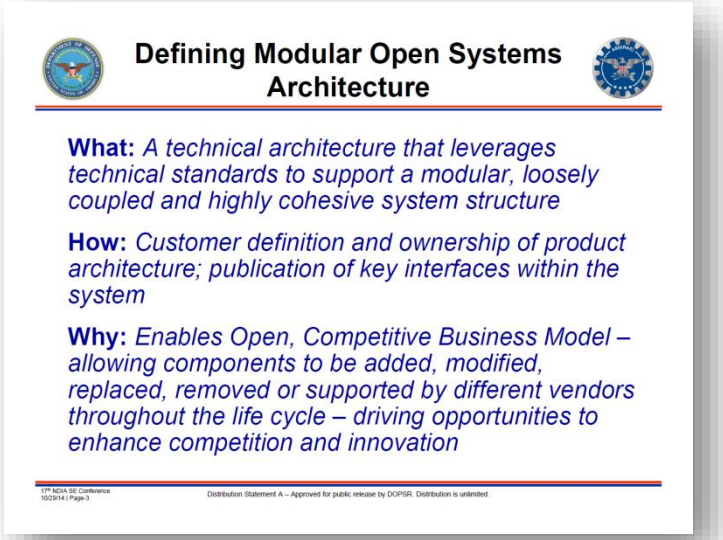
1. Modular designs based on standards, with loose coupling and high cohesion, that allow for independent acquisition of system components:
2. Enterprise investment strategies, based on collaboration and trust, that maximize reuse of proven hardware system designs and ensure we spend the least to get the best;
3. Transformation of the life cycle sustainment strategies for software intensive systems through proven technology insertion and software product upgrade techniques;
4. Dramatically lower development risk through transparency of system designs, continuous design disclosure, and Government, academia, and industry peer reviews;
5. Strategic use of data rights to ensure a level competitive playing field and access to alternative solutions and sources, across the life cycle.

A mandate of OSA is that technical requirements be based to the maximum extent practicable on open standards. Where there are no standards, the OSA methodology creates them. At a minimum, technical standards and related specifications, requirements, source code, metadata, interface control documents (ICDs), and any other implementation and design artifacts that are necessary for a qualified contractor to successfully perform development or maintenance work for the Government are made available throughout the life cycle.



OSA Contract Guidebook for PMs

"The essence of Open Systems Architecture (OSA) is organized decomposition, using carefully defined execution boundaries, layered onto a framework of software and hardware shared services and a vibrant business model that facilitates competition."



Defining Modular Open Systems Architecture

What: *A technical architecture that leverages technical standards to support a modular, loosely coupled and highly cohesive system structure*

How: *Customer definition and ownership of product architecture; publication of key interfaces within the system*

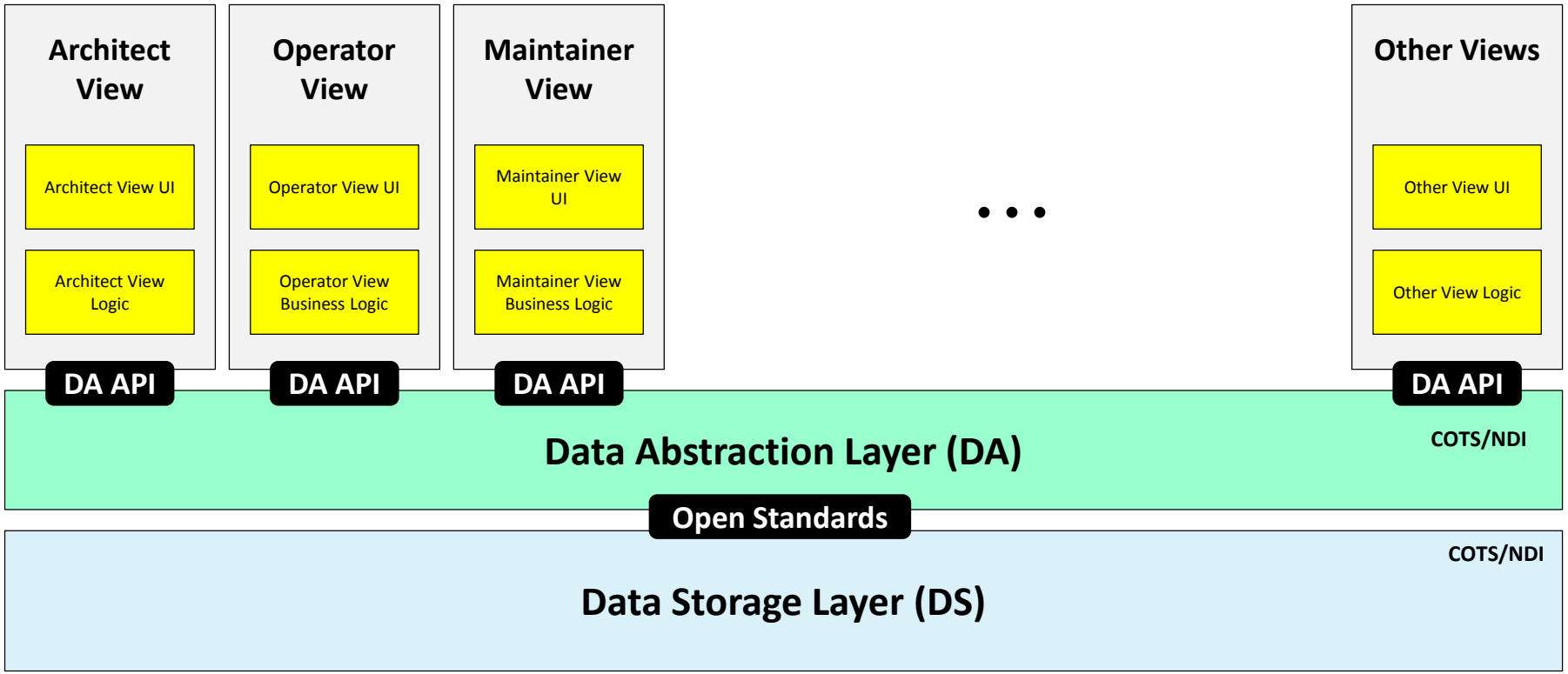
Why: *Enables Open, Competitive Business Model – allowing components to be added, modified, replaced, removed or supported by different vendors throughout the life cycle – driving opportunities to enhance competition and innovation*

17th NDIA SE Conference
10/29/14 | Page-3

Distribution Statement A – Approved for public release by DOPSR. Distribution is unlimited.

"Modular Open Systems Architecture in DoD Acquisition"
Mr. Stephen Welby, DASD(SE)

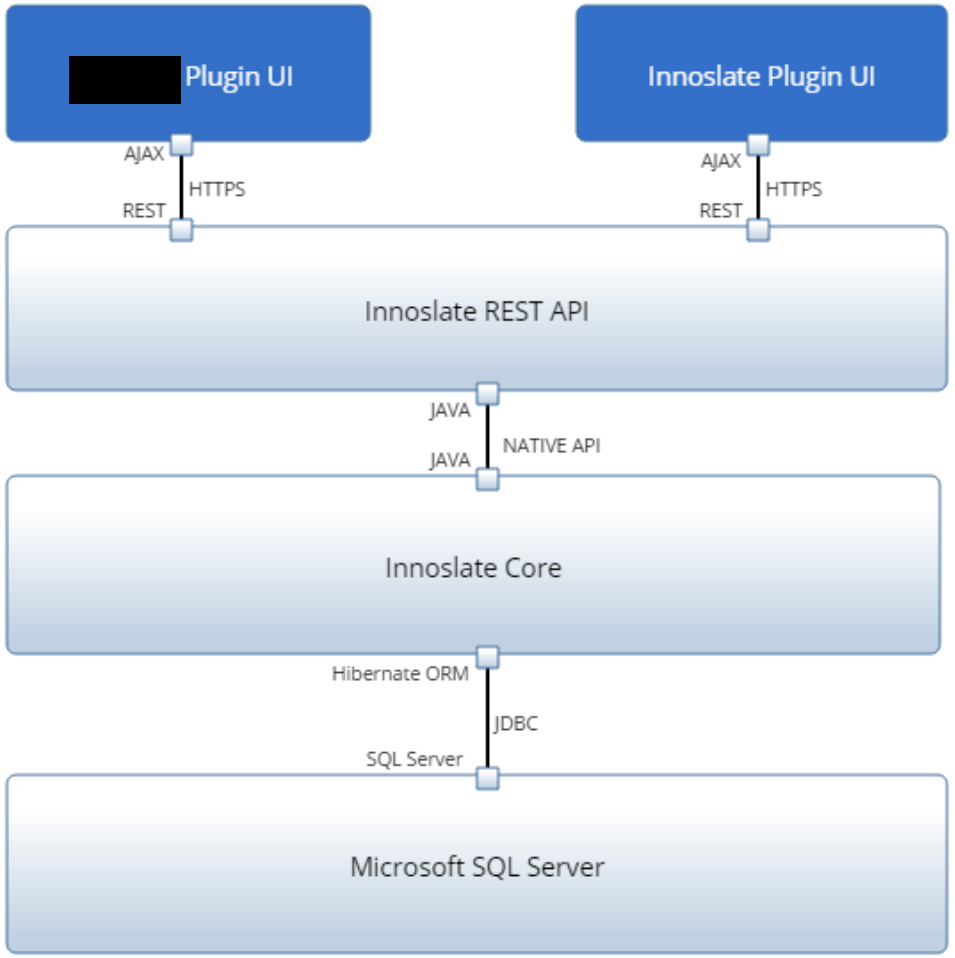
A MOSA Reference Architecture



Reference Architecture (RA) supports MOSA objectives through defined interfaces, open standards, and a severable modular design

Plugin Architecture Example

- Plugins are viewpoints of the Innoslate database
- Plugin features
  - Not a standalone application (requires Innoslate Core)
  - All authentication is through Innoslate Core with the options for:
    - Single-Sign-On CAC (Default)
    - Native Email/Password (Optional)
    - LDAP (Optional)
  - All data is stored in the U.S. Government managed MSSQL database using Innoslate Core
  - Innoslate REST API facilitates plugin data exchange



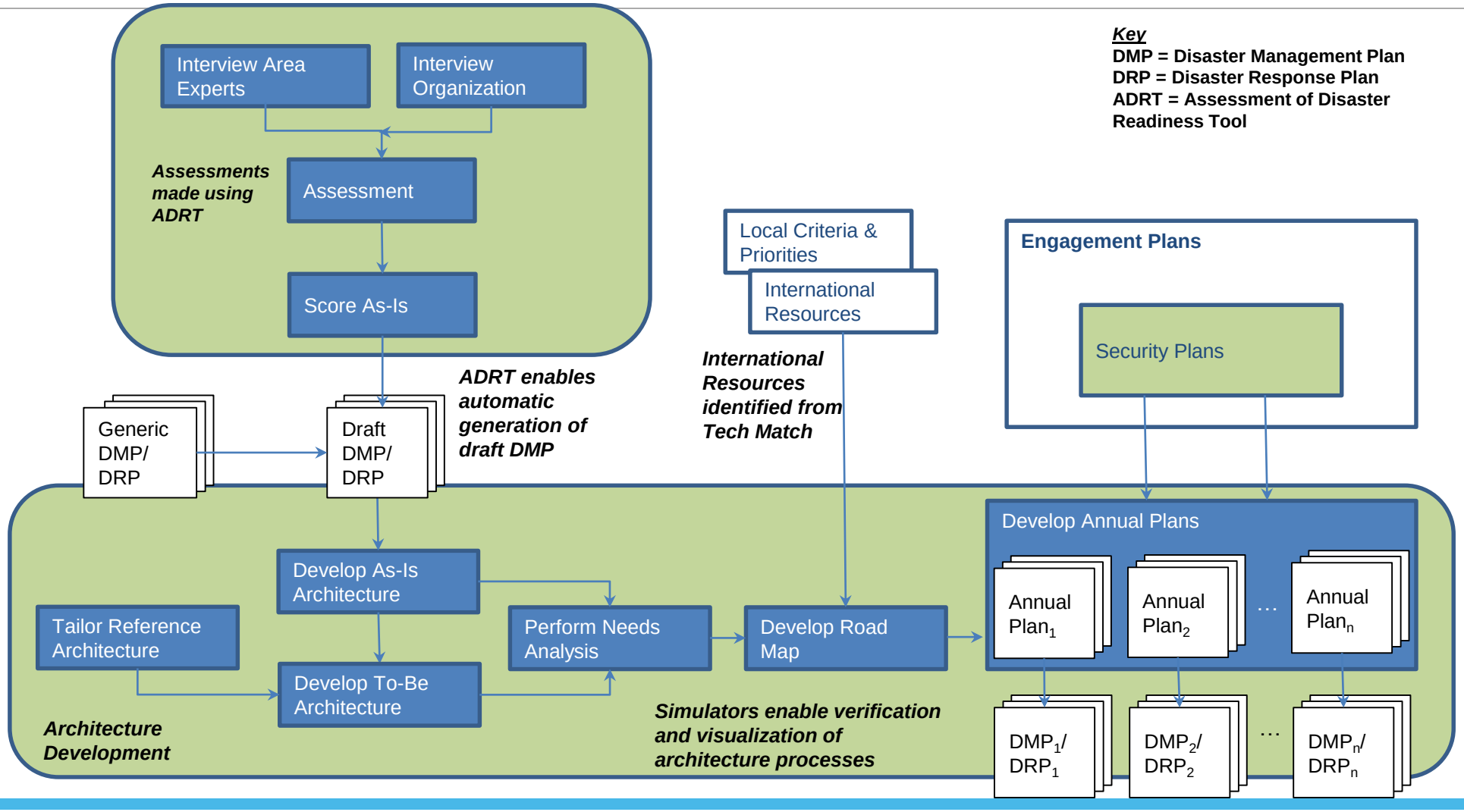
3. HOW CAN WE USE OPERATIONAL INFORMATION TO PREPARE FOR THE NEXT ARCHITECTURE?



Operational Data Utility

- Operational data can be used to identify problems areas and user needs
  - Issues may provide a window into the kinds of problems users face or unclear features
  - Feature suggestions may also be ”hidden” in issues
  - Maintenance logs show where components do not meet their expected lifetimes or where they exceed them
- This data forms the basis for gap analysis that can then be turned into architecture improvements
- This approach requires the creation and maintenance of a reference architecture

Use of Other Tools to Feed Architecture Work



Summary

- Architecture work needs to include the perspectives of operators and maintainers
- We need to get more out of the architecture work that's performed
- Reusing and evolving the architecture databases into operational tools is essential to obtaining the full value for this work

UMass | Dartmouth UNIVERSITY OF MASSACHUSETTS DARTMOUTH

Free and Open Source Tools to Assess Software Reliability and Security



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

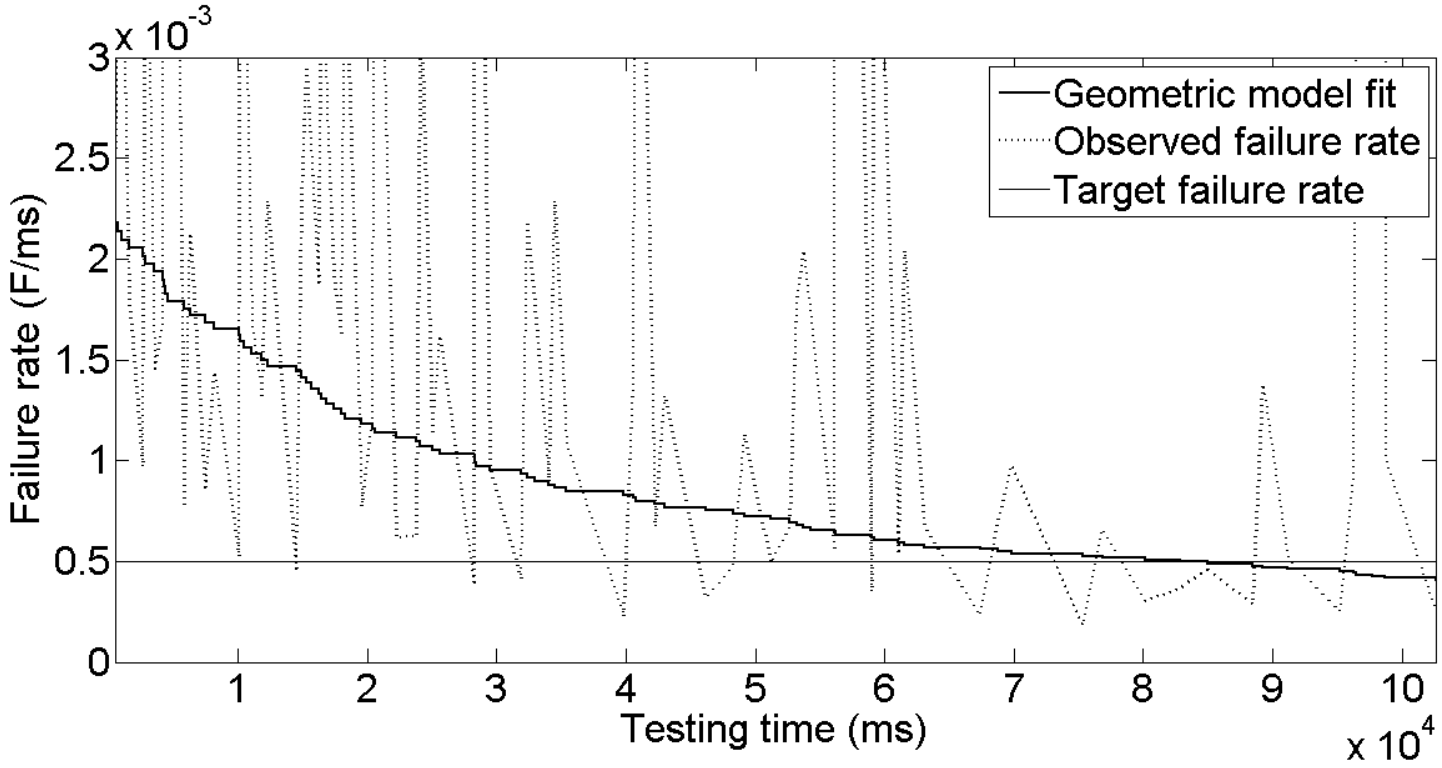
Summary of Year I deliverables

- 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

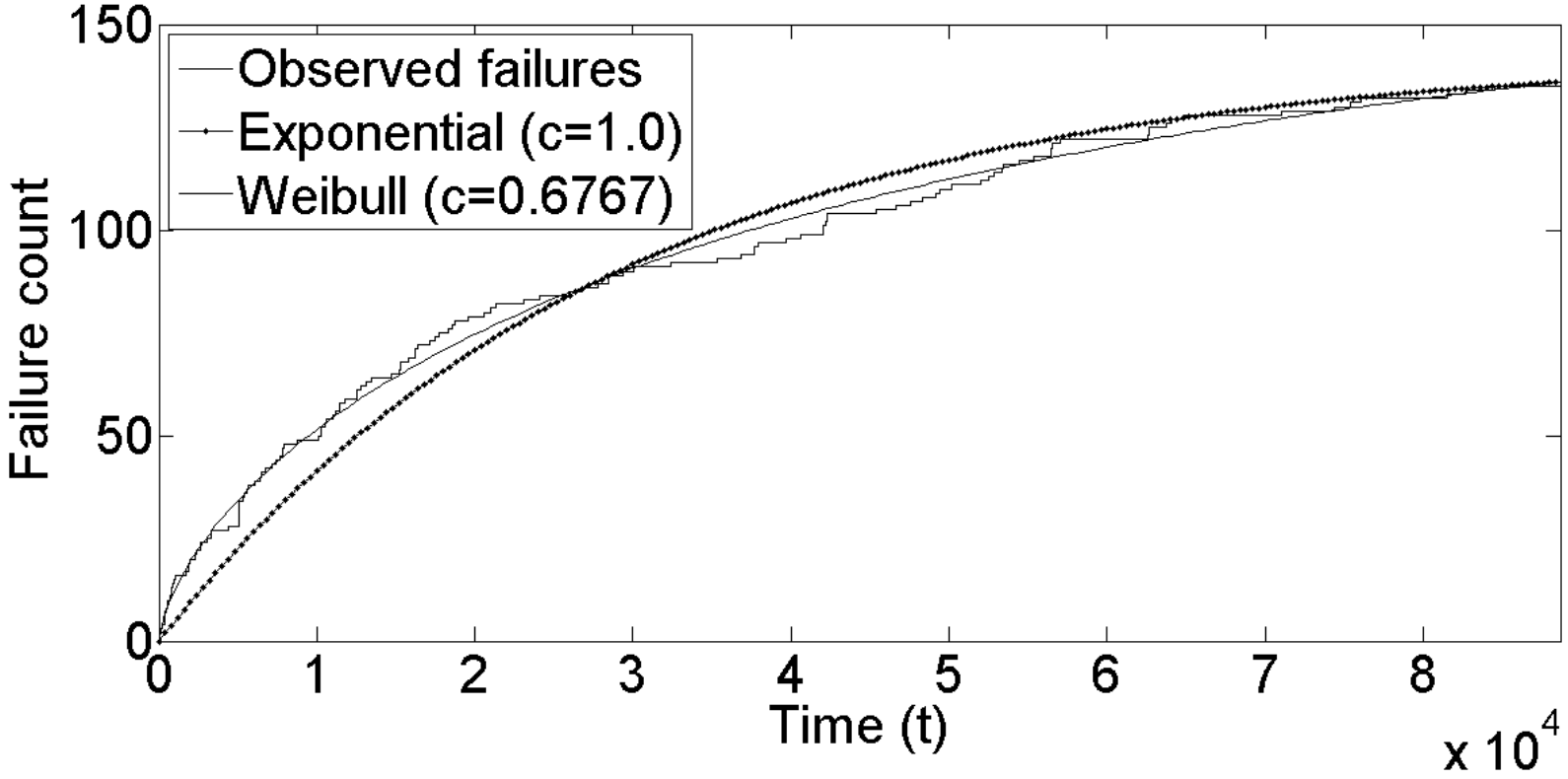
- Number of
  - Faults detected with additional testing
  - Remaining faults
- Mean time to failure (MTTF) of next fault
  - Testing time needed to remove next k faults
- Probability software does not fail before completion of fixed duration mission

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,
      $$\mathbf{T} =< t_1, t_2, \ldots, t_n >$$
  - Failure Counting models
    - Failure count data - length of the interval and number failures observed within it,

    $< \mathbf{T}, \mathbf{K} >=< (t_1, k_1), (t_2, k_2), \ldots, (t_n, k_n) >$
  - 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

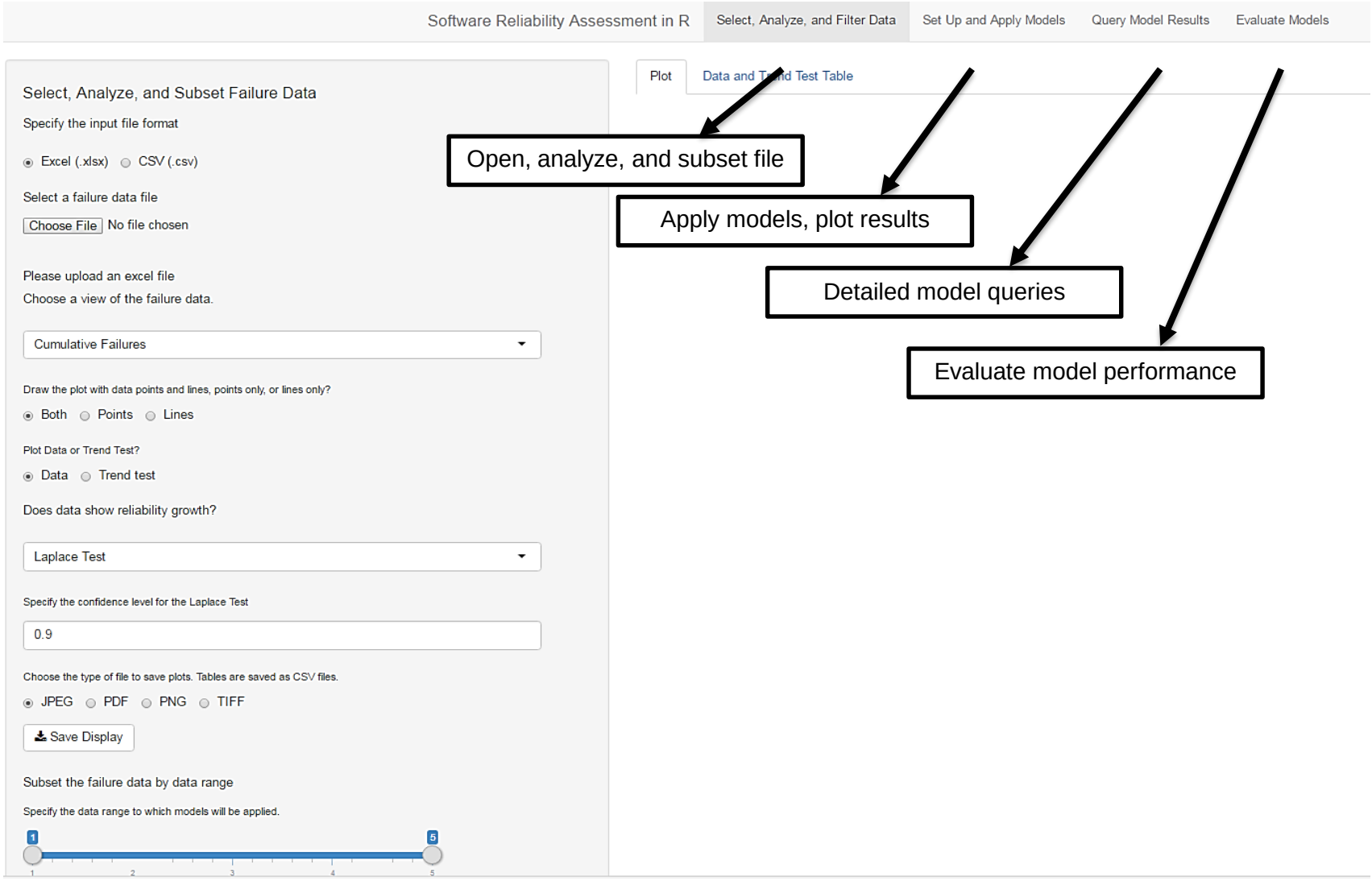
New models added in the “models” folder

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

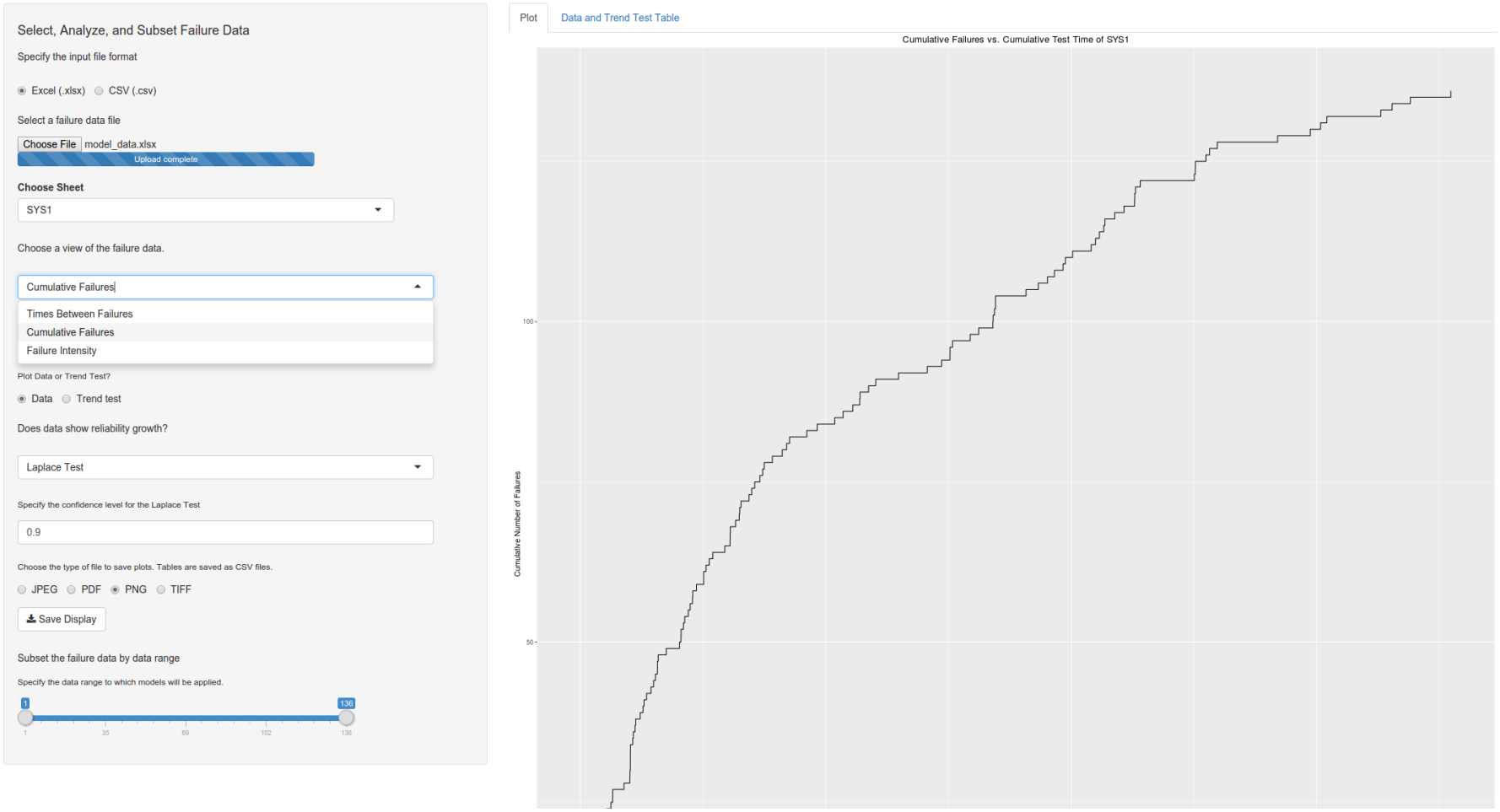
REVIEW OF YEAR I FUNCTIONALITY

SFRAT - Tab view



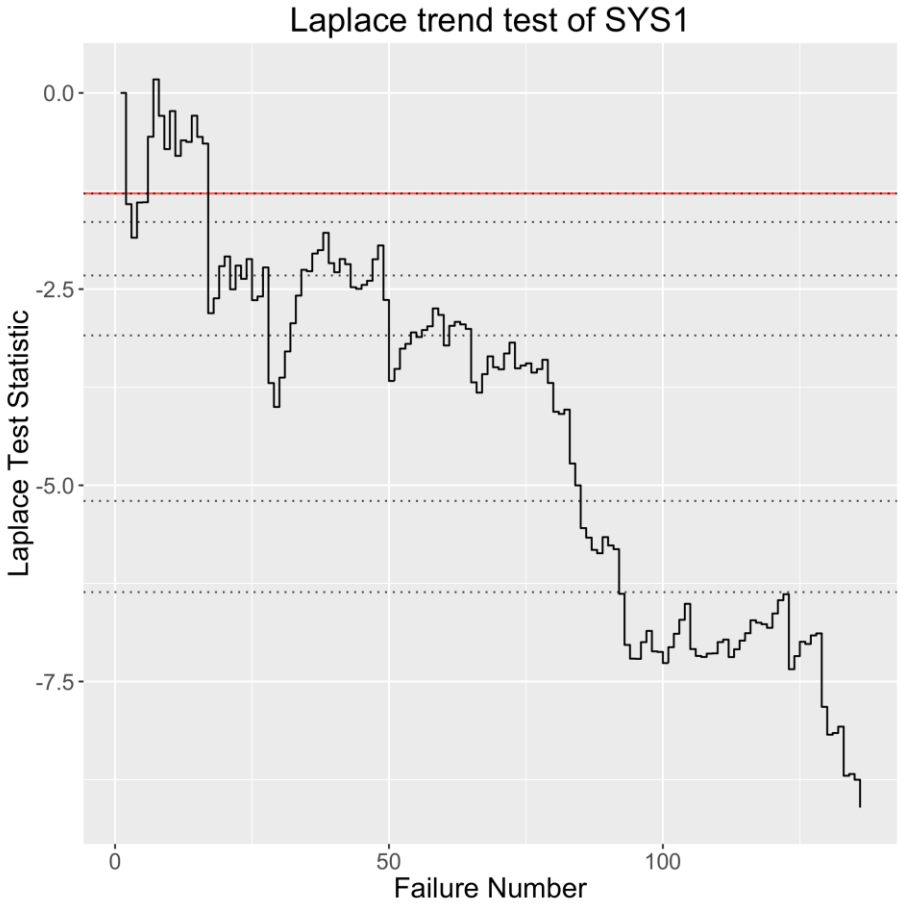
Tab 1
Select, Analyze, and Filter data

Tab 1 – After data upload



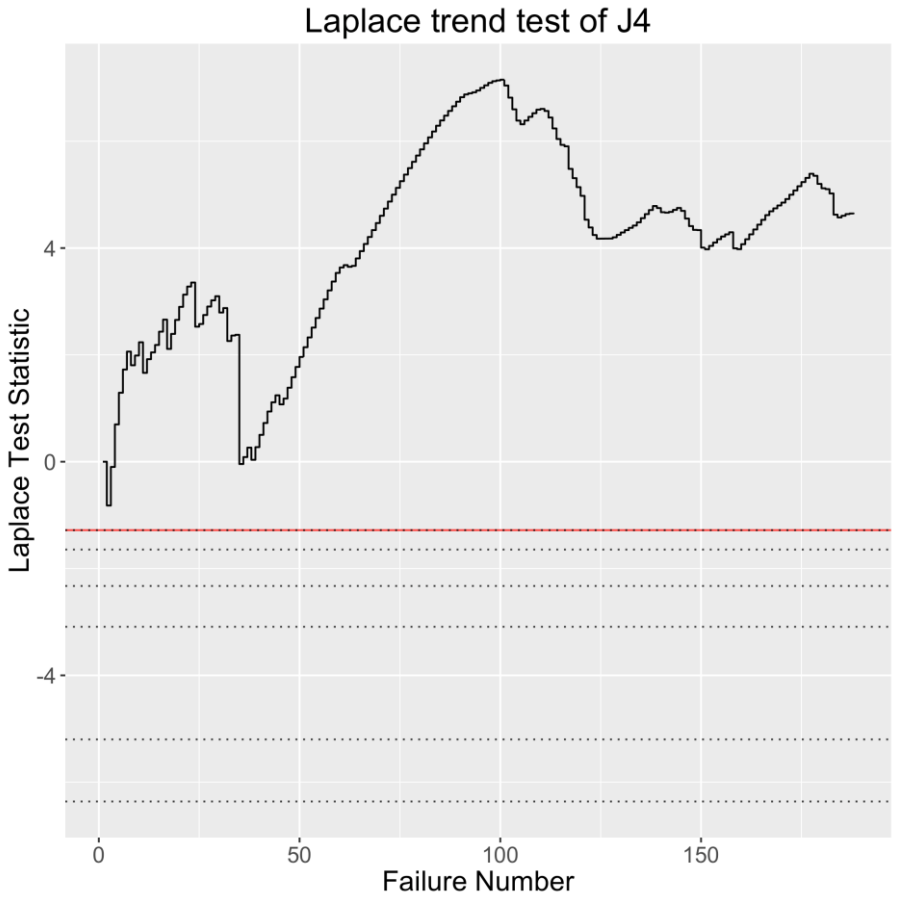
Cumulative failure data view

Laplace trend test – SYS1 data



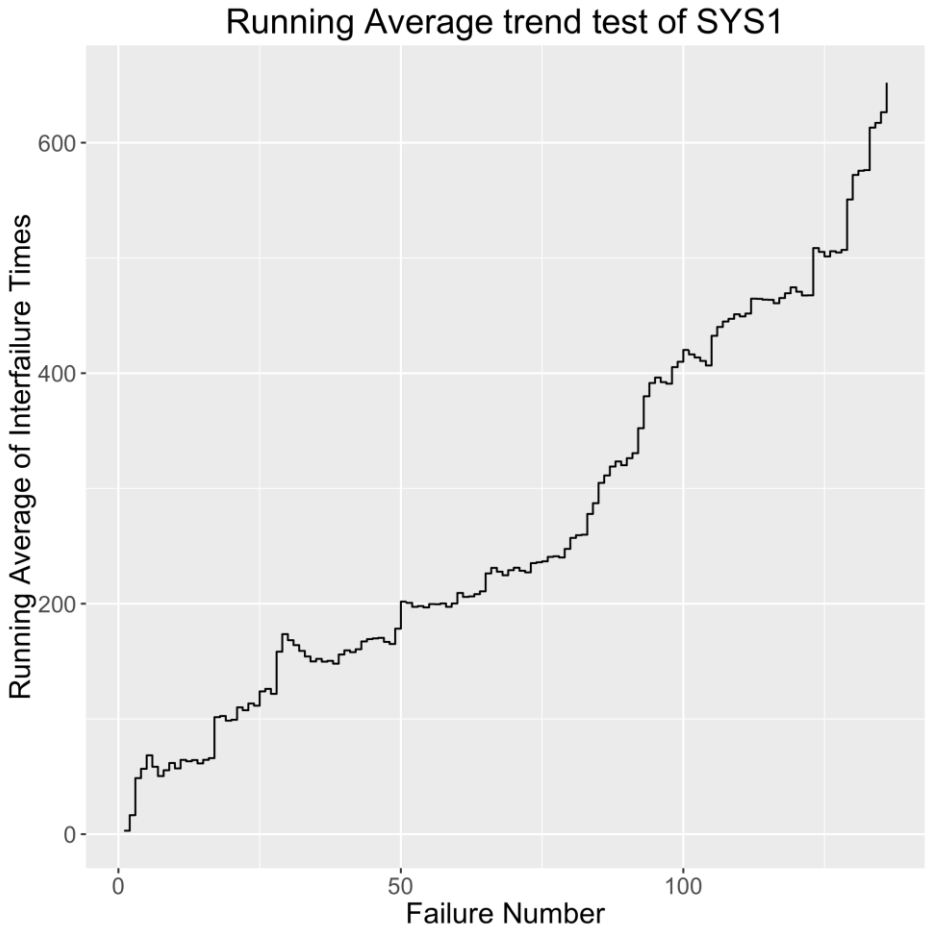
Decreasing trend indicates reliability growth
(Indicates application of SRGM appropriate)

Laplace trend test – J4 data



Does not exhibit reliability growth
(Indicates additional testing required)

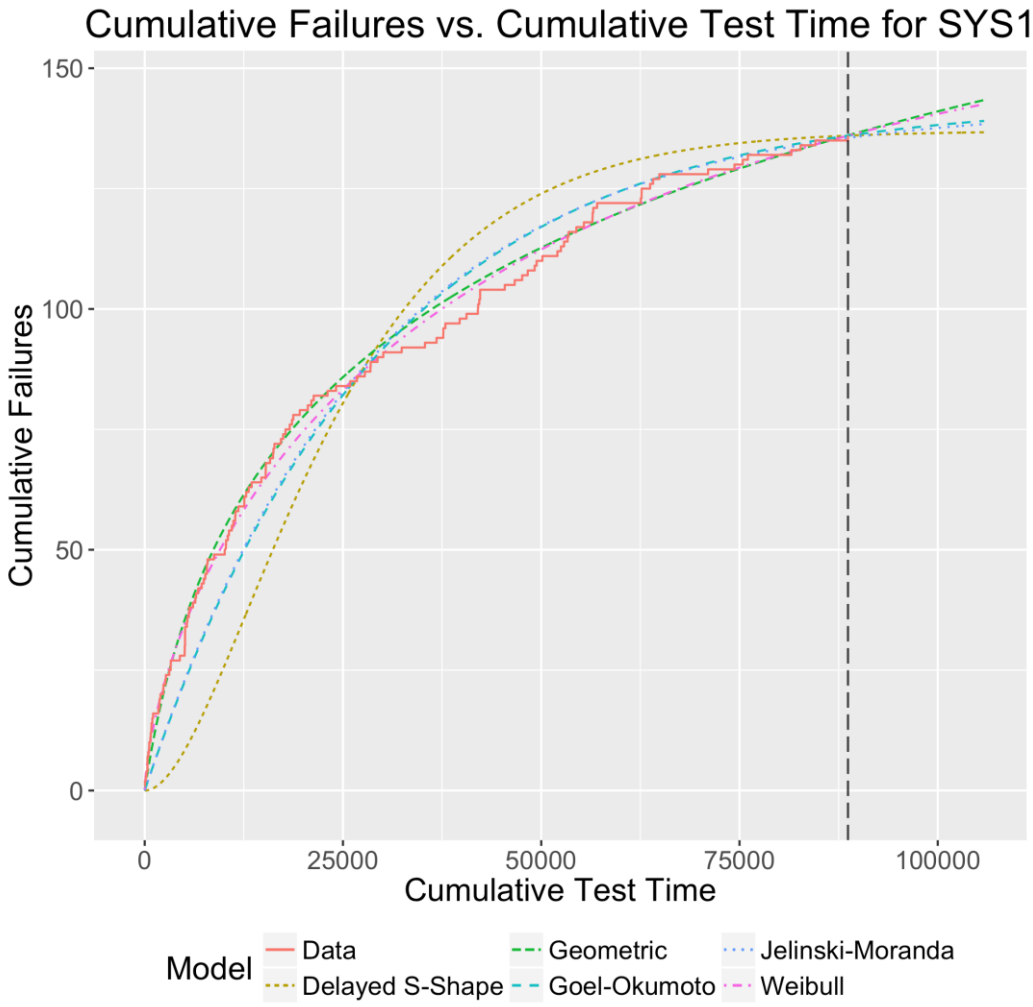
Running Arithmetic Average – SYS1 data



Increasing trend indicates reliability growth

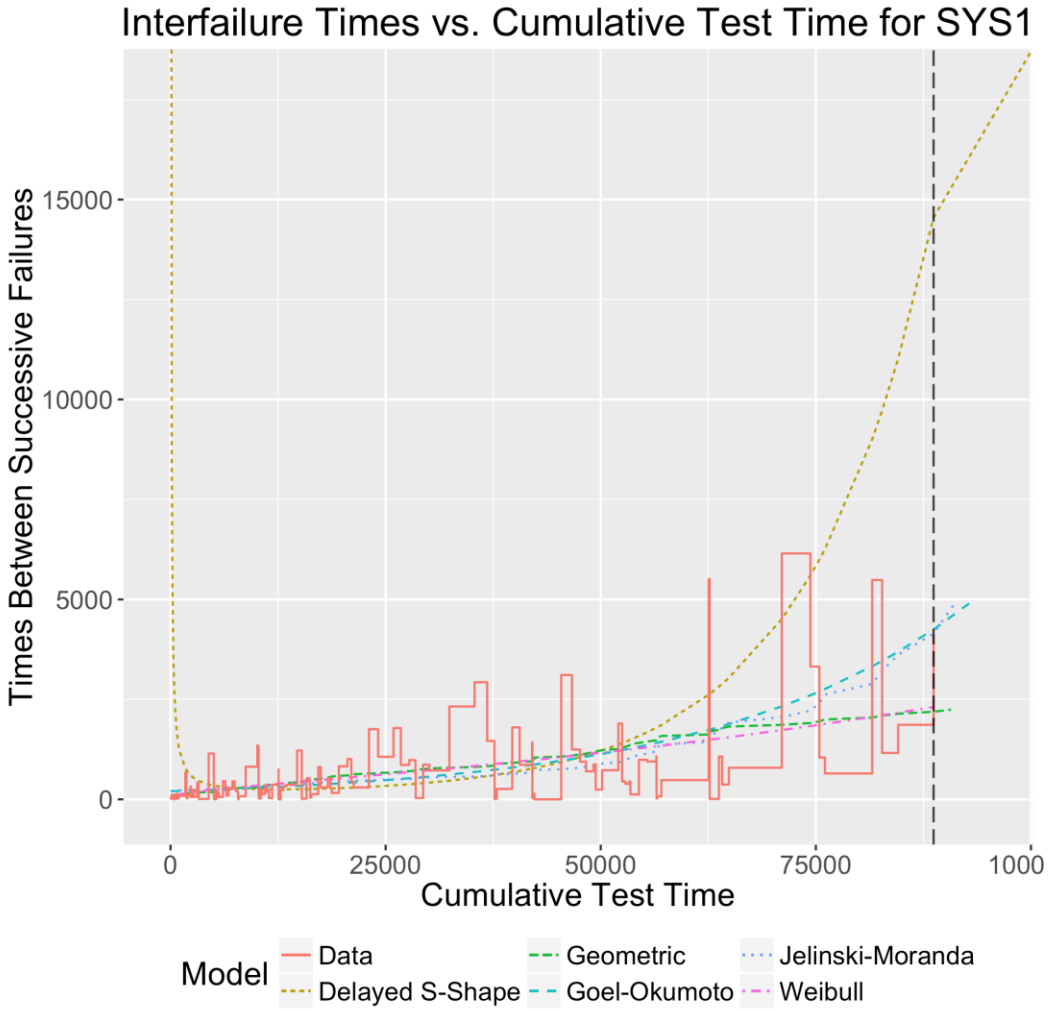
Tab 2
Set Up and Apply Models

Cumulative failures



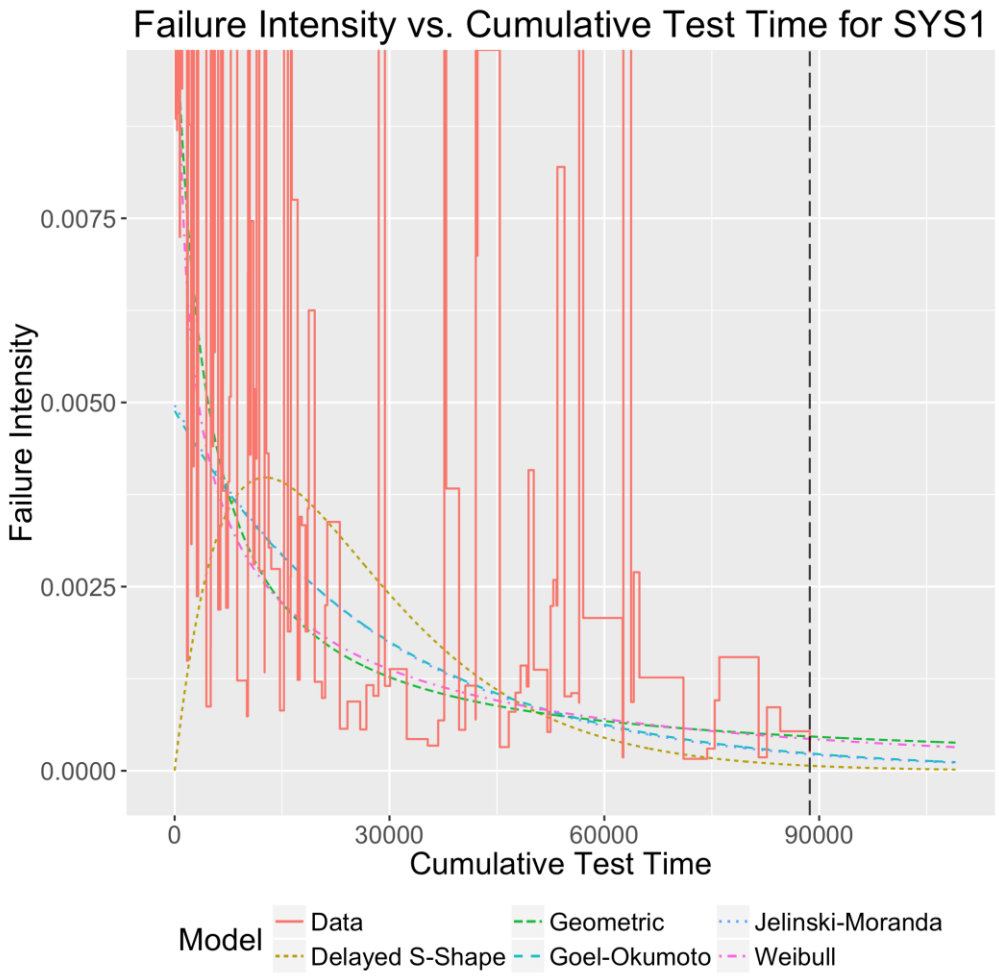
Plot enables comparison of data and model fits

Time between failures



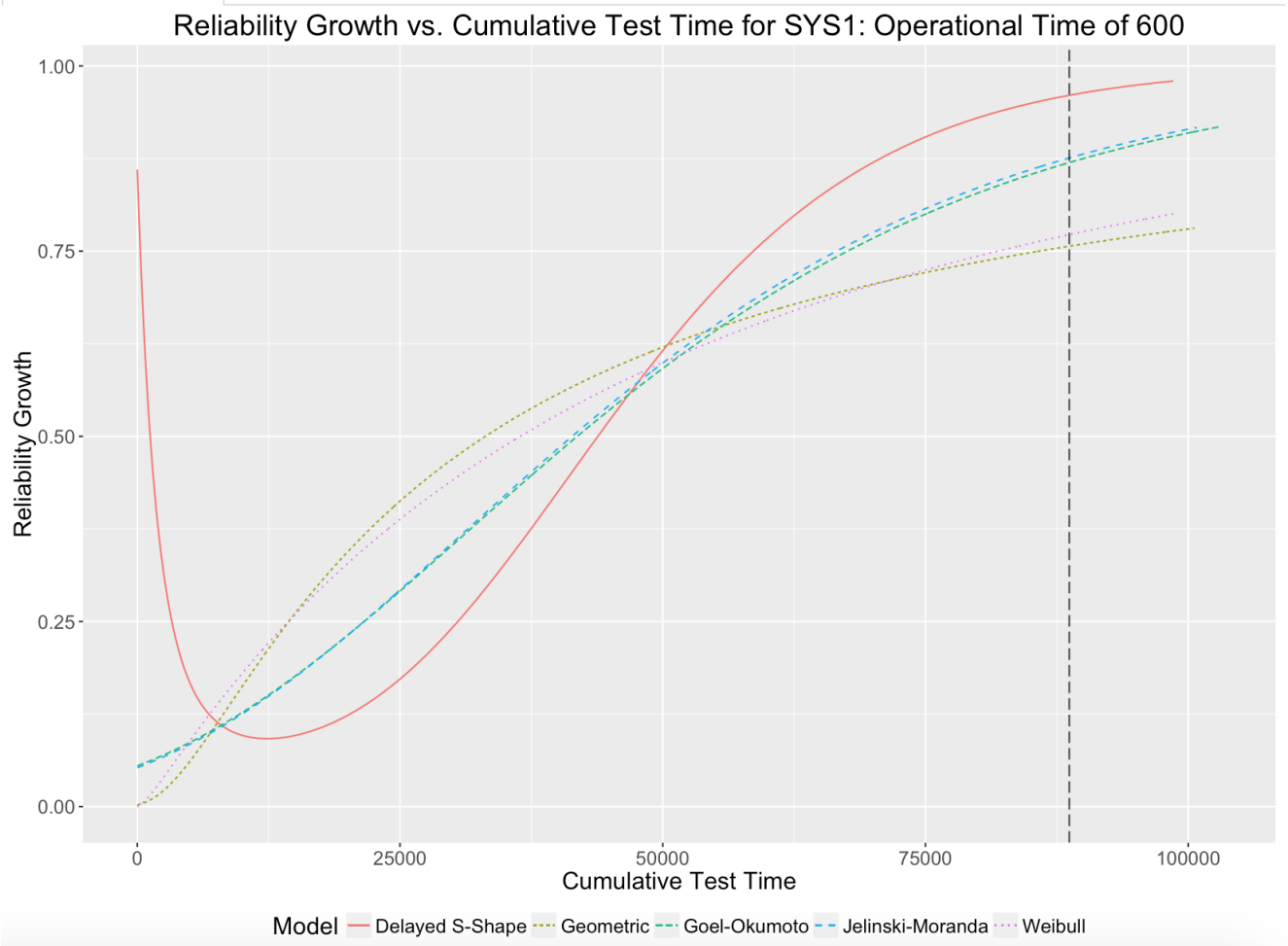
Times between failures should increase (indicates reliability growth)

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

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

~/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

Configure and Apply Models

Specify the number of failures for which the models will make predictions

Specify the last data point for the initial parameter estimation interval.

1 68 135

1 15 29 43 57 71 85 99 113 127 135

Specify a confidence interval for parameter estimates.

0.95

Specify for how many failures into the future the models will predict

1

Choose one or more models to run, or exclude one or more models.

Geometric | Goel-Okumoto | Jelinski-Moranda

Run Selected Models

Display Model Results

Choose one or more sets of model results to display.

Goel-Okumoto

Model Result Plot | Model Result Table

Show most likely parameter values or confidence bounds. Low | Most Likely | High



~/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?

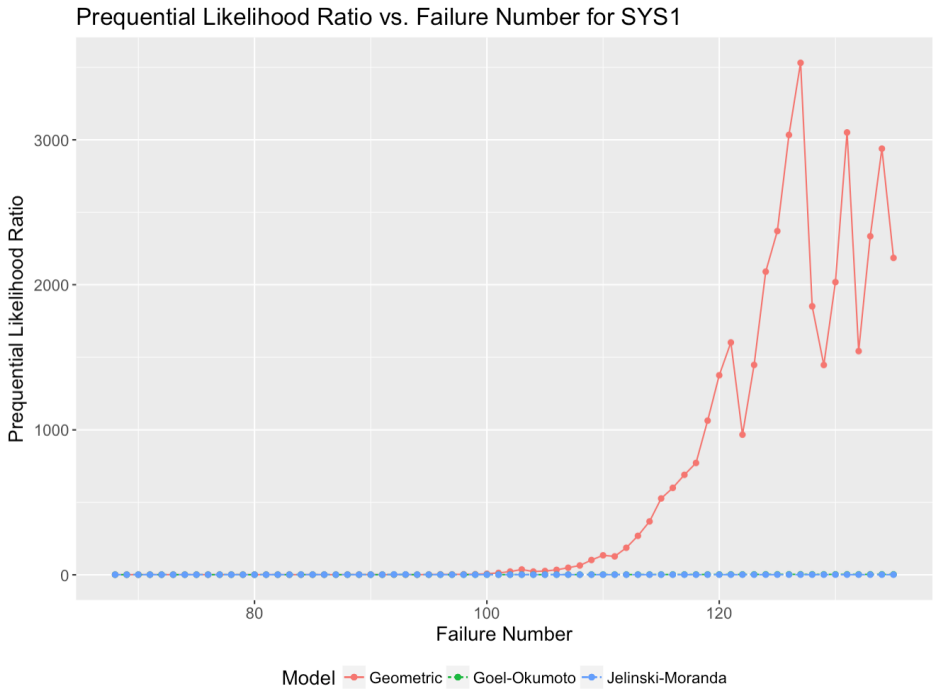
(•) CSV ( ) PDF

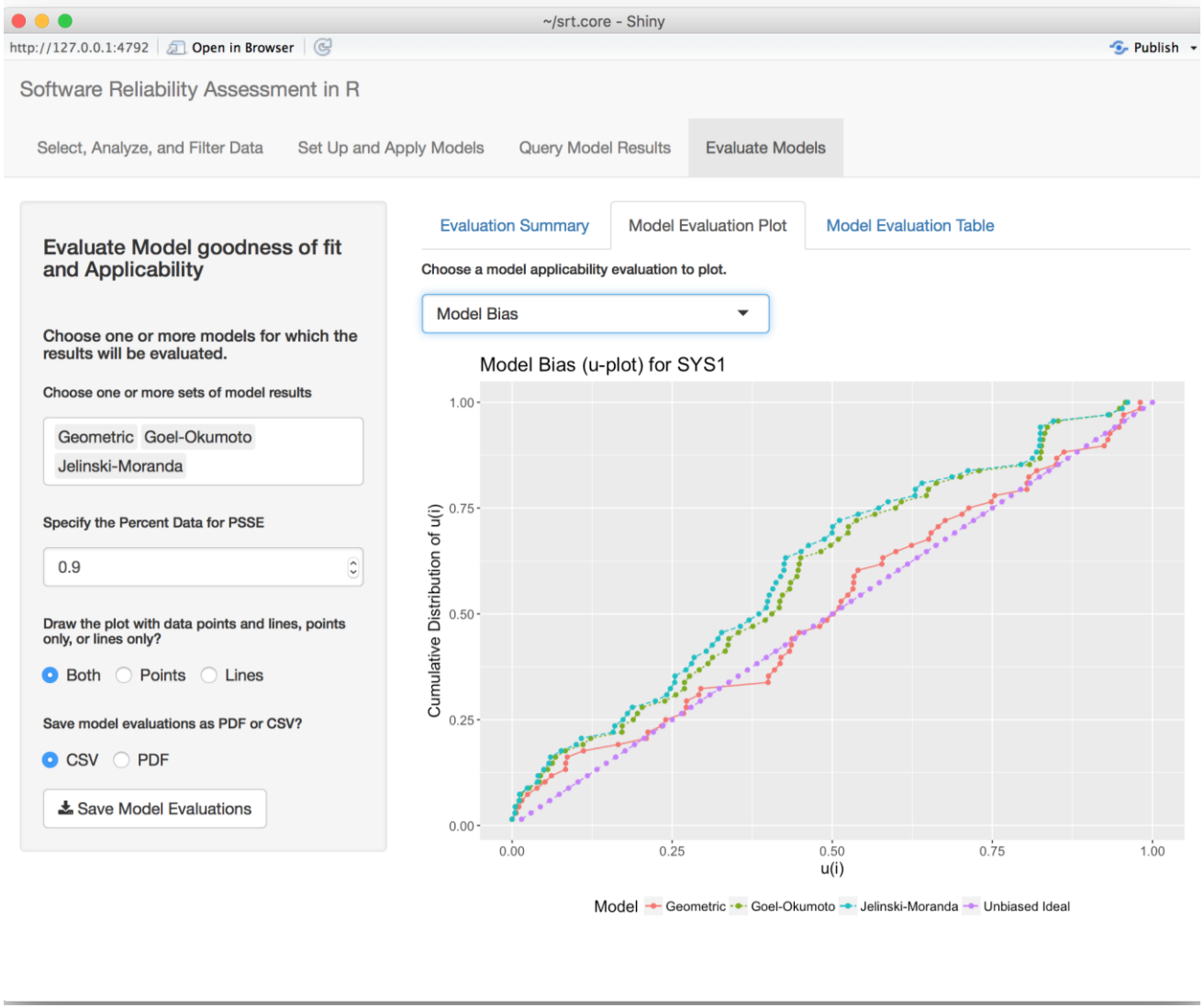
Save Model Evaluations

Evaluation Summary | Model Evaluation Plot | Model Evaluation Table

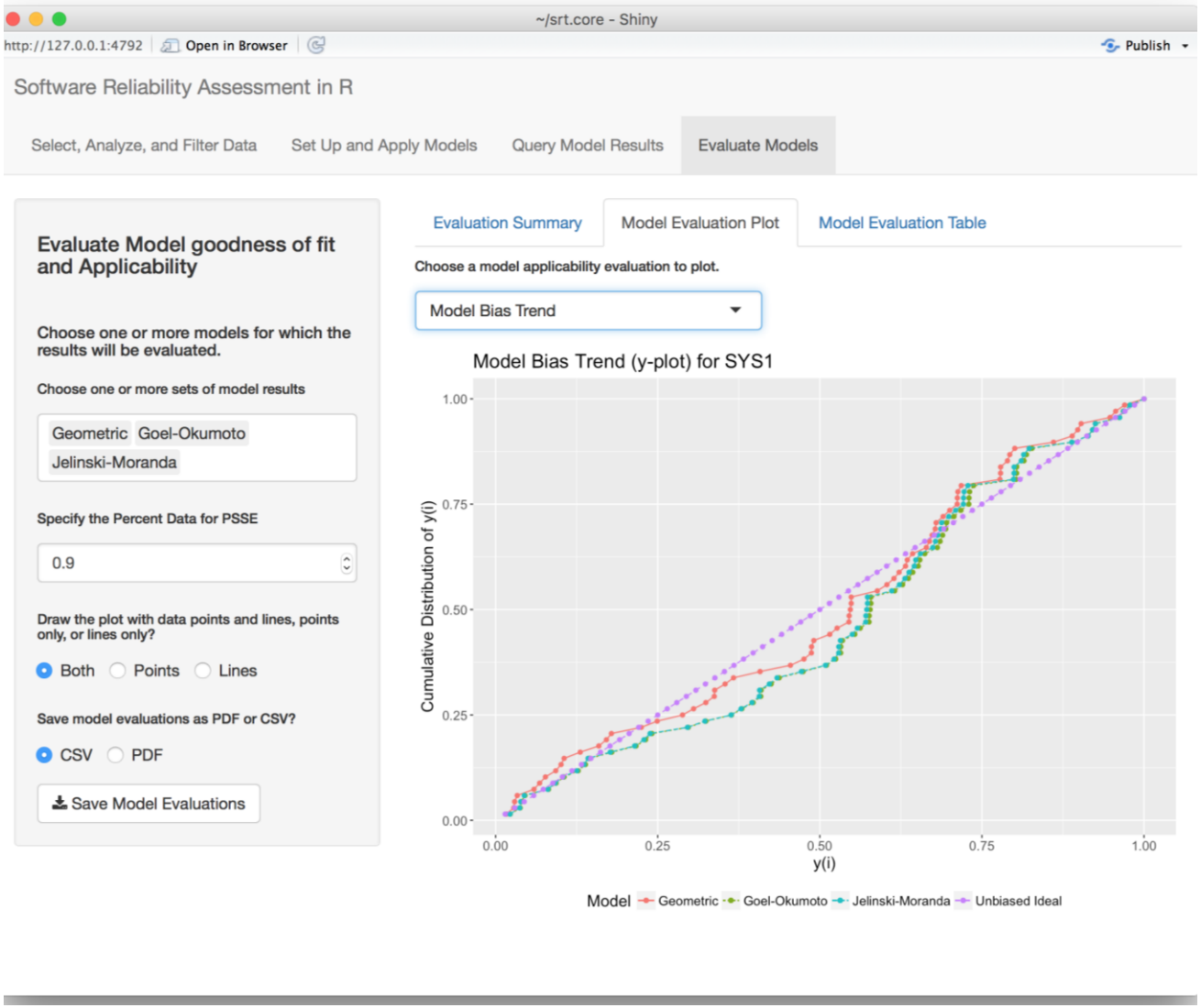
Choose a model applicability evaluation to plot.

Prequential Likelihood Ratio

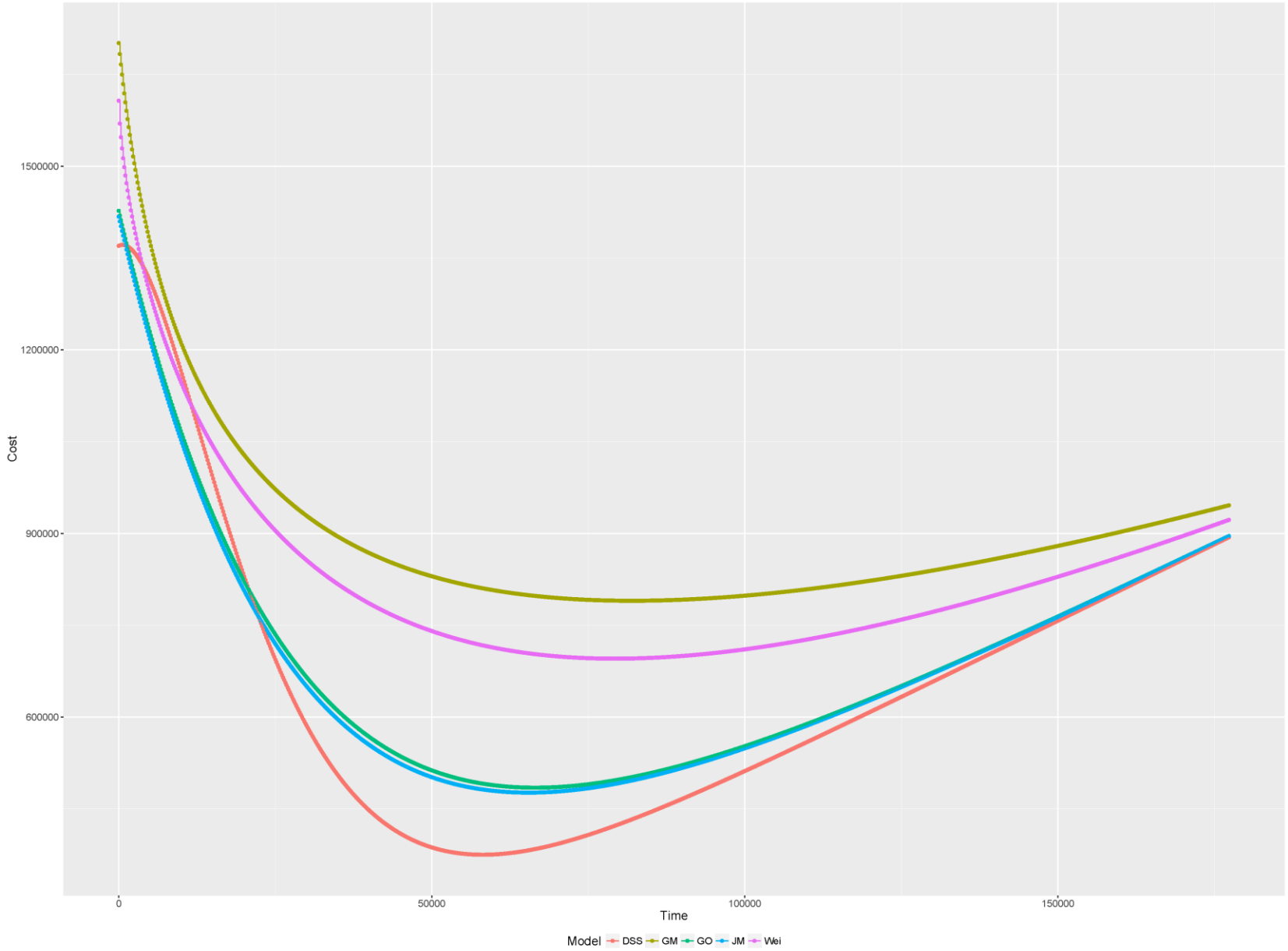




Models above line estimate more frequent times between failures than those observed



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

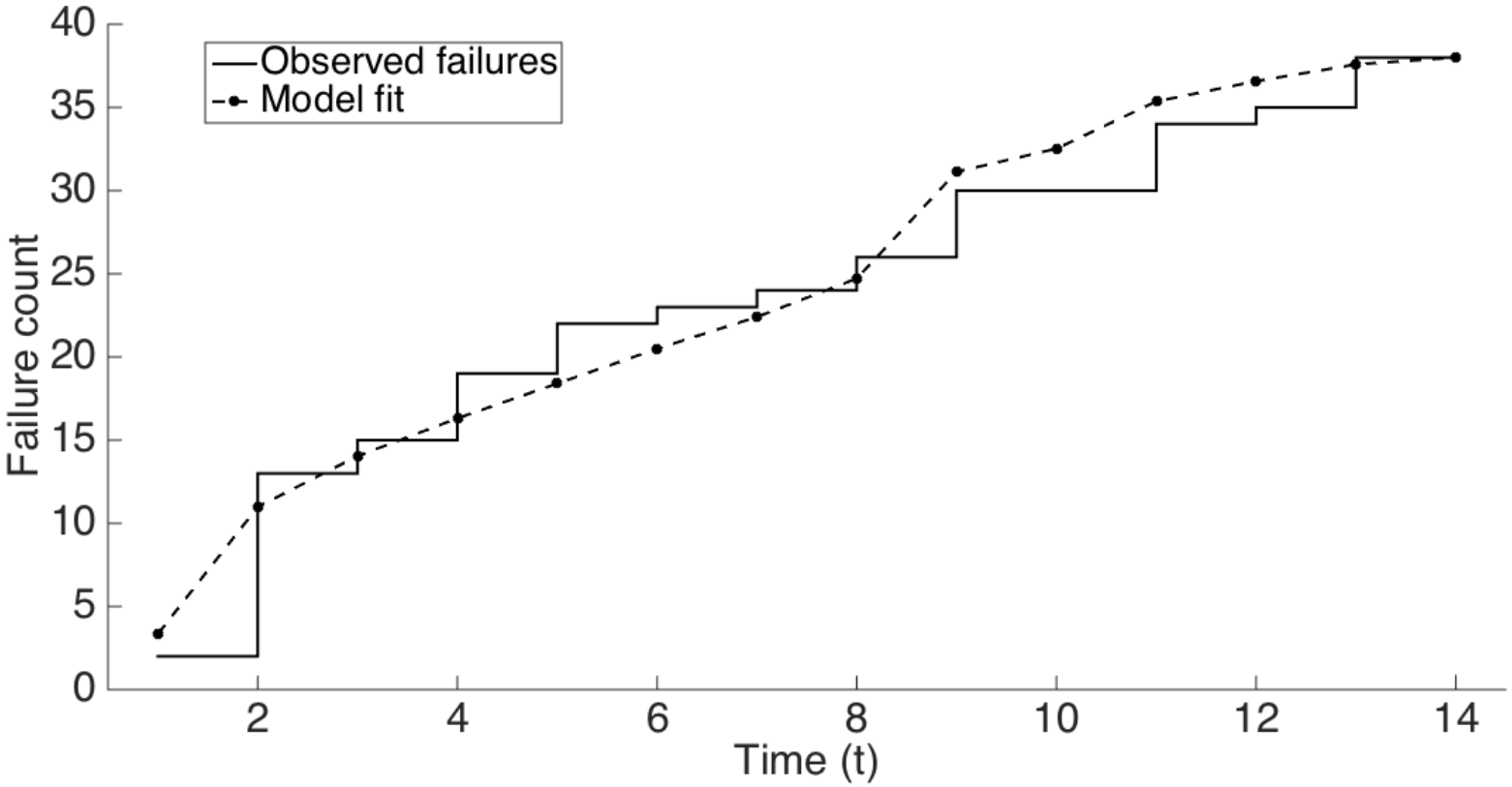
Activities

- 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 the Naval Air Warfare Center (NAVAIR) under contract N00421-16-T-0373.





EFFICIENT USE OF ENTERPRISE AND SYSTEM ARCHITECTING IN COMBINED ENVIRONMENT

H. GANS, F. MARKHAM, M. OSAISAI, J PRATCHIOS, D WOOD

Contact info: Howard Gans, Harris Corporation, (321) 727-4379, hgans@harris.com

HARRIS® TECHNOLOGY TO CONNECT, INFORM AND PROTECT™

Introduction: architecting in a combined environment

Today's architect must consider several levels

- Enterprise level
  - System-of-systems, business models, customer framework mandates
- System level
  - System architecture, interfaces, functional allocation, requirements development
- Design level
  - Code development, service development, performance analysis and simulation

Modeling languages have been developed to address these needs

- Profiles developed by the Object Management Group (OMG) as an aid for modeling
- Unified Modeling Language (UML) defines semantics and stereotypes for object-oriented modeling
- SysML extends UML to systems engineering
- Unified profile for DoDAF and MoDAF (UPDM) supports full compliance with UML, SysML, and elements of the Service Oriented Architecture Modeling Language (SoaML)

Analysis at different levels

Enterprise Architecting

Why this program?
What's the process?



How to use the models for business

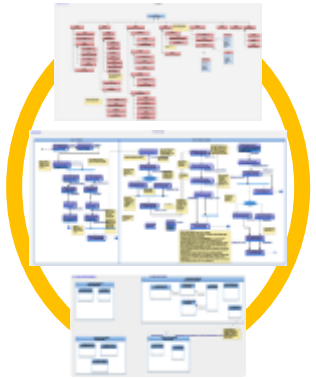
Model Based Architecting

End results – capability view
Desired effects

Operational view
What steps need to be done?

Systems/service views
What parts are needed?

(Others)



Understanding the problem domain from customer needs and platform capabilities to end user

Model Based System Engineering

System components
Requirements
Behavior
Structure
Interfaces



Engineering a reference system framework and instantiating specific solutions for customers

Mode Based Software Engineering

Software components
Implementation options, analysis, simulation

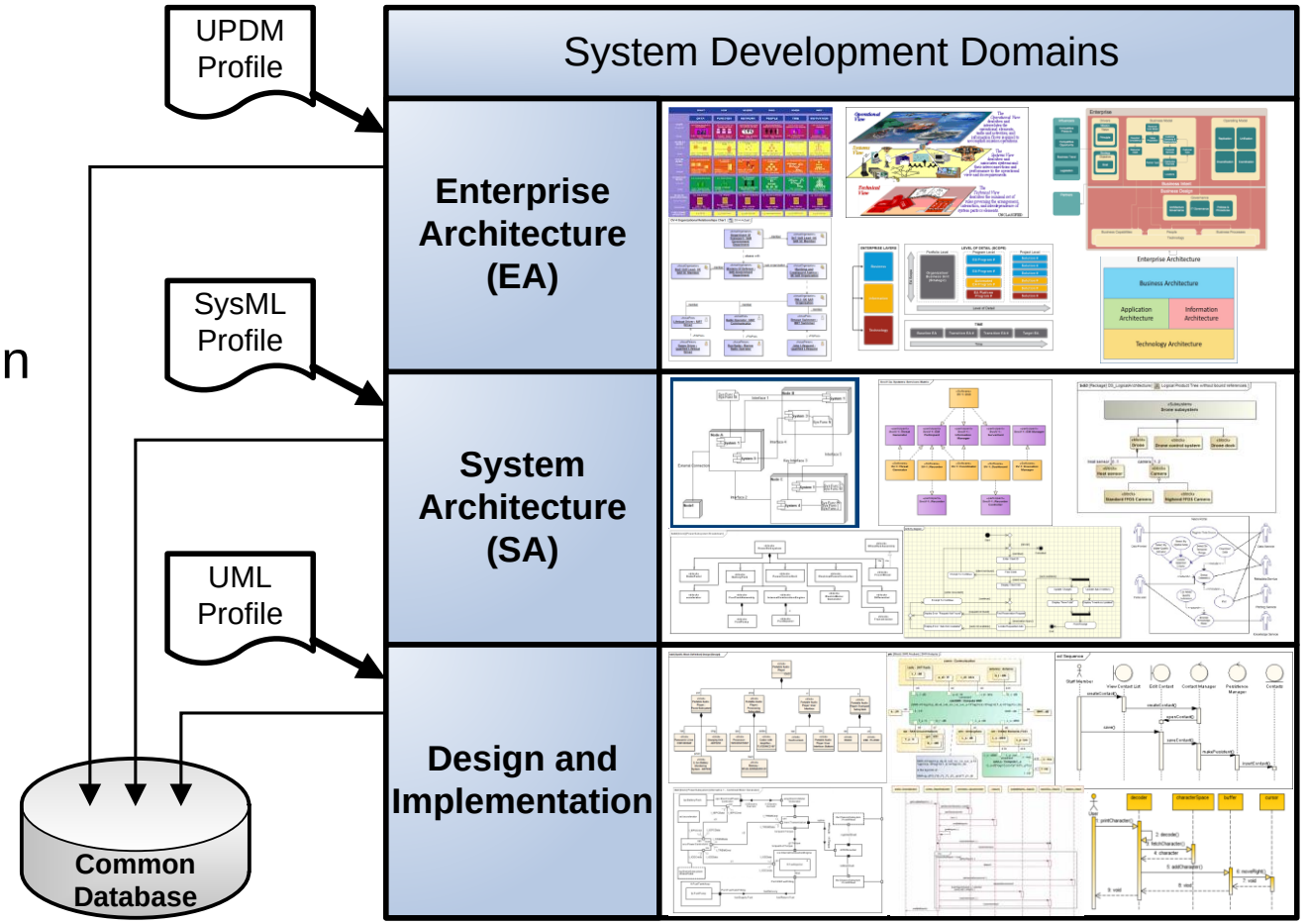


Engineering software solutions/options for specific customer needs

Enterprise and system architecting

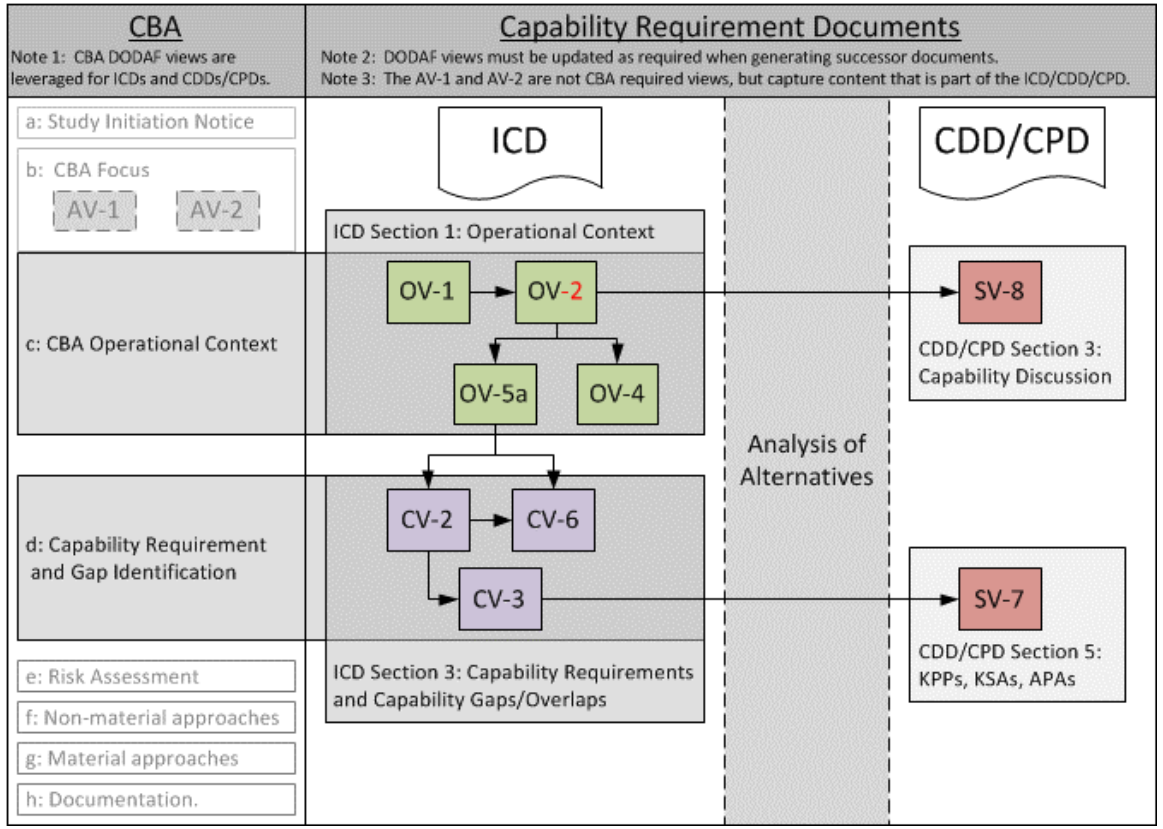
3 levels: enterprise, system, design

- Use the right tool for the job
  - EA for the mission domain
  - MBSE for the solution domain (SysML)
  - UML for the implementation domain
- With proper tools, all levels can exist within the same modeling framework
  - Linked together
  - Consistent
  - Same database
- The perspective is linked to the profile
  - Enterprise architecting – DoDAF (UPDM)
  - System architecting/design (SysML)
  - Implementation and coding (UML)



DoD mandates for DoDAF

- **Per the JCIDS Manual (12 Feb 2015), "...DoDAF views and associated data provide a structured means to document data associated with the CBA (Capabilities Based Assessment)…."**
  - Focus for CBAs is on the Capability Viewpoint (CV) and the Operational Viewpoint (OV)
- **Requires use of DoDAF products for development and evaluation of the net ready key performance parameter (NR-KPP)**
  - Use of all viewpoint (AV), data and information viewpoint (DIV), System and service viewpoints (SV, SvcV)
- **Includes specific direction to "(p)roduce architectures using a tool that focuses on architectural data rather than only upon individual artifacts/views."**



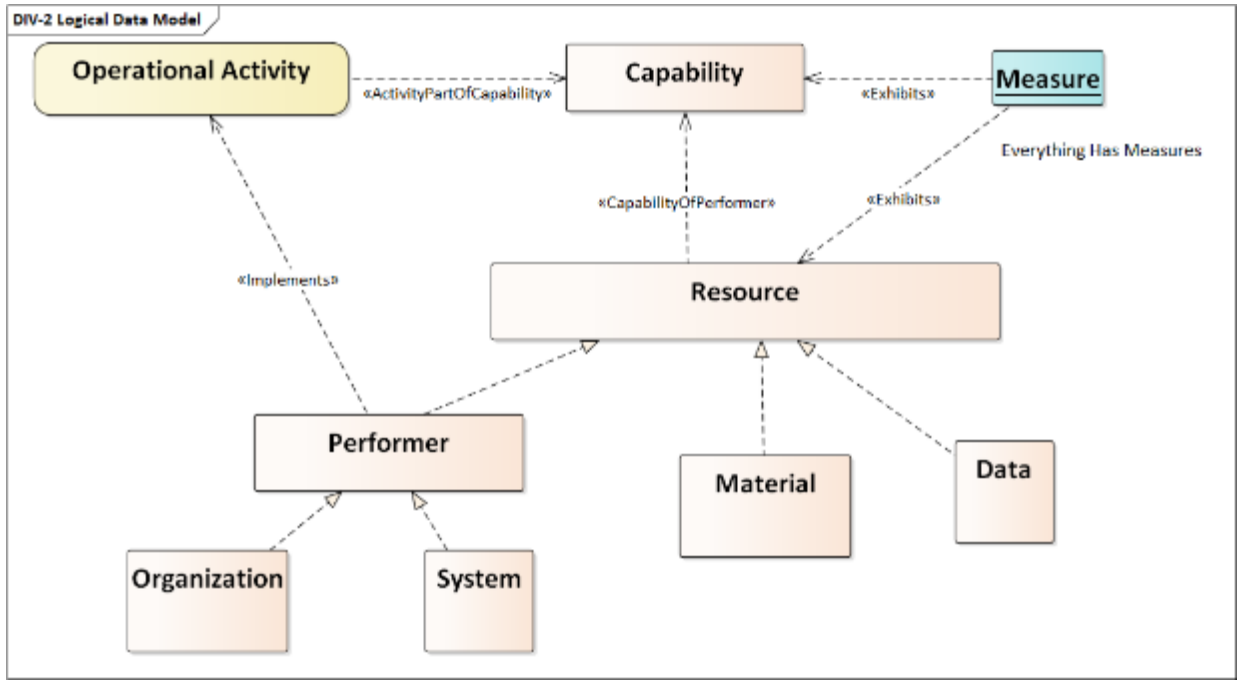
The DoDAF MetaModel (DM2)

DoDAF is an "…(O)vearching, comprehensive *framework* and *conceptual model* for architectural descriptions…." (DoDAF v2.02, Chng 1, Managers Guide)

- Frameworks used to develop architectural descriptions (viewpoints)
- Conceptual model involves high-level data constructs supporting the architectural descriptions

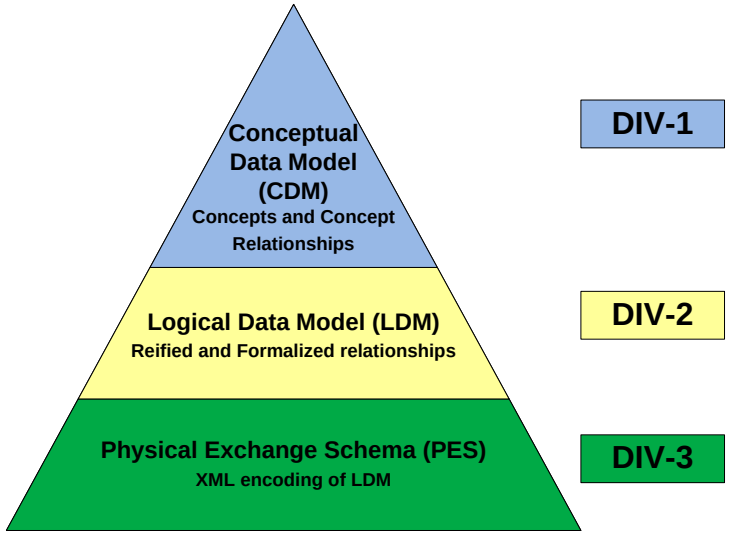
DoDAF MetaModel (DM2)

- Establishes a basis for describing the relationship between architectural artifacts
- Used to build a set of strategic information about the architecture and are described in the DM2 Conceptual Data Model
- Forms the basis of defining data for the CBA and the NR-KPP



DM2 Conceptual Data Model (Example)

Use of DM2 for system architecting and design



❖ **DIV-1 Conceptual Data Model (CDM)**

- Description of the information flow between high-level resources in UPDM
  - OV-2 node connectivity
  - OV-5 activity diagrams
  - SV-2 communications descriptions

❖ **DIV-2 Logical Data Model (LDM)**

- Activity flow within the system model
  - SysML signals in activity diagram
  - SysML block operations in sequence diagrams
- Data at rest
  - SysML block attributes

❖ **DIV-3 Physical Exchange Schema (PES)**

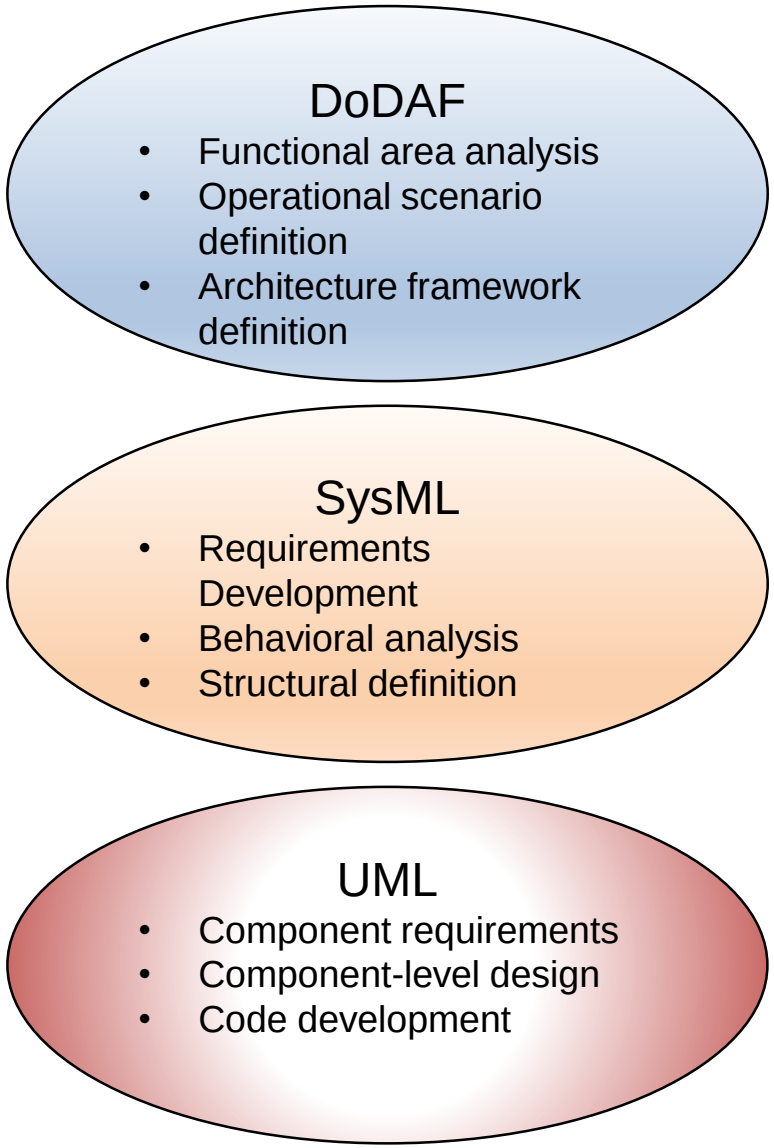
- Creating and using interface definitions (WSDL) for use in UML sequence and activity diagrams
- Creating (and importing) source code with the UML structural model

Data Traceability from concept to implementation

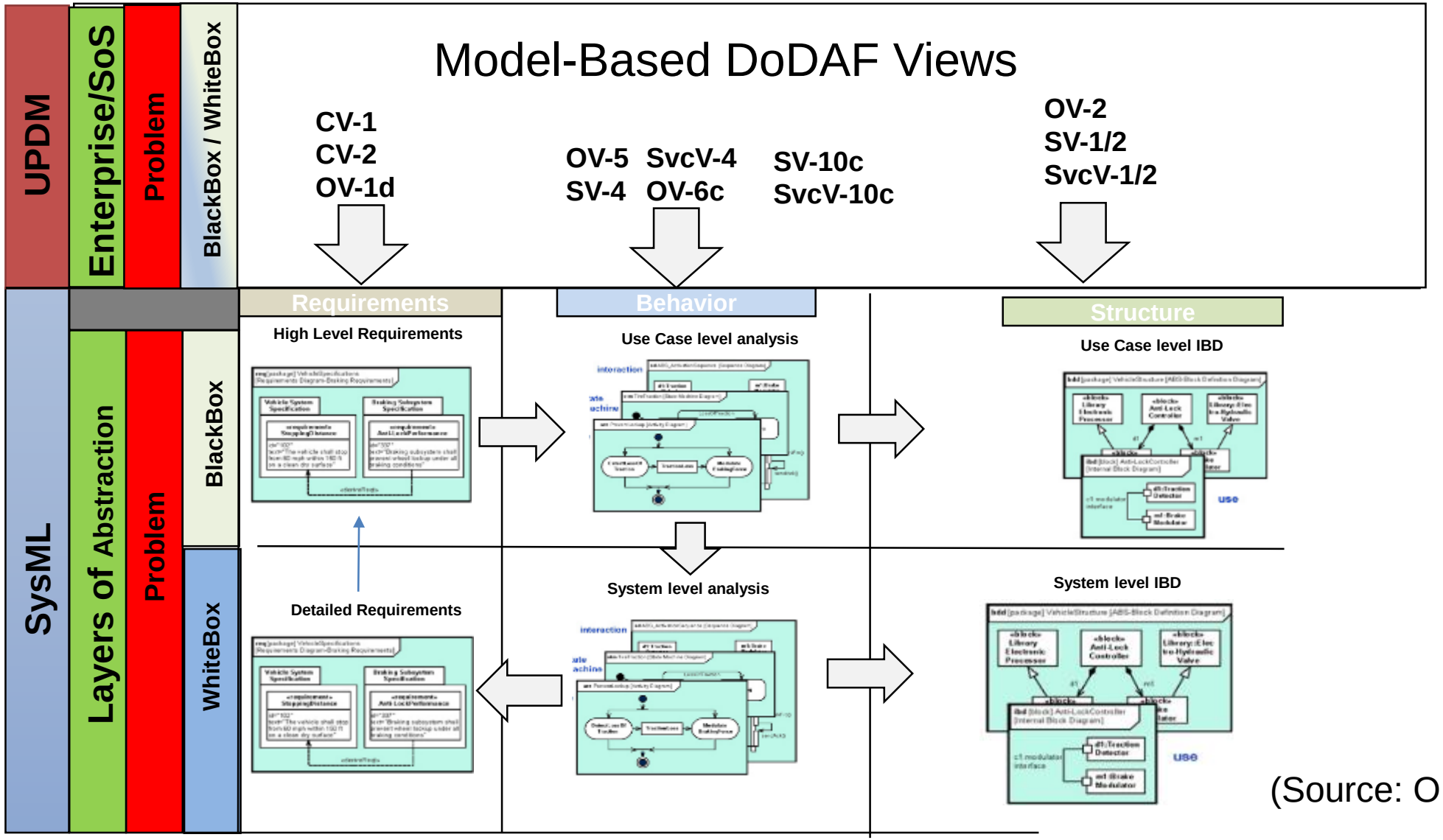
We are doing this now with Linked UPDM – SysML – UML models

Issue: mission, solution, and implementation architecting and design

- **Our tools provide profiles and prospective for working in all 3 domains**
- **The selected prospective not only "guides" the diagram creation, but also our mindset while modeling**
- **Mission domain (DoDAF views) speak to the stakeholder's viewpoint**
- **Using the profiles and prospective for mission domain while working in the solution (system) domain does not focus on the correct level**
  - Functional system models are required by the software teams
  - Structural models are required by the hardware and integration teams
- **System modeling must be reused by other engineering disciplines**
  - Successful programs develop their system details in the model
  - Struggling programs develop their system details in the integration lab



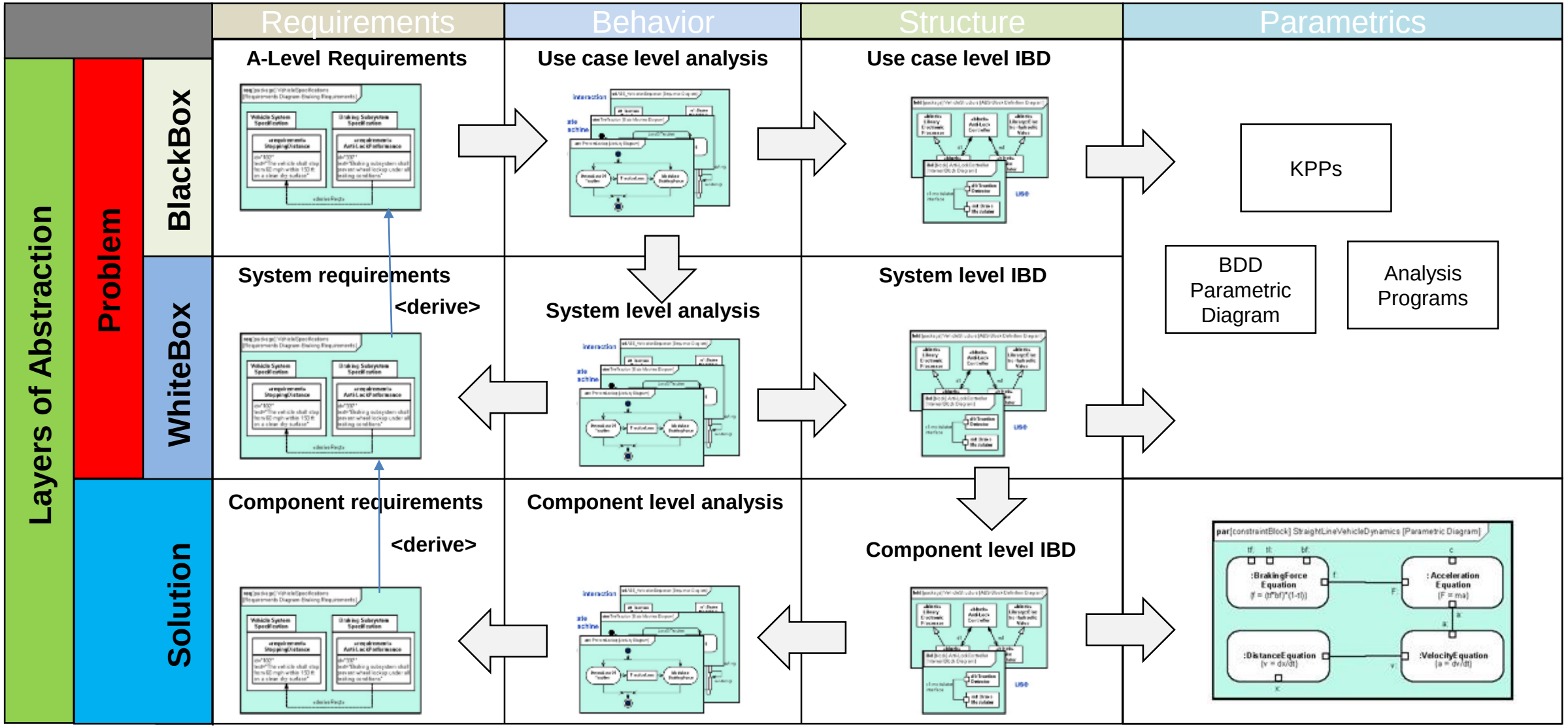
Alternative strategies (UPDM to SysML)



Consistent with DM2

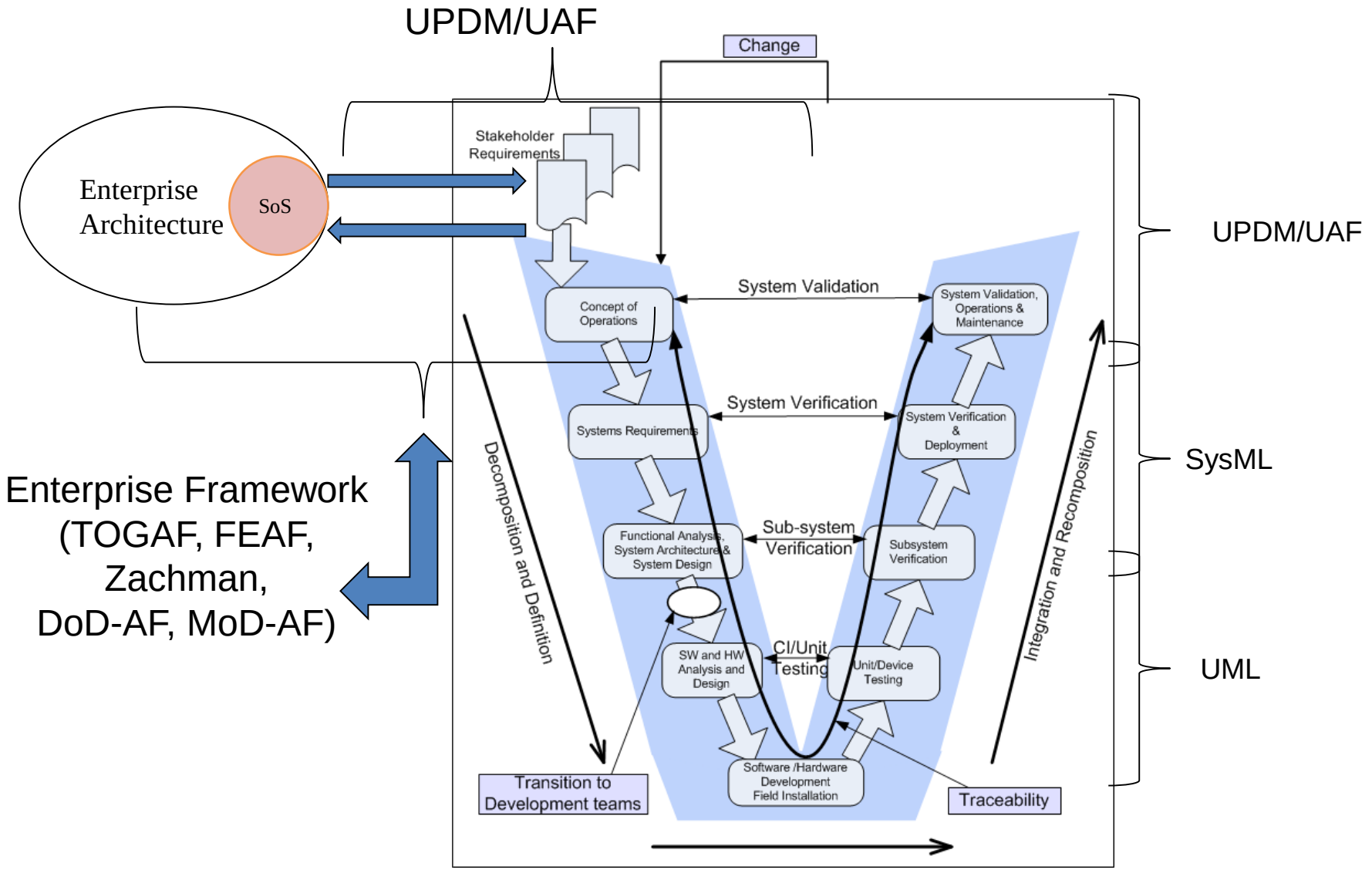
(Source: OMG)

Alternative strategies (SysML to UML)



(Source: OMG)

Workflow consistent with systems engineering “VEE” diagram



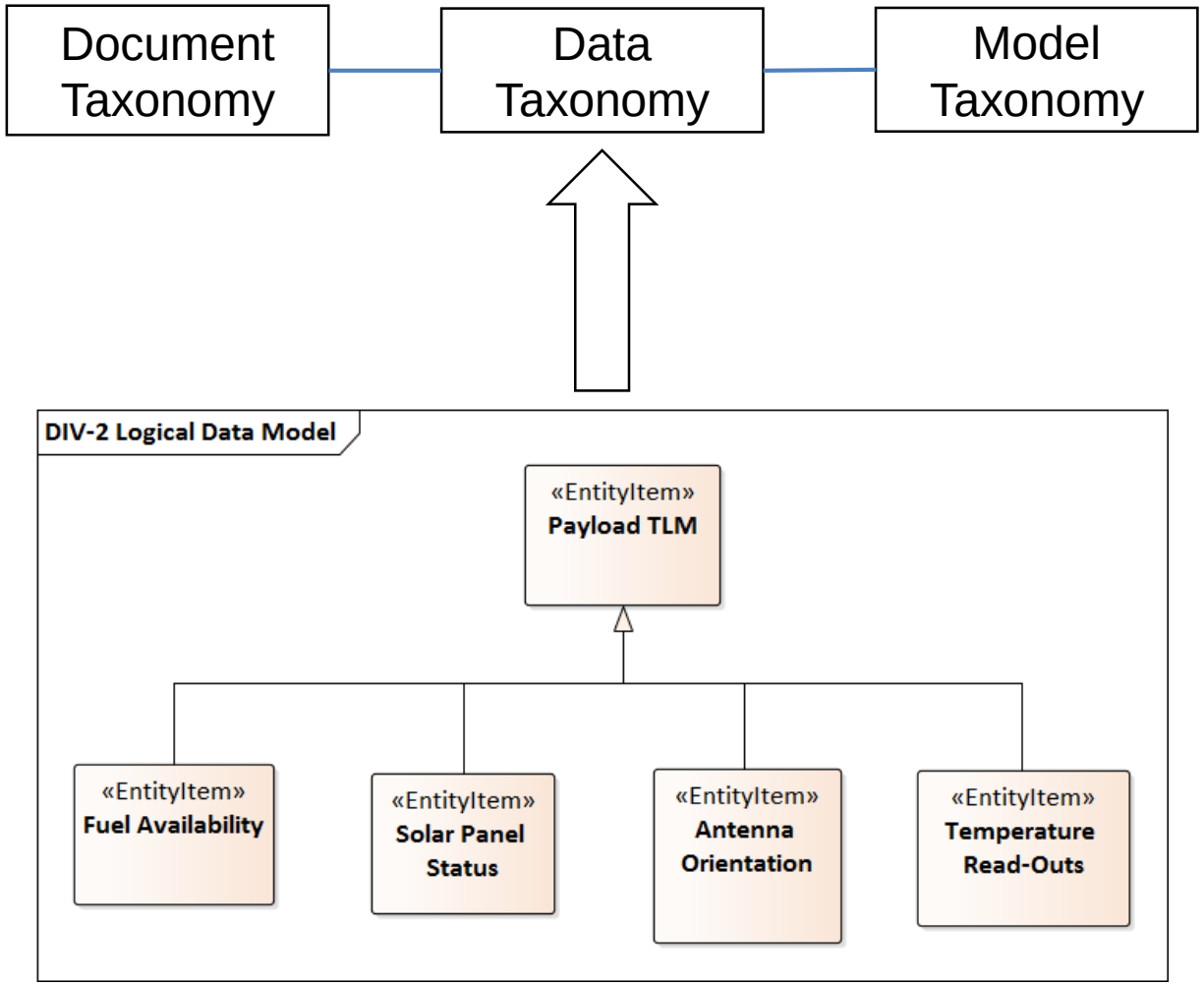
- Tier 1- Specifier: EA develop stakeholder views (DoDAF/MoDAF)
- Tiers 2 & 3 – Implementer: Functional requirements analysis, behavior analysis and system decomposition, system solution implementation

DOD Digital Engineering (DE) initiative

- An initiative developed and championed by Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD-SE)
- This initiative rebrands Model Based Engineering (MBE) and Model Based Systems Engineering (MBSE) to some extent. DE is basically the DOD chosen name for MBE
- DE Working Group (DEWG) represented by stakeholders of various segments of the acquisition community – (Program Executive Officers, Program Manager Engineering and Science and Technology components)
  - Promote DE principles throughout the services and in other government agencies
  - Explore ways to transfer traditional acquisition processes to a digital model-centric environment
  - Develop and implement the digital engineering concept across engineering functions and within the Defense Acquisition System
- Initiative is tool agnostic; emphasis is on integration of technical data employing a modeling ecosystem of varying tools

DE Initiative is encouraging increased MBE/MBSE use across the community

Proposed Digital System Model (DSM) taxonomy and DM2



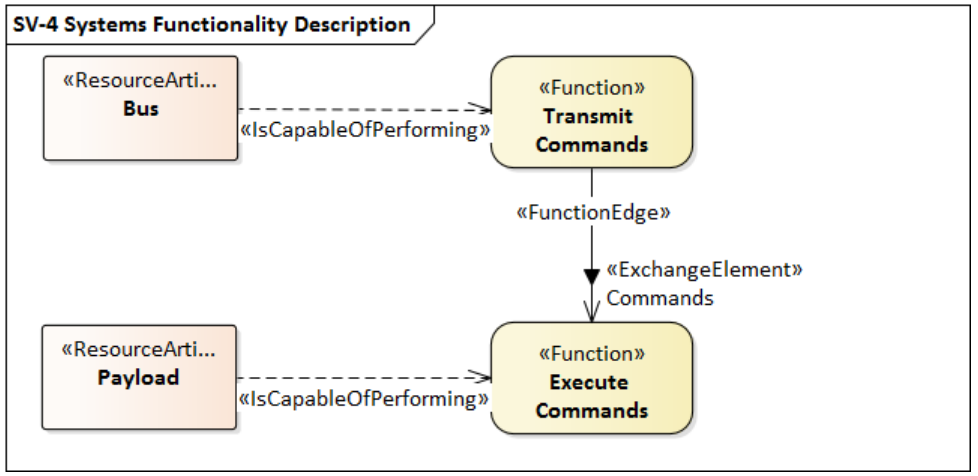
Model DM2

- DM2 can be used as an element of the data taxonomy
- DM2 represents data classes and data types organized in a consistent framework
- Each program should have a single, consistent DM2 compatible with all profiles in the model
- Data elements once defined can be reused, linked to information flows, and traced via model utilities
- Candidate presentations for model taxonomy:
  - Sequence of model views
  - Structural block definition diagrams as developed during modeling process

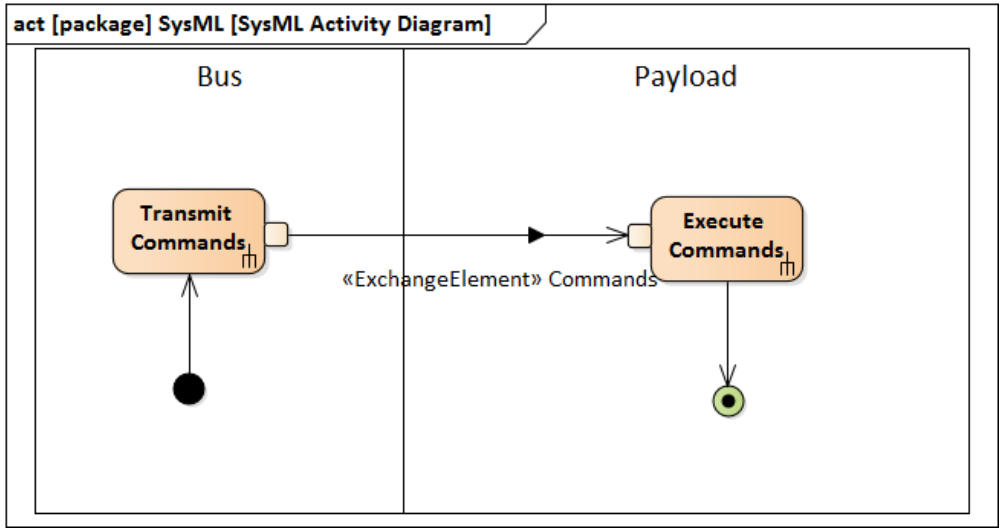
Recommendations on use of DoDAF

DoD guidance places DoDAF viewpoint mandates on Program Office, but gives discretion on details

- Seek to define architecture goals rather than specific DoDAF view requirements
  - Use modeling best practices
- Perform modeling in a tool using a profile-consistent database that will satisfy DM2 requirements
- Tailor required views based on consensus between Program Office and contractor
  - Produce an integrated architecture with consistent data, not just views
  - Focus program efforts on vision and system development vs. detailed CDRL
  - Permit the required views to be combined in documents as a single CDRL, e.g., Architecture Description Document
  - Avoid duplicative views (e.g., OV-6b vs SV-10b)
- Build views using appropriate modeling language but in a consistent environment



DoDAF SV-4



SysML Activity Diagram

Recommendations to customer, policy changes

Industry has made significant progress in model since DoDAF 2.02 roll out

- DoDAF 2.02 was the last published direction from OSD-CIO
- Industry (OMG lead, tool vendors cooperating) is making necessary changes and defining consistent representations of DoDAF views
- Continued efforts at joint industry-USG architecture development; example, DE Initiative

CJCSI 6212.01 (cancelled) goals are now in CJCSI 3170.01I and the JCIDS Manual. These goals can be met in heterogenous model environments.

- DM2 PES XML schema (XSD) provides a neutral format for data exchange
- Limits exist among the tools during import (views lose layout, folder hierarchy lost)

CJCSI 3170.01 now drives DoDAF view and similar artifact inclusion

- CJCSI 3170.01 now invokes DoDAF views from several topic areas and programmatic needs within the context of the entire list of required program documentation
- There needs to be negotiations between customer and contractor as to acceptable alternatives to DoDAF views and where they may be used

Summary/conclusion

Issues with use of UPDM/UAF at all levels of architecting

- Can be done but there are challenges
- Different Architectural levels have different abstractions and relationships
- Model representations may not be preferred by practitioners at all architectural levels

Technical alternatives

- Separate models with import/export integration
- Common model with individual profiles for appropriate architectural levels

Tailoring of CDRLS

- Accept equivalent diagrams from other models in place of DoDAF views (i.e., SysML)

Policy changes

- Relax rigidity on use of DoDAF views in favor of accepting SysML diagrams as tailored CDRL equivalents
- Negotiate format of MBSE artifacts; support customer needs versus contractor needs

Advancing U.S. Marine Corps Warehouse Management Operations Through System Architecture and Analysis

Chris Melkonian
Chief Engineer, GCSS-MC

Developed in collaboration with the Naval Postgraduate School

October 26, 2017

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Background

- A critical enabler of military superiority is operational availability
  - The probability warfighting systems will be functional when called upon
- A critical enabler of operational availability is delivering parts where and when needed in order to reduce downtime
- A critical enabler of reduced downtime is staging parts close to their demand
- Therefore, the need for warehouses (storing for future demand)

This presentation is not about hardware or software functionality…

it is about architectural behavior

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Agenda

- System Overview
- Fault Tree Analysis
- Monte Carlo Analysis
- Findings and Conclusions

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

System Overview

Increasing complexity (functions, data, and responsiveness)



Kitchen Pantry



USMC Warehouse



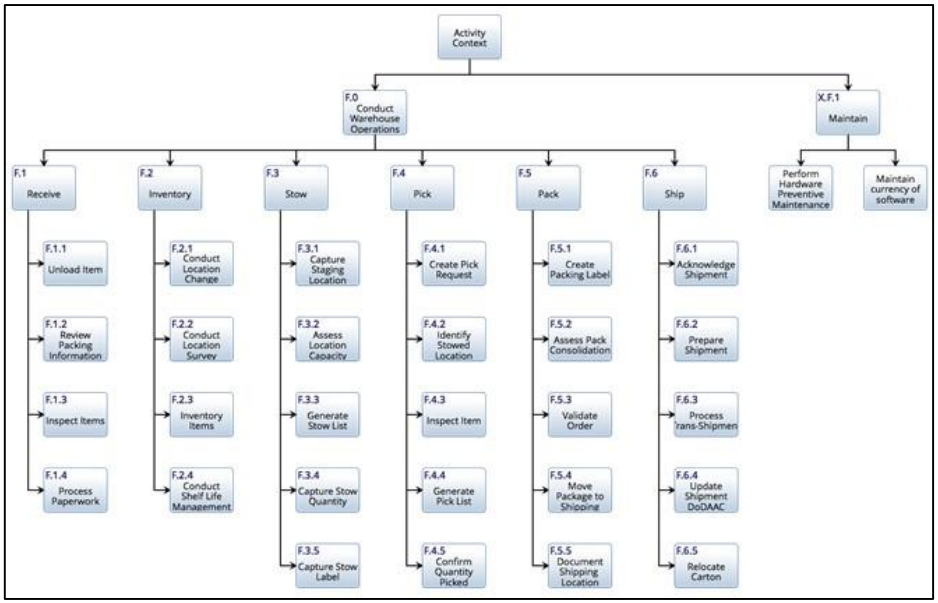
Amazon Distribution Center

- **Globally pre-positioned permanent and temporary locations for storage of items to satisfy military demands and high operational availability**
  - Supply Maintenance Units (SMU)
  - Repairable Issue Points (RIP)
  - Using Units (UU)
  - Initial Issue Provisioning (IIP)
- **Warehouse capability accounts for item:**
  - Volume
  - Weight
  - HAZMAT category
  - Incompatibility with other materials
  - Shelf life

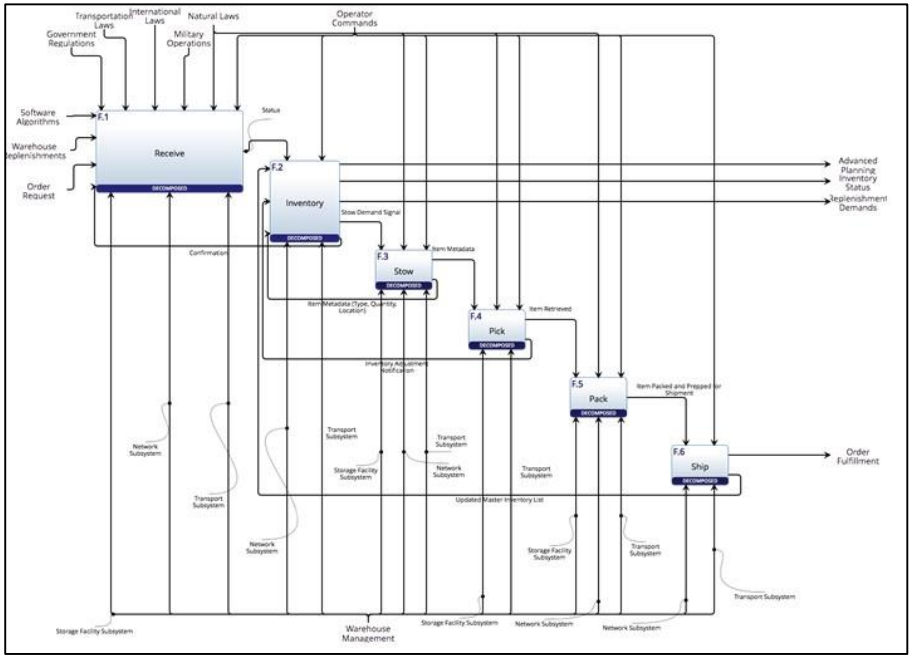


DISTRIBUTION A. Approved for public release. Distribution is unlimited.

System Overview



Activity Context



IDEF0 Diagram

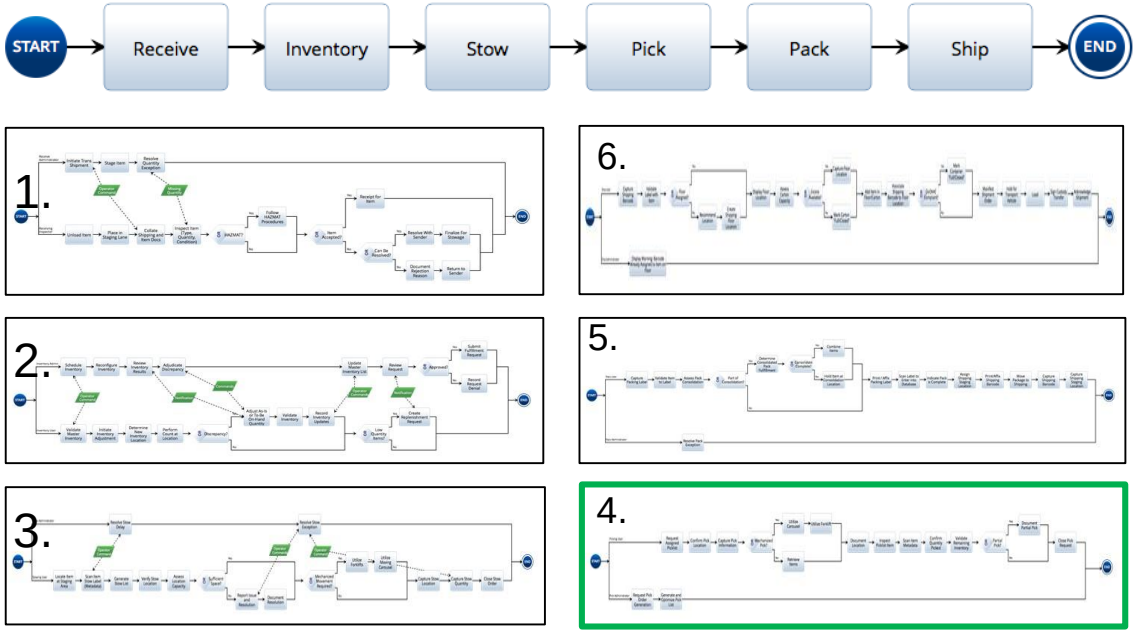
DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Warehouse Process Analysis

Operational View

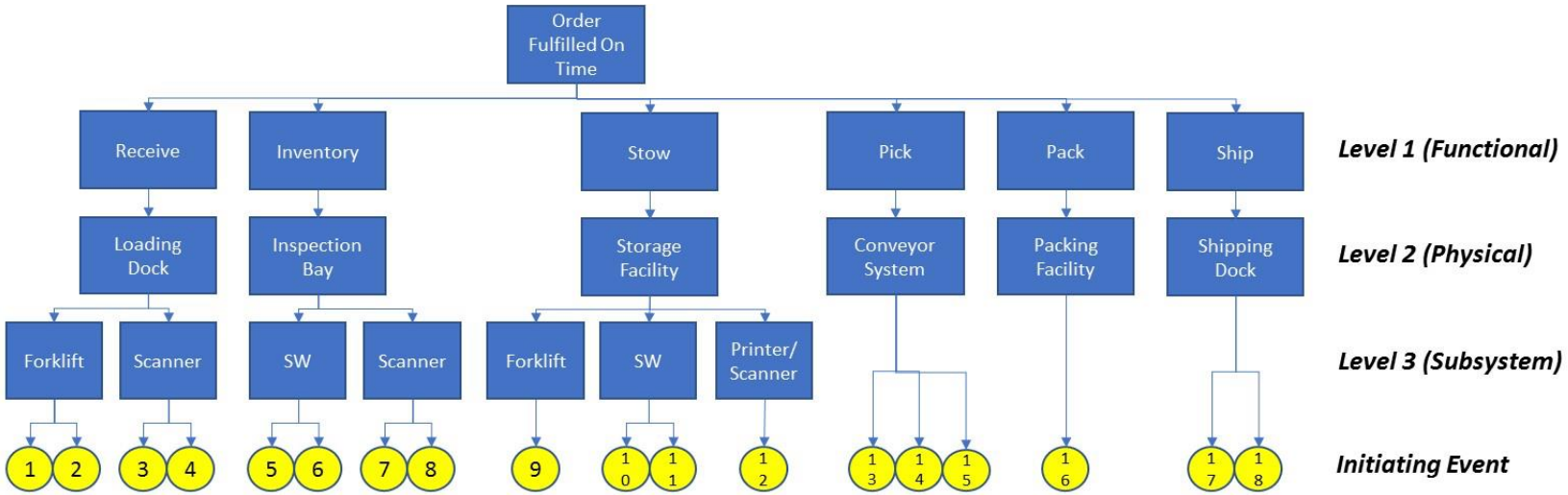


System Top Level Functions



DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Master Logic Diagram (Identify Initiating Events)



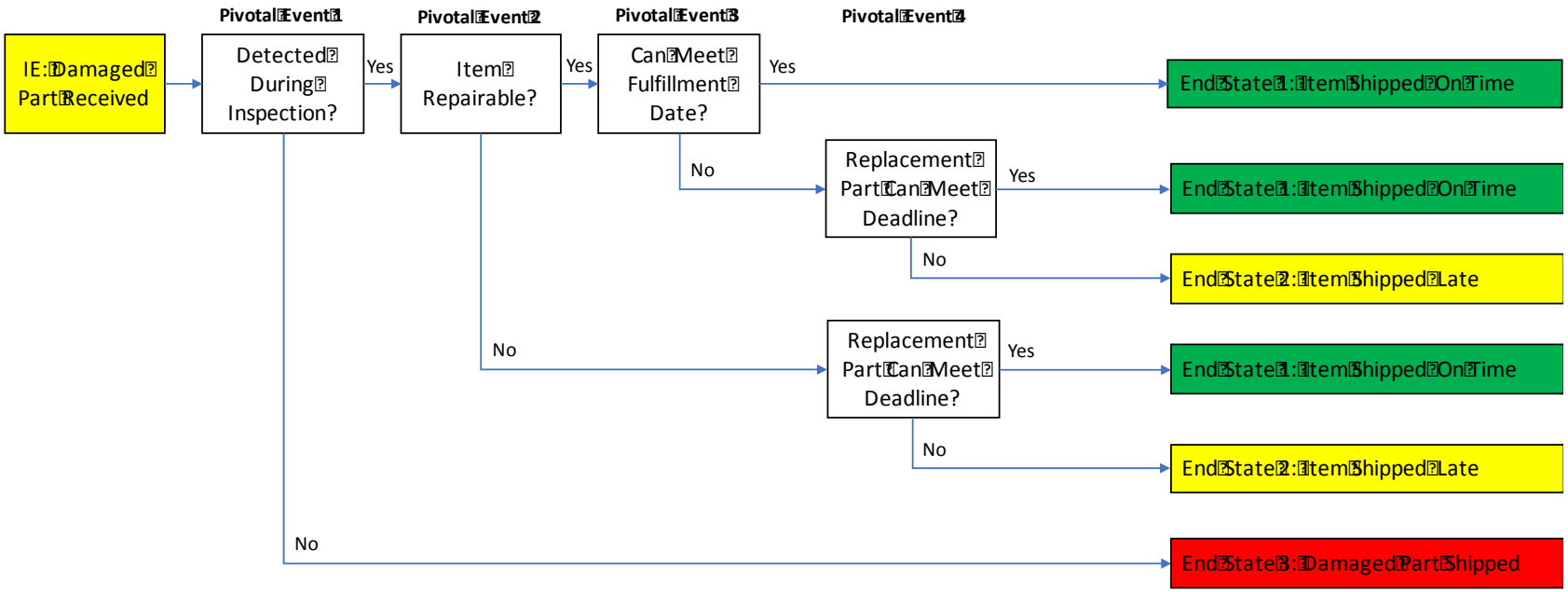
1. **Damage to Item**
2. Incorrectly Placed
3. Malfunction
4. Incorrect Item Scanned
5. Incorrect Information Entered
6. Incorrect Shelf Life Entered
7. Malfunction
8. Faulty Data Entry
9. Faulty Equipment (Damage to Item)

10. **Loss of Network Connectivity**
11. Incorrect Inventory Record
12. Incorrectly Labeled
13. Incorrectly Placed (Stowed)
14. **Inadequate Inventory**
15. Incorrectly Picked Item
16. Incorrect Quantity Picked
17. Wrong Truck Loaded
18. Labels Not Verified

* Reference: NASA/SP-2011-3421, 2nd Ed. 2011.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

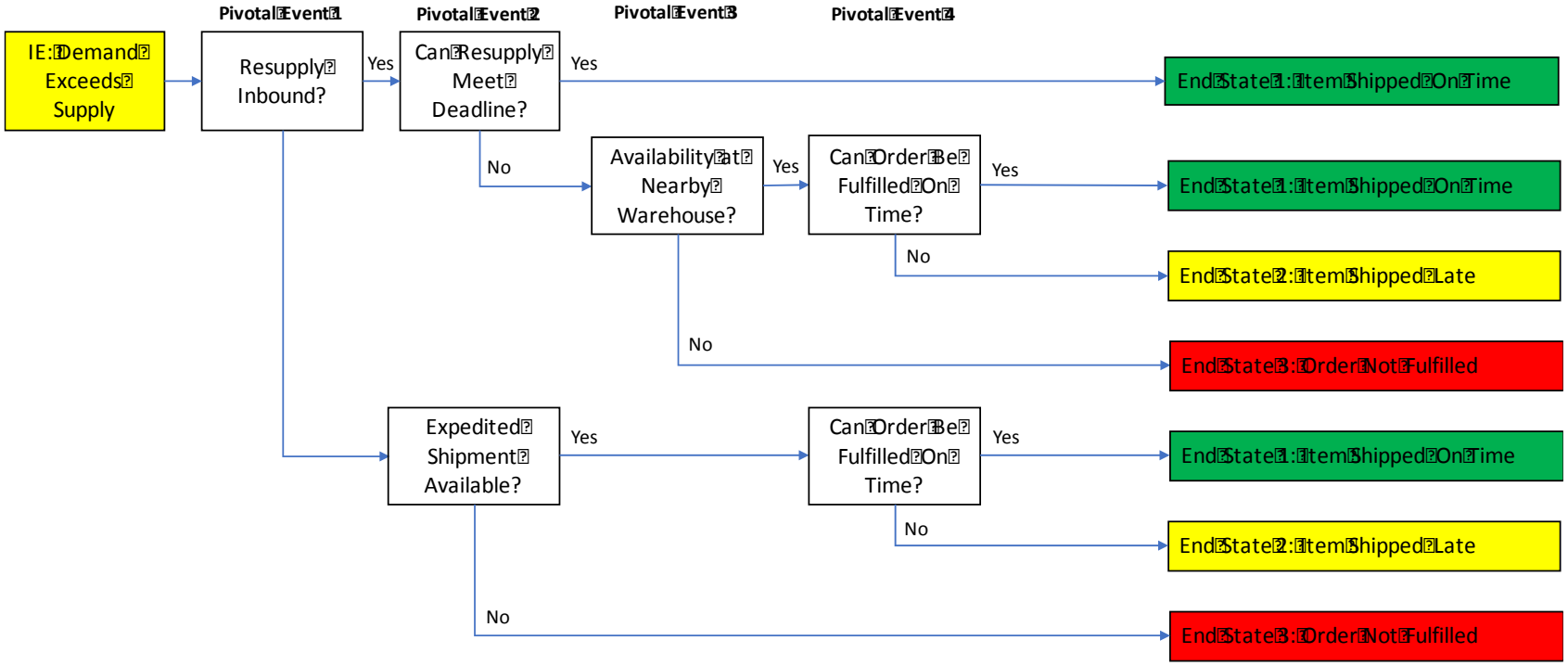
Event Tree (IE1: Damaged Part Received)



* Reference: NASA/SP-2011-3421, 2nd Ed. 2011.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

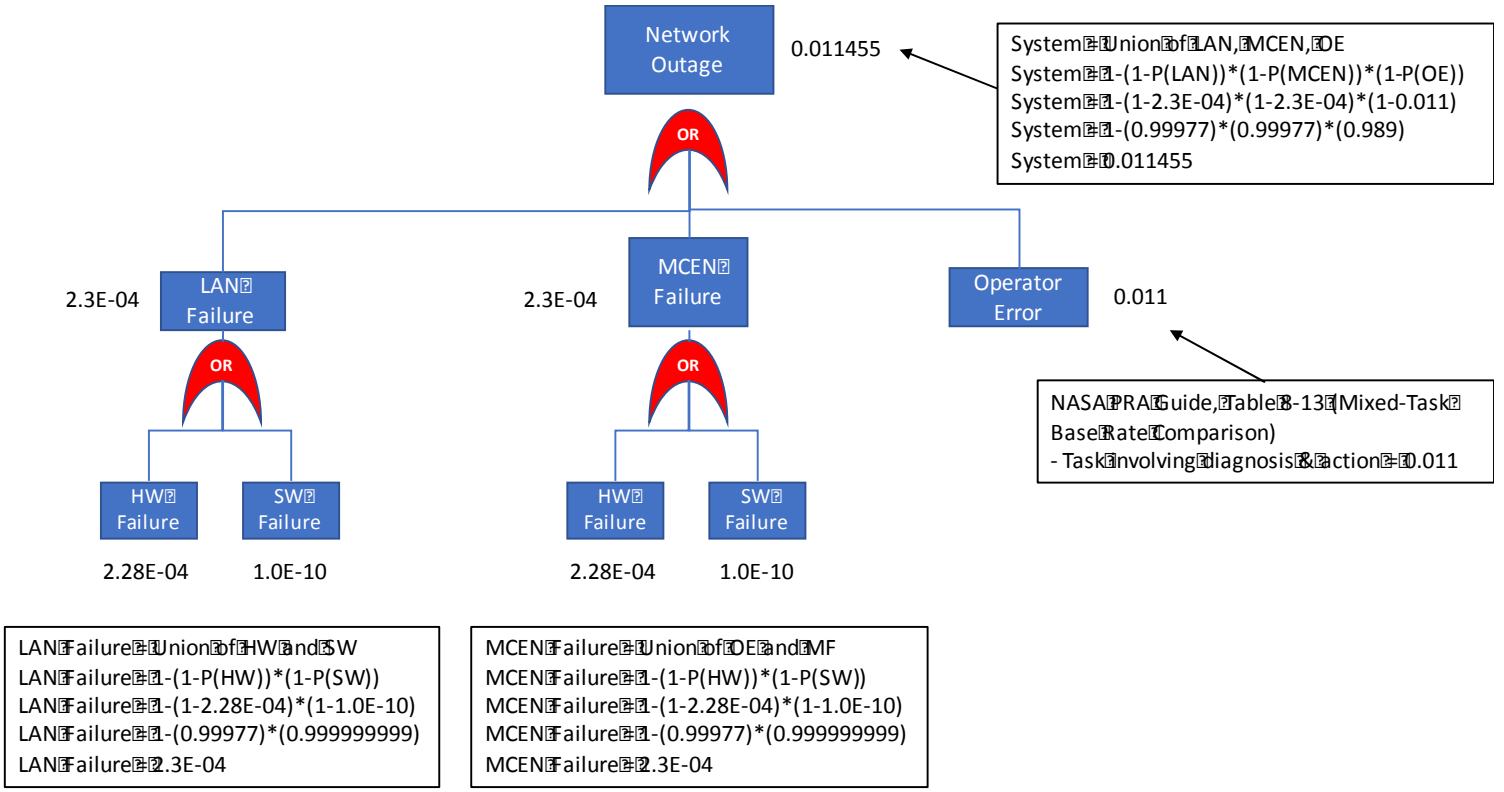
Event Tree (IE2: Demand Exceeds Supply)



* Reference: NASA/SP-2011-3421, 2nd Ed. 2011.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

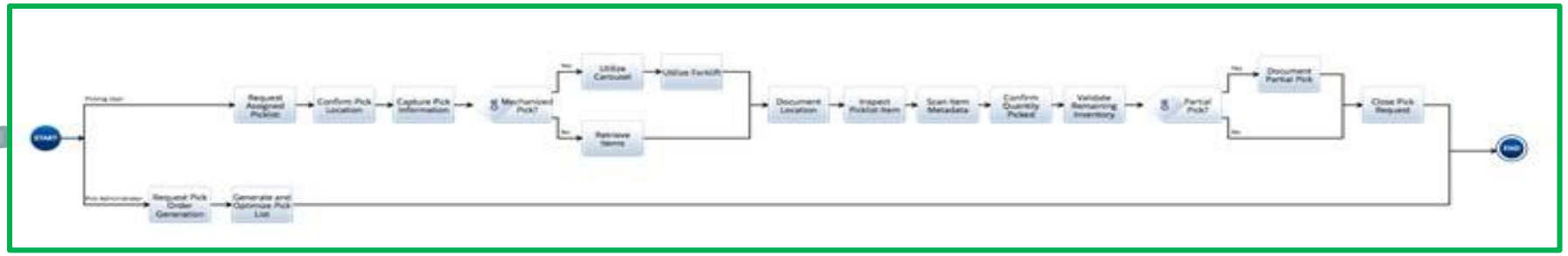
Fault Tree Analysis



* Reference: NASA/SP-2011-3421, 2nd Ed. 2011.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Schedule Analysis Inputs (Pick Sub Process)



Task #	Title	Basic Duration (min)	Best Case	Most Likely	Worst Case	Risk Factor	Distribution
1	Request Pick Order	0.2	0.2	0.208	0.22	L	Triangular
2	Generate Pick Order	0.2	0.2	0.218	0.248	M	Triangular
3	Request Assigned Picklist	0.2	0.2	0.212	0.23	L+	Triangular
4	Confirm Pick Location	1	1	1.04	1.1	L	Triangular
5	Capture Pick Information	1	1	1.04	1.1	L	Triangular
6	Utilize Carousel	5	5	5.3	5.75	L+	Triangular
7	Utilize Forklift	10	10	12	15.5	H	Triangular
8	Retrieve Items	5	5	5.3	5.75	L+	Triangular
9	Document Location	1	1	1.04	1.1	L	Triangular
10	Inspect Packlist Item	2	2	2.12	2.3	L+	Triangular
11	Scan Item Metadata	0.2	0.2	0.208	0.22	L	Triangular
12	Confirm Quantity Picked	1	1	1.04	1.1	L	Triangular
13	Validate Remaining Inventory	3	3	3.12	3.3	L	Triangular
14	Document Partial Pick	2	2	2.08	2.2	L	Triangular
15	Close Request	0.2	0.2	0.208	0.22	L	Triangular

Path #1	Duration
1	0.200
2	0.200
3	0.200
4	1.000
5	1.000
6	5.000
7	10.000
9	1.000
10	2.000
11	0.200
12	1.000
13	3.000
14	2.000
15	0.200
Total Path #1	27.000
P1 CR path?	1

Path #2	Duration
1	0.200
2	0.200
3	0.200
4	1.000
5	1.000
8	5.000
9	1.000
10	2.000
11	0.200
12	1.000
13	3.000
15	0.200
Total Path #2	15.000
P2 CR path?	0

Path #3	Duration
1	0.200
2	0.200
3	0.200
4	1.000
5	1.000
8	5.000
9	1.000
10	2.000
11	0.200
12	1.000
13	3.000
14	2.000
15	0.200
Total Path #3	17.000
P3 CR path?	0

Path #4	Duration
1	0.200
2	0.200
3	0.200
4	1.000
5	1.000
6	5.000
7	10.000
9	1.000
10	2.000
11	0.200
12	1.000
13	3.000
15	0.200
Total Path #4	25.000
P4 CR path?	0

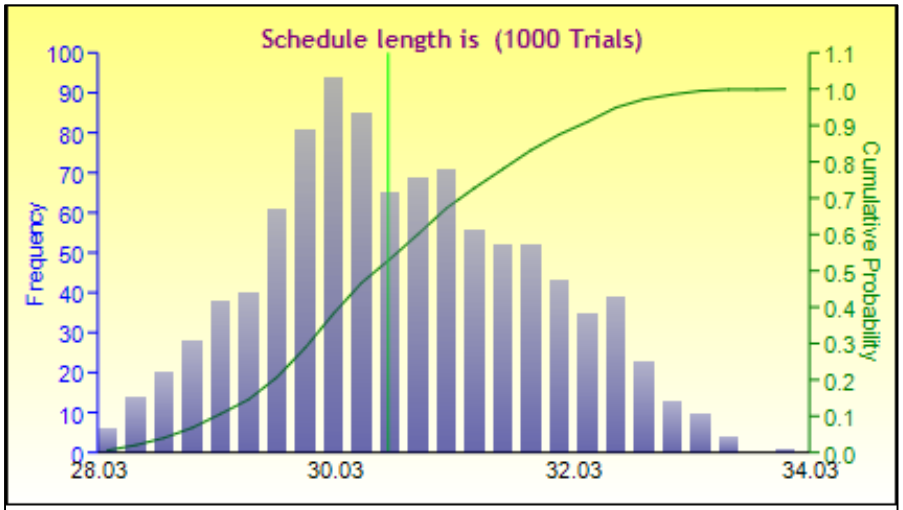
Schedule length is 27.000

How Long Should It Take From Order Fulfillment Request To Prepping For Shipment?

* Reference: NASA/SP-2011-3421, 2nd Ed. 2011.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Schedule Analysis (Pick Sub-Process)



Type: Two-Tail, Lower: -Infinity, Upper: Infinity, Certainty: 100.0000%

Number of Trials	1000
Mean	**30.4831**
Median	30.3745
Standard Deviation	**1.1349**
Variance	1.2880
Coefficient of Variation	0.0372
Maximum	33.8297
Minimum	27.8794
Range	5.9504
Skewness	0.1856
Kurtosis	-0.5743
25% Percentile	29.6828
75% Percentile	31.3082
Percentage Error Precision at 95% Confidence	0.2308%

Baseline Run: Mean of 30.4831 minutes to pick an item from when an order is placed.

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Concluding Remarks

- **Process steps are consistent with current warehouse operations**
  - Verified by warehouse operators
- **Modeling enabled identification of largest contributing factors for each process**
  - Varying operator skillsets
  - Varying pick items (low vs. high shelves, easier vs. more difficult items to pull)
  - Varying distances of pick item from forklift storage location
- **Process baselining helped bring clarity to warehouse management operations**
- **Fault Tree Analyses uncovered potential failure modes and their probability of occurrence**
  - Mitigating steps can be put into place to reduce the likelihood or consequence
- **Schedule analysis applied quantitative methods**
  - Establishes benchmarks that operators can assess against

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Contact Information

Thank you for your time

Chris Melkonian
Marine Corps Systems Command
Global Combat Support System – Marine Corps
(GCSS-MC) Program Office
Phone: (703) 432-5817
Email: chris.melkonian@usmc.mil

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

Investigating Approaches to Achieve Modularity Benefits in the Acquisition Ecosystem

20th Annual NDIA Systems Engineering Conference

October 24-27 Waterford, Springfield, VA.

Dr. Daniel DeLaurentis
Dr. Navindran Davendralingam
Dr. Cesare Guariniello
Dr. Mitchell Kerman
Dr. Lu Xiao

Background

- Current DoD acquisition challenges
  - to affordably address emerging threats
  - component obsolescence
  - loss of critical suppliers, and planned technology upgrade for tightly coupled, highly integrated systems

- DoD acquisitions strategy : Better Buying Power 3.0 (BBP 3.0)
  - Implement best practices to improve productivity, affordability, capabilities, reduce unproductive states across DoD acquisitions
  - Includes encouraged use of modularization strategies to achieve desired end benefits
  - Strategy: Modular Open Systems Approach (MOSA)

MOSA Initiative

- ODASD/SE Modular Systems Approach (MOSA)
  - Open System Architecture (OSA)
    - Business side of acquisition process - data rights, IP, legal matters
    - Most MOSA work currently under auspices of OSA efforts – need to extend to technical as well
    - Requirement under law on including MOSA in acquisition language
  - Modularity (in DoD)
    - Viewed as technical approach in defense acquisitions
    - Complex system decomposition: physical and functional architecture
    - Largely separated from OSA tenets that are more business oriented
    - Modular open systems leverages business driven benefits of adopting Open Architecture standards for development

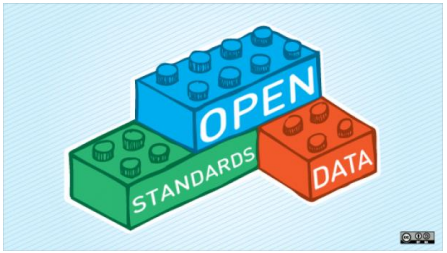
MOSA Goals

- **Cost savings/cost avoidance**
  - Savings via reduced burden on acquisition processes,
- **Allow technology refresh**
  - Rapid updates of modules individually easier than addressing total monolithic complex system
- **Interoperability of systems/components**
  - Open standards use ensures compliance in interoperability
- **Increase competition between suppliers**
  - Leverage open standards and modularity to engage more business units for development (e.g. SBIRs etc)
- **Incorporate innovation**
  - Innovation can be more readily focused at localized modular level

MOSA Guidelines

- **Establish an enabling environment**
  - PM to generate business practices, technology development, test and evaluate, etc. needed for development of open systems
- **Employ modular design**
  - Four main characteristics: cohesive, encapsulated, self-contained, highly binned
- **Designate Key Interfaces**
  - Module interfaces defined to enable designers and configuration managers
- **Use Open Standards**
  - Utilization of community accepted standards that are well defined/matured
- **Certify Conformance**
  - Use rigorous assessment mechanisms, interface control management and proactive conformance testing.



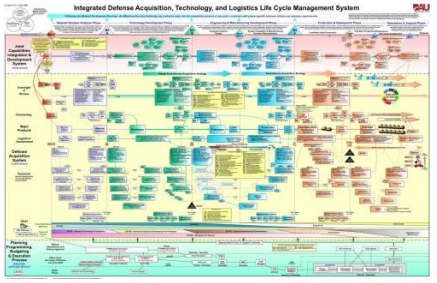


How to bring business and technical elements together in an ecosystem?

** http://www.acqnotes.com/acqnote/careerfields/modular-open-systems-approach

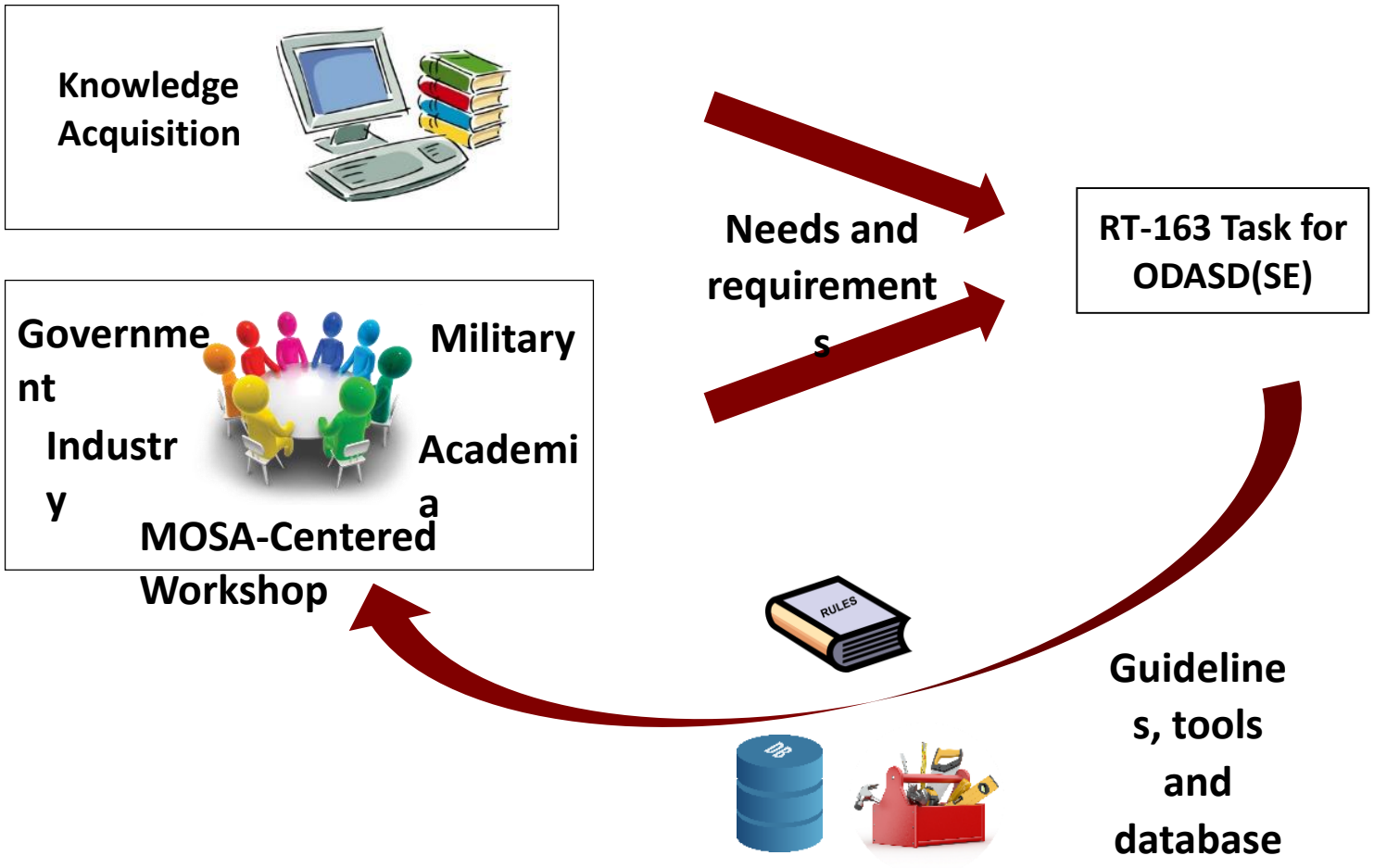
Research Needed

- Investigate development of systems to **exploit modularity** to enhance defense acquisitions and military capabilities.
- Explore **concept of an ecosystem** that facilitates adoption of modular solutions to achieve benefits (business + technical ends)
- Investigate how to **encourage modularity** to gain its benefits – conducive modular patterns, decompositions, methods, factors, catalysts etc.
- Provide **guidance and insights** to aids program managers in decision-making on modularization and achieving the intended benefits
- Work under RT-163 currently ongoing





RT-163 Research Approach



Modularity – An Intuitive Perspective

- **Definition:** *A general set of principles that help with managing complexity through breaking up a complex system into discrete pieces, which can then communicate with one another through standardized interfaces* [Langlois, 2002]
- **Types** of modularity [Baldwin 2006]
  - Modularity in Design
    - Product divided into modules independently with minimal interactions
  - Modularity in Production
    - Mass production driven that promotes flexibility and parallelism
    - Efficient innovations in production phases (e.g. vehicle production)
  - Modularity in Operations
    - Shared components for increased operational flexibility
    - Interchangeable components for different missions

Modularity

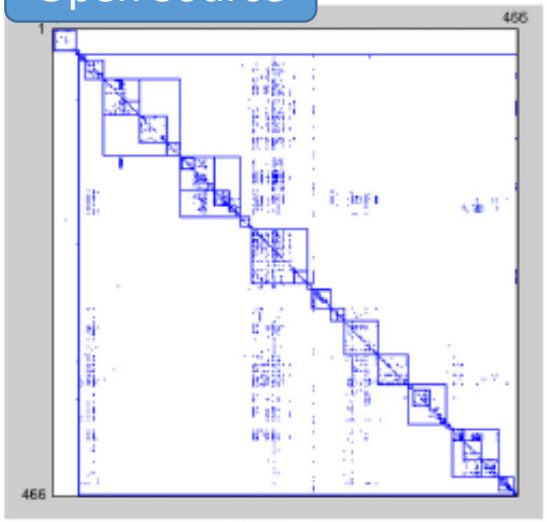
- **Benefits of Modularity**
  - Managing complex systems by breaking down into smaller pieces
  - Facilitates rapid evolution through changes at module level
  - Enables parallelisms (operations, development)
  - Accommodate future uncertainties

SECURITY ?

- **Potential Drawbacks**
  - Duplicated subsystems at local levels
  - Limited innovation due to compartmentalization
  - Many choices of measure for modularity
  - Unseen impacts on complex system due to changes at module level

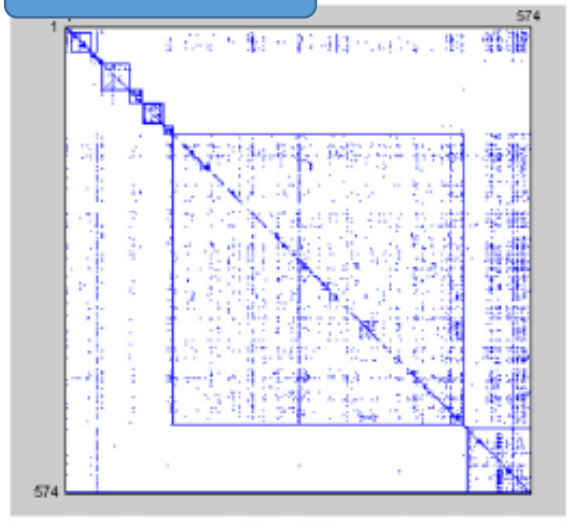
Case: Modularity and Organizational Structure

Open Source



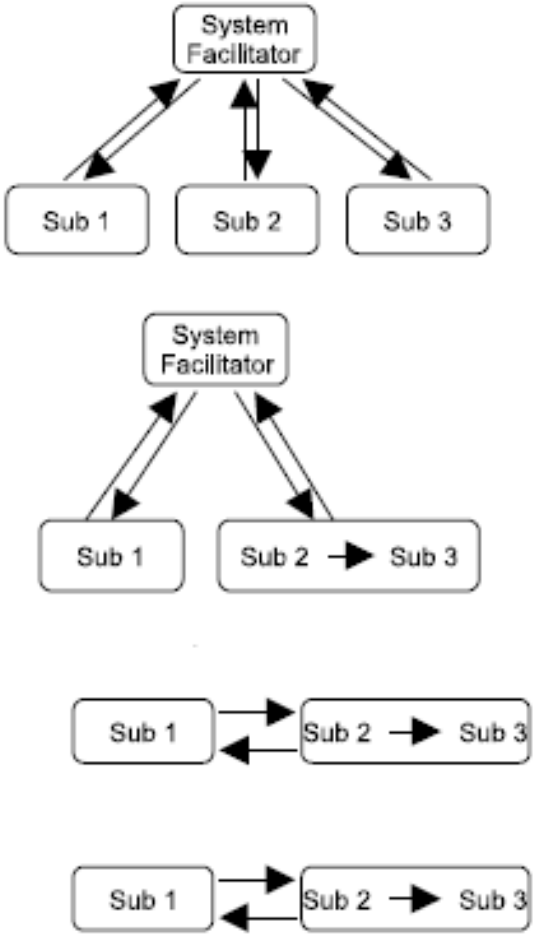
Size = 466
Dependency Density = 1.3672%
Propagation Cost = 7.7428%

Commercial



Size = 574
Dependency Density = 1.8903%
Propagation Cost = 47.1394%

- Prior work by McCormack et al on mirroring effect/Conway's Law (propagation costs, IP modularity)
- Honda work on information passing → impacts end design



*From McCormak et al., "Exploring the Duality between Product and Organizational Architectures: a Test of the Mirroring Hypothesis", 2012

Case: Modularity and Supply Chain

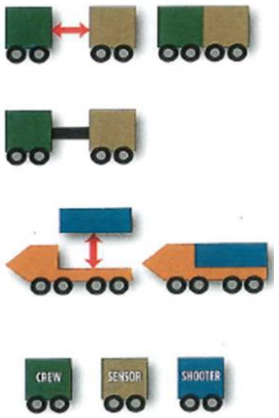
- Daimler designs closely knit and carefully designed integrated component

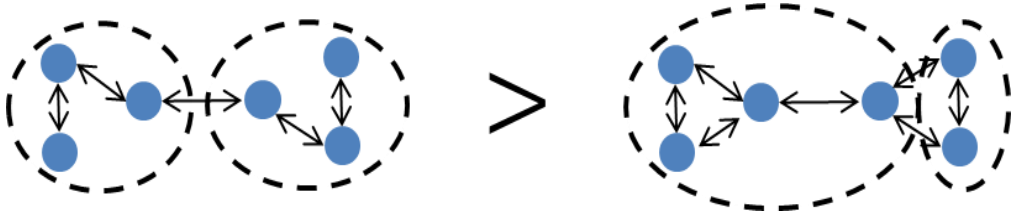
- Chrysler design focus on modular designs
  - Autonomous suppliers design, supply and innovate based on standards

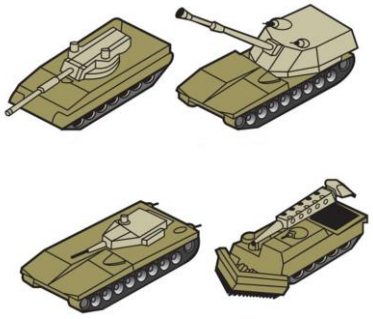
- Merger of Daimler-Chrysler was overall deemed detrimental
  - Mixing JIT supply chain with Daimler supply chain proved challenging and costly

Case: Modularity Measures

- How to choose a measure (metric) for modularity? How is one system more modular than another? Openness?
- TARDEC choice of vertical vs. horizontal modularity metric observed to drive effectiveness of approach
- Openness – Navy Open Architecture Assessment Tool (OAAT) to measure level of openness







*Dasch,J., Gorisch, D., "Survey of Modular Military Vehicles: Benefits and Burdens", Defense Acquisition Research Journal, January 2016, Vol 24 No1.:2-27

MOSA Workshop

- MOSA workshop held in Washington DC [Government, Academia, Industry attendees]
  - 31 attendees [13 Gov, 6 Industry, 12 Academia]
- Purpose to focus on exploring key question/have in depth discussions on:
  - **Defining, quantifying** and **assessing** modularity
  - **Generating candidate strategies**, cognizant of current barriers
  - Synthesizing key list of **stakeholder needs**/concerns in MOSA ecosystem
  - **Mapping beneficial elements** of modularization strategies to appropriate acquisition processes
  - Generate **repository** of useful case studies/anecdotes







Some MOSA Workshop Outcomes

- Modularity should not be seen as an "output" but **as means to achieve end benefits**
- Need **"feedback measures"** to inform choices
- Care for multiple stakeholders and their needs
- To show "compliance", **evaluate** the degree to which programs show that their approaches are good **in terms of the of the estimated benefits**
- **"good modularity" is same as "good architecting**" – can be hard for complex systems development
- Encourage greater intentionality in adequate amount and style of modularity

Ecosystem Needs & Future Work

- **Establish the long-term business strategy, drivers and objectives for each stakeholder,** and their time horizons for MOSA-generated benefits
  - Keep into account competing interests
- Provide **tools to categorize and assess consequences** of modularization choices, under uncertainty
  - Holistic level tools (e.g. **MBSE**) to capture main viewpoints
  - Measure the consequences of available data, for example on the 5 benefits
- **Provide feedback mechanisms**, to help stakeholders understand the consequence of their actions and that of others (e.g. decision support framework)
- **Develop a database of case studies,** based on best practices, tacit knowledge, anecdotes, that is well mapped to the acquisition process
- **Map case studies to appropriate parts of the overall acquisition lifecycle, in order to develop "principles" and guidelines with case studies tagged**

Focus of current SERC RT-185 Effort

Thank you

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-0004-0063. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

SYSTEMS ENGINEERING RESEARCH CENTER

CISA Center for Integrated Systems in Aerospace

Investigating Approaches to Achieve Modularity Benefits in the Acquisition Ecosystem

20th Annual NDIA Systems Engineering Conference

October 24-27 Waterford, Springfield, VA.

Dr. Daniel DeLaurentis
Dr. Navindran Davendralingam
Dr. Cesare Guariniello
Dr. Mitchell Kerman
Dr. Lu Xiao

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-0004-0063. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Motivation

- Current DoD acquisition challenges
  - to affordably address emerging threats
  - component obsolescence
  - loss of critical suppliers, and planned technology upgrade for tightly coupled, highly integrated systems
- DoD acquisitions strategy : Better Buying Power 3.0 (BBP 3.0)
  - Implement best practices to improve productivity, affordability, capabilities, reduce unproductive states across DoD acquisitions
  - Includes encouraged use of modularization strategies to achieve desired end benefits…via a Modular Open Systems Approach (MOSA)
  - CHALLENGE: program managers need strategies and tools to be successful in a MOSA ecosystem

MOSA Initiative

- ODASD/SE Modular OPEN Systems Approach (MOSA)
  - Open System Architecture (OSA)
    - Business side of acquisition process
      - data rights, IP, legal matters
    - Most MOSA work currently under auspices of OSA efforts
      - need to extend to technical as well
    - *Requirement under law to include MOSA in acquisition language → current guidance on law and policy vs technical implications*
  - Modularity (in DoD)
    - Viewed as technical approach in defense acquisitions
    - Complex system decomposition: physical and functional architecture
    - Largely separated from OSA tenets that are more business oriented
    - Modular open systems leverages business driven benefits of adopting Open Architecture standards for development

MOSA Goals

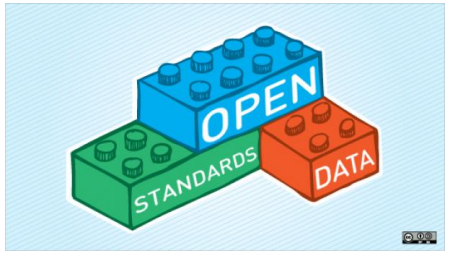
- **Cost savings/cost avoidance**
  - Savings via reduced burden on acquisition processes
- **Allow technology refresh**
  - Rapid updates of modules individually easier than addressing total monolithic complex system
- **Interoperability of systems/components**
  - Open standards use ensures compliance in interoperability
- **Increase competition between suppliers**
  - Leverage open standards and modularity to engage more business units for development (e.g. SBIRs etc)
- **Incorporate innovation**
  - Innovation can be more readily focused at localized modular level

Need to <u>connect desired program outcome</u> to a MOSA goal

MOSA Guidelines

- **Establish an enabling environment**
  - PM to generate business practices, technology development, test and evaluate, etc. needed for development of open systems
- **Employ modular design**
  - Four main characteristics: cohesive, encapsulated, self-contained, highly binned
- **Designate Key Interfaces**
  - Module interfaces defined to enable designers and system configuration managers
- **Use Open Standards**
  - Utilization of community accepted standards that are well defined/matured
- **Certify Conformance**
  - Use rigorous assessment mechanisms, interface control management and proactive conformance testing.





How to bring business and technical elements together in an ecosystem?

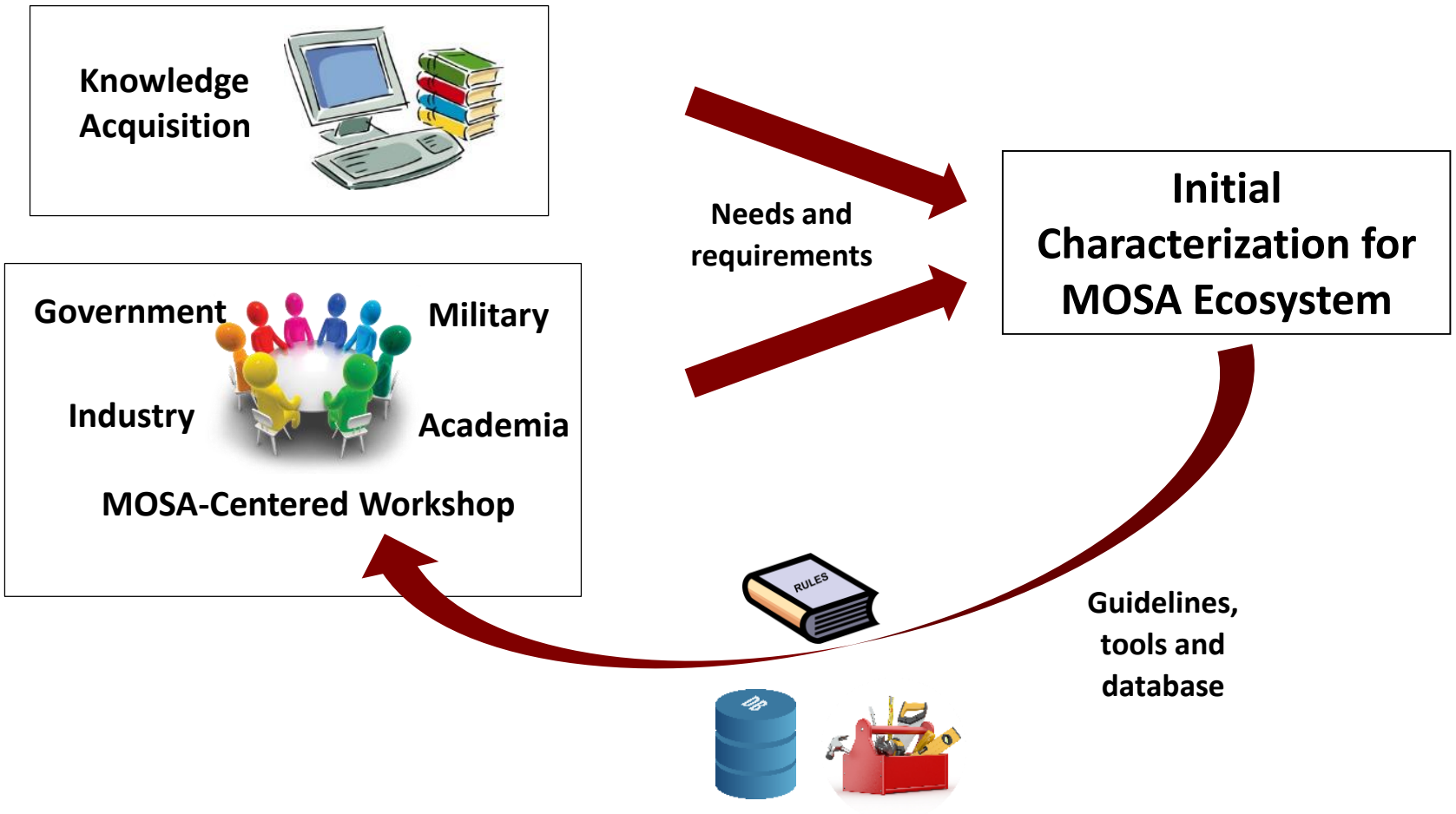
http://www.acqnotes.com/acqnote/careerfields/modular-open-systems-approach

Research Needed

MOSA Research Tasks with SERC have commenced: FY17 RT-163, FY 18 RT-185

- Investigate development of systems to **exploit modularity** to enhance defense acquisitions and military capabilities.
- Explore **concept of an ecosystem** that facilitates adoption of modular solutions to achieve benefits (business + technical ends)
- Investigate how to **encourage modularity** to gain its benefits – conducive modular patterns, decompositions, methods, factors, catalysts etc.
- Provide **guidance and insights** to:
  - aid program managers in decision-making on modularization and achieving the intended benefits
  - Connect desired program outcomes to a MOSA goal

RT-163 Research Approach



Modularity – An Intuitive Perspective

- **Definition:** *A general set of principles that help with managing complexity through breaking up a complex system into discrete pieces, which can then communicate with one another through standardized interfaces* [Langlois, 2002]

- **Types** of modularity [Baldwin 2006]
  - —*Modularity in Design*
    - Product divided into modules independently with minimal interactions
  - —*Modularity in Production*
    - Mass production driven that promotes flexibility and parallelism
    - Efficient innovations in production phases (e.g. vehicle production)
  - —*Modularity in Operations*
    - Shared components for increased operational flexibility
    - Interchangeable components for different missions

Benefits and Drawbacks

- **Benefits of Modularity**
  - Managing complex systems by breaking down into smaller pieces
  - Facilitates rapid evolution through changes at module level
  - Enables parallelisms (e.g. operations, development)
  - Accommodate future uncertainties

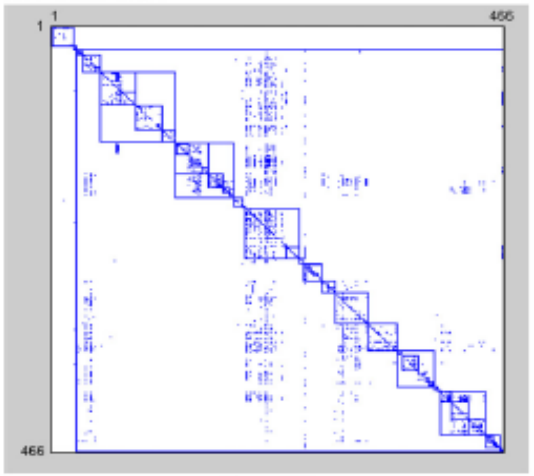
SECURITY ?

- **Potential Drawbacks**
  - Duplicated subsystems at local levels
  - Limited innovation due to compartmentalization
  - Many choices of measure for modularity
  - Unseen impacts on complex system due to changes at module level

Case: Modularity and Organizational Structure

Open Source

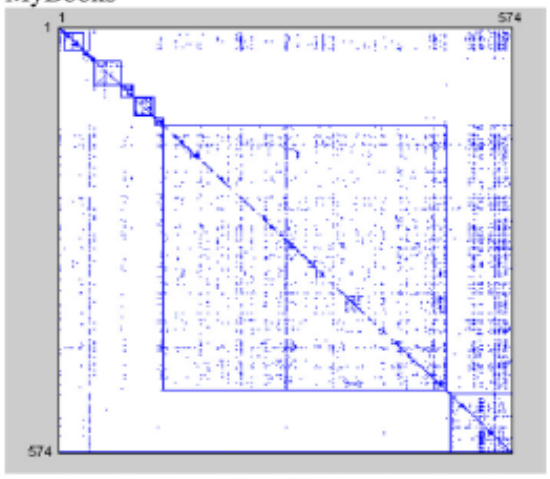
Gnucash 1.8.4



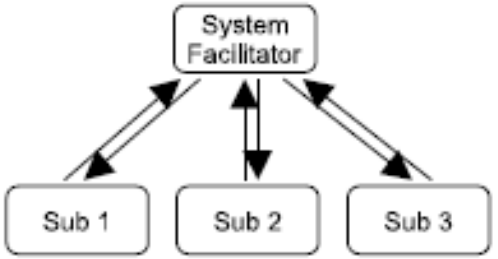
Size = 466
Dependency Density = 1.3672%
Propagation Cost = 7.7428%

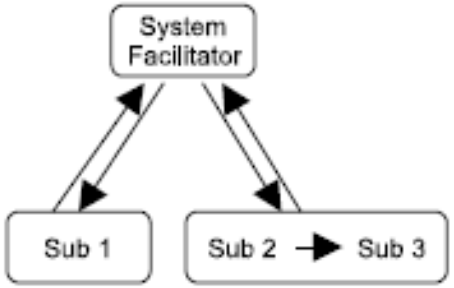
Commercial

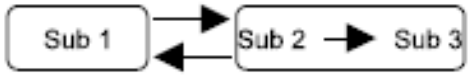
MyBooks

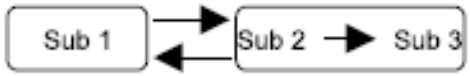


Size = 574
Dependency Density = 1.8903%
Propagation Cost = 47.1394%









- Prior work by McCormack et al on mirroring effect/Conway's Law (propagation costs, IP modularity)
- Honda work on information passing → impacts end design

*From McCormak et al., "Exploring the Duality between Product and Organizational Architectures: a Test of the Mirroring Hypothesis", 2012

Case: Modularity and Supply Chain

- Daimler designs closely knit and carefully designed integrated component



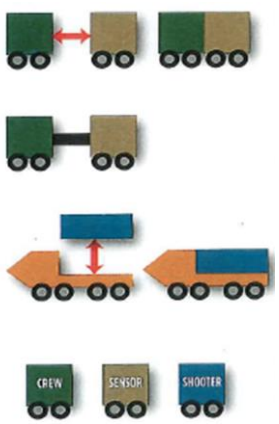
- Chrysler design focus on modular designs
  - Autonomous suppliers design, supply and innovate based on standards



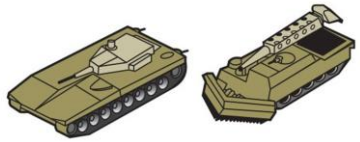
- Merger of Daimler-Chrysler was overall deemed detrimental
  - Mixing JIT supply chain with Daimler supply chain proved challenging and costly

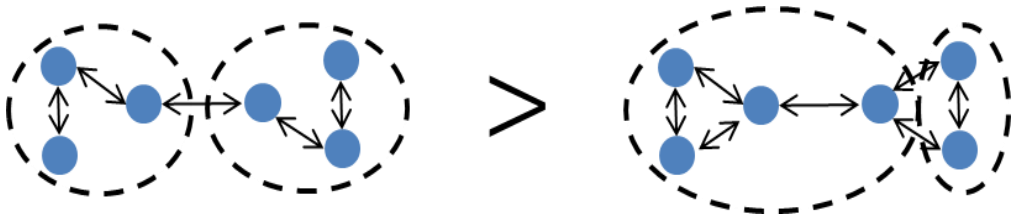
Case: Modularity Measures

- Choice of measure (metric) for modularity? How is one system more modular/open than another?
- TARDEC choice of vertical vs. horizontal modularity metric observed to drive effectiveness of approach
- Openness – Navy Open Architecture Assessment Tool (OAAT) to measure level of openness
- Need to focus on metrics that inform attainment of MOSA benefits for program goals









*Dasch,J., Gorisch, D., "Survey of Modular Military Vehicles: Benefits and Burdens", Defense Acquisition Research Journal, January 2016, Vol 24 No1.:2-27

MOSA Workshop

- MOSA workshop held in Washington DC [Government, Academia, Industry attendees] 5th October 2016
  - 31 attendees [13 Gov, 6 Industry, 12 Academia]



- Purpose to focus on exploring key question/have in depth discussions on:
  - **Defining, quantifying** and **assessing** modularity
  - **Generating candidate strategies**, cognizant of current barriers
  - Synthesizing key list of **stakeholder needs**/concerns in MOSA ecosystem
  - **Mapping beneficial elements** of modularization strategies to appropriate acquisition processes
  - Generate **repository** of useful case studies/anecdotes





Some MOSA Workshop Outcomes

- Modularity should not be seen as an "output" but **as means to achieve end benefits**
- Need **"feedback measures"** to inform choices
- Care for multiple stakeholders and their needs
- To show "compliance", **evaluate** the degree to which programs show that their approaches are good **in terms of the of the estimated benefits**
- **"good modularity" is same as "good architecting"** – can be hard for complex systems development
- Encourage greater intentionality in adequate amount and style of modularity

RT-163 produced an Initial MOSA Guidance Document for PMs

- Guidance Categories
  - *What to Measure and Why*
  - *Useful Strategies Exist at Different Acquisition Lifecycle Phases*
  - *Caution! Emergent phenomenon in benefits and risks*
  - *Ouch! Technical and programmatic pain points*

- Preliminary 'living' document informed by prior research effort
  - Current refinement efforts:
    - Further exchanges with key collaborators and contributors from government, industry, academia
    - Directed knowledge acquisition and canvassing of case studies based on prior efforts

Ecosystem Needs & Future Work

- **Establish the long-term business strategy, drivers and objectives for each stakeholder,** and their time horizons for MOSA-generated benefits
  - Keep into account competing interests
- Provide **tools to categorize and assess consequences** of modularization choices, under uncertainty
  - Holistic level tools (e.g. **MBSE**) to capture main viewpoints
  - Measure t[illegible]ts

Focus of current SERC RT-185 Effort

- **Provide feedback mechanisms**, to help stakeholders understand the consequence of their actions and that of others (e.g. decision support framework)
- **Develop a database of case studies,** based on best practices, tacit knowledge, anecdotes, that is well mapped to the acquisition process
- **Map case studies to appropriate parts of the overall acquisition lifecycle, in**

Concept Decision-Support Framework







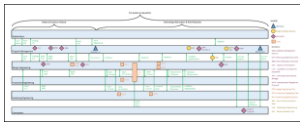
SME Knowledge Base

Literature/ Case Study Knowledge Base

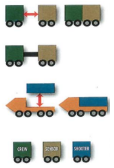


Decision Support Framework

Impact on Acquisition Processes







Program Manager Queries

PM Decision Feedback

Acquisition Process relevant outputs

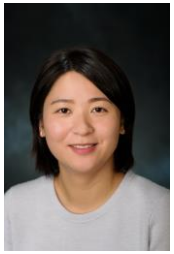
RT-185 Research Team



Dr. Gary Witus
Wayne State University



Dr. Daniel DeLaurentis
Purdue University



Dr. Lu Xiao
Stevens Institute of Technology



Dr. Jean (Charles) Domercant
Georgia Tech Research Institute



Dr. Cesare Guariniello
Purdue University



Dr. Navindran Davendralingam
Purdue University

Thank you

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-0004-0063. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Contact: Dr. Daniel DeLaurentis
Director
Center for Integrated Systems in Aerospace (CISA)
ddelaure@purdue.edu

Trusted Microelectronics Joint Working Group

Dr. Brian S. Cohen, Institute for Defense Analyses (IDA)

Dr. Daniel Radack, IDA

Ms. Catherine Ortiz, Defined Business Solutions

Mr. David Chesebrough, NDIA

October 26, 2017



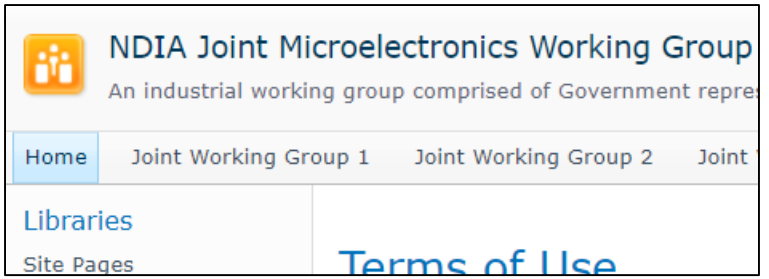
NVIDIA Tesla V100 data center GPU, courtesy nvidianews.nvidia.com

Trusted Microelectronics Background

- **First Workshop Held on June 28, 2013**
- **Ten Workshops have since been held**
  - Hundreds have participated from government, industry and academia
  - A great deal of focus on **Trust** but also on **Access, Industrial Base, National Competitiveness, Cost** and **Collaboration/Cooperation**
  - Participant interest in ongoing activity led to:
    - A call for a working group to be formed during the February 2016 workshop the group was subsequently formed from volunteers (many more than expected)

Trusted Microelectronics Joint Working Group

- Obtaining Trusted and assured microelectronics is critical to maintaining the U.S. military's technological advantage
  - As consolidation and the migration offshore of integrated circuit design and manufacturing capabilities continue, the defense industry faces increasing challenges to obtain those critical components from Trusted Suppliers



TM JWG Members Collaborated on private Sharepoint Site

- An NDIA Trusted Microelectronics Joint Working Group (TM JWG) was formed to collaboratively develop mitigation strategies for the decreasing access to assured microelectronics for defense and national security systems
  - Over the 14-month study period, the NDIA TM JWG membership reached 80 participants from nine government offices, 28 separate defense companies, and nine non-profit and FFRDC organizations

TM JWG Organization

- The TM JWG formed four teams to address critical challenges impacting defense microelectronics supply
  - Future Needs & System Impact of Microelectronics Technologies: Team Leader: Charley Adams, Northrop Grumman
  - Trustable Access to Leading Edge Technology: Team Leader: Ezra Hall, GLOBALFOUNDRIES
  - Trustable Microelectronics Standard Products: Team Leader: Ken Lebo, Jacobs Engineering Group
  - New Methods to Instill Trust in Commercial Semiconductor Fabrication: Team Leader: Pat Hays, Boeing

TM JWG Members

As of February 15th, 2017

Charles Adams Northrop Grumman	**Dean Brenner** Honeywell International Inc.	**Gerry Etzold** Etzold Technology Consulting	**Adam Hauch** DSS	**Scott Jordan** Jazz Semiconductor Trusted Foundry, Inc.	**Grant Meyer** SRI International	**Paul Quintana** Microsemi	**Nicolas Sramek** The Aerospace Corporation
John Adams The Aerospace Corporation	**Edward Chatters** Contract Support to ODASD(SE)	**Saverio Fazzari** Booz Allen Hamilton	**Pat Hays** Boeing	**Taffy Kingscott** IBM	**Eric Miller** Boeing	**Dan Radack** Institute for Defense Analyses	**Paul Syers** Potomac Institute for Policy Studies
Scott Anderson Lockheed Martin	**James Chew** Cadence	**Brad Ferguson** Cypress Semiconductor	**Kenneth Heffner** Honeywell International Inc.	**Elizabeth Klein-Lebbink** The Aerospace Corporation	**John Monk** Northrop Grumman	**Kirk Reynolds** Rockwell Collins	**Major Manny Trejo** DoD
Brett Attaway AIM Photonics Institute	**Rob Ciccariello** Contractor to MIBP	**Michael Fritze** Potomac Institute for Policy Studies	**Kelly Hennig** Northrop Grumman	**Ken Lebo** Jacobs	**Jeremy Muldavin** DASD(SE)	**Christine Rink** The Aerospace Corporation	**Roger Van Art** Vantagepoint Advisors
Anita Balachandra TechVision21	**Brian Cohen** Institute for Defense Analyses	**Aman Gahoonia** Defense Microelectronics Activity	**Craig Herndon** NSWC Crane	**Tim Lee** Boeing	**Mike Newman** Aeroflex (Cobham)	**Tyler Schmidt** Intel Federal	**John Verwey** Department of Commerce
Todd Bauer Sandia National Laboratories	**Mark Crawford** Department of Commerce	**Aaron Gilbert** DoD	**Dan Holladay** University Of Central Florida	**Neal Levine** Defense Microelectronics Activity	**Ken O'Neill** Microsemi	**Neil Schumacher** IBM GBS	**David Weaver** SRI International
Gerry Borsuk Naval Research Laboratory	**Greg Creech** GLC Consulting, LLC	**Jim Gobes** Intrinsix Corp	**Mike Holmes** Sandia National Laboratories	**Daniel Marrujo** Defense Microelectronics Activity	**Greg Orne** Honeywell International Inc.	**Tim Scott** Novati Technologies	**John Weaver** Techtonic Labs
Brad Botwin Department of Commerce	**Eric Dauler** MIT Lincoln Laboratory	**David Gottfried** Alfred University	**Robert Irie** OSD Manufacturing and Industrial Base Policy	**Erika Maynard** Department of Commerce	**Catherine Ortiz** Defined Business Solutions	**Ray Shanahan** DASD(SE)	**Ken Wetzel** SMI Inc.
Bryan Brady Avnet	**Dave Davis** USAF SMC	**Ezra Hall** GLOBALFOUNDRIES	**Michael James** IBM GBS	**Steve McNeil** Xilinx	**Doug Palmer** Booz Allen Hamilton	**Vashisht Sharma** Institute for Defense Analyses	**Pete Wheatley** DoD
Gordy Braun Honeywell International Inc.	**Antonio de la Serna** DRAPER	**John Hallman** MacAulay-Brown, Inc.	**Sean Johnson** DoD	**David Meshel** The Aerospace Corporation	**David Pentrack** Defense Microelectronics Activity	**Chris Sims** NSWC Crane	**Ed Yarbrough** Honeywell International Inc.

# of Organizations / # of Participants

Industry: 28/40 | **FFRDCs: 3/10** | **Academia/Non-Profits: 6/8** | **Government: 9/22** | **Total: 46/80**

TM JWG Members

As of February 15th, 2017

Government

DASD (SE)
Defense Microelectronics Activity
DSS
Department of Commerce
Department of Defense (NSA)
Naval Research Laboratory
NSWC Crane
OSD Manufacturing & Industrial Base Policy
USAF SMC

Industry

Aeroflex (Cobham)	DRAPER	Intrinsix Corp	Novati Technologies
Avnet	Etzold Technology Consulting	Jacobs	Rockwell Collins
Boeing	GLC Consulting, LLC	Jazz Semiconductor Trusted Foundry, Inc.	SMI Inc.
Booz Allen Hamilton	GLOBALFOUNDRIES	Lockheed Martin Corporation	Techtonic Labs
Cadence	Honeywell International Inc.	MacAulay-Brown, Inc.	TechVision21
Cypress Semiconductor	IBM/IBM GBS	Microsemi	Vantagepoint Advisors
Defined Business Solutions	Intel Federal	Northrop Grumman	Xilinx

	#Org.	#Participants
Government	9	22
Companies	28	40
Academia/Non-Profits	6	8
FFDRCs	3	10
Total:	**46**	**80**

FFRDCs

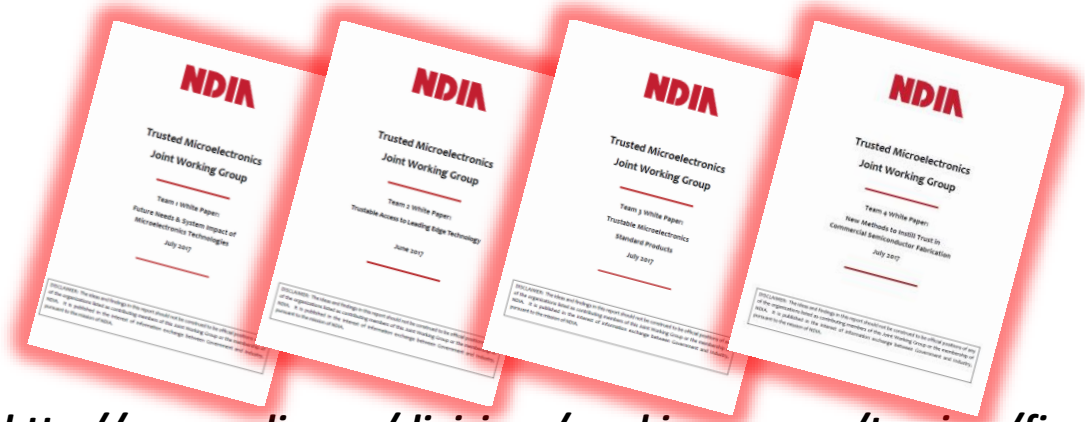
The Aerospace Corporation
Institute for Defense Analyses
Sandia National Laboratories

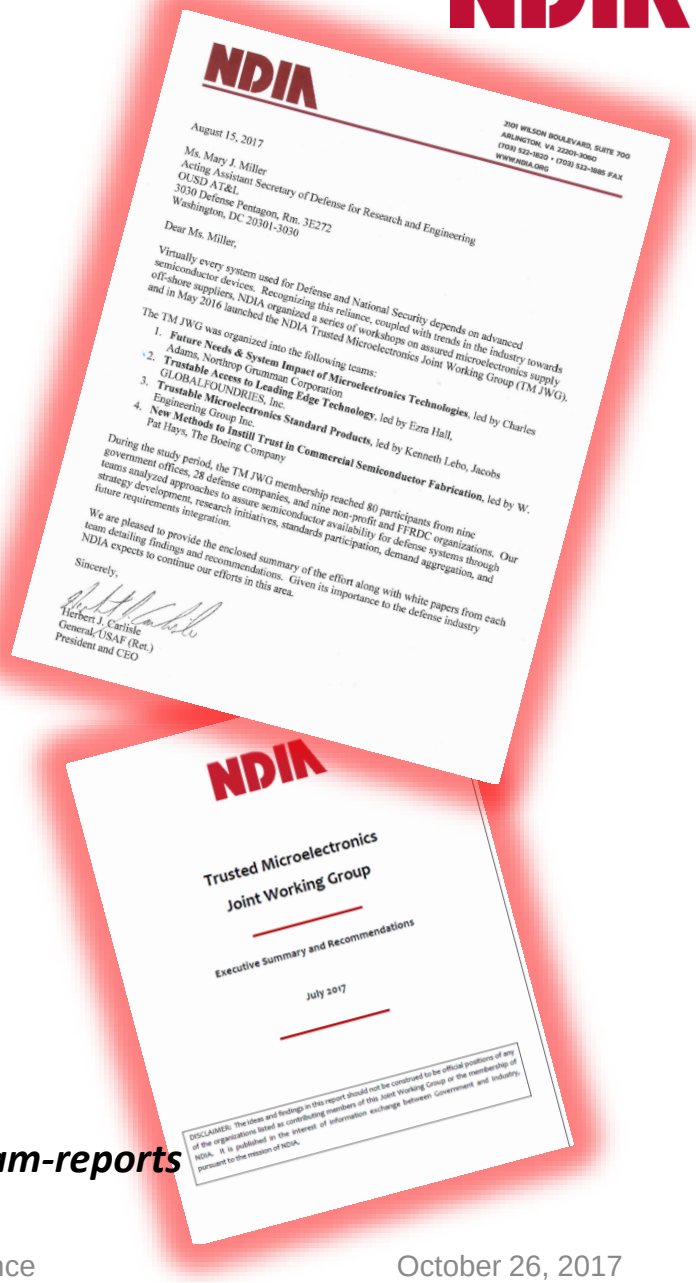
Academia/Non-Profits

Alfred University	Ohio State University
AIM Photonics Institute	SRI International
MIT Lincoln Laboratory	University of Central Florida
Potomac Institute for Policy Studies	

The Results from the TM WG

- **TMW WG Findings Transmitted to ASD(R&E) on August 29, 2017**
- **Findings Publicly Posted on the NDIA site**
- **Includes Reports from All 4 Teams**





http://www.ndia.org/divisions/working-groups/tmejwg/final-team-reports

Key Recommendations

- Create a U.S. National Semiconductor Strategy
- Adapt DoD Acquisition Practices to Align with Commercial Market
- Increase DoD Market Influence
- Adopt New Trust and Assurance Models
- Launch R&D to Achieve Trust and Security in Un-trusted Fabs

Key Recommendations

Create a U.S. National Semiconductor Strategy

- Viewed by the TM JWG as single most impactful action to assure access to technologies
- Recommends a Government-Industry-Academia consortia or coalition to develop plan, including and beyond DoD's requirements
- Would prioritize essential technologies for loss contingency protections and create a technology roadmap to identify investments

Key Recommendations

Adapt DoD Acquisition Practices to Align with Commercial Market

- Recommends defense programs be provided new methods to purchase technology on commercial terms after trustworthiness evaluation
- Develop approaches to adopt commercial solutions and intellectual property with well-defined risk mitigations
- Develop a process to plan sustainment needs during initial product purchases

Key Recommendations

Increase DoD Market Influence

- Increase market influence by exchanging research investment for access to commercial products
- Aggregate demand across DoD programs, other USG offices, and non-USG industries that have similar component and system integrity concerns.

Key Recommendations

Adopt New Trust and Assurance Models

- Develop program-specific Trust Plans and Technical Implementation Guides to identify security measures for each step in the product flow from design through test
  - The Guides would factor technology-enabled mitigations and countermeasures into security requirements
  - The Plans could expand today's Trust offerings by defining the boundaries for assurance spectrums or "tiers of trust" levels, and would cover component categories beyond ASICs.

Key Recommendations

Launch R&D to Achieve Trust and Security in Un-trusted Fabs

- Launch near-term research and development to address the security concerns of existing commercial technology capabilities
  - Separate from, but coordinated with, the national semiconductor strategic plan
- Establish a government focus to track future technology trends and impacts is recommended to continuously identify technology renewal opportunities and capabilities gaps.

Outcome and Impact

- **The NDIA Trusted Microelectronics Joint Working Group demonstrated the value of government-industry collaboration when addressing critical issues facing the Department of Defense and the Defense Industrial Base**
  - There was immense participation throughout government, industry and academia
- **This work coincided with accelerated concern over the issues**
  - DoD establishment of the JFAC and T&AM program
  - Studies – PCAST, DSB Cyber Supply Chain Task Force . . .
  - Presidential EO on Industrial Base (Includes semiconductors)
- **Given the importance of this work to National Security Community NDIA plans to leverage the Joint Working Group into a standing NDIA Division so that it may continue under an officially recognized charter**
  - This division is tentatively being called the NDIA Electronics Division
- **Further information on the Workshops and TM JWG reports can be found at www.ndia.org/divisions/working-groups/tmejwg**

Dr. Brian Cohen

Institute for Defense Analyses

bcohen@ida.org

703-845-6684