NDIA
AT THE HEART OF THE MISSION

2021 VIRTUAL **SYSTEMS & MISSION ENGINEERING** CONFERENCE

Systems & Mission Engineering Transformation and Modernization

December 6 – 8 | NDIA.org/vSME21

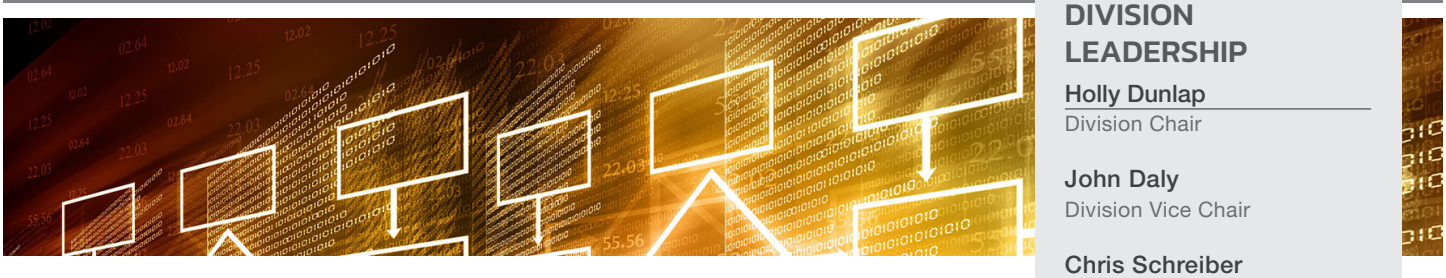
TABLE OF CONTENTS

WHO WE ARE

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit **NDIA.org**

GET INVOLVED

Learn more about NDIA's Divisions and how to join one at **NDIA.org/Divisions**



DIVISION LEADERSHIP

Holly Dunlap
Division Chair

John Daly
Division Vice Chair

Chris Schreiber
Division Vice Chair

Dr. Patricia Griffin
Conference Chair

SYSTEMS ENGINEERING DIVISION

WHO WE ARE

The Systems Engineering Division advocates for the widespread use of systems engineering in the Defense Department acquisition process to achieve affordable, supportable, and interoperable weapon systems that meet the needs of military users. In addition to supporting the open exchange of ideas and concepts between government and industry, the Division works for a new understanding of a streamlined systems engineering process.

CONFERENCE PURPOSE

The purpose of this conference is to focus on Systems and Mission Engineering Transformation and Modernization to improve defense program acquisition and system performance. It addresses emerging concepts such as digital engineering, modeling, product line engineering, iterative development methods, new risk models to ensure system survivability and cyber resiliency, and shifting test earlier in the system development lifecycle.

This year, the NDIA Systems Engineering Division is partnering with our Test & Evaluation Division and Integrated Program Management Division, and is supported by the Office of the Under Secretary of Defense for Research & Engineering, the IEEE Aerospace and Electronic Systems Society, the IEEE Systems Council, and the International Council on Systems Engineering.

WELCOME TO 2021 VIRTUAL SYSTEMS & MISSION ENGINEERING CONFERENCE

On behalf of the National Defense Industrial Association's Systems Engineering Division, we would like to extend a very warm welcome to the 24th Annual Systems & Mission Engineering Conference. The defense industry has been working together on systems engineering topics for over 20 years. We continue to have extensive opportunities to modernize our approaches, processes, tools, and techniques to provide the most sophisticated and technologically advanced capabilities to our US and Allied Nation warfighters.

Our defense community includes industry, government, FFRDCs, and academia, all of whom collaboratively challenge the status quo. We work to address barriers and seek opportunities to transform Systems Engineering, and in doing so improve efficiencies, affordability, quality, safety, security, as well as ensure overall system mission success.

NDIA offers a unique opportunity for everyone to have a voice regardless of years of experience, and to propose new ideas and innovative ideas to make us better. This forum provides a great opportunity to hear from senior executive leaders as well as subject matter experts in diverse areas of systems engineering.

We are very pleased this year to partner with the NDIA Test & Evaluation Division and Integrated Program Management Division to complement our Systems Engineering Division. We appreciated everyone's flexibility and willingness to work with us as we adapted to uncertain times and transitioned from a face-to-face to virtual environment. We have impressive keynotes speakers, with over 120 live presentations, and 30 pre-recorded on-demand presentations. These presentations will be recorded and available for 30 days after the event. This provides an incredible opportunity to view other presentations or review presentations later for where you may have focused interest.

We encourage each of you to be actively present, ask questions, learn something new, and offer insights and mentoring to those newer to our community. As you participate in the conference, please consider becoming an active NDIA Systems Engineering Committee member throughout the year by joining one of our 13 committees. Please reach out to the track chairs for more information. And if there is anything that the conference committee, the undersigned, or the outstanding NDIA staff can do to assist you, please let us know.

Holly Dunlap
Raytheon Missiles & Defense
NDIA Systems Engineering Division Chair

Pat Griffin
NDIA Systems Engineering Division
Transformation & Communication Chair, Clear-Com

EVENT INFORMATION

SURVEY AND PARTICIPANT LIST

You will receive via email a survey and list of participants (name and organization) after the conference. Please complete the survey to make our event even more successful in the future.

EVENT CONTACT

Meredith Mangas
Associate
Director, Meeting
(703) 247-9467
mmangas@NDIA.org

Jae Yu
Director, Divisions
(703) 247-2564
jyu@NDIA.org

Allison Carpenter
Director,
Exhibits & Sponsorships
(703) 247-2573
ahcarpenter@NDIA.org

SPEAKER GIFTS

In lieu of speaker gifts, a donation is being made to the Fisher House Foundation.

HARASSMENT STATEMENT

NDIA is committed to providing a professional environment free from physical, psychological and verbal harassment. NDIA will not tolerate harassment of any kind, including but not limited to harassment based on ethnicity, religion, disability, physical appearance, gender, or sexual orientation. This policy applies to all participants and attendees at NDIA conferences, meetings and events. Harassment includes offensive gestures and verbal comments, deliberate intimidation, stalking, following, inappropriate photography and recording, sustained disruption of talks or other events, inappropriate physical contact, and unwelcome attention. Participants requested to cease harassing behavior are expected to comply immediately, and failure will serve as grounds for revoking access to the NDIA event.

EVENT CODE OF CONDUCT

NDIA's Event Code of Conduct applies to all National Defense Industrial Association (NDIA), National Training & Simulation Association (NTSA), and Women In Defense (WID) meeting-related events, whether in person at public or private facilities, online, or during virtual events. NDIA, NTSA, and WID are committed to providing a productive and welcoming environment for all participants. All participants are expected to abide by this code as well as NDIA's ethical principles and practices. Visit NDIA.org/CodeOfConduct to review the full policy.

ANTITRUST STATEMENT

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

JOIN THE CONVERSATION

@NDIAToday | @NDIAMembership | NDIA.org/LinkedIn | @NDIAToday | @NDIAToday

TRACK INFORMATION

Agile

John Daly
Booz Allen Hamilton

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

Bob Scheurer
The Boeing Company

Ed Moshinsky
OUS (R&E) SE

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

Digital Engineering

Chris Schreiber
Lockheed Martin Space Systems Company

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 cohesiveness across engineering activities and 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. Moreover, risk reduction in the end item can be achieved.

Engineered Resilient Systems

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

Dr. Robert Ragygan
Defense Acquisition University

The Education & Training track for 2020 is an excellent collection of presentations from government, industry, and academia. The presentations describe a wide range of systems engineering (SE) workforce development activities covering the core of SE, agile approaches, an MBSE learning environment, modular online open education, and the future of SE.

Environment, Safety, & Occupational Health

Sherman Forbes
U.S. Air Force

Diane Dray
Booz Allen Hamilton

Engineering design considerations included under the DoD acronym "ESOH," as defined in MIL-STD-882E, the DoD Standard Practice for System Safety. Mr. David Asiello, the Acquisition ESOH lead in the Office of the Assistant Secretary of Defense for Sustainment will make the ESOH Track's keynote presentation. He will provide an overview of the Office of the Secretary of Defense's (OSD) reorganization that has separated Systems Engineering from Acquisition & Sustainment and has separated Safety & Health Management from Environmental Management. He will also emphasize the importance of incorporating ESOH risks and requirements management into Acquisition & Sustainment as a way to promote readiness and summarize the new Defense Acquisition System (DAS) Adaptive Acquisition Framework and its challenges to Systems Engineering and ESOH policy. The remainder of the ESOH track presentations will address specific acquisition ESOH issues, to include integrating ESOH risks and requirements management into Digital Engineering and the new Middle Tier Acquisition framework, specifically ESOH system design issues, hazardous materials management, and acquisition and sustainment programs' lessons learned.

Human Systems Integration

Dr. Matthew Risser
Pacific Science & Engineering

Randi Rohrer
The Boeing Company

The HSI track focuses on the human component in systems development to ensure systems are usable, useful, and support operational needs. The goal is to demonstrate value by aligning HSI processes with acquisition and systems engineering processes, in accordance with DoD HSI policy, standards, and guidance. Topics include HSI methods and best practices, standards and guidance, process innovation, metrics, applications, and approaches to program integration.

Mission Engineering

Dr. Judith Dahmann
The MITRE Corporation

Rick Poel
The Boeing Company

John Daly
Booz Allen Hamilton

Jennie Horne
Raytheon

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 approaches to ME.

Model-Based Systems Engineering

Dave Allsop
The Boeing Company

Jon Backhausr
Lockheed Martin Corporation

The Modeling & Simulation (M&S) Track highlights the use of models and simulations in the Systems Engineering process. Included are presentations on integrated environments, tools and technologies, and M&S applications in several Systems Engineering process phases. Topics focused specifically on Digital Engineering/Digital Thread/Model-Based Systems Engineering are also covered in this track.

Integrated Program Management

Linda Adams
Pratt & Whitney

Stewart Tague
Lockheed Martin Corporation

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.

Test & Evaluation

Jeff Bilco
The Boeing Company

The Test and Evaluations (T&E) track will focus on the increasing importance of developmental, operational live-fire T&E processes in both private and public sectors on defense.

Modular Open Systems Approach

Edward Moshinsky
OUSD, R&E

Modular Open Systems Approach (MOSA) is an integrated acquisition and design strategy, consisting of technical architectures, that adopts open standards and supports a modular, loosely coupled, and highly cohesive system structure. The MOSA Track will feature technical sessions highlighting new methods to develop assessment criteria, implementing digital engineering, and mission-level optimization.

System of Systems

Dr. Judith Dahmann
The MITRE Corporation

Rick Poel
Boeing

John Daly
Booz Allen Hamilton

Jennie Horne
Raytheon

The System of Systems (SoS) Track will feature papers highlighting the development of SoS engineering approaches, particularly SoS SE application areas, as well as SoS tools and modeling, including SoS SE applied to defense missions in mission engineering. See directly related track in Mission Engineering & Assurance, above.

System Security Engineering

Cory Ocker
Raytheon Technologies

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.
It includes the integration and risk management of all the security specialties to include: system security engineering, cybersecurity, anti-tamper, software assurance, hardware assurance, cyber supply chain risk management, and general program security throughout the system development lifecycle.
This holistic approach will ensure battlefield system survivability for system mission success.

AGENDA

MONDAY, DECEMBER 6

9:00 – 9:10 am

OPENING REMARKS

Gen Hawk Carlisle, USAF (Ret)
President & CEO, NDIA

Holly Dunlap
Raytheon Missiles & Defense
NDIA Systems Engineering Division Chair

9:10 – 10:00 am

SYSTEMS ENGINEERING TRANSFORMATION AT THE F-35 JOINT PROGRAM OFFICE

Lt Gen Eric Fick, USAF
Program Executive Officer, F-35 Lightning II Joint Program Office, Department of Defense

10:00 – 10:15 am

NETWORKING BREAK

10:15 – 10:55 am

KEYNOTE SPEAKER

Honorable Heidi Shyu
Under Secretary of Defense for Research and Engineering (OUSD(R&E))

11:00 – 11:40 am

TRANSFORMING ACQUISITION

David Cadman
Acting Deputy Assistant Secretary of Defense and Director, Acquisition Data and Analytics, OUSD A&S

11:45 am – 12:25 pm

HOW DIGITAL DESIGN IS DRIVING CHANGE IN DEFENSE

Wes Kremer
President, Raytheon Missiles & Defense

12:25 – 1:00 pm

NETWORKING LUNCH BREAK

1:00 – 1:40 pm

REVOLUTIONIZING OPERATIONAL TEST & EVALUATION BY 2025

Dr. Raymond O'Toole
Acting Director, Office of the Secretary of Defense, Operational Test and Evaluation (DOT&E)

1:45 – 2:05 pm **FERGUSON AND T&E AWARD CEREMONY**

CONCURRENT BREAKOUT SESSIONS

	1C1 – Digital Engineering	1C2 – Model-Based Systems Engineering (MBSE)	1C3 – Systems Security Engineering	1C4 – Test & Evaluation
Moderator	Chris Schreiber	David Allsop	Cory Ocker	Jeff Bilco
2:10 – 2:40 pm	23751 Model Readiness Levels: A Mathematical Construct for Validation and Trust **Dr. Darryl Ahner** STAT COE Director and Interim Dean for Research, Air Force Institute of Technology (AFIT)	Panel Discussion: Advancements and Challenges in MBSE in the Context of Digital Engineering **Ryan Noguchi** Aerospace Corp **Sean McGervey** JHU APL **Marc Blackburn** SERC **Brittany Friedland** Boeing Corp	23951 System Security Committee & Track Welcome **Cory Ocker** Raytheon Technologies, System Security Engineer	23764 Mission Engineering and Digital Engineering Enabling a Unified Evaluation Framework **Dr. Suzanne Beers** Department Manager, Defense System Engineering & OUSD(R&E) D,DTE&A DEF Technical Lead, Mitre
2:45 – 3:15 pm	23766 Integrating Digital Engineering and Modeling and Simulation to Support Technology Adoption in Department of Defense Systems **Philomena Zimmerman** Director, ET&E OUSD (R&E) **John Daly** Senior Engineer (Support), OUSD(R&E)		23823 Technology and Program Protection in the Department of Defense **Melinda Reed** Resilient Systems Director, STPE OUSD RE	23797 Digital Development and Test Transformation **Vu Hoang** Consulting Engineer System Architect, Northrop Grumman **Shailesh Sujanani** Manager Software Engineering, Northrop Grumman
3:20 – 3:50 pm	23772 Concept for Establishing Consistent System Digital Representation Across the System Lifecycle at All Required Fidelities **Dr. Charles Sanders** M&S SME, Army Modeling and Simulation Office	23720 An Argument for Why the Future of Requirements Lies in Model-Based Systems Engineering **Chris Swickline** Systems Architect, Northrop Grumman	23773 Agile Authorizations Approach to Risk Management Framework **Daniel Holtzman** USAF Director, Cyberspace Innovation, SAF/CN	23816 The Automation Framework: Using Data Volume, Variety, and Veracity to Accelerate DevSecOps **Kevin Visalli** Director of Software Products, Epsilon Systems Solutions, Inc.
3:55 – 4:15 pm	**NETWORKING BREAK**			

	1D1 – Digital Engineering	1D2 - Model-Based Systems Engineering	1D3 - Systems Security Engineering	1D4 – Test & Evaluation
Moderator	Chris Schreiber	David Allsop	Cory Ocker	Jeff Bilco
4:15 – 4:45 pm	23784 Ontologies for Engineering with Examples: A Pragmatic Perspective **Dr. Mark Blackburn** Senior Research Scientist, Stevens Institute of Technology	23721 A Vision for High Fidelity Multi-Disciplinary Simulation Built Surrogates Influencing the Design and Assessment of Military Systems **Dr. Scott Morton** Associate Director, DoD HPCMP, U.S. Army ERDC/ITL	23872 Army Cyberspace Survivability **Matthew Picerno** Chief Cyber Acquisition Officer, U.S. Army, ASA(ALT)	23839 Capabilities Based T&E / Capabilities Based Acquisition **Ken Senechal** Director for Naval Capabilities Based T&E
4:50 – 5:20 pm	23963 Acquisition and Sustainment Data Package (ASDP) and Contractual Language **Nicholas Shouse** AFLCMC/EZSI SE TA / AFMC LOE 2431 Co-lead, AFLCMC/EZSI - AFMC Digital Campaign	23776 MBSE Placeholder Pattern **Michael Reynolds** Systems Engineer, L3Harris Corp **David Wood** Senior Systems Engineer, Applied MBSE	23825 System Security Engineering and Anti-Tamper in the DoDI 5000.02 Operation of the Adaptive Acquisition Framework Policy Series **Randy Woods** System Security Engineering & Anti-Tamper Director, STPE, OUSD RE	23829 Developmental Test and Evaluation (DTE&A) and Cyberattack Resilient Systems **Dr. Peter Beling** Professor and Associate Director, Virginia Tech Intelligent Systems Laboratory
5:25 – 5:55 pm	23970 Advancing the State of R&M Engineering Practice to Deliver Reliable, Maintainable, and Supportable Advanced Capabilities to the Warfighter **Chris DeLuca** Director, Specialty Engineering OUSD(R&E)	23878 Lessons Learned in the Creation a Digital Thread **Dr. Steven Dam** President and COO, SPEC Innovations	23743 Recommendations for Systems Analysis in Support of Secure Architecture in Acquisition **Rich Kutter** Technical Advisor, Embedded Computing, AFLCMC Engineering Directorate	Test & Evaluation Panel MBSE as an enabler for Navy Capabilities Based Test & Evaluation **Introductions: Mike Rabens** Chair, Industrial Committee on Test and Evaluation **Moderator: Joe Manas** Raytheon Missiles & Defense **Ken Senechal** Director for Naval Capabilities Based T&E **Virginia Aguilar** Raytheon Missiles & Defense **Kelly Zimmerman** Boeing **Policarpio Soberanis** Northrop Grumman **David Harrison** Lockheed Martin
6:00 – 6:30 pm		23757 Integrating Digital Engineering Technical Models with MBSE Cost Models **Dr. Mark Blackburn** Senior Research Scientist, Stevens Institute of Technology	23774 Cyber Supply Chain Risk A System Security Engineering Requirement **Holly Dunlap** Senior Principal Engineer, System Security Engineering, Raytheon Missiles & Defense NDIA Systems Engineering Division Chair	

TUESDAY, DECEMBER 7

CONCURRENT BREAKOUT SESSIONS

	2A1 – Digital Engineering	2A2 - Model-Based Systems Engineering	2A3 - Systems Security Engineering	2A4 – Integrated Program Management
Moderator	**Chris Schreiber**	**David Allsop**	**Cory Ocker**	**Stewart Tague** **Linda Adams**
9:00 – 9:30 am	INCOSE Digital Engineering Information Exchange Working Group **Sean McGervey** DEIXWG Chairperson	23799 Measurement Framework Design for Digital and Model-Based Engineering **Kaitlin Henderson** PhD Candidate, Virginia Tech	23810 Managing Supply Chain Complexity with the Acquisition Security Framework **Dr. Carol Woody** Principal Researcher, SEI	23739 A Rocket Scientist's Approach to Launch Vehicle Flight Risk Management **Leo Childs** Chief Engineer, Mission Assurance Branch Space Systems Command – Launch Enterprise **Andy Inkeles** Senior Manager, Risk and Innovation Management Space Systems Command – Launch Enterprise **Col John Strizz, USAF** Chief Engineer Space Systems Command – Launch Enterprise
9:35 – 10:05 am	23742 Information Security Marking for MagicDraw® Models **Tom Alberi** Chief Scientist, Johns Hopkins University Applied Physical Lab	23740 Guide for Best Practices for Model Portfolio Management **Misak Zetilyan** Senior Project Engineer, The Aerospace Corporation **Jordan Howie** Member of Technical Staff, The Aerospace Corporation	23717 Right to Left and Outside-In: Systems Engineer's Role in Software-Dominant Organizations of the 21st Century – Special Emphasis on Cyber Security and the DoD **Dr. Kenneth Nidiffer** Professor, George Mason University	23901 The Most Important Trades Often Happen During Project Planning: Using Set-Based Practices to Optimize Those Trade-Off Decisions **Brian Kennedy** CTO, Targeted Convergence Corporation
10:10 – 10:40 am	23853 Leveraging the Digital Thread for ESOH Acquisition and Design **Dirk Zwemer** President, Intercax LLC	23836 Integrating MBSE and Product Lifecycle Management **David Segal** Senior Director, Federal, Aerospace and Defense, PTC	23847 Software Modernization and the Joint Federated Assurance Center **Bradley Lanford** Software Assurance Lead, OUSD(R&E) / SAIC	The Negatively Pressurized Conex (NPC) Program – How Acquisition and Systems Engineering Agility Delivered Capability to United States Transportation Command in 95 Days **Lt Col Paul Hendrickson, USAF** Materiel Leader, AF CBRN Defense Systems
10:40 – 11:00 am	**NETWORKING BREAK**			

	2B1 - Digital Engineering	2B2 - Model-Based Systems Engineering	2B3 - Systems Security Engineering	2B4 - Integrated Program Management
Moderator	Chris Schreiber	David Allsop	Cory Ocker	Stewart Tague Linda Adams
11:00 – 11:30 am	23756 The Importance of Metadata for the Discovery of Digital Engineering Artifacts **Dr. James Coolahan** Chief Technology Officer, Coolahan Associates, LLC	23837 The MBSE Digital Thread for Systems Failure Prediction **David Segal** Senior Director, Federal, Aerospace and Defense, PTC	23782 Security in the Future of Systems Engineering (FuSE), a Roadmap Review of Foundation Concepts **Rick Dove** Strategist, Independent	23900 Incorporating Technical Measures of Performance into Project Metrics **Chris Hassler** Software Support Specialist, SNA Software, LLC **Nick Pisano** President and CEO, SNA Software, LLC
11:35 am – 12:05 pm	23791 Taking Authority Over Your Modeling Enterprise: ManTech's Elastic Model Governance Approach **Dr. Heidi Davidz** Intelligent Systems Engineering SME, ManTech International Corporation		23852 Closing the Systems to Silicon Gap: MBSE-Enabled Digital Electronics Verification **Dr. Lisa Murphy** Technology Consultant, Siemens Industry Software	23752 Agile Program Management - Moving From Predictive Planning to Empirical Planning **Robin Yeman** Chief Technical Officer, Catalyst Campus
12:10 – 12:40 pm		23848 Use of SysML for Launch System Reliability and Availability Modeling **Myron Hecht** Senior Project Leader, Aerospace Corp	23869 Exemplar Design Patterns for Cyber Resilience **Brooke Guare** Cybersecurity Engineer, JHU/APL	23842 Conflict Is Your Friend - Managing Healthy Conflict in the Systems Engineering Workplace **Zane Scott** Vice President, Professional Services, Vitech

12:40 – 1:10 pm	NETWORKING LUNCH BREAK			
	2C1 – Digital Engineering	**2C2 - Model-Based Systems Engineering**	**2C3 – Systems Security Engineering**	**2C4 -System of Systems**
Moderator	Chris Schreiber	David Allsop	Cory Ocker	Dr. Judith Dahmann
1:10 – 1:40 pm	23948 Latest Developments with the Semantic Broker **Mark Schriner** Chief Digital Engineer, SAIC	23877 Modeling and Analysis of Standard Operating Procedures **Dr. Steven Dam** President and COO, SPEC Innovations	23763 Panel Discussion: Zero Trust for Hardware Security **Donald Davidson (moderator)** Director, Cyber-SCRM Programs, Synopsys **Dr. Zachary Collier** President, Collier Research Systems **Michael Bear** Technical Director - Systems Engineering, BAE Systems **David Pentrack** Senior Electronics Engineer, Defense Microelectronics Activity **Daniel Dimase** President & CEO, Aerocyonics	23809 Feature-based Product Line Engineering in Aerospace and Defense **Dr. Charles Krueger** CEO, BigLever Software
1:45 – 2:15 pm	23949 DID Modeling to Support the DoD Program Life Cycle **Robert Wojcik** Senior Member of the Technical Staff, Software Solutions Division, Software Engineering Institute, Carnegie Mellon University			23903 Leveraging Set-Based Practices to Make Agile Practices More Effective for System-of-Systems Engineering **Brian Kennedy** CTO, Targeted Convergence Corporation
2:20 – 2:50 pm	23906 Intellectual Property Considerations in Digital Engineering Implementation for Acquisition in the DoD **John Daly** Chief Engineer, Booz Allen Hamilton	23807 A State-Based Approach for ESOH Analysis **Michael Vinarcik** Chief Systems Engineer, SAIC	**Architecture** **Edward Moshinsky** Moderator 23973 OUSD(R&E) Systems Engineering Modernization Strategy **Nadine Geier** Director, Systems Engineering OUSD (R&E) **Dr. Kelly Alexander** Chief Engineer, Systems Engineering Modernization (OUSD R&E)	23926 Tilting at Windmills: Value Chains, Risk, Opportunity, and the 2021 Texas Electricity Grid Failure **Matthew Hause** Principal, SSI
2:55 – 3:25 pm	23930 – Embry Digital Engineering Requirements for Evolving Design and Analysis Tools **Paul Embry** Digital Engineering, L3Harris Technologies	23911 Product Line Engineering in the New Age of Digital Engineering **Dr. Charles Krueger** CEO, BigLever Software	23731 Overview of the Revised Standard on Architecture Description – ISO/IEC 42010 **Dr. James Martin** Principal Engineer, The Aerospace Corporation	23961 Systems of Systems and Complexity: INCOSE Initiative **Dr. Judith Dahmann** Technical Fellow, MITRE
3:25 – 3:45 pm	NETWORKING BREAK			

	2D1 – Digital Engineering	2D2 - Model-Based Systems Engineering	2D3 - Architecture	2D4 – Human Systems Integration
Moderator	Chris Schreiber	David Allsop	Edward Moshinsky	Matthew Risser
3:45 – 4:15 pm	23928 A View of The Digital Engineering Process **Jeffery Bryson** Systems Engineer, Northrop Grumman		23916 Air Force Government Reference Architectures: Strategy, Approach, Challenges, and Path Forward **Robert Bond** Plans and Program Engineer, Systems Engineering Division (AFMC/ENS)	
4:20 – 4:50 pm	23965 Digital Engineering Competency Framework (DECF) **Dr. Nicole Hutchison** Research Engineer, Systems Engineering Research Center	23915 The Impact of Technical Debt in Requirements on Product Lines and Composable Components **Larri Rosser** RIS Chief Architect, Raytheon Intelligence and Space	23732 Enterprise Architecture Guide for the Unified Architecture Framework (UAF) **Dr. James Martin** Principal Engineer, The Aerospace Corporation	23918 Human Systems Centered Digital & Mission Engineering (HSCDME) within a Model Based Human Systems Engineering (MBHSE) Approach **Dr. C.J. Hutto** Senior Research Scientist, Georgia Tech Research Institute
4:55 – 5:25 pm	23793 An Elastic Approach to Digital Engineering **Matthew Taylor** Intelligent Systems Engineering SME, ManTech International	23941 Feature Based Product Line Engineering: What, Why, and How to Do It Best! **Rowland Darbin** Working Group Chair, INCOSE	23855 UAF in Practice **Eran Gery** WW A&D Solutions Lead, IBM Engineering Solutions	23749 Mission Engineering Approach for Influencing Warfighter Actions using Computational Social Sciences (IWACSS) **Dr. Paul Hershey** Principal Engineering Fellow, Raytheon Technologies
5:30 – 6:00 pm	23765 Updating DoD Policy and Guidance for Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A) **Philomena Zimmerman** Director, ET&E OUSD (R&E) **Joseph Carnell** Systems Engineer (Support), OUSD(R&E)	23978 Model-Based Requirement Authoring Approach to Improve Efficiencies in the DoD RFP Process **Richard Wise** Senior Research Engineer, Georgia Tech Research Institute	23894 Defining Architecture Requirements for Results that Deliver: Open, Flexible, Scalable, Sustainable **Gordon Hunt** Vice President of Skayl, LLC	

WEDNESDAY, DECEMBER 8

CONCURRENT BREAKOUT SESSIONS

	3A1 – Engineered Resilient Systems: Program Achievements	3A2 – Mission Engineering	3A3 — Architecture	3A4 – Education & Training
Moderator	Lois Hollan	Dr. Judith Dahmann	Robert Scheurer	Dr. Robert Raygan
9:00 – 9:30 am	Engineered Resilient Systems: Digital Engineering and Computational Testing **Dr. Robert Wallace** ERDC ITL and ERS Technical Director	Mission Engineering Panel - Importance and Advancement of Mission Engineering **Elmer Roman** Director Mission Integration, OUSD (R&E) **Christopher O'Donnell** Performing the Duties of the Assistant Secretary of Defense for Acquisition, OUSD (A&S) **Dr. Paul Dreyer** Corporate Director of Modeling, Simulation, and Analysis, Northrup Grumman Corporation **Representative Joint Staff J8**	23929 AI for Meta-Systems Architecting Meta-System Architecting for AI **Dr. Cihan Dagli** Professor, Missouri University of Science & Technology	
9:35 – 10:05 am	Government Built, Production Quality, Multi-Disciplinary, Multi-Fidelity Software for Acquisition Engineering Support **Dr. Scott Morton** Associate Director, DoD HPCMP		23806 Encapsulating Variability: Applying Design Structure Matrices to Righting Software's Principles **Michael Vinarcik** Chief Systems Engineer, SAIC	23724 A Systems Engineering Approach to Cyber SCRM **Alexander Wright** Computer Scientist, U.S. Air Force
10:10 – 10:40 am	Transforming Design Requirements and Evaluation Through Effectiveness-Based Design Measures **Dr. Ian Dettwiller** Program Manager, U.S. Army ERDC Information Technology Lab		23922 You Can't Touch This: Logical Architectures in the MBSE and the UAF **Matthew Hause** Principal, SSI	23843 Making Your Case-Negotiation and Persuasion for The Systems Engineer **Zane Scott** Vice President for Professional Services, Vitech
10:40 – 11:00 am	**NETWORKING BREAK**			

	3B1 - Engineered Resilient Systems: DARPA CRANE Project	3B2 - Mission Engineering	3B3 – Architecture	3B4 – Education & Training
Moderator	Lois Hollan	Dr. Judith Dahmann	Robert Scheurer	Dr. Robert Raygan
11:00 – 11:30 am	DARPA Control of Revolutionary Aircraft with Novel Effectors (CRANE) Program Philosophy and Achievements **Dr. Alexander Walan** Program Manager, DARPA Tactical Technology Office (TTO)	23974 Overview of R&E Mission Analysis and Methodology **Marc Goldenberg** Chief Engineer, Mission Engineering, OUSD(R&E) **Dr. Judith Dahmann** Technical Fellow, MITRE	23898 DEWS Open Reference Architecture Development **Dr. Steven Davidson** Chief Scientist for Systems Architecture, MITRE Corporation	23844 The Overlooked Power of Systems Thinking **Zane Scott** Vice President, Professional Services, Vitech
11:35 am – 12:05 pm	Unique Public-Private Partnerships Provide HPC-Enabled, High-Fidelity Design and Analysis Techniques for Industry Engineering Teams T that Speed Development **Dr. Justin Foster** Research Mechanical Engineer, U.S. Army ERDC Information Technology Lab	23769 Mission Engineering Digital Ecosystem **Dr. Owen Eslinger** Computer Scientist, U.S. Army Engineer Research and Development Center (ERDC) **Darryl Howell** Engineering Tools and Environments, OUSD(R&E)	23876 Implementing SysML 2.0 **Dr. Steven Dam** President and COO, SPEC Innovations	23866 Toxic Substances Control Act (TSCA) Risk Management Impacts to the Defense Industrial Base (DIB) **Drew Rak** Senior Environmental Health Scientist, Noblis
12:10 – 12:40 pm	Incorporating Active Flow Control Technology into Aircraft Design for DARPA's CRANE Program **Juan Montoro** Manager, Conceptual Design and ADP Program Manager, Lockheed Martin Aeronautics	23957 Mission Engineering Landscape – A Federally Funded Research and Development Center (FFRDC) View **Dr Judith Dahmann** Technical Fellow, MITRE **Meg Adams** Technical Fellow, MITRE		23802 Scaled Agility in the DoD Acquisition Environment **Dr. Michael Orosz** Research Director/ Professor, USC Information Sciences Institute
12:40 – 1:10 pm	**NETWORKING LUNCH BREAK**			

	3C1 - Engineered Resilient Systems	3C2 - Mission Engineering	3C3 – Modular Open Systems Approach	3C4 – Education & Training
Moderator	Lois Hollan	Dr. Judith Dahmann	Edward Moshinsky	Dr. Robert Raygan
1:10 – 1:40 pm	23846 Using Value Engineering to Propel Cyber-Physical Systems Acquisition **Alfred Schenker** Software Solutions Division, Carnegie Mellon University/ Software Engineering Institute	23975 Reusable Digital Engineering Environment to Support Mission Engineering Studies **Marc Goldenberg** Chief Engineer, Mission Engineering, OUSD(R&E) **Dr. Judith Dahmann** MITRE **Michael Pennock** MITRE **Gabriela Driscoll** MITRE	23971 Assessing MOSA – New Methods to Develop Quantitative Assessment Criteria **Nadine Geier** Director, Systems Engineering, OUSD(R&E) **John Tindle** Systems Engineer, OUSD (R&E)	Education and Training Panel: Transformation of Defense Workforce **Stephanie Possehl** Acting Deputy Director for Engineering (DD, ENG), OUSD Research and Engineering **Dr. Laura Milham** Deputy Director, Advanced Distributed Learning Initiative, OUSD Personnel and Readiness **Dr. Cliff Whitcomb** Systems Engineering Professor, Naval Postgraduate School / INCOSE Systems Engineering Editor **RADM (Ret) Mike Manazir** Vice President, Government Services Sales Boeing Global Services / Chair, National Defense University Executive Committee **Dave Pearson** Director, Engineering and Technology and Test & Evaluation Centers, Defense Acquisition University
1:45 – 2:15 pm	23856 Protection of Software for the Adaptive Acquisition Framework **Bradley Lanford** Software Assurance Lead, OUSD(R&E) / SAIC	23890 Implementing Digital Engineering Environment for Mission Engineering **Jon Kim** Principal, Business and Technology Strategist, MITRE Corporation **Zach Moore** JS J8 JIAMDO/ Systems Engineer	23908 Intellectual Property Considerations for Modular Open Systems (MOSA) Implementation in the DoD **Patrick Bains** Engineer, Booz Allen Hamilton	
2:20 – 2:50 pm	23824 Application of Criticality Analysis to Risk Based Engineering Design **Randy Woods** System Security Engineering & Anti-Tamper Director, STPE, OUSD RE	23939 Towards Mission Engineering in a MOSAIC Warfare Context using Explainable AI **Dr. Daniel DeLaurentis** Professor, Purdue University	23972 DoD MOSA Community of Practice (CoP) Update **Nadine Geier** Director, Systems Engineering, OUSD(R&E) **Nathaniel Barley** Systems Engineer, OUSD (R&E)	
2:55 – 3:25 pm		23864 Mission-Level Optimization: A New Method for Designing Successful Systems **Dr. Brian Chell** Postdoctoral Researcher, Systems Engineering Research Center		
3:25 – 3:45 pm	**NETWORKING BREAK**			

	3D1 - Agile	3D2 – Mission Engineering	3D3 – Environment, Safety, & Occupational Health	3D4 – Education & Training
Moderator	John Daly	Dr. Judith Dahmann	Sherman Forbes Diane Dray	Dr. Robert Raygan
3:45 – 4:15 pm	23753 Agile Across the Value Stream **Robin Yeman** Chief technical Officer, Catalyst Campus	23804 Network Digital Twins for 21st Century Wargaming **Jeremy Smith** Account Manager, Navy and Marine Corps, SCALABLE Network Technologies	23813 Best of Both Worlds: Implementing The National Defense Strategy In A Resilient, Safe and Sustainable Way **David Asiello** Program Manager OUSD (A&S)/ODASD(E&ER)	
4:20 – 4:50 pm	23792 USAF Digital Campaign Think Big, Start Small, Scale Fast **Chris Garrett** Technical Advisor for SE, AFLCMC/EN-EZ		23950 Revising MIL-STD-882 **Lee Wood** Booz Allen Hamilton	23822 Cyber Resilient Weapon System Body of Knowledge (CRWS-BoK) **Burhan Adam** Program, Policy, Guidance, and Standards Director - STPE, OUSD RE **Angela Lungu** CRWS-BoK Project Lead Senior System Security Engineer, Support to OUSD(R&E), Resilient Systems **Madison Rudy** CRWS-BoK Lead Analyst, Support to OUSE(R&E), Resilient Systems
4:55 – 5:25 pm		23889 Model Based Systems Engineering in a Digital Environment: Creating a Virtual Testbed for Complex System Architectures **Claudeliah Roze** Technical Director, Mission Modernization Solutions	23937 Lessons Learned from Implementing New NAS411 Requirements **Yvonne Pierce** Engineer, The Boeing Company	23966 Individual and Organizational Systems Engineering Effectiveness **Dr. Nicole Hutchison** Research Engineer, Systems Engineering Research Center
5:30 – 6:00 pm	23814 Agile Insight - Gating Alternatives for Agile Programs **Larri Rosser** Engineering Fellow, Raytheon Intelligence and Space	23892 Probabilistic Graphical Models to Support Trade Study Evaluation and Scoring to Support Navy POM Budget Assessments **Jason Baker** Research Engineer, Georgia Tech Research Institute	23895 Impact of the American Innovation and Manufacturing Act on DoD **Peter Mullenhard** Environmental Engineer, DoD ODS Subcommittee (BMT)	23770 Developing a Digital Engineering Body of Knowledge for the DoD **Philomena Zimmerman** Director, ET&E OUSD (R&E) **Mary Davidson** Engineering Tools and Environments, OUSD(R&E) **Frank Salvatore** Engineering Tools and Environments, OUSD(R&E)

LIVE SESSIONS

Model Readiness Levels: A Mathematical Construct for Validation and Trust

1C1 – Digital Engineering • 23751

Dr. Darryl Ahner

Model validation is a contentious and ill-defined practice within DoD. Development of a Model Readiness Level (MRL) Framework serves two purposes: 1) provides developers a clear standard to develop their models, and 2) provides decision makers a better construct to understand risk to make decisions.

Model-Based Systems Engineering Panel

1C2 – Panel Discussion: Advancements and Challenges in MBSE in the Context of Digital Engineering

Jonathan Backhaus | David Allsop

System Security Committee & Track Welcome

1C3 – Systems Security Engineering • 23951

Cory Ocker

The National Defense Industrial Association (NDIA) System Security Engineering Committee's mission is to promote System Security Engineering integration into the Systems Engineering and Mission Assurance processes in the Department of Defense (DoD) acquisition of weapon systems. The committee fosters the development of System Security Engineering methods, tools, techniques, and processes required for the role of System Security Engineers, and provides a forum for the open exchange of ideas and concepts between government, industry, FFRDC and academia. The committee also works to develop a new understanding of System Security Engineering and the critical role it plays to ensure system survivability in a cyber contested environment. This briefing will introduce the audience to the committee, provide a status update on completed, ongoing, and future projects as well as invitations/ opportunities for additional engagement.

Mission Engineering and Digital Engineering Enabling a Unified Evaluation Framework

1C4 – Test & Evaluations • 23764

Dr. Suzanne Beers

The OSD DTE&A, DOT&E, and Service T&E communities have come together to develop a Unified Evaluation Framework (UEF) to guide evaluation-focused full continuum test planning to inform decision-making throughout adaptive acquisition framework (AAF) system life cycles.

Integrating Digital Engineering and Modeling and Simulation to Support Technology Adoption in Department of Defense Systems

1C1 – Digital Engineering • 23766

Philomena Zimmerman | John Daly

This presentation will discuss the benefits, challenges, and emerging concepts that meet the challenges in integrating digital engineering with modeling and simulation to improve technology adoption in defense systems.

Technology and Program Protection in the Department of Defense

1C3 – Systems Security Engineering • 23823

Melinda Reed

The recently published Department of Defense Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage" establishes the overarching technology protection policy for both DoD-sponsored research and technology activities and defense acquisition programs. This presentation addresses the new policy changes and efforts underway to implement the policy including the impact of the new Acquisition Pathways.

Digital Development and Test Transformation

1C4 – Test & Evaluations • 23797

Vu Hoang | Shailesh Sujanani

Over the last few decades little has changed in the design, test, and build processes in the Aerospace Defense Industry. Due to this the Department of Defense (DoD) has challenged companies by contractually obligating them to be Agile and conform to the DoD Enterprise DevSecOps Reference Design. The motivation behind this shift comes out of the need to keep up with our adversaries and to tackle the challenges of first time quality and reduced delivery time.

Concept for Establishing Consistent System Digital Representation Across the System Lifecycle at All Required Fidelities

1C1 – Digital Engineering • 23772

Dr. Charles Sanders

This presentation proposes a concept for digital engineering infrastructure for the collection, curation, and sharing of systems digital representation across the system lifecycle.

An Argument for Why the Future of Requirements Lies in Model-Based Systems Engineering

1C2 – Model-Based Systems Engineering • 23720

Chris Swickline

This paper presents an argument for why our approach to requirements must or will change as a result, in part, of the Digital Engineering movement.

Agile Authorizations Approach to Risk Management Framework

1C3 – Systems Security Engineering • 23773

Daniel Holtzman

Applying an agile foundational Systems Engineering / Systems Engineering approach to the Risk Management Framework Execution, via the DAF Fast Track Process. Assessing Risk of Use in an informed operational context.

The Automation Framework: Using Data Volume, Variety, and Veracity to Accelerate DevSecOps

1C4 – Test & Evaluations • 23816

Kevin Visalli

This presentation will discuss The Automation Framework (TAF), describing how it accelerates the DevSecOps process by automating software testing. TAF is equipped to handle the volume and variety of very large modern datasets, while ensuring the veracity, accuracy, and reliability of that data. Mr. Visalli will address the problems that TAF solves, how it benefits various programs, and the future of TAF in the transformation and modernization of today's defense landscape.

Ontologies for Engineering with Examples: A Pragmatic Perspective

1D1 – Digital Engineering • 23784

Dr. Mark Blackburn

This presentation will explain and demystify the fundamental aspect of ontologies, and how they enable technologies referred to as semantic web technologies (SWT). This is a key enabler for realizing the intent of the Digital Engineering Strategy. Given that tool-to-tool integration is fragile and cannot be sustained, Ontologies allow us to realize semantically consistent and rich interoperability at the data level. This presentation will provide examples that discuss how ontologies and SWT can be used to support engineering analysis and design.

A Vision for High Fidelity Multi-Disciplinary Simulation Built Surrogates Influencing the Design and Assessment of Military Systems

1D2 – Model-Based Systems Engineering • 23721

Dr. Scott Morton

This presentation describes a software infrastructure to support a vision for a digital transformation of US DoD acquisition using Physics Based Analytics, Data Driven Analytics, Surrogates, and Decision Support Apps being developed by the DoD High Performance Computing Modernization Program (HPCMP) Computational Research and Engineering Acquisition Tools and Environments (CREATE) program available to the government and industry.

Army Cyberspace Survivability

1D3 – Systems Security Engineering • 23872

Matthew Picerno

Implementing systems security engineering to enable Army Multi-Domain Operations through a total force arsenal that is survivable in cyberspace.

Capabilities Based Acquisition

1D4 - Test & Evaluations • 23839

Kenneth Senechal

Capabilities Based Acquisition (CBA) is fundamentally changing how we do acquisition. Using a model based system-engineering construct, we utilize warfare analysis and mission engineering to understand the concept of employment (CONEMP) to fight the future war. We then leverage our partnership with our operational test agency to build the final exam to provide the foundation that breaks down the tasks, conditions, systems, and performance attributes required for our acquisition programs to win that future war. The requirements/behaviors derived via this methodology are all captured in a SysML model. The linking of system models allows for gap identification along with early and ongoing trade space analysis. Likewise, our training and sustainment communities leverage the same CONEMP to build an overarching training curriculum and sustainment plan to enable the fleet to employ and sustain the new capabilities when delivered.

Acquisition and Sustainment Data Package (ASDP) and Contractual Language

1D1 – Digital Engineering • 23963

Nicholas Shouse

For successful digital transformation, the model-based acquisition and systems engineering processes need to be understood and the enterprise data architecture must be defined. The government must ensure weapon system program model-based data content is delivered by contract and useable across the tools in the Air Force's Integrated Digital Environment (IDE). To do this, we must be able to consistently dictate the appropriate data requirements on contract via the SOW, CDRLs and DIDs.

MBSE Placeholder Pattern

1D2 – Model-Based Systems Engineering • 23776

David Wood | Mike Reynolds

This presentation describes a modeling pattern that, coupled with a component library, accelerates the development of a system model and allows architectural trades and analysis to be completed early in the development lifecycle

System Security Engineering and Anti-Tamper in the DoDI 5000.02 Operation of the Adaptive Acquisition Framework Policy Series

1D3 – Systems Security Engineering • 23825

Randy Woods

As the Department of Defense Instruction (DoDI) 5000.02 Adaptive Acquisition Framework (AAF) Series policies are implemented, this presentation will discuss how Systems Security Engineering (SSE) and Anti-Tamper (AT) are accounted for under the updates. This presentation will focus on how the DoDI 5000.83 provides for both SSE and AT protections for various pathways.

Developmental Test and Evaluation (DTE&A) and Cyberattack Resilient Systems

1D4 – Test & Evaluations • 23829

Dr. Peter Beling

The research objective is to normalize expectations, enhance quality, and create reuse opportunities associated with the development of test plans related to achieving operational cyber-attack resilience for physical systems.

Advancing the State of R&M Engineering Practice to Deliver Reliable, Maintainable, and Supportable Advanced Capabilities to the Warfighter

1D1 – Digital Engineering • 23970

Chris DeLuca

This presentation will discuss modernized reliability and maintainability (R&M) practices such as instantiating digital engineering into R&M and advancing software development practice to provide reliable, maintainable, and supportable capabilities to the warfighter.

Lessons Learned in the Creation a Digital Thread

1D2 – Model-Based Systems Engineering • 23878

Dr. Steven Dam

For Digital Engineering to become a reality, many people envision that this requires systems and design engineering tools be fully integrated. This paper will discuss some of the lesson learned so far in developing a digital thread for a DoD customer.

Recommendations for Systems Analysis in Support of Secure Architecture in Acquisition

1D3 – Systems Security Engineering • 23743

Rich Kutter

Cybersecurity is often viewed through a risk and issue lens. Traditional systems engineering is founded on the integration of system analysis and design trades throughout the system life cycle. We will discuss how to leverage an understanding of cyber adversity into the systems engineering framework via systems analysis and trades. We will address understanding of the architectural contributions to the technical risks and issues to be addressed in the development of a Cyber Secure Resilient and Survivable Architectures for a weapon system.

Test & Evaluation Panel: MBSE as an enabler for Navy Capabilities Based Test & Evaluation

1D4 – Test & Evaluations

Mike Rabens | Ken Senechal | Virginia Aguilar | Joe Manas | Kelly Zimmerman | Policarpio Soberanis | David Harrison

MBSE as an enabler for Navy Capabilities Based Test & Evaluation

Integrating Digital Engineering Technical Models with MBSE Cost Models

1D2 – Model-Based Systems Engineering • 23757

Dr. Mark Blackburn

The presentation summarizes Digital Engineering modeling methods that produce artifacts for a "full stack" of technical models that are linked with a Cost Model using a Model-Based Systems Engineering (MBSE) methodology. We discuss this method using a NAVAIR Surrogate Pilot use cases for a search and rescue mission, and a hypothetical unmanned air vehicle (UAV) system called Skyzer. The "Full Stack" of models include mission, system and a contractor request for proposal response models (i.e., technical models).

Cyber Supply Chain Risk A System Security Engineering Requirement

1D3 – Systems Security Engineering • 23774

Holly Dunlap

This presentation will introduce Cyber Supply Chain Risk Management (SCRM). Cyber SCRM requires a partnership between System Security Engineers (SSE) and Supply Chain. Cyber SCRM manages the inherent risks of the global supply chain threats and vulnerabilities to system mission critical functions and system mission critical components we procure from our suppliers and suppliers' suppliers. We will review DoD policy, customer requirements, and NIST standards.

NCOSE Digital Engineering Information Exchange Working Group

2A1 – Digital Engineering

Sean McGervey

The INCOSE Digital Engineering Information Exchange Working Group (DEIXWG) has been working closely with the US DoD, industry partners, and academic organizations to advance a critical aspect of Digital Engineering: how to exchange digital work products between organizations in a semantically meaningful way. Since its inception in late 2017 due to the support of OSD(R&E), the DEIXWG has been modeling a conceptual ontology for describing digital work products and the information they contain. With that ontology in hand, the DEIXWG has been soliciting stakeholder needs from the broader community in the form of desired information exchange scenarios that require combining data from a variety of different digital sources. This presentation will provide an overview of the DEIXWG's ongoing activities and a look ahead at future efforts.

Measurement Framework Design for Digital and Model-Based Engineering

2A2 – Model-Based Systems Engineering • 23799

Kaitlin Henderson

A causal model is presented that links the primary benefits of Digital Engineering (DE) transformation to benefit measures and related enterprise adoption measures. The causal model is being used to develop a community set of standard DE measurement specifications. This presentation will discuss the development of the causal model and subsequent use to design standard measurement processes for DE.

Managing Supply Chain Complexity with the Acquisition Security Framework

2A3 – Systems Security Engineering • 23810

Dr. Carol Woody

In systems design, we see engineers decompose the system into its technology components and delegate requirements to these various pieces. In many cases these pieces may be bought, reused, or downloaded to meet programmatic needs driven by cost and schedule without consideration of the inherited risks these options bring to the overall system. To make the challenge more difficult, the number of disparate pieces and participants continue to expand to ever more specialized groups and third-party suppliers. These complexities in conjunction with the evolving threat environment require that new methods be deployed to help manage systems across their lifecycle. The Acquisition Security Framework (ASF) which is built on proven approaches to acquisition, engineering and deployment provides innovative approaches that can help with managing these challenges and complexities. The ASF is collection of cybersecurity practices that an acquisition program should perform when acquiring a software-intensive system.

A Rocket Scientist's Approach to Launch Vehicle Flight Risk Management

2A4 – Integrated Program Management • 23739

Leo Childs | Andy Inkeles | Col John Strizzi

The United States Space Force's (USSF) National Security Space Launch (NSSL) organization developed a Technical Issue Resolution Process (TIRP) as a standard to consistently assess and determine flight risk due to specific Launch Vehicle (LV) technical issues. If not adequately addressed, these technical issues may result in a launch failure. This presentation will describe and provide unique insights into the NSSL methodology for assessing the potential of launch failure (i.e., flight risk) as driven by an identified technical issue on the NSSL Program.

Information Security Marking for MagicDraw® Models

2A1 – Digital Engineering • 23742

Tom Alberi

A description and demonstration of the latest version of Johns Hopkins University Applied Physics Laboratory's Information Security Plugin for the MagicDraw® modeling tool.

Guide for Best Practices for Model Portfolio Management

2A2 – Model-Based Systems Engineering • 23740

Misak Zetilyan | Jordan Howie

The Model Portfolio Management (MPM) guide identifies goals and practices necessary to manage an organization's portfolio of models. It defines the specific actions and work products to ensure that the collection of models meet organizational needs, are maintained, and integrated. The goal is to streamline and organize the management of models across a portfolio so that models are accessible, relevant, and the full breadth of models is known.

Right to Left and Outside-In: Systems Engineer's Role in Software-Dominant Organizations of the 21st Century – Special Emphasis on Cyber Security and the DoD

2A3 – Systems Security Engineering • 23717

Dr. Kenneth Nidiffer

This presentation leverages the work of an international team that has examined key challenges in finding meaningful roles for systems engineering in the secure joint development and operations (briefly, Dev/Sec/Ops)-dominant software engineering/computer science

world. It addresses the systems engineer's role in software-dominant organizations of the 21st Century with a special emphasizes on cyber security and the DoD.

The Most Important Trades Often Happen During Project Planning: Using Set-Based Practices to Optimize Those Trade-Off Decisions

2A4 – Integrated Program Management • 23901

Brian Kennedy

Some of the most critical design decisions are locked in during the project planning effort, before trade studies have typically been run. Project managers should leverage set-based practices to reverse that, so they can properly optimize those critical trade-off decisions.

Leveraging the Digital Thread for ESOH Acquisition and Design

2A1 – Digital Engineering • 23853

Dirk Zwemer

State-of-the art practices in digital transformation MBSE and DevOps support the effective incorporation of ESOH issues in defense programs.

Integrating MBSE and Product Lifecycle Management

2A2 – Model-Based Systems Engineering • 23836

David Segal

Model-Based Engineering (MBE) is an "approach to engineering that uses models as an integral part of the technical baseline that includes the requirements, analysis, design, implementation, and verification of a capability, system, and/or product throughout the acquisition life cycle." This includes system development from concept through to manufacturing and distribution. MBE is wide in scope in that it encompasses the entire lifecycle process. This approach requires integrated digital engineering tools that provide traceability, interoperability and exchange throughout the development lifecycle including between systems engineering and Product Lifecycle Management (PLM)"

Software Modernization and the Joint Federated Assurance Center

2A3 – Systems Security Engineering • 23847

Bradley Lanford

With the adoption of the DoD Adaptive Acquisition Framework (AAF) and rapid modernization of DoD software, the Joint Federated Assurance Center (JFAC) must also modernize its approach to assurance. This presentation will review JFAC's 2021 accomplishments and provide an overview of how these 2021 efforts are being used to support JFAC's modernization.

The Negatively Pressurized Conex (NPC) Program – How Acquisition and Systems Engineering Agility Delivered Capability to United States Transportation Command in 95 Days

2A4 – Integrated Program Management

Lt. Col. Paul Hendrickson, USAF

In March 2020, US Transportation Command issued a Joint Urgent Operational Need for the High Capacity Airlift of COVID infected passengers. The NPC team took an idea to a prototype, tested it, proved it, and achieved certifications for Air Worthiness and Bio-Containment | fielding the systems for their first operational mission in less than 95 days."

The Importance of Metadata for the Discovery of Digital Engineering Artifacts

2B1 – Digital Engineering • 23756

Dr. James Coolahan

This presentation will discuss the importance of discovery metadata for Digital Engineering. After showing an example digital collaborative environment for a system, the presentation will illustrate how a metadata standard such as one currently evolving within the Simulation Interoperability Standards Organization, can be applied to this use case.

The MBSE Digital Thread for Systems Failure Prediction

2B2 – Model-Based Systems Engineering • 23837

David Segal

Systems Failure Prediction is based on the analysis of components to predict and calculate the rate at which a product or system will fail. When failure is imminent, the component can be replaced by a larger system failure. Analysis techniques can identify the leading contributors to system failure and measure the impact of environment and stress on the system and its components. System failure prediction has most recently been enabled by the availability of actionable data via the Internet of Things (IoT) combined with Artificial Intelligence (AI) and Machine Learning in an integrated digital thread. The main emphasis for these techniques is in the deployed operational system. Achieving additional benefits will require integration with the Model-Based Systems Engineering (MBSE) digital thread.

Security in the Future of Systems Engineering (FuSE), a Roadmap Review of Foundation Concepts

2B3 – Agile • 23782

Rick Dove

The Future of Systems Engineering (FuSE) is an INCOSE-led multiorganizational collaborative initiative encompassing a number of topic areas with active projects to shape the future of systems engineering. The work discussed here addresses the FuSE Security topic area and provides a roadmap of eleven foundational concepts for building the future security vision.

Incorporating Technical Measures of Performance into Project Metrics

2B4 – Integrated Program Management • 23900

Chris Hassler | Nick Pisano

The presenters will demonstrate that the emphasis in project performance must include work and effort expended across the entire project life cycle, that incorporates all of the essential disciplines that constitute the project effort. In particular, the presenters will provide a methodology applied in a live proof-of-concept in a hybrid development program for new flying propulsion technologies that incorporated integration and contextualization of technical performance, risk, and uncertainty into their project measures.

Taking Authority Over Your Modeling Enterprise: ManTech's Elastic Model Governance Approach

2B1 – Digital Engineering • 23791

Dr. Heidi Davidz

As the digital ecosystem swells, there is a heightened challenge to robustly govern heterogeneous linked models across disciplines and across contractual boundaries. In addition, as more advanced analytics, automation, and artificial intelligence are used by the enterprise, the linked models also need to comply with enterprise data protocols. ManTech's Elastic Model Governance Approach is shown as an example for providing robust authority over the actual modeling enterprise throughout the full model lifecycle, integrating proven practices with mechanisms for flexibility, scalability, and automated validation.

Closing the Systems to Silicon Gap: MBSE-Enabled Digital Electronics Verification

2B3 – Agile • 23852

Dr. Lisa Murphy

Exploiting developments in MBSE and Electronics Design Automation (EDA), we show how microelectronics verifications can be traced from the system level models down through the full EDA design stack with a seamless flow. Use of virtual verification capabilities in this context helps achieve trust in microelectronics design by discovering potential issues to be addressed earlier.

Agile Program Management – Moving from Predictive Planning to Empirical Planning

2B4 – Integrated Program Management • 23752

Robin Yeman

I will describe why complex safety critical systems are the ideal place to leverage Agile and how to successfully implement for a large scale Cyber Physical System

Use of SysML for Launch System Reliability and Availability Modeling

2B2 – Model-Based Systems Engineering • 23848

Myron Hecht

Use of SysML for Launch System Reliability and Availability Modeling This presentation describes how to integrate reliability and availability modeling and prediction into Model Based Systems Engineering (MBSE) using SysML

Exemplar Design Patterns for Cyber Resilience

2B3 – Agile • 23869

Brooke Guare

In order to serve as a basis for developing solutions to a variety of cybersecurity challenges and/or cyber requirements, the Johns Hopkins University Applied Physics Laboratory (JHU/APL) has developed and compiled design patterns that have proven successful in past systems. By doing so, we hope to aid engineers in applying intuitive principles to system designs to meet cybersecurity requirements, in addition to complying with cybersecurity policy.

Conflict Is Your Friend- Managing Healthy Conflict in the Systems Engineering Workplace

2B4 – Integrated Program Management • 23842

Zane Scott

Conflict is the engine that drives innovation and it should be constructively managed rather than “resolved.”

Latest Developments with the Semantic Broker

2C1 – Digital Engineering • 23948

Mark Schriner

SAIC has previously shown the promise of the Semantic Broker. This presentation will showcase the latest capabilities available for use on programs.

Modeling and Analysis of Standard Operating Procedures

2C2 – Model-Based Systems Engineering • 23877

Dr. Steven Dam

This ½ day tutorial describes how to model SOPs and perform SOP analysis using MBSE and provides a hands-on opportunity to explore new technologies in assessing SOP viability.

Panel Discussion: Zero Trust for Hardware Security

2C3 – Systems Security Engineering & Architecture • 23763

Donald Davidson | Dr. Zachary Collier | Michael Bear | David Pentrack | Daniel Dimase

This panel discussion will bring together experts in the defense microelectronics field to discuss the core tenets of Zero Trust and Quantified Assurance, and lay out a path forward, that includes the development of industry standards, policy, and guidance.

Feature-based Product Line Engineering in Aerospace and Defense

2C4 -System of Systems • 23809

Dr. Charles Krueger

Feature-based Product Line Engineering is the subject of a new ISO standard (ISO/IEC 26580). Although the standard is new, Feature-based PLE has been around for over two decades, and in service in the A&D sector for nearly all of that time, resulting in tens to hundreds of millions of dollars in cost avoidance each and every year. It is in widely used by most of the top ten defense contractors in the United States. This presentation shows how the approach has earned its stripes by rising to the realities and hard challenges that are emblematic of the extremely challenging A&D sector: High-security systems, safety-critical systems, multi-contract funding, export control compliance, working with agile and digital engineering, and more.

DID Modeling to Support the DoD Program Life Cycle

2C1 – Digital Engineering • 23949

Robert Wojcik

This presentation will discuss an effort to develop guidelines that a contractor would use to develop models based on DOD Data Item Descriptions (DID) requirements to support System Engineering Technical Review (SETR) events

Leveraging Set-Based Practices to Make Agile Practices More Effective for System-of-Systems Engineering

2C4 -System of Systems • 23903

Brian Kennedy

We present a number of key hurdles that you will likely encounter when trying to apply Agile Practices, which have proven very effective in the development of software systems, to system-of-systems engineering. We then show how Set-Based Practices can be leveraged to overcome those hurdles.

Intellectual Property Considerations in Digital Engineering Implementation for Acquisition in the DoD

2C1 – Digital Engineering • 23906

John Daly

Rapidly advancing Digital Engineering (DE) capabilities being adopted by the Department bring some unique challenges, and possibilities. In a move from paper-based acquisition to digital systems engineering (fueled by adoption of Model Based Systems Engineering (MBSE) methodology and tools), re-thinking of Intellectual Property (IP) is stimulated in an effort to be more efficient and agile in DoD acquisition.

A State-Base Approach for ESOH Analysis

2C2 – Model-Based Systems Engineering • 23807

Michael Vinarcik

The continuing transformation of systems engineering from a document-intensive (DISE) to model-based (MBSE) discipline is enabling richer systems analysis. System models are inherently unambiguous and rigorous representations of design intent (especially when supplemented with

automated validation rules that detects errors, inconsistencies, and gaps). They enable direct analysis by specialty engineering (such as reliability & maintainability, ESOH, and cybersecurity). State-machine behavioral representations are particularly useful for ESOH and cybersecurity analysis. This presentation builds upon techniques described in prior NDIA papers on failure mode and effects analysis, cybersecurity, and pragmatic hazard identification and risk management to demonstrate the value that can be extracted from a system model in support of these stakeholders.

OUSD(R&E) Systems Engineering Modernization Strategy

2C3 – Systems Security Engineering & Architecture • 23973

Nadine Geier | Dr. Kelly Alexander

OSD is pursuing an SE Modernization effort that will review and assess the combined impact the SE focus areas have on SE technical and technical management processes. The OSD SE Modernization effort will also assess SE roles and responsibilities relative to the SE acquisition workforce. The Systems Engineering Modernization effort will also develop Best Practices and use cases from a wholistic perspective that is inclusive of the combined impact of several emerging and mature SE focus areas. A briefing on the emerging OSD SE Modernization approach will be provided.

Tilting at Windmills: Value Chains, Risk, Opportunity, and the 2021 Texas Electricity Grid Failure

2C4 -System of Systems • 23926

Matthew Hause

The 2021 Texas electricity grid failure was caused by a multitude of failures including lack of winterization, over-reliance on renewable energy, and poor planning. Mostly however, it was due to value chains and trade-off analysis that did not make preparation profitable. This presentation examines the problems and possible solutions.

Digital Engineering Requirements for Evolving Design and Analysis Tools

2C1 – Digital Engineering • 23930

Paul Embry

The AIA has been outlining the challenges and key requirements that will need to be addressed in the software tools environment to achieve the vision of an interoperable, integrated product development and delivery ecosystem across the supply chain. Our data must be mobile and collaborative. Perspectives will include those of how requirements for data sharing, interoperability will need to evolve current state of software tools.

Product Line Engineering in the New Age of Digital Engineering

2C2 – Model-Based Systems Engineering • 23911

Dr. Charles Krueger

This presentation will provide an introduction and overview of the new ISO/IEC 26580 standard on Feature-based PLE and how it has become an essential element in the new age of digital engineering. In addition, it will describe how Feature-based PLE specializes and removes the unintentional complexity of previous approaches to PLE, give examples of where and how it is being used by the top aerospace and defense organizations in the world, and show the economic model behind its success.

Overview of the Revised Standard on Architecture Description – ISO/IEC 42010

2C3 – Systems Security Engineering & Architecture • 23731

Dr. James Martin

An updated version of the international standard for Architecture Description is expected to be published in 2021 as the new version of ISO/IEC/IEEE 42010. This paper provides an overview of the key concepts defined by this standard and the rationale for them.

Systems of Systems and Complexity: INCOSE Initiative

2C4 -System of Systems • 23961

Dr. Judith Dahmann

This presentation will describe a cooperative effort between the INCOSE SoS and Complexity working groups to leverage work coming from the complexity community to address the challenges of SoS complexity

A View of The Digital Engineering Process

2D1 – Digital Engineering • 23928

Jeffery Bryson

A simple definition of the problem DE is solving, how DE can be used to solve the problem, and an overview of the needed technologies required to implement the solution.

Air Force Government Reference Architectures: Strategy, Approach, Challenges, and Path Forward

2D3 – Architecture • 23916

Robert Bond

Government Reference Architectures (GRAs), built on open architecture principles and consensus-based standards, are designed to guide and constrain system designs to produce highly modular and interoperable systems. These GRAs yield great benefits to both the government and industry but are all too often managed through disparate and disconnected initiatives with little enterprise perspective. This presentation will discuss the latest breakthroughs in Air Force and Space Force GRA development, current challenges, lessons learned, and ongoing activities.

Digital Engineering Competency Framework (DECF)

2D1 – Digital Engineering • 23965

Dr. Nicole Hutchison

Digital Engineering Competency Framework Overview and Assessment of Existing Training Resources

The Impact of Technical Debt in Requirements on Product Lines and Composable Components

2D2 – Model-Based Systems Engineering • 23915

Larri Rosser

The technical debt metaphor provides a common, easily understandable framework for discussing deficiencies in our systems and elements that impact productivity and quality in product realization. This presentation focuses on the ways in which technical debt manifests in requirements with examples, and how requirements debt impacts product lines and composable components.

Enterprise Architecture Guide for the Unified Architecture Framework (UAF)

2D3 – Architecture • 23732

Dr. James Martin

This paper describes a workflow for creating Enterprise Architecture (EA) views in accordance with the Unified Architecture Framework (UAF) standard published by the Object Management Group (OMG). This workflow will be the foundation for a new EA Guide to be published as part of the OMG standard. The nine steps of the workflow are laid out in alignment with the stakeholder domains in the UAF for producing the requisite UAF views in each of those domains.

Human Systems Centered Digital & Mission Engineering (HSCDME) within a Model Based Human Systems Engineering (MBHSE) Approach

2D4 – Human Systems Integration • 23918

Dr. C.J. Hutto

This presentation discusses advancements on a human centered digital approach to mission engineering developed by GTRI to support tradespace analysis across the DoD. The approach includes a paradigm of mission performance oriented total system modeling (where the total system comprises humans, hardware, and software). A digital/computational analytical framework is introduced which assimilates well-established human performance constructs like situation awareness, human error/reliability, workload, and risk together with explicit consideration of mission engineering concerns into generalized formalisms capturing their quantitative interrelationships, providing data science analytics and visualizations for tradespace analysis and decision support.

An Elastic Approach to Digital Engineering

2D1 – Digital Engineering • 23793

Matthew Taylor

Groups can become so enthralled with Digital Engineering (DE) and connecting information, that this becomes the end goal, rather than using DE to support the mission within planned cost. This presentation summarizes current understanding of optimized DE sizing, use of elastic methods, and relevant organizational transformation literature, then provides guidance for an elastic DE approach using ManTech's fleX-engineering™ framework.

Feature Based Product Line Engineering: What, Why, and How to Do It Best!

2D2 – Model-Based Systems Engineering • 23941

Rowland Darbin

The state of the practice for Product Line Engineering is significantly more advanced than many people realize, with a growing body of knowledge, an increasing focus on system family engineering in industry, and a growing body of success in the Aerospace and Defense sector. INCOSE's International Working Group on Product Line Engineering is an important resource for advancing industry awareness and building a strong community of practitioners to share knowledge and collaborate on PLE best practices.

UAF in Practice

2D3 – Architecture • 23855

Eran Gery

We will present and demonstrate a concrete SoS scenario and how it is modeled with UAF and integrated tooling such as requirements management and planning tools.

Mission Engineering Approach for Influencing Warfighter Actions using Computational Social Sciences (IWACSS)

2D4 – Human Systems Integration • 23749

Dr. Paul Hershey

In this paper, we present mission engineering method and system for Influencing Warfighter Actions using Computational Social Sciences (IWACSS) to fill the gap in both in traditional DoD wargaming and in emerging Computational Social Science. IWACSS incorporates the social domain into battle management where real-time analysis is required to support timely decision-making. Our extensive research of prior literature and patents reveals that, although prior wargaming has incorporated aspects of social science, these attempts fail to provide calculated results derived from mathematically-based prediction that consider the effects (e.g., 1st, 2nd, and 3rd order effects) of social parameters on the outcome of the battle. In fact, for these approaches, the concept of applying predictive techniques is limited based on the perceived randomness of human social behavior. IWACSS overcomes this limitation by applying foundational stochastic mathematics and CSS techniques in combination with Reinforcement Learning (RL) to improve timely decision making and provide predictive results that include confidence levels.

Updating DoD Policy and Guidance for Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A)

2D1 – Digital Engineering • 23765

Philomena Zimmerman | Joseph Carnell

This presentation describes the Office of the Under Secretary of Defense for Research and Engineering effort to update DoD policy for Modeling and Simulation Verification, Validation, and Accreditation (DoDI 5000.61) and associated guidance on best practices and documentation standards.

Model-Based Requirement Authoring Approach to Improve Efficiencies in the DoD RFP Process

2D2 – Model-Based Systems Engineering • 23978

Richard Wise

This presentation describes an effort exploring whether requirement templates expressed in the form of SysML modeling patterns coupled with semantic libraries can yield atomized, contextually bound, well-written model-based requirements when applied using a standard SysML modeling method. The aim is to ensure that the resulting requirements and authoritative model accompanying RFP documents are of a sufficient quality that contributes to the justifiable defense of offeror proposal selection within the RFP process.

Defining Architecture Requirements for Results that Deliver: Open, Flexible, Scalable, Sustainable

2D3 – Architecture • 23894

Gordon Hunt

We are experiencing a sea change in the world of systems architecture. Advances in technology, increasingly complex systems, and greater warfighter expectations require supporting architectures that deliver more than ever before. But how do we define the architectural requirements to ensure we meet these heightened demands? And, given a set of requirements, how do we test and measure them prior to implementation?

Engineered Resilient Systems: Digital Engineering and Computational Testing

3A1 – Engineered Resilient Systems

Dr. Robert Wallace

Design environments, particularly in novel materials and environments, require integration of modeling and simulation, data analyses, and scalable computation components. ERS has developed a Virtual Wind Tunnel capability used directly with industry acquisition projects which reduces time and risk."

Mission Engineering Panel: Importance and Advancement

3A2 – Mission Engineering

Senior Leaders in OSD, JS, and Industry

Meta-System Architecting for AI

3A3 – Architecture • 23929

Dr. Cihan Dagli

In this presentation interplay between AI and Meta-Architecting is introduced in connection with deep learning and heath care system architecting

Government Built, Production Quality, Multi-Disciplinary, Multi-Fidelity Software for Acquisition Engineering Support

3A1 – Engineered Resilient Systems

Dr. Scott Morton

This presentation will describe a set of software products and infrastructure to support a digital transformation of US DoD acquisition being developed by the DoD HPCMP CREATETM program available to the government and industry and show impact on current high priority DoD acquisition programs."

Encapsulating Variability: Applying Design Structure Matrices to Righting Software's Principles

3A3 – Architecture • 23806

Michael Vinarcik

The application of design structure matrices to systems architectures.

A Systems Engineering Approach to Cyber SCRM

3A4 – Education & Training • 23724

Alexander Wright

A new systems engineering approach to securing the cyber supply chain of cyber physical systems, firmware, and software.

Transforming Design Requirements and Evaluation Through Effectiveness-Based Design Measures

3A1 – Engineered Resilient Systems

Dr. Ian Dettwiller

The Engineered Resilient System's Decision Support Tool with Operational Analysis is facilitating a paradigm-shift in design through coupled conceptual design and operational analysis with automated workflows and remote computing.

You Can't Touch This: Logical Architectures in the MBSE and the UAF

3A3 – Architecture • 23922

Matthew Hause

Logical Architecture is an often misunderstood and misused concept. This presentation examines its benefits and best practices.

Making Your Case- Negotiation and Persuasion for The Systems Engineer

3A4 – Education & Training • 23843

Zane Scott

INCOSE's Competency Model lists "negotiation" as a competency essential to requirements management, verification and validation, and acquisition and supply. In this presentation, we will discuss the structure of persuasion and identify tools and techniques that will make us better communicators on both sides of the conversation- listening and expression.

DARPA Control of Revolutionary Aircraft with Novel Effectors (CRANE) Program Philosophy and Achievements

3B1 – Engineered Resilient Systems

Dr. Alexander Walan

The Control of Revolutionary Aircraft with Novel Effectors (CRANE) program aims to design, build, and flight test a novel X-plane that incorporates Active Flow Control (AFC) as a primary design consideration. Crane seeks to optimize the benefits of active flow control by maturing technologies and design tools, and incorporating them early in the design process. Active flow control could improve aircraft performance by removing jointed surfaces, which currently drive design configurations that increase weight and mechanical complexity. Demonstrating AFC for stability and control in-flight would help open the design trade space for future military and commercial applications.

Overview of R&E Mission Analysis and Methodology

3B2 – Mission Engineering • 23974

Marc Goldenberg | Dr. Judith Dahmann

OUSD(R&E)/ DDRE(AC)/ ENG Mission Integration is leading eight mission capability-focused studies in FY21. Each study addresses threat-informed technical challenges in OSD/ Joint Staff-prioritized mission threads. These studies inform modernization investment decisions, the integration of mature technologies, and the development and delivery of warfighting capability.

DEWS Open Reference Architecture Development

3B3 – Architecture • 23898

Dr. Steven Davidson

The technology behind Directed Energy Weapon Systems (DEWS) has matured to the point where DEWS is both operationally and technically viable, so that current Service DEWS are moving from the laboratory into the field | from Research and Development (R&D) to prototyping, and then on to early weapon systems. This crop of DEWS is custom designed for specific Service missions and platforms. They feature high levels of instance-unique optimization, long lead times for critical components due to custom design and manufacturing, and limited reuse of subsystems and subassemblies from one DEWS to the next. Reuse still requires redesign and modification.

The Overlooked Power of Systems Thinking

3B4 – Education & Training • 23844

Zane Scott

Systems thinking is the foundational element of our discipline. But, in practice, it is so revolutionary that it is often misunderstood or even overlooked. This presentation examines the causes and symptoms of our failure to move with the new paradigm into the age of systems. It suggests solutions to position us for success in solving the socio-technical problems of today and tomorrow with our new way of thinking about systems.

Unique Public-Private Partnerships Provide HPC-Enabled, High-Fidelity Design and Analysis Techniques for Industry Engineering Teams That Speed Development

3B1 – Engineered Resilient Systems

Dr. Justin Foster

In highly-computational design projects, the ERS-ERDC team has successfully embedded with industry partners under PEO sponsorship. The result is acceleration via the incorporation of HPC-enabled, high-fidelity design and analysis techniques for acquisition projects of interest to the DoD.

Mission Engineering Digital Ecosystem

3B2 – Mission Engineering • 23769

Dr. Owen Eslinger | Darryl Howell

This presentation will discuss an effort within OUSD(R&E) to create a DoD-owned Mission Engineering Digital Ecosystem (MEDE). The MEDE is providing a collaborative environment accessible to DoD Government and selected FFRDCs, contractors and academia.

Implementing SysML 2.0

3B3 – Architecture • 23876

Dr. Steven Dam

This paper shows an analysis of the prototype SysML 2.0 and how it's new ontology maps to other ontologies. Implementation issues result from this analysis.

Toxic Substances Control Act (TSCA) Risk Management Impacts to the Defense Industrial Base (DIB)

3B4 – Education & Training • 23866

Drew Rak

This session will highlight recent and anticipated risk evaluation and risk management issues relevant to U.S. Department of Defense (DoD) chemicals of concern and how DoD is engaging with the U.S. Environmental Protection Agency (EPA) and integrating the risk management determinations and proposed restrictions across the defense industrial base supply chain.

Incorporating Active Flow Control Technology into Aircraft Design for DARPA's CRANE Program

3B1 – Engineered Resilient Systems

Juan Montoro

Advanced technologies such as Active Flow Control (AFC) offer the potential to revolutionize next generation aircraft design through augmenting and enhancing aircraft control and operation. This presentation will discuss some of the challenges, solutions developed, and lessons learned to date in the incorporation of AFC in the design process.

Mission Engineering Landscape – A Federally Funded Research and Development Center (FFRDC) View

3B2 – Mission Engineering • 23957

Dr. Judith Dahmann | Meg Adams

This presentation provides the results of an initial examination of the 'landscape' of mission engineering activities across MITRE.

Scaled Agility in the DoD Acquisition Environment

3B4 – Education & Training • 23802

Dr. Michael Orosz

The University of Southern California Information Sciences Institute (USC/ISI) is undertaking a research and systems engineering analysis effort to explore the mission engineering methods, analysis, and metrics needed to transition from a traditional DoD 5000 waterfall software development environment to an Agile/DevSecOps environment. The transition includes an integration of emerging technologies and an Agile/DevSecOps related education program for the future workforce. Results from several projects will be presented.

Using Value Engineering to Propel Cyber-Physical Systems Acquisition

3C1 – Engineered Resilient Systems • 23846

Alfred Schenker

This analysis will identify the aspects of VE that can be applied to the acquisition and lifecycle of CPS employing embedded computing resources. Programs will be able to identify the future cost of change and the ability to ensure investments in modeling and analysis are preserved instead of traded off in the early stages of an acquisition when they do the most good.

Reusable Digital Engineering Environment to Support Mission Engineering Studies

3C2 – Mission Engineering • 23975

Marc Goldenberg | Dr. Judith Dahmann | Michael Pennock | Gabriela Driscoll

This presentation provides an implementation perspective on the development of a reusable digital engineering environment to support OUSD Research and Engineering Office of Engineering Mission Engineering studies.

Assessing MOSA – New Methods to Develop Quantitative Assessment Criteria

3C3 – Modular Open Systems Approach • 23971

Nadine Geier | John Tindle

Employing a Modular Open Systems Approach (MOSA) is mandated by law. In the past, the Department of Defense has used inconsistent qualitative means to assess MOSA. This presentation describes efforts to develop consistent, quantitative methods to assess the extent to which programs employ MOSA.

Education and Training Panel: Transformation of Defense Workforce

3C4 – Education & Training

Stephanie Possehl | Dr. Laura Milham | Dr. Cliff Whitcomb | RADM (Ret) Mike Manazir | Dave Pearson

Protection of Software for the Adaptive Acquisition Framework

3C1 – Engineered Resilient Systems • 23856

Bradley Lanford

The DoD Adaptive Acquisition Framework, Software Modernization Strategy, and adoption of software factories have changed the way the department develops software. The July 2020 issuance of Department of Defense Instruction (DoDI) 5000.83, established responsibilities and procedures for Science and Technology (S&T) managers and engineers to shape the way software is protected from adversarial attack.

Implementing Digital Engineering Environment for Mission Engineering

3C2 – Mission Engineering • 23890

Jon Kim | Zach Moore

The use of MBSE in conjunction with DE has led to the development of many innovative capabilities, including the use of virtual simulation environments that enable a digital representation of a system concept to be created, experimented with, and manipulated to achieve robust SoS solutions. With this Virtual Testbed, analyses can be performed that allow the end-user the ability to verify their end product and make architectural changes as needed.

Intellectual Property Considerations for Modular Open Systems (MOSA) Implementation in the DoD

3C3 – Modular Open Systems Approach • 23908

Patrick Bains

Modular Open Systems (MOSA) requirements for DoD acquisition have been steadily increasing since 2017 in successive National Defense Authorization Acts (NDAA) of Congress. MOSA is also driven by industry in the way modern capabilities and software are developed, manufactured, and fielded. In this evolution towards increased MOSA use in the Department, the critical importance of MOSA interface availability provides significant technical and programmatic/administrative challenges in the use, protection, and visibility of Intellectual Property (IP).

Application of Criticality Analysis to Risk Based Engineering Design

3C1 – Engineered Resilient Systems • 23824

Randy Woods

Utilizing an open source design, an end-to-end criticality analysis is performed that includes application of enterprise ICT supply chain risk management activities. The exemplar starts with the identification of Mission Critical Functions, Critical Components, and potential Critical Program Information. Potential mitigation methods and risk tracking are then applied to the system.

Towards Mission Engineering in a MOSAIC Warfare Context using Explainable AI

3C2 – Mission Engineering • 23939

Dr. Daniel DeLaurentis

Applying Mission Engineering and Design (ME&D) to a Mosaic warfare context as envisioned by DARPA, with rapid composition and adaptation of effects and strategies, ME&D becomes more challenging. The rise in applications of games, specifically real-time strategy (RTS) games, in engineering promises to provide test beds to support ME&D in a Mosaic warfare context. We believe that game balance is an important characteristic of a game environment that translates to a competitive ME&D. Our proposed framework leverages this knowledge of balance in an engagement to make decisions to support mission objectives in domains such as acquisition, scenario planning, and strategy execution.

DoD MOSA Community of Practice (CoP) Update

3C3 – Modular Open Systems Approach • 23972

Nadine Geier | Nathaniel Barley

The DoD MOSA CoP provides a collaborative environment supporting the community by collecting and sharing information, cultivating assistance groups through the development of tiger teams to sustain implementation across acquisition, and generating new knowledge to transform the application of MOSA.

Mission-Level Optimization: A New Method for Designing Successful Systems

3C2 – Mission Engineering • 23864

Dr. Brian Chell

This presentation describes research which proposes, tests, and validates a method for optimizing systems to maximize the probability of mission success.

Agile Across the Value Stream

3D1 – Agile • 23753

Robin Yeman

In order to decrease the lead time in delivery of mission critical capabilities we need to have a common vision with Agile practices across the entire delivery.

Network Digital Twins for 21st Century Wargaming

3D2 – Mission Engineering • 23804

Jeremy Smith

This paper describes the integration of a network digital twin with a wargaming simulator to provide a comprehensive platform for wargames capable of modeling all aspects of military missions, including communications performance and cyber effects. A Marine Corps Expeditionary Advanced Base Operations mission scenario is utilized to demonstrate the benefits of augmenting wargaming tools with network digital twin capabilities.

Best of Both Worlds: Implementing The National Defense Strategy in a Resilient, Safe and Sustainable Way

3D3 – Environment, Safety, & Occupational Health • 23813

David Asiello

Meeting the challenges of rapidly developing and deploying an enhanced warfighting capability while meeting resilience, system safety and sustainability goals.

USAF Digital Campaign Think Big, Start Small, Scale Fast

3D1 – Agile • 23792

Chris Garrett

Industry has realized the benefit of better decision making, agility, and savings by embracing digital transformation. Seeing the realized benefits in industry, the United States Air Force decided to digitally transform to keep up with ever-increasing rates of technical performance advances to stay ahead of its adversaries. The Air Force is a large and complex organization with an acquisition system forged out of the World War II-era Defense Industrial Base with a Vietnam War era-budgeting and resource allocation system. Weapon system acquisition complexity continues to grow and the Air Force is turning to digital transformation to quicken the speed of delivering weapon system capability to the warfighter. The Air Force has created a Digital Campaign to tackle this digital transformation for its acquisition enterprise. This paper advocates a strategy of “think big, start small, and scale fast” for the acquisition enterprise to achieve this transformation and meet the needs of the warfighter.

Model Based Systems Engineering in a Digital Environment: Creating a Virtual Testbed for Complex System Architectures

3D2 – Mission Engineering • 23889

Claudeliah Roze

The use of MBSE in conjunction with DE has led to the development of many innovative capabilities, including the use of virtual simulation environments that enable a digital representation of a system concept to be created, experimented with, and manipulated to achieve robust SoS solutions. With this Virtual Testbed, analyses can be performed that allow the end-user the ability to verify their end product and make architectural changes as needed.

Revising MIL-STD-882

3D3 – Environment, Safety, & Occupational Health • 23950

Lee Wood

DOD efforts stand up a working group to revise MIL-STD-882 or replace it with a non-governmental standard.

Cyber Resilient Weapon System Body of Knowledge (CRWS-BoK)

3D4 – Education & Training • 23822

Burhan Adam | Angela Lungu | Madison Rudy

The Cyber Resilient Weapon Systems Body of Knowledge (CRWS-BoK) is an educational browser supported repository for resources pertaining to researching, and developing, resilient systems. This presentation provides an overview of the resource's capabilities, and its anticipated impact on the greater community.

Lessons Learned from Implementing New NAS411 Requirements

3D3 – Environment, Safety, & Occupational Health • 23937

Yvonne Pierce

The abstract is pending Boeing Release approval.

Individual and Organizational Systems Engineering Effectiveness

3D4 – Education & Training • 23966

Dr. Nicole Hutchison

Overview of Helix Systems Engineering Effectiveness Model

Agile Insight – Gating Alternatives for Agile Programs

3D1 – Agile • 23814

Larri Rosser

Traditional stage-gate reviews are intended to provide insight and oversight to leaders, stakeholders and program participants, but the current structure and approach doesn't align well with agile product development. In this presentation, we will explore the challenges and potential solutions for overseeing agile programs and

Probabilistic Graphical Models to Support Trade Study Evaluation and Scoring to Support Navy POM Budget Assessments

3D2 – Mission Engineering • 23892

Jason Baker

Probabalistic Graphical Models in the form of Bayesian networks have shown great promise in capturing complex relationships and providing useful analysis. This presentation describes the implementation of PGMs as an aggregation and assessment tool when evaluating the utility of many proposed budget items in a multi-objective and constrained environment.

Impact of the American Innovation and Manufacturing Act on DoD

3D3 – Environment, Safety, & Occupational Health • 23895

Peter Mullenhard

A presentation on the impact of the hydrofluorocarbon (HFC) production phase down required under the American Innovation and Manufacturing Act.

Developing a Digital Engineering Body of Knowledge for the DoD

3D4 – Education & Training • 23770

Philomena Zimmerman | Mary Davidson | Frank Salvatore

The Digital Engineering Body of Knowledge (DEBoK) will serve as a reference for the DoD engineering community to use in implementing digital engineering. The community will be able to contribute content and build digital engineering solutions based on collective experience and knowledge.

ON DEMAND

Performing Mission and System Simulation Trades based on structure, behavior and performance

Modeling & Simulation • 23875

Subodh Chaudhari

This presentation will provide descriptions and demonstrations of the utilization and capabilities of unique technologies that provide Automated evaluation of Mission and Systems architectures, designs, validations and operational performance prediction, enhanced MDAO through the addition of automated variations to CONOPS to multi-disciplinary physics trades, Direct execution and linkage of all 4 elements of MBSE descriptive models with physics-based analysis and simulation tools.

Safety and Environmental Engineering Risks and Requirements Management for the DoD Adaptive Acquisition Framework (AAF)

Environment, Safety, & Occupational Health • 23796

Sherman Forbes

A proposed approach for how the six different Adaptive Acquisition Framework Pathways can identify and manage critical safety and environmental issues that can adversely impact the cost, schedule, and performance of systems across their life cycle. It also provides for a core safety and environmental data set for programs that are transitioning between pathways or using multiple pathways with the data being maintained within the core program data bases (e.g., HAZMAT data in the Logistics Product Data) to facilitate transition to Digital Engineering.

Conducting Safety Review Board Meetings in the Digital Engineering Environment

Environment, Safety, & Occupational Health • 23733

Bob Smith

The future impact of using digital engineering/model-based systems engineering on program interaction with safety review boards.

Leveraging Digital Transformation Initiatives to Optimize Readiness & Simulate Mission Performance Across the Fleet

Digital Engineering • 23805

Justin Woulfe

Over the past twenty years, siloed logistics and supply chain management systems throughout the DoD has led to disparate approaches to modeling and simulation, a lack of understanding of how one system impacts the whole, and issues with "optimal" solutions that are good for one organization but have dramatic negative impacts on another. Many different systems have evolved to try to understand and account for uncertainty and try to reduce the consequences of the unknown. As the DoD undertakes expansive digital transformation initiatives, there is an opportunity to fuse and leverage traditionally disparate data into a centrally hosted source of truth. With a streamlined process incorporating machine learning (ML) and artificial intelligence (AI), advanced modeling and simulation will enable informed decisions guiding program success through optimized operational readiness and improved mission success.

Distributed Integration Launch Assessment Approach

Agile • 23914

Tyle Peterson

In order to provide efficiency to Space Launch Systems, ManTech has developed an approach to complete early integration studies (EIS) that allows distributed organizations to collaborate and ensure mission success. The ManTech-Accelerated Digital Engineering Process Technology (MT-ADEPT) method provides a vendor agnostic fast, useful, and adaptable solution under a single secure ecosystem.

Applying optimization algorithms to system-level trade studies with MATLAB and System Composer

Model-Based Systems Engineering • 23887

Kirsten McCane | Becky Pettey

A design optimization problem is defined and trade analysis is performed using System Composer to identify an optional quadcopter solution

Methods to Evaluate System Resilience Across the Full System Design Lifecycle

Systems Security Engineering • 23790

Tom McDermott

We present methods to extend DoD Mission Focused Cyber Hardening programs to the development of new systems. The “Mission Aware” cyber resilience methodology and modeling approach is extended to support mission resilience analysis, operational simulation, and formal assurance case design.

Architecture for MOSA

Modular Open Systems Approach • 23883

Mike Stokes

This paper will focus on how a System Architecture is developed in a manner that supports the MOSA objectives.

The Convergence of Systems of Systems MBSE and EDA for Early Top-Level Specification Validation During Concept Design for Complex Dynamically Coupled DoD Networked Architectures

Digital Engineering • 23897

Robert Sarkissian

From Mission Architectures to Silicon Architectures. Today’s Mil Aero Systems consist of dynamically coupled architectures driven by the most sophisticated secure silicon devices. The interdependences and emergent behavior of these chips must be correlated to the mission specification and requirements during the concept stage to ensure first pass success. This paper provides a unified methodology for the convergence of MBSE tools and processes to EDA (Electronic Design Automation), proven to reduce risk and uncertainty on several large-scale full vehicle programs.

Modeling and Simulation Body of Knowledge: Collecting Information Critical to the Modeling and Simulation Enterprise

Modeling & Simulation • 23768

Ralph Gibson

Having a thorough knowledge base is vital to successful development, integration, and operation of modeling and simulation systems and federations. This presentation discusses the ongoing effort to build a comprehensive knowledge base to support modeling and simulation activities.

Space Range: Building a Cyber-Physical Digital Twin for Assessing Cyber Resilience

Digital Engineering • 23787

Steven Huang

Space is no longer uncontested. Our space systems must be resilient to not just physical threats but a growing number of cyber threats. ManTech has used its expertise in systems engineering, cyber, and information technology to develop a comprehensive approach to constructing, assembling, and curating comprehensive space system digital twins to execute robust cyber-physical analyses of space systems and concepts. These efforts provide customers a robust and deployable environment that maximally replicates their existing enterprise to perform cyber analysis, execute architectural forklifts, and to practice transformational architectural changes in a realistic and re-configurable environment to enable enhanced decision making.

Intro to S-Series Specifications: Integrated Product Support Data Exchange Strategy

Digital Engineering • 23874

Andre’ Evans

Organizations are at a critical juncture as they transition to a digital environment. The following presentation introduces the S-Series -- an international suite of specifications that uses .XML to author, manage, and exchange Integrated Product Support data across all phases of the product lifecycle.

Applying optimization algorithms to system-level trade studies with MATLAB and System Composer

Digital Engineering • 23887

Kirsten Mcane | Becky Pettey

A design optimization problem is defined and trade analysis is performed using System Composer to identify an optional quadcopter solution.

Leveraging Target Levels and Trade-Off Charts for a Richer Dialog on Customer Requirements (and Supplier Specs/RFQs)

Agile • 23902

Brian Kennedy

As system/mission complexity rises and become more optimized (closer to the edge of feasibility), we need to enable a much richer dialog between customer and supplier, sharing critical knowledge from each side to the other, so that the right trade-off decisions can be made. We propose a solution.

Digital Engineering with Model Based Product Line Engineering: Achieving a Composable Digital Twin

Digital Engineering • 23945

Dr. Bobbi Young

Digital Engineering practices have transformed how we design and build Missiles at Raytheon Missile and Defense Systems. Our digital engineering approach includes: (1) composability by designing modular common components connected through identified standards, (2) Model Based Product Line Engineering combining industry standard Feature-based Product Line Engineering (FbPLE) and Model Based Engineering (MBE) concepts and practices, and (3) implementing digital transformation through digital engineering capabilities to compose a missile’s digital twin. Much more ambitious than simply reusing existing component designs from previously built missiles, this approach involves automatic generation, exploration, and pruning of an automatically generated trade space of possible missile designs that satisfy a given set of requirements. The scope of this presentation is to share how we are applying a Model Based Product Line Engineering approach to digital engineering through a Digital Ecosystem to transform our design process and rapidly achieve the digital twin.

MOSA-sw:3d. Modular Open Systems Approach – Software: Data-processing, Development & Deployment

Model-Based Systems Engineering • 23841

Richard Halliger

Digital Engineering in the field: Pushing implementation and efficient development of data processing and "AI"-enhanced software via MOSA patterns.

Zero Trust – NSS PIT Systems / PIT (A Longstanding Requirement)

Systems Security Engineering • 23771

David Olmstead

Zero Trust is a "Sizzle" Moniker created by John Kindervag in 2010. Trust, without authentication and audit is a delicate brittle concept that is effortlessly broken. A useful Zero Trust state can only exist to a defined useful cryptographic strength based in authentication. This presentation will show from whence the requirement derives for NSS PIT Systems / PIT and how we know its strength.

Take Set-Based Design to the Next Level: Compute All Infinite Possibilities and then Completely Reverse the Design Process!

Agile • 23905

Brian Kennedy

Rather than do a set of point-based analyses to generate a set of point designs, you can do a set-based analysis that computes all infinite points. You can then reverse the design process by selecting the most desirable point and work backwards to determine the corresponding design inputs.

Zero Trust for Hardware Supply Chains: Moving from Absolute Trust to a Quantifiable Assurance Model

Systems Security Engineering • 23762

Joel Heebink

The Zero Trust security model has recently emerged as a strategy to protect electronic hardware. The core design principle of Zero Trust is that no component or actor in the system should be trusted by default or in isolation. Zero Trust should not mean that there is no trust in the system, but rather Zero Trust is about how to make risk-based decisions to grant limited trust in a system based on continuous monitoring and layered security.

Integrating Software and Systems Engineering Tools

Digital Engineering • 23879

Dr. Steven Dam

This paper discusses the integration of software engineering repository tools, such as GitHub, Jira, and Azure DevOps Server with systems engineering tools.

Link-16 Protocol stack modeling and analysis with AADL

Systems Security Engineering • 23854

Dr. Siddhartha Bhattacharyya

With the advancement of technology, the complexity of systems has increased, as a result, it is even more important today to integrate architecture modeling and analysis of systems much earlier in the design phase. Modeling and analysis supports capturing architectural inconsistencies, conflicts, security or safety violations before it becomes costlier to make a change. We discuss in our proposed approach to investigate the implementation of a layered modeling paradigm for Link-16 in Architecture Analysis and Design Language (AADL) with assume-guarantee based reasoning. AADL allows us to create an abstract representation of the link-16 stack protocol. With this representation, we can model properties of the individual stack layers such as security, latency, and quality of performance. When interlayer behaviors are incorporated, we allow for a higher-level analysis of these properties through the use of compositional verification which guarantees the behavior of a system whether it be mission-critical, safety-critical or security-critical.

Evaluating Chemical and Material (C/M) Content Data in the DoD Supply Chain

Environment, Safety, & Occupational Health • 23849

Emma Williams

This session features an overview of a pilot assessment conducted to evaluate two of the U.S. Department of Defense's (DoD) existing data systems to (1) search for needed environment, safety and occupational health (ESOH) data | (2) find gaps in policy implementation | and (3) develop a process to search for chemical and material content data with the current information technology (IT) resources available.

Reimagining the "Software Engineering Life Cycle" Due to DoD Digital Transformation

Software • 23767

Allan Dianic

Reimagining the software engineering (SwE) process requires reimagining the DoD acquisition process. Modernizing DoD SwE practices for rapid and continuous delivery demands that we engineer and acquire software-enabled systems differently that we have in the past.

Environment, Safety, & Occupational Health

Environment, Safety, & Occupational Health • 23896

Michael Bruckner

This session highlights the various aspects of sustainability analysis as detailed in the U.S. Department of Defense's (DoD) Sustainability Analysis Guidance: Integrating Sustainability into Acquisition Using Life Cycle Assessment including demonstrating the value added and identifying how the guidance remains integral to the defense acquisition community.

NAVIGATE-3D – The NEPA Analysis and Visualization Interactive Geospatial Alternatives Tool for the Environment

Environment, Safety, & Occupational Health • 23789

Jennifer Salerno

Under increasing scrutiny, Federal agencies are facing pressure to conduct environmental reviews—particularly for National Environmental Policy Act (NEPA) projects—in an expedited manner. Booz Allen's web-mapping tool, the NEPA Analysis and Visualization Interactive Geospatial Alternatives Tool for the Environment, or NAVIGATE-3D, is an easy-to-use 2D and 3D GIS tool to comprehensively help the user to visualize and identify environmental baseline conditions and potential impacts. Data outputs from the tool, such as maps and tables, allow the user to illustrate and document existing conditions easily and efficiently for environmental compliance reports.

Data Architecture and Strategy to Support Weapons Systems Engineers

David Stuart

Engineers have moved beyond the era of computer modeling and now entered the era of AI/ML where the amount of data needed is exploding, and the previous methodologies used to deal with data are no longer adequate. ERS has developed tools and strategies to support AI/ML projects for engineers.

A Systematic Mapping Study of Systems Security Engineering for Modular Open Systems

Architecture • 23835

Giselle Bonilla-Ortiz

This paper describes the design and execution of a systematic mapping study to identify security concerns, threat vectors and security mechanisms as described for modular open systems in literature. The aim is to build on this knowledge of security considerations to further the research in this area. Research questions will be presented as well as a data synthesis and driving conclusions based on the publications reviewed.

Introduction to Air Force Occupational and Industrial Hygiene Program: Electronic Safety Data Sheet Initiative

Environment, Safety, & Occupational Health • 23886

Jonathan Luu

The Air Force Occupational and Industrial Health Program aims to amplify the speed, precision and accuracy of Hazardous Material identification and communication.

Automatically Measuring Inter-Disciplinary Program Execution Metrics Using a Digital Thread

Digital Engineering • 23834

Kenneth Heyen

In this presentation we show how use of digital thread technology can result in the ability to automatically capture meta data regarding inter team collaboration and data transfer. We show how that data can be used in a way to enable data-based decision making by program leaders.

Synchronizing custom software middleware concepts between C++ source code and Magic Draw using a digital thread

Digital Engineering • 23833

Kenneth Heyen

This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations. Traditional model based software engineering approaches have been able to achieve forward and reverse engineering operations between models and code for a number of years. However, these approaches are limited in that they only understand the standard features of a programming language. Advanced software concepts such as middleware, multi-threading and messaging patterns are commonly used across multiple industries. SysML and UML have the appropriate relationship and meta-class definitions to represent these patterns. Despite their prevalence, reverse and forward engineering support for these concepts are unsupported out-of-box by traditional model based software toolsets. This occurs because these concepts often use third party software packages that are not part of the C++ language standard. Since each implementation of these concepts follows its own pattern it would be extremely difficult, if not impossible for vendors to maintain support. In this paper we show that we can maintain synchronization between source code and a cameo model by teaching a model based semantic broker about these concepts. Enabling synchronization via this method requires a few steps. First, creating an ontology that describes the concepts we want to synchronize. Second, enabling “reverse” code engineering by indexing of the source code via an open source indexer (ANTLR). Third, enabling “forward” generation via a template engine (JINJA). Finally we show that once the semantic broker is enabled we can easily synchronize between the source code and the model of the software. We will then show how this technique can be used to maintain traceability between the software requirements and the software itself.

BIOGRAPHIES

LT GEN ERIC FICK, USAF

Program Executive Officer
F-35 Lightning II Joint Program Office

Lt. Gen. Eric T. Fick is the Program Executive Officer for the F-35 Lightning II Joint Program Office in Arlington, Virginia. The F-35 Lightning II Joint Program Office is the DoD's agency responsible for developing, delivering and sustaining the F-35A/B/C, the next-generation strike aircraft weapon system for the Air Force, Navy, Marine Corps, seven international partners and six current foreign military sales customers.

Lt. Gen. Fick entered the Air Force in September of 1990 after graduating from the University of Notre Dame with a Bachelor's degree in Aerospace Engineering. He has served as a Logistics Plans and Programs Officer, F-16Fighting Falcon Mechanical Systems Engineer, Computational Fluid Dynamics Research Engineer, Joint System Program Office Chief of Test, Air Staff Branch Chief, Deputy Chief of the Air Force Senate Liaison Office and Director of Global Reach Programs, Office of the Assistant Secretary of the Air Force for Acquisition. Lt. Gen. Fick has commanded at the squadron and group level and previously served twice as an Air Force Program Executive Officer. Additionally, he has logged more than 350 hours in the T-38 Talon, F-15 Eagle, F-16 and other military and civilian experimental aircraft.

Prior to his current assignment, Lt. Gen. Fick was the Deputy Program Executive Officer for the F-35 Lightning II Joint Program.

THE HONORABLE HEIDI SHYU

Under Secretary of Defense for Research and Engineering (OUSD(R&E))
Department of Defense

Ms. Heidi Shyu is the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). In this role, she serves as the Chief Technology Officer for the Department of Defense (DoD), mandated with ensuring the technological superiority of the U.S. military, and is responsible for the research, development, and prototyping activities across the DoD enterprise. She also oversees the activities of the Defense Advanced Research Projects Agency (DARPA), the Missile Defense Agency (MDA), the Defense Innovation Unit (DIU), the Space Development Agency (SDA), the DoD Laboratory and Engineering Center enterprise, and the Under Secretariat staff focused on developing advanced technology and capability for the U.S. military.

Previously, she served as the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), from September 2012 to January 2016. Prior to this, she was Acting ASA(ALT) beginning in June 2011 and appointed the Principal Deputy in November 2010. As the ASA(ALT), she served as the Army Acquisition Executive, the Senior Procurement Executive, the Science Advisor to the Secretary of the Army, and the Army's Senior Research and Development official. She had principal responsibility for all Department of the Army matters related to logistics. Ms. Shyu also led the execution of the Army's acquisition function and the acquisition management system. Her responsibilities included providing oversight for the life cycle management and sustainment of Army weapons systems and equipment from research and development through test and evaluation, acquisition, logistics, fielding, and disposition.

Prior to her government service, Ms. Shyu was the Vice President of Technology Strategy for Raytheon Company's Space and Airborne Systems.

Ms. Shyu holds a Bachelor of Science Degree in Mathematics from the University of New Brunswick (UNB) in Canada, a Master of Science Degree in Mathematics from the University of Toronto, Master of Science Degree in System Science (Electrical Engineering) from UCLA, and the Engineer Degree from UCLA. She received an Honorary Doctorate of Science from the UNB. She is also a graduate of the UCLA Executive Management Course Program.

A member of the Air Force Scientific Advisory Board from 2000 to 2010, she served as the Vice Chairman from 2003 to 2005 and Chairman from 2005 to 2008. Ms. Shyu is a member of the National Academy of Engineering and AIAA Honorary Fellow.

WESLEY KREMER

President
Raytheon Missiles & Defense

Wesley D. Kremer is president of Raytheon Missiles & Defense, a business of Raytheon Technologies. He leads 31,000 employees and is responsible for a broad portfolio of air and missile defense systems, precision weapons, radars, command and control systems and advanced defense technologies.

Kremer, an electrical engineer and U.S. Air Force veteran, has decades of executive experience in aerospace and defense. He held multiple leadership positions at Raytheon Company prior to its merger with United Technologies Corporation in 2020, including president of both the Raytheon Missile Systems and the Integrated Defense Systems businesses. In the U.S. Air Force, he served as a weapon systems officer on F-111 and F-15E aircraft and flew more than 90 combat sorties in Iraq and Bosnia.

He holds a bachelor's degree in electrical engineering

DR. RAYMOND O'TOOLE JR.

Acting Director, Operational Test and Evaluation
Office of the Secretary of Defense

Dr. O'Toole is the Acting Director, Operational Test and Evaluation as of January 20, 2021. Dr. O'Toole was appointed as the Principal Deputy Director, Operational Test and Evaluation in February 2020. In this capacity he is the principal staff assistant for all functional areas assigned to the office. He participates in the formulation, development, advocacy, and oversight of policies of the Secretary of Defense and in the development and implementation of test and test resource programs. He supports the Director in the planning, conduct, evaluation and reporting of operational and live fire testing. He serves as the Appropriation Director and Comptroller for the Operational Test and Evaluation, Defense Appropriation and the principal advisor to the Director on all Planning, Programming, and Budgeting System matters.

Dr. O'Toole is the former Deputy Director for Naval Warfare within DOT&E. He oversaw the operational and live-fire testing of ships and submarines and their associated sensors; combat and communications systems, and weapons. He was also responsible for overseeing the adequacy of the test infrastructure and resources to support operational and live-fire testing for all acquisition programs across the Defense Department.

Dr. O'Toole was previously an employee of the Naval Sea Systems Command as the Deputy Group Director of Aircraft Carrier Design and Systems Engineering. Prior to that, he was the Director of Systems Engineering Division (Submarines and Undersea Systems) where he led a diverse team of engineers who supported all Submarine Program Managers. His other assignments include being a Ship Design Manager/Navy's Technical Authority for the USS VIRGINIA Class submarines during design and new construction and for Amphibious Ships, Auxiliary Ships, and Command & Control Ships during in-service operations.

Dr. O'Toole has also held other positions within the Department of Defense such as Deputy Program Executive Officer (Maritime and Rotary Wing) at the United States Special Operations Acquisition Command, Staff to the Deputy Assistant Secretary of the Navy for Research, Development & Acquisition (Ship Programs), and Deputy Director of Regional Maintenance for COMPACFLT (N43).

In addition, Dr. O'Toole has over 30 years of experience as a Naval Officer (Active and Reserve) retiring at the rank of CAPTAIN. His significant tours include 5 Commanding Officer tours.

DAVID CADMAN

Acting Deputy Assistant Secretary of Defense, Acquisition Enablers
Department of Defense

Mr. David S. Cadman is currently serving as the Acting Deputy Assistant Secretary of Defense, Acquisition Enablers. He also serves as the Director for Acquisition Data and Analytics (ADA) where he is responsible for the development and implementation of acquisition portfolio based analytical methods focused on data analytics which includes but is not limited to data mining, simulation, machine and statistical learning, probability theory, mathematical optimization, and visualization of results. ADA establishes program management policy that applies these methods as appropriate to acquisition portfolios, Major Defense Acquisition Programs and business systems and functions.

Before the A&S reorganization, he served as Director for Performance Assessments and Root Cause Analyses (PARCA) and Deputy Director, Root Cause Analyses (RCA). Where he identified root causes on Major Acquisition Programs that had a critical Nunn-McCurdy cost breach or upon request of the Secretary of Defense.

Additional assignments Mr. Cadman has had while at the Office of the Secretary of Defense (OSD) include serving as Deputy Director for the Technology Security and Foreign Disclosure Office (TSFDO) within the Defense Technology Security Administration (DTSA) where he supported DoD's security cooperation efforts, to include international armaments cooperation, strategic planning, and Defense Technology and Trade Initiatives. Mr. Cadman also worked as the aviation sector lead for the Office of Industrial Policy in OSD where he was responsible for industrial base oversight. In this role, Mr. Cadman assessed the capabilities and overall health of the aviation industrial base upon which the Department of Defense relies for current and future war fighting capabilities.

Previously, Mr. Cadman served in the Joint Strike Fighter (JSF) Program Office as the Deputy Director, Air Vehicle where he oversaw government and contractor activities related to the F-35's vehicle systems, mission systems, airframe structures and materials, manufacture and build risk reduction. Mr. Cadman was accountable for cost, schedule, and performance on the $13 billion air vehicle design and the development effort of the multinational industry team. Mr. Cadman also served as the JSF X-program Science and Technology Coordinator developing requirements, assessing science and technology trends, and evaluating potential technology gaps. Mr. Cadman's other positions include a leading role on the F/A-18 E/F airframe development program and serving as an F-14 structural engineer at the Naval Aviation Depot. Prior to entering federal service, Mr. Cadman worked for Boeing Helicopter, performing dynamic analysis of developmental vertical lift aircraft.

Mr. Cadman holds a Bachelor of Science in Aerospace Engineering from the University of Maryland and a Master's of Science in National Resource Strategy from the Industrial College of the Armed Forces. Mr. Cadman is a graduate of the Defense Acquisition University Advanced Program Managers course and has Acquisition Workforce Level III certifications in Program Management; Systems Planning, Research and Engineering; and Production Quality and Manufacturing.

SPONSOR DESCRIPTIONS

PREMIER

SAIC® is a premier Fortune 500® technology integrator driving our nation's technology transformation. Our secure high-end solutions across the defense, space, civilian, and intelligence markets include engineering, digital, artificial intelligence, and mission solutions. Headquartered in Reston, Virginia, SAIC has more than 26,500 employees and annual revenues of about $7.1 billion.

ELITE

AMERICAN SYSTEMS is an employee-owned federal government contractor supporting national priority programs through our strategic solutions in the areas of: Enterprise IT, Test & Evaluation, Acquisition & Lifecycle Support, Engineering & Analysis, and Training. AMERICAN SYSTEMS is at the forefront of Research and Engineering modernization priorities to further our National Defense Strategy. We work with a broad portfolio of Science & Technology programs, liaise with Academia and Federally Funded Research Centers, and assist in the development of investment strategy through mission analysis in areas such as 5G, Microelectronics, Hypersonics, Directed Energy, and C4ISR. We develop and assess future joint warfighting concepts through digital engineering, modeling & simulation, data analytics, and wargaming. We support the services and Joint missions by modernizing legacy architectures through mission engineering of new capabilities and operations. For more information, please visit: www.AmericanSystems.com

HANDOUT AND VIDEO

Raytheon Missiles & Defense brings global customers the most advanced end-to-end solutions delivering the advantage of one innovative partner to detect, track, and intercept threats. With a broad portfolio of air and missile defense systems, precision weapons, radars, command and control systems and advanced defense technologies Raytheon Missiles & Defense solutions protect citizens, warfighters and infrastructure in more than fifty countries around the world.

REGISTRATION

From the mission to the microchip, AGI and Ansys software help transform your digital engineering enterprise at the speed of your needs. AGI's mission-level software helps engineers, operators, and analysts working on land, sea, air, and space systems. Our combined portfolio of simulation and analysis tools help aerospace and defense organizations make critical decisions faster throughout the life cycle — from concept design to operations and sustainment — in an operational context.

jama software®

CONTRIBUTING

Jama Software is focused on maximizing innovation success. Numerous firsts for humanity in fields such as fuel cells, electrification, space, autonomous vehicles, surgical robotics, and more all rely on Jama Connect® to minimize the risk of product failure, delays, cost overruns, compliance gaps, defects, and rework. Jama Connect® uniquely creates Living Requirements™ that form the digital thread through siloed development, test and risk activities to provide end-to-end compliance, risk mitigation, and process improvement. Our rapidly growing customer base of more than 12.5 million users across 30 countries spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, financial services, and insurance industries.

SPEC INNOVATIONS

VIDEO

SPEC Innovations (Systems and Proposal Engineering Company) has been a leader in mission systems engineering, since 1993. Our goal is to move the systems engineering discipline into the future. We developed and released the first collaborative cloud-native MBSE tool, Innoslate, in 2012. Since then, we have evolved Innoslate into a full lifecycle solution through requirements management to verification and validation.

SPEC Innovations continues to push the boundaries of the systems engineering discipline by recognizing that both program management and systems engineering must optimize cost, schedule, and performance for both the program and system, while identifying and managing risk. We do this by applying open standards, such as the Lifecycle Modeling Language (LML), and new technologies, such as cloud computing and artificial intelligence. We are the future of systems engineering, today. SPEC Innovations newest software product, Sopatra, develops and simulates SOP models from text using natural language processing.

Caltech

VIDEO

Systems engineering education for the national security enterprise

At Caltech, we customize unique learning experiences for organizations and their people, working one-on-one with leadership to design practical programs and certificate courses for teams and individuals alike.

With programs that span the systems spectrum, we drive digital readiness and scale teams of high-performance thinkers and doers who develop technologies and ideas to advance science, build connective systems, and secure a sustainable world.

Over 10,000 professionals have turned to Caltech for education tailored to the defense industrial base, government agencies, and research institutes across aerospace, electronics, energy, and life sciences.

#BuildingBetterInnovators

LEADING THE WAY IN ENGAGEMENT, NETWORKING, AND NATIONAL DEFENSE

PLAN AHEAD FOR SUCCESS | 2022 FEATURED MEETINGS, CONFERENCES, AND EVENTS

2022 VIRTUAL EXPEDITIONARY WARFARE CONFERENCE

February 8 – 10, 2022 | Virtual

Expeditionary | Strategic Sealift | Joint All Domain | Force Protection

2022 UNDERSEA WARFARE SPRING CONFERENCE

March 28 – 30, 2022 | San Diego, CA

Aviation USW | C4I | Mine Warfare | Undersea Sensors & Vehicles | Warfighter Performance

2022 AIRCRAFT SURVIVABILITY SYMPOSIUM*

February 15 – 17, 2022 | Monterey, CA

Combat Survivability | Concealment and Deception | Countermeasures | Urban Warfare | Vulnerability Reduction

2022 JOINT NDIA/AIA SPRING INDUSTRIAL SECURITY CONFERENCE

April 25 – 27, 2022 | Clearwater Beach, FL

Industrial Security | Insider Threat | Cybersecurity/CMMC | NISPOM Updates

2022 TACTICAL WHEELED VEHICLES CONFERENCE

February 28 – March 2, 2022 | Norfolk, VA

Autonomous Vehicles | Electric Drive | Modernization & Sustainment | Acquisition

22ND ANNUAL SCIENCE & ENGINEERING TECHNOLOGY CONFERENCE

April 26 – 28, 2022 | Miami, FL

Defense Research & Development | Science & Technology

2022 PACIFIC OPERATIONAL SCIENCE & TECHNOLOGY (POST) CONFERENCE**

March 7 – 8 (Open), **9 – 10** (Closed), **2022 | Honolulu, HI**

Regional Security | Science & Engineering Technology | Technology Engagement

65TH ANNUAL FUZE CONFERENCE

May 10 – 12, 2022 | Seattle, WA

Fuze | Missiles | Munitions Technology | Safety & Arming Devices | Warheads

36TH ANNUAL NATIONAL LOGISTICS FORUM

March 15, 2022 | Salt Lake City, UT

Defense Logistics | Logistics Management

2022 SPECIAL OPERATIONS FORCES INDUSTRY CONFERENCE & EXHIBITION (SOFIC)

May 16 – 19, 2022 | Tampa, FL

Communications | Light Vehicles | Small Arms | Special Operations

*All Classified | **Partially Classified

VISIT NDIA.ORG FOR MORE INFORMATION ON ALL OF OUR MEETINGS, CONFERENCES, AND EVENTS

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

A Plugin for Information Security Marking of MagicDraw Models

Version 1.0.1

Tom Alberi
GBSD Assistant Program Manager (Ground Systems)
Weapon Systems Engineering Group Chief Scientist
Johns Hopkins Applied Physics Laboratory

DISTRIBUTION STATEMENT A:
Approved for public release.

Agenda

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

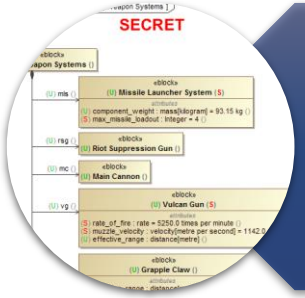
Presentation Objectives


DoD Humanitarian Assistance Activities
Fiscal Year 1996

April 1997

Office of the Assistant Secretary of Defense for Strategy and Requirements

Describe the motivation behind the development of the plugin



Present the latest version of APL's Information Security Plugin for MagicDraw

Generate community interest in the plugin

- Distribute version 1.0.1 to a broader community
- Determine if a model marking standard can be established across the modeling community

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Background

Motivation for the Plugin

In some industries, there are policies and procedures for protecting sensitive information

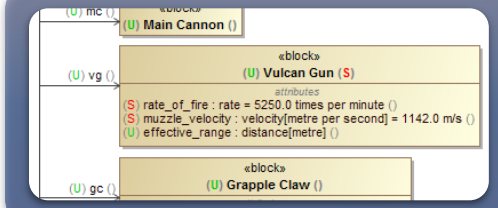
- Example: Department of Defense (DoD) Information Security Program for classified information
- Example: An organization's internal policies and procedures to protect their inventions and trade secrets

Marking is a key component of information security processes

- If the information is properly marked, then it's clear how the information should be handled

Traditional documents and information media have well-defined marking and identification procedures

- Example: DoD has explicit procedures for marking documents, briefing slides, e-mail, web pages and even instant messages (DoD Manual 5200.01 Volume 2)



Marking and identification procedures not as well defined for elements within MBSE models

- Model structures are more complex than traditional documents
- Many information security marking methods are possible, leading to lack of standardization

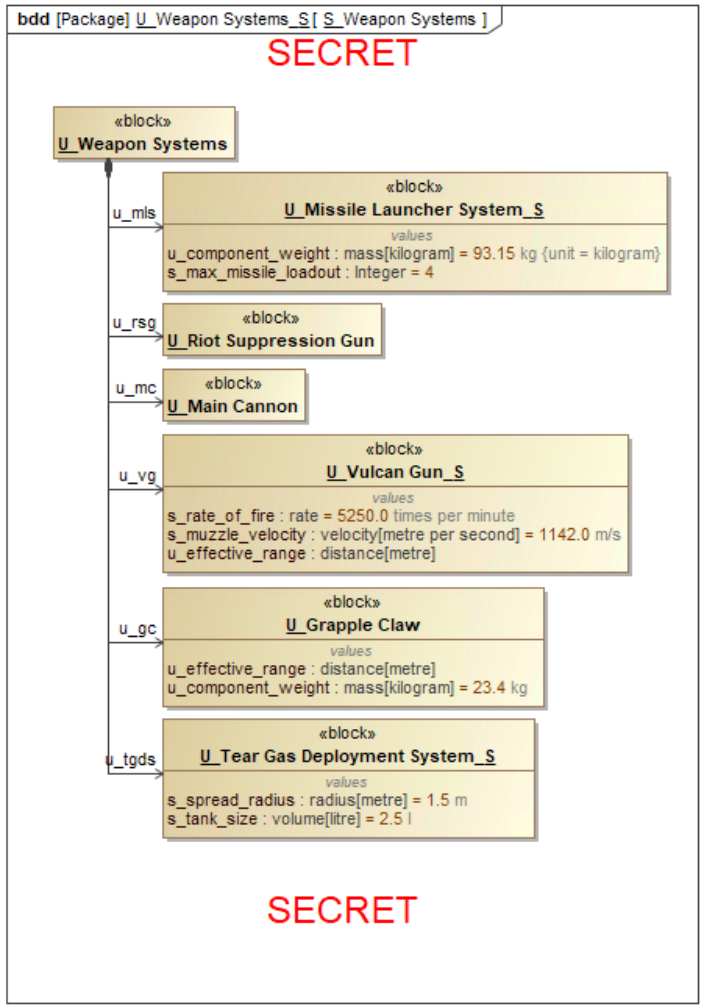
UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Background

Information Security Plugin History

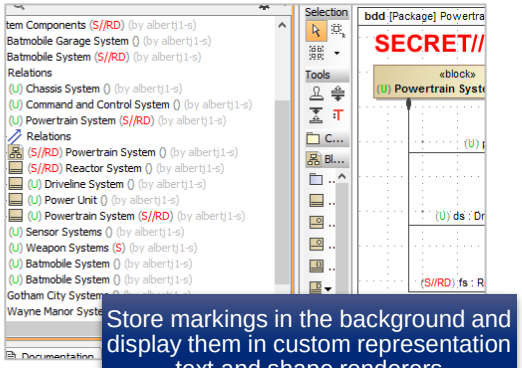
- APL developed the Information Security Plugin for MagicDraw initially during a 2019 internal research and development project
- The original plugin provided several capabilities:
  - Leveraged element names to capture portion and containment markings
  - Validated element containment markings based on child portion markings
  - Validated diagram portion markings based on the portion markings of displayed elements
  - Implements markings database XML file to define available markings and rules for how they are applied and formatted
- Version 0.1 Beta was released to several organizations for beta testing
  - Additional beta releases followed with incremental improvements
- Several improvements were requested as a result of beta testing and conferences presentations
  - Improved marking performance and appearance
  - Automated marking options
  - Usability improvements

Version 0.1 Beta

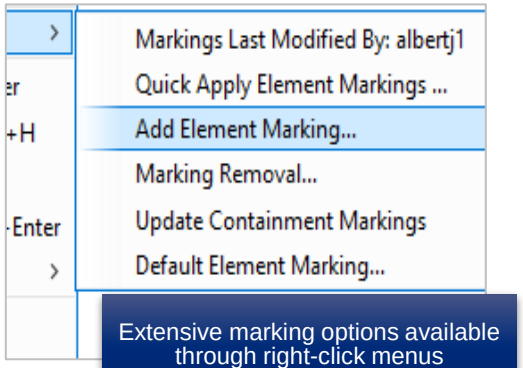


UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Highlights of Latest Plugin Version



Store markings in the background and display them in custom representation text and shape renderers



Extensive marking options available through right-click menus

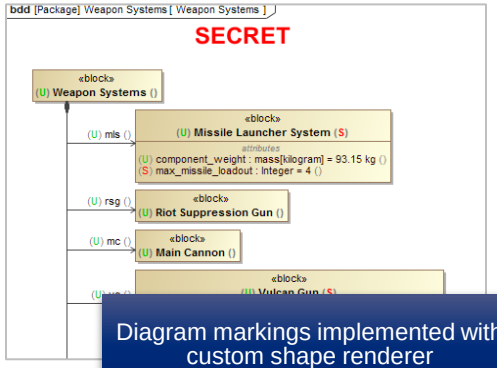
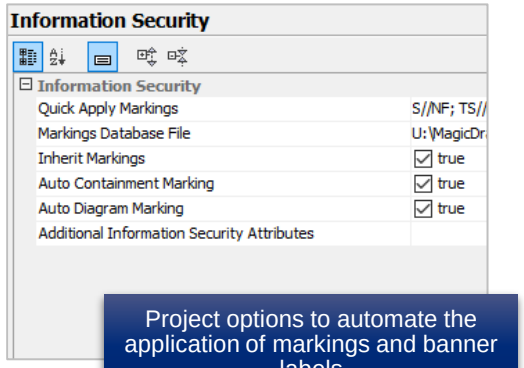
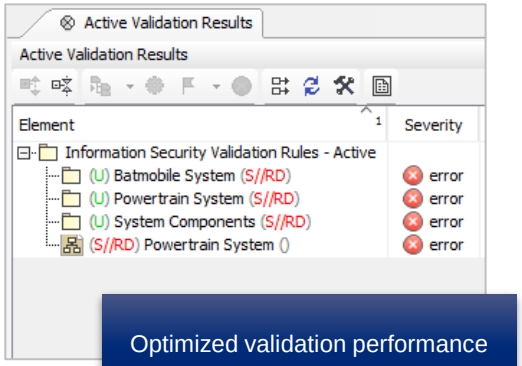


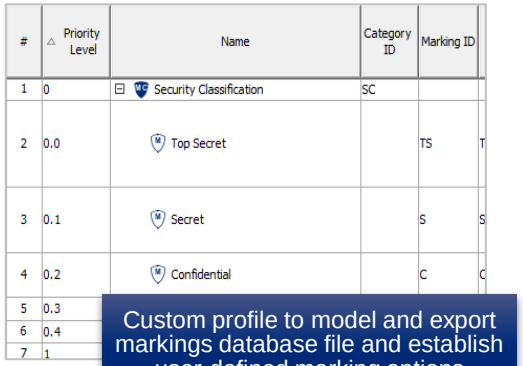
Diagram markings implemented with custom shape renderer



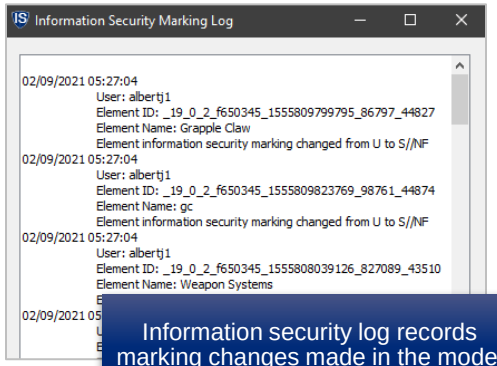
Project options to automate the application of markings and banner labels



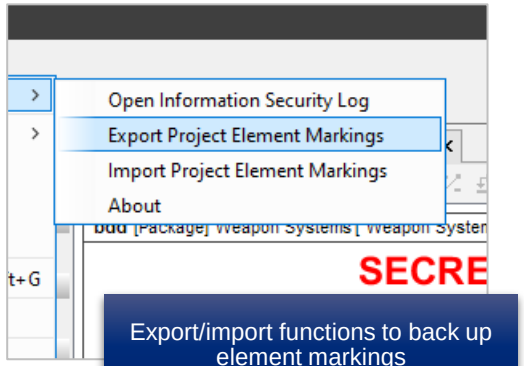
Optimized validation performance



Custom profile to model and export markings database file and establish user-defined marking options



Information security log records marking changes made in the model



Export/import functions to back up element markings

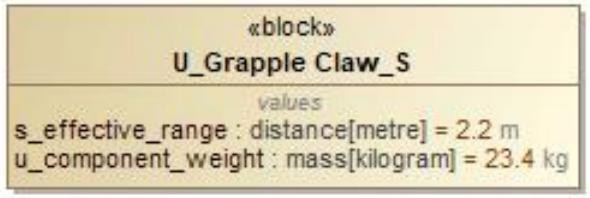
UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Plugin Capabilities

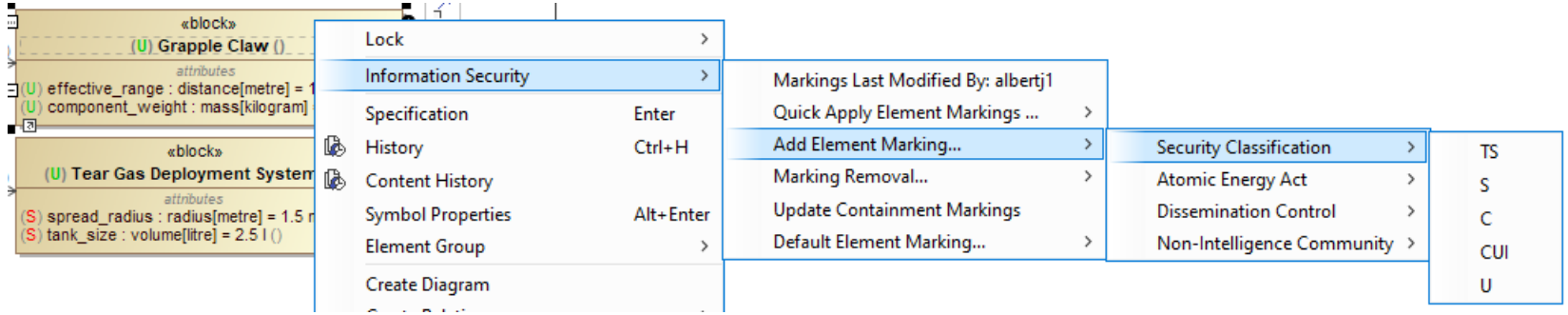
Element Marking

- Version 0.1 Beta used the element name field to capture portion and containment markings
  - Not all element types have names
  - May not want to modify the name of an element just to include information security markings
- In version 1.0.1, markings are now stored in the background as an invisible project option
  - Works for all element types
  - No need to modify any element properties
  - Modifiable through menu actions
  - Made visible through custom representation text and shape renderers
- Additional marking capabilities
  - Quick marking application
  - Default marking for new elements
  - Marking removal

Version 0.1 Beta



Version 1.0.0

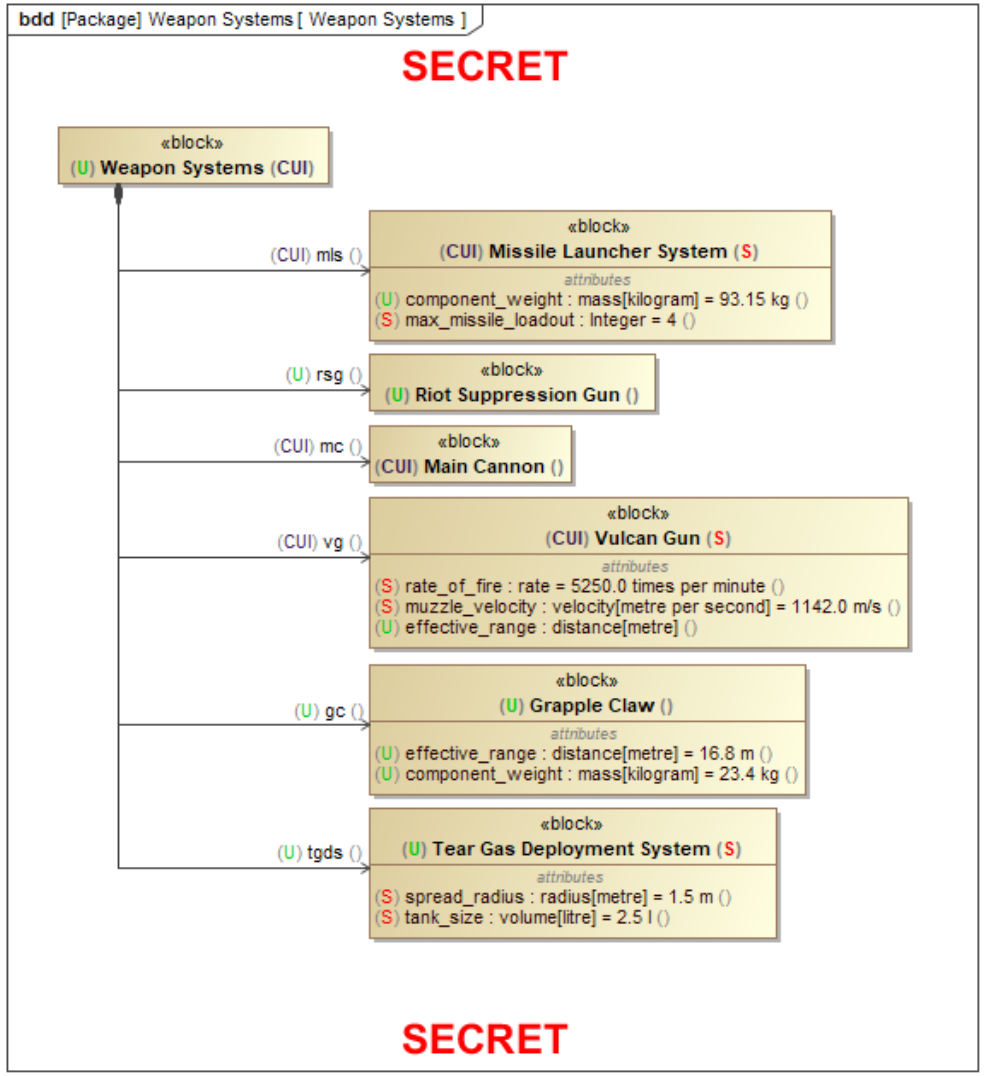


UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Plugin Capabilities

Diagram Banner Labels

- Banner labels automatically applied to diagrams, based on diagram portion marking
- Version 0.1 Beta used text boxes on diagram to apply labels
  - Text box content and position were modifiable by the user
  - Issues with updating banner labels when other text boxes were on the diagram
- Version 1.0.1 uses a custom diagram shape renderer to apply banner labels
  - Not modifiable by the user without changing diagram markings
  - Labels appear on all diagrams (with exceptions of diagrams like tables and relationship maps)
  - Labels appear in diagrams exported from the model, such as in reports generated from the Report Wizard



UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Plugin Capabilities

Specifying Available Markings

- Available markings are specified in the Markings Database XML file
- Database file includes rules that enforce marking patterns and formatting
- Project option is used for specifying the location of the database file
- A profile (with included report template) is provided for modeling a marking database and exporting the XML file

```
<markingsDatabase>
    <markingCategories>
        <markingCategory id="SC">
            <name>Security Classification</name>
        </markingCategory>
        <markingCategory id="AEA">
            <name>Atomic Energy Act</name>
        </markingCategory>
        <markingCategory id="DC">
            <name>Dissemination Control</name>
        </markingCategory>
        <markingCategory id="NIC">
            <name>Non-Intelligence Community</name>
        </markingCategory>
    </markingCategories>
    <markings>
        <marking id="TS" category="SC">
            <bannerMarkingFull>TOP SECRET</bannerMarkingFull>
            <bannerMarkingShort>TOP SECRET</bannerMarkingShort>
            <portionMarking>TS</portionMarking>
            <dontUseInSuffix>false</dontUseInSuffix>
            <overmarks>
                <overmark>S</overmark>
                <overmark>C</overmark>
```

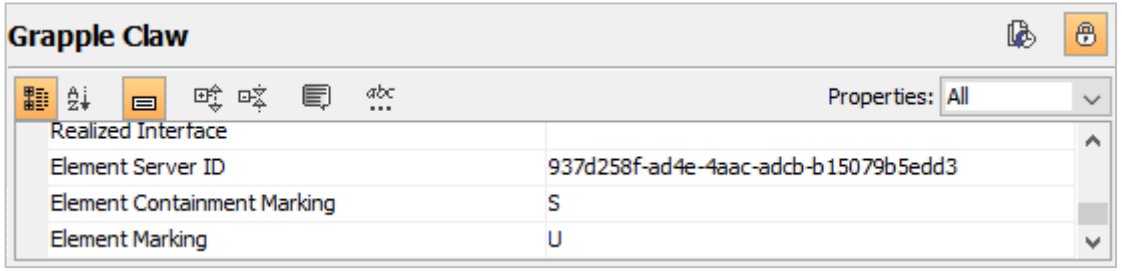
#	Priority Level	Name	Category ID	Marking ID	Banner Marking Full	Banner Marking Short	Portion Marking	Dont Use In Suffix	Overmarks	Incompatible With	Marking Color Red Value	Marking Color Green Value	Marking Color Blue Value
1	0	Security Classification	SC										
2	0.0	Top Secret		TS	TOP SECRET	TOP SECRET	TS	false	0.1 Secret 0.2 Confidential 0.4 Unclassified 0.3 Controlled Uncl		255	128	0
3	0.1	Secret		S	SECRET	SECRET	S	false	0.2 Confidential 0.4 Unclassified 0.3 Controlled Uncl		255	0	0
4	0.2	Confidential		C	CONFIDENTIAL	CONFIDENTIAL	C	false	0.4 Unclassified 0.3 Controlled Uncl		0	0	205
5	0.3	Controlled Unclassified Information		CUI	CUI	CUI	CUI	false	0.4 Unclassified		60	27	88
6	0.4	Unclassified		U	UNCLASSIFIED	UNCLASSIFIED	U	true			0	205	0
7	1	Atomic Energy Act	AEA										
8	2.0	Restricted Data		RD	RESTRICTED DATA	RESTRICTED DATA	RD	false			0	0	0
9	2.1	Formerly Restricted Data		FRD	FORMERLY RESTRICTED DATA	FORMERLY RESTRICTED DATA	FRD	false			0	0	0

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

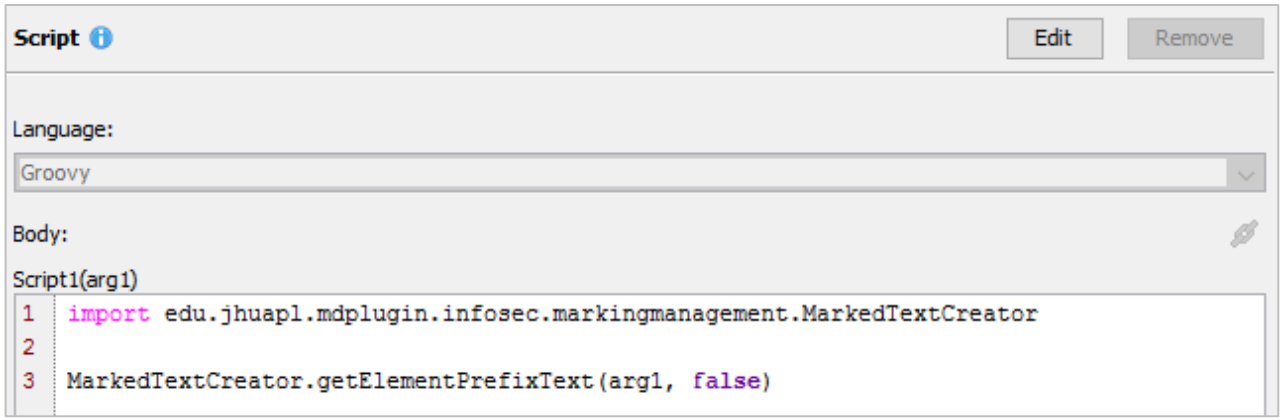
Plugin Capabilities

Access to Element Marking Information

- In addition to visual display of element markings, marking data can be accessed through two additional means:
  - Derived properties provided in Element meta class customization in the validation rule model



  - Plugin API

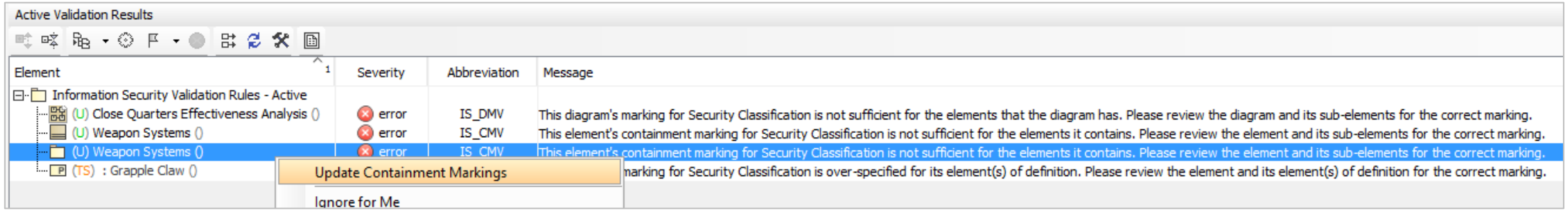


UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Plugin Capabilities

Marking Verification

- Validation rules are provided to verify some marking aspects
  - Corrective actions are included
- Containment marking verification
  - Verify that an element's containment marking is consistent with the strictest portion markings of all of its child elements, recursively
- Diagram marking verification
  - Verify that a diagram's portion marking (and banner labels) are consistent with the strictest portion markings of all of the elements depicted in the diagram
- Usage element marking verification
  - Verify that an element of usage (part property, call behavior action, etc.) has a portion marking that is consistent with the marking of its element of definition (type, activity, etc.)
  - Only active when the "Inherit Markings" project option is enabled



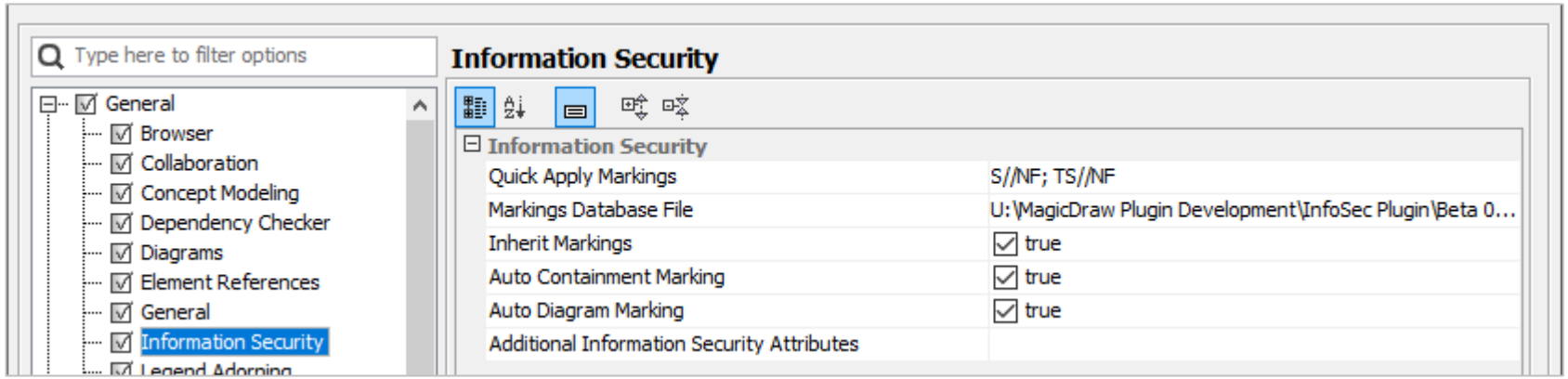
UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Plugin Capabilities

Automation Options

- Several project options available to automate the application of information security markings
- Inherit Markings
  - Elements of usage (types elements, call behavior actions, etc.) inherit prefix markings from their elements of definition (types, activities, etc.)
- Auto Containment Marking
  - Element containment markings will automatically update as child element prefix markings change
- Auto Diagram Marking
  - Diagram prefix markings update as prefix markings of elements in the diagram change
  - Does not currently work for certain diagram types like tables and relationship maps

NOTE: Enabling automated options will negatively impact application performance

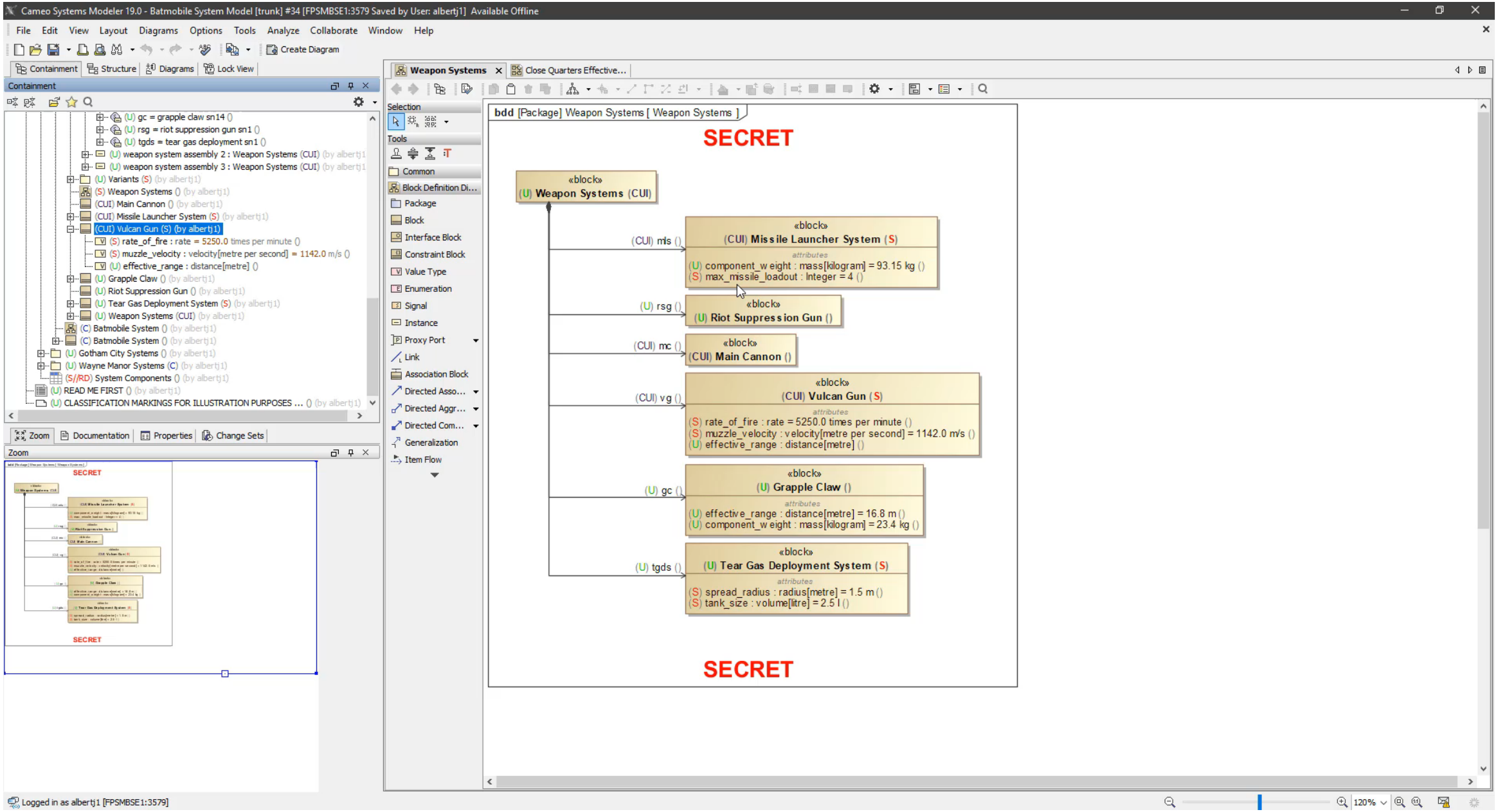


UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

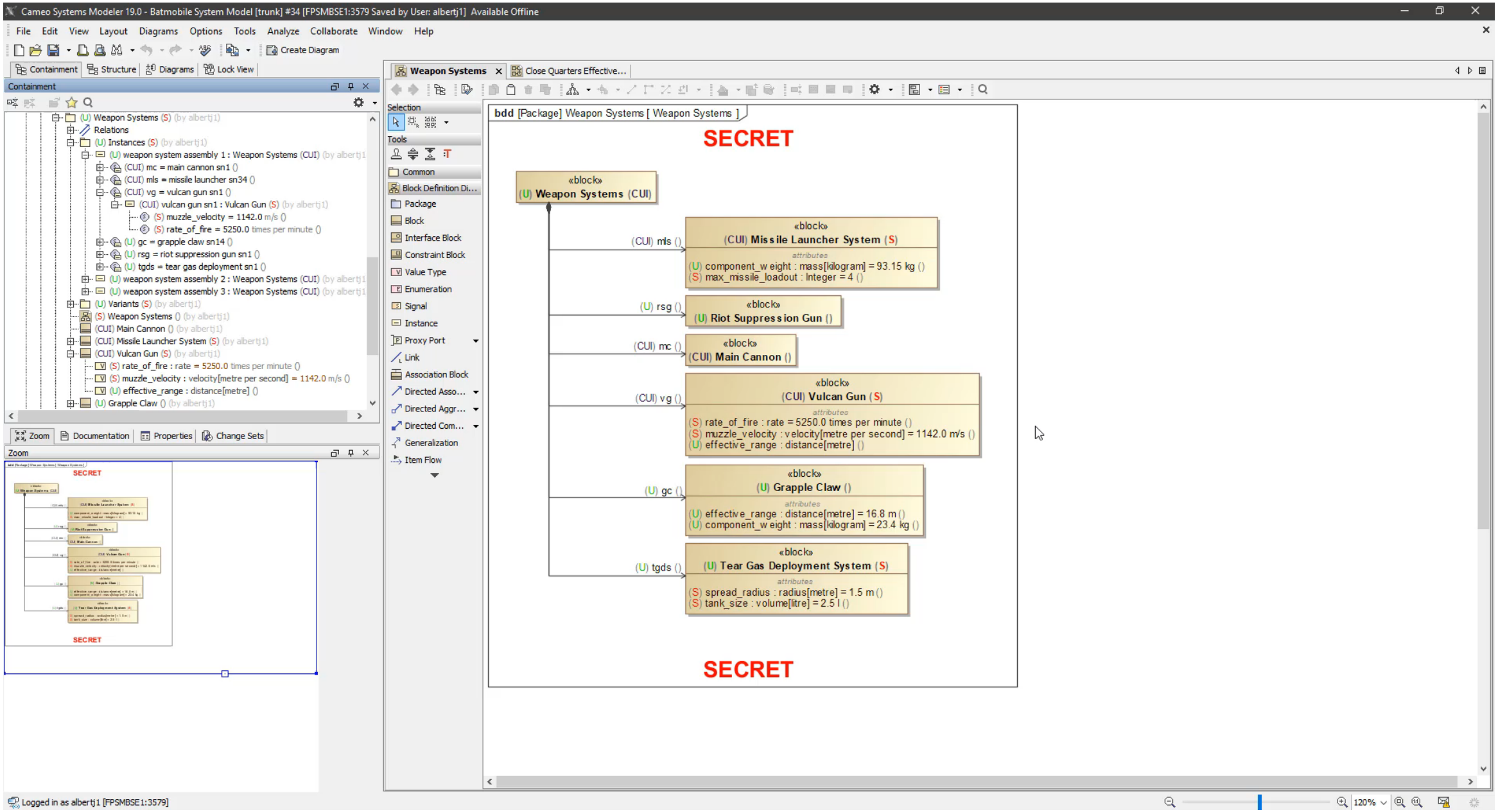
Case Study Example

Batmobile Development Program

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.



UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

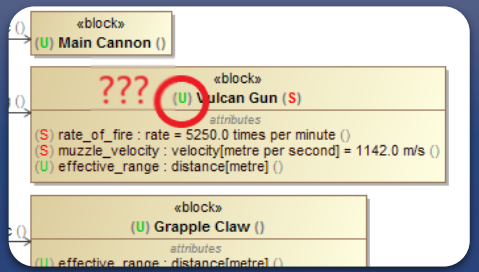


UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Future Development

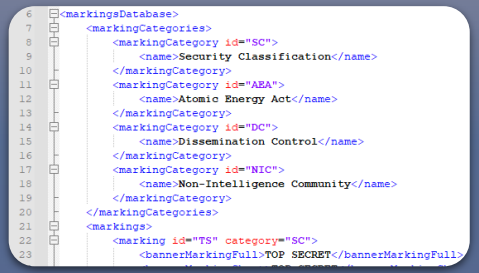
Improve performance, update capabilities, and fix bugs

- Leverage feedback from 1.0.1 release
- Interested in plugin performance for large models
- Identify new feature and capability requests



Verify element *portion markings*

- Integrate a machine readable digital classification guide
- Infer element classification based on it its properties and context within the model
- Notify the user when element portion markings may be in conflict with classification guidance
- Currently in development



Establish a digital information security marking standard

- Work with relevant stakeholders in DoD and beyond
- Support information security in digital engineering (more than just MagicDraw models)

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Version 1.0.1 Now Available!

- Currently available to government organizations
  - Provided under Distribution Statement D government purpose rights
  - Can be distributed by DoD organizations to other organizations as long as they are using the plugin only for DoD work
  - APL is working on method of plugin distribution and licensing for non-DoD uses
- Plugin package includes:
  - Plugin JAR file
  - Example markings database XML file
  - Information Security Validation Profile
  - Information Security Marking Schema Profile
  - Information Security Marking Schema Example Model
  - User manual
- Install via MagicDraw Resource/Plugin Manager
- Contact me for access to the plugin

UNCLASSIFIED. THIS PRESENTATION CONTAINS NO CLASSIFIED MATERIAL. ALL CLASSIFICATION MARKINGS ARE FOR EXAMPLE ONLY.

Questions?

Tom Alberi

Tom.Alberi@jhuapl.edu

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY

The Importance of Metadata for the Discovery of Digital Engineering Artifacts

2021 Virtual Systems and Mission Engineering Conference
December 6-8, 2021

James E. Coolahan, Ph.D.
Coolahan Associates, LLC
3013 Boones Lane
Ellicott City, MD 21042
+1 410-440-2425
jim@coolahan.com

Approved for Public Release

Presentation Outline

- Digital Engineering Strategy – Background, Definition, and Goals
- The Digital Engineering Collaborative Environment for a System
  - A Reference Architecture for Discussion Purposes
  - Resource Discovery Challenges
- Some Potential Discovery Metadata Repository Use Cases
- Metadata Definitions and Background on Two Discovery Metadata Specifications
  - Modeling and Simulation Community of Interest Discovery Metadata Specification (MSC-DMS), Version 1.5, 2012
  - Discovery Metadata Specification for Modeling and Simulation Resources (DMS-MSR), an in-progress product development by the Simulation Interoperability Standards Organization
- Some Potential Resource Types for Inclusion in a Discovery Metadata Repository
- An Illustration of Discovery Metadata Application Using the MSC-DMS Resource Metacard
- Summary

Digital Engineering Background

- New effort on modeling for systems engineering emerged in 2012 in ODASD(SE) under Ms. Philomena Zimmerman and the Acquisition M&S Working Group (AMSWG)
  - Initially known as the “System Model”; evolved to be called the “Digital System Model” (DSM)
- By early 2016, the DSM and engineering/modeling efforts surrounding it were re-named and expanded to be termed “Digital Engineering” by Mr. Stephen Welby [DASD(SE)]
- *Digital Engineering Strategy* issued by Dr. Michael Griffin [USD(R&E)] in June 2018

Source: *Digital Engineering Strategy*, June 2018

Digital Engineering Definition and Goals

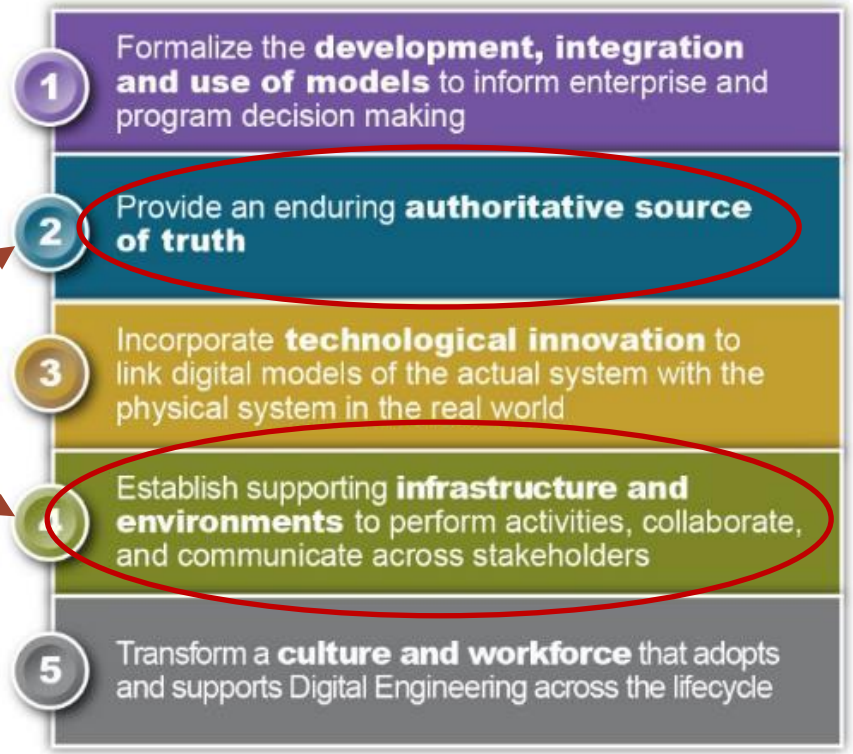
Digital Engineering: An integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support life cycle activities from concept through disposal.

Source: "Digital Engineering Discussions", Philomena Zimmerman, NDIA Systems Engineering Division, May 2019

Digital Engineering Definition and Goals

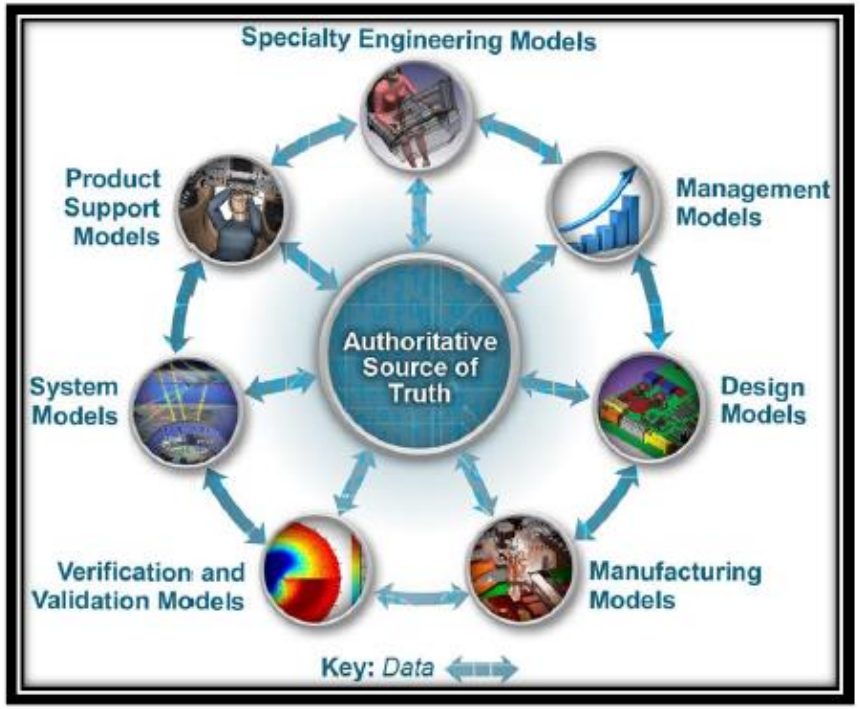
Digital Engineering: An integrated digital approach that uses authoritative sources of systems' data and models as a continuum across disciplines to support life cycle activities from concept through disposal.

Focus areas for this presentation



Digital Engineering Strategy Goal 2: Providing an Enduring Authoritative Source of Truth

- The Digital System Model has evolved to become the "Authoritative Source of Truth"
  - Need to capture the current state and history of the technical baseline
  - Need a central reference point for models and data across the lifecycle
  - Need to facilitate a sharing process across engineering disciplines
  - Need authorized users to have access to the right information at the right time
  - Need to enable teams to work collaboratively, with access to up-to-date models, data, and information



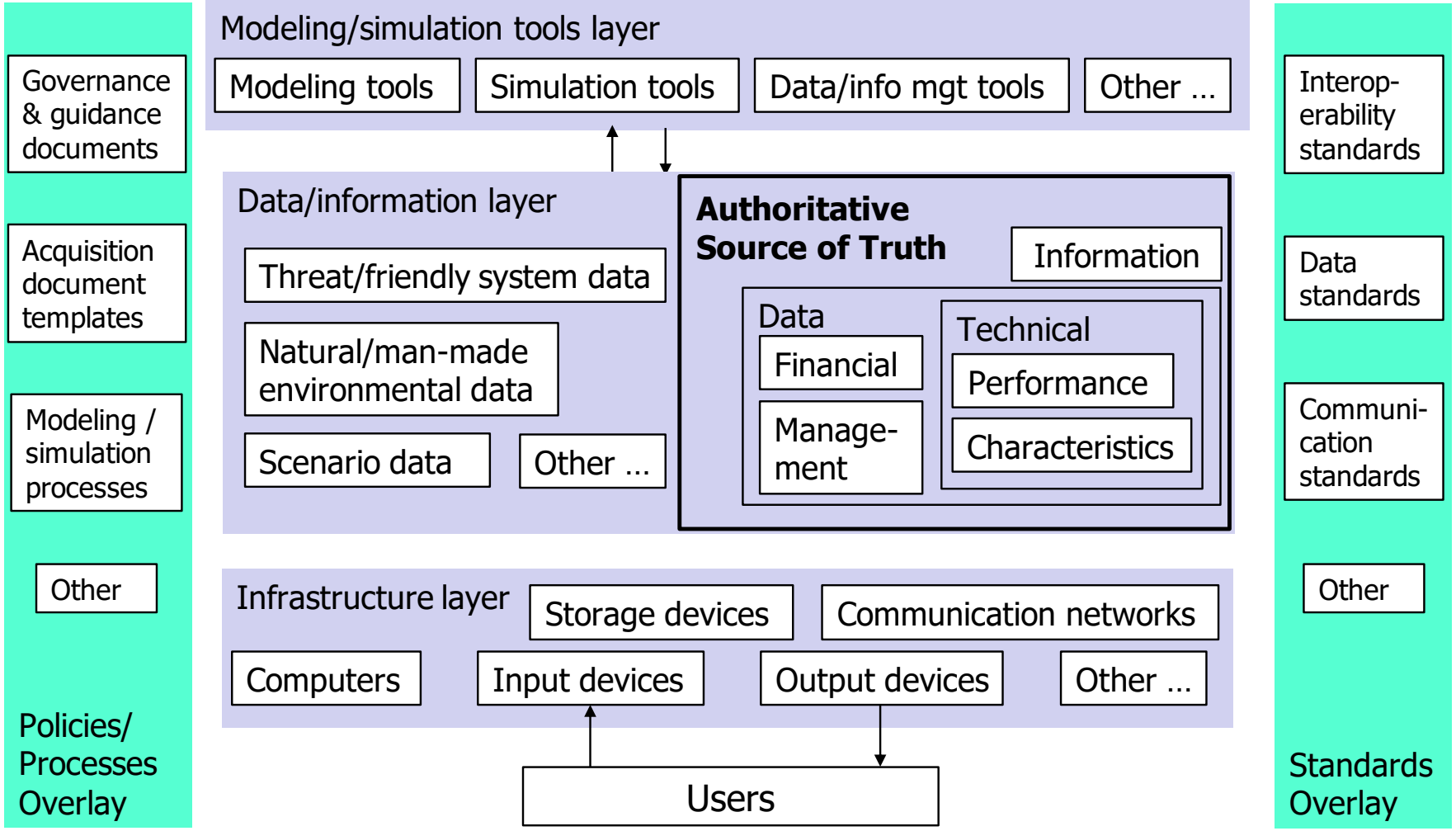
Source: *Digital Engineering Strategy,* June 2018

Digital Engineering Strategy Goal 4: Develop a Supporting Infrastructure and Environments …

Goal 4.1: Digital engineering IT infrastructures include a collection of hardware, software, networks, and related equipment. They span geographical locations and organizations, and they must satisfy security requirements. …

Source: *Digital Engineering Strategy*, June 2018

So What Might a Digital Engineering Collaborative Environment Centered on the Authoritative Source of Truth Look Like?



Adapted from: "A System-Model-Centric Collaborative Environment for the Acquisition Lifecycle," J.E. Coolahan and J.J. Bergenthal, 2015 Interservice/Industry Training, Simulation & Education Conference, Nov.-Dec. 2015.

Digital Engineering Collaborative Environment Resource Discovery Challenges

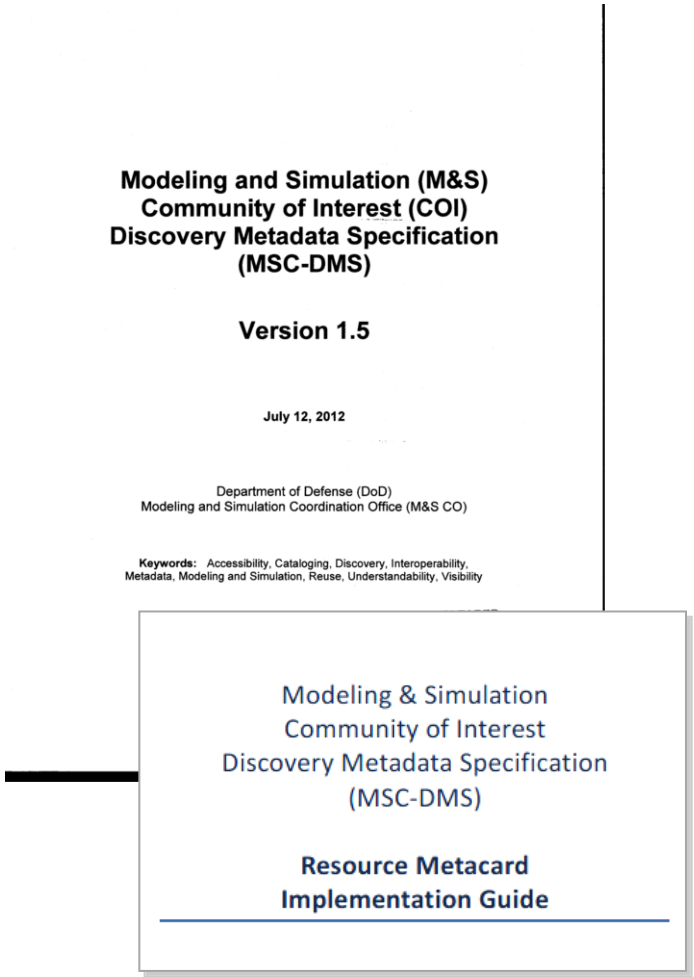
- Stakeholders in a Digital Engineering Collaborative Environment (DECE) for a major system need to be able to discover and access:
  - A wide range of resources in the Data/Information Layer that are stored in a large variety of locations.
  - Applicable policies and processes for the digital engineering of the system in the Policies/Processes Overlay
  - Standards relevant to the digital engineering of the system in the Standards Overlay
- DECE stakeholders need to be able to discover the degree to which system data and information stored in the Authoritative Source of Truth is authoritative, from both technical and management perspectives.
- An aid in meeting the above challenges is the formulation of a Discovery Metadata Repository for the system's digital engineering artifacts.

Some Potential Use Cases for a Discovery Metadata Repository for a Digital Engineering Collaborative Environment

- How can one find a particular information or data resource in the Authoritative Source of Truth?
- What organization is the owning authority for a resource asset?
- What person is the technical authority for a dataset's contents?
- When was a resource asset last updated?
- What is the security classification for a dataset's contents?
- To whom is a resource asset's contents releasable?
- … Others

Discovery Metadata
Definitions and Example Specifications

- Metadata: Data about data; specification of the content, meaning, structure, and use of the data.
- Discovery Metadata: Metadata that is focused on tagging of information assets so that an asset can be discovered.
- Example metadata specifications (focused on M&S assets):
  - Modeling and Simulation (M&S) Community of Interest (COI) Discovery Metadata Specification (MSC-DMS) Version 1.5, 2012 (and its associated implementation guide)
  - Discovery Metadata Specification for Modeling and Simulation Resources (DMS-MSR), in-progress



Background on the MSC-DMS

- Purpose: To standardize on the set of metadata used to describe assets in the then Modeling and Simulation Resource Repository (MSRR) nodes and similar applications, and to align with the (no longer supported) DoD Discovery Metadata Specification (DDMS)
- Sponsor: Defense Modeling and Simulation Coordination Office (DM&SCO)
- Contributors: Approximately two dozen individuals from the Office of the Secretary of Defense (OSD), the Services, and industry
- Development History: 5 September 2007 - Version 0.8 (Preliminary Internal Review Version) thru 12 July 2012 – Version 1.5 (last update)
- Key Constructs: “Metacards” (32) defining sets of metadata fields

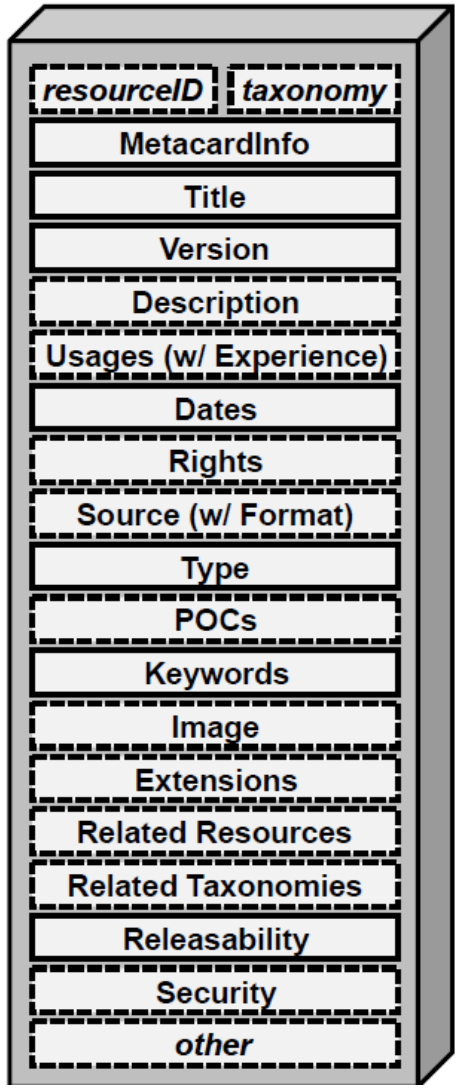
Background on the DMS-MSR

- Purpose: To develop a metadata standard to describe modeling and simulation (M&S) resources in a manner that will be useful to the international M&S community in discovering various types of M&S-related resources
- Sponsor: Simulation Interoperability Standards Organization (SISO)
- Contributors: Approximately two dozen (to date) SISO members from government, industry, and academia, from the U.S. and several other countries
- Development History: Product Development Group began in February 2020, standard still in early-to-mid development stage; new members welcome
- Key Constructs: Metadata sets for several resource types, drawing significantly, but not exclusively, from the MSC-DMS

Some Potential Resource Types (Preliminary) from SISO DMS-MSR Product Development Group Discussions

- **Models**, e.g., Computer Aided Design (CAD) models, data models, cost models
- **Simulations**, e.g., system stimulators, simulations of system effectiveness, cockpit simulators
- **Simulation Environments**, e.g., High Level Architecture (HLA) federations, Test and Training Enabling Architecture (TENA) logical ranges
- **Datasets**, e.g., terrain elevation data files for specific geographic regions, CAD data files for systems, sound velocity profiles for specific maritime regions
- **Services**, e.g., measurement unit conversion services, geodetic coordinate conversion services, cloud-based data storage services
- **Tools**, e.g., CAD modeling tools, process modeling tools, system modeling tools
- **Facilities**, e.g., hydrodynamic tow tanks, crash-test facilities, test ranges
- **Documents**, e.g., model/simulation development plans, user guides, Verification, Validation, and Accreditation (VV&A) artifacts, standards for M&S tools and processes

Two Key "Metacards" from MSC-DMS v1.5



Resource Metacard

M&S Resource Assets Supported

1. M&S Software (models / simulations)
2. M&S Adjunct Tools (data loggers, visual)
3. Federations of Simulations
4. M&S Software Components
5. M&S Services
6. M&S Data
7. M&S Data Models
8. Interface Specifications
9. Documents

Contact Metacard

M&S Contact Assets

1. Person
2. Organization

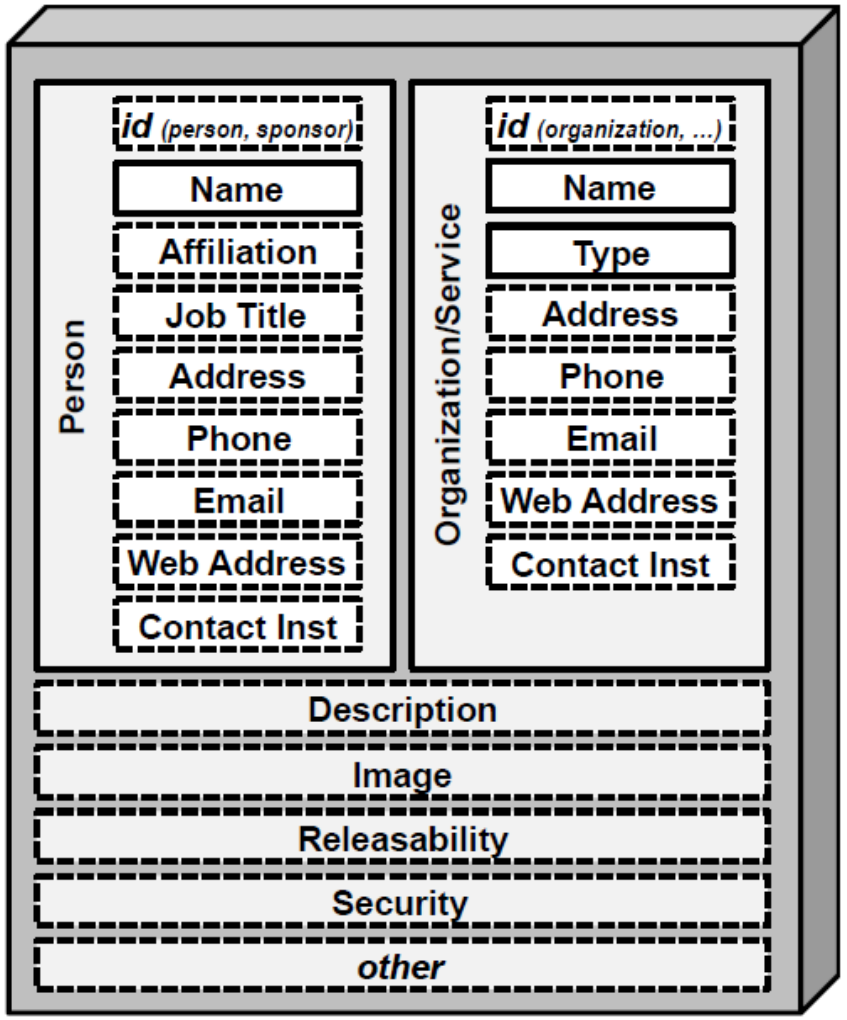


Illustration of Discovery Metadata Application Using the MSC-DMS Resource Metacard (1 of 4)

- MetacardInfo
  - e.g., dates of entry and update, POC organization/person
- Title
  - e.g., unique name for a dataset
- Version
  - e.g., version identifier for a document
- Description
  - e.g., text description of a dataset, using proper semantics
- Usages
  - e.g., intended use of a simulation and limitations on use

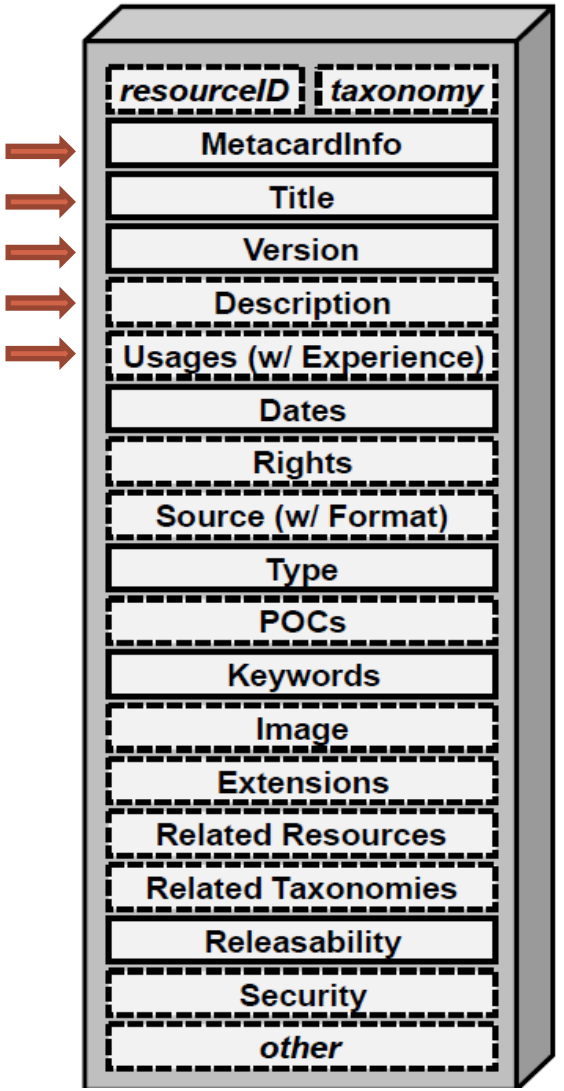


Illustration of Discovery Metadata Application Using the MSC-DMS Resource Metacard (2 of 4)

- Dates
  - e.g., creation date and update dates for a dataset
- Rights
  - e.g., flags a document as intellectual property, with owning organization
- Source
  - e.g., a format qualifier (e.g., *data bytes*), size (e.g., *byte count*) and location of a dataset; or the file type and URL of a document
- Type
  - e.g., *model*, *dataset*, or *document*; with designation as *authoritative* (or other category)

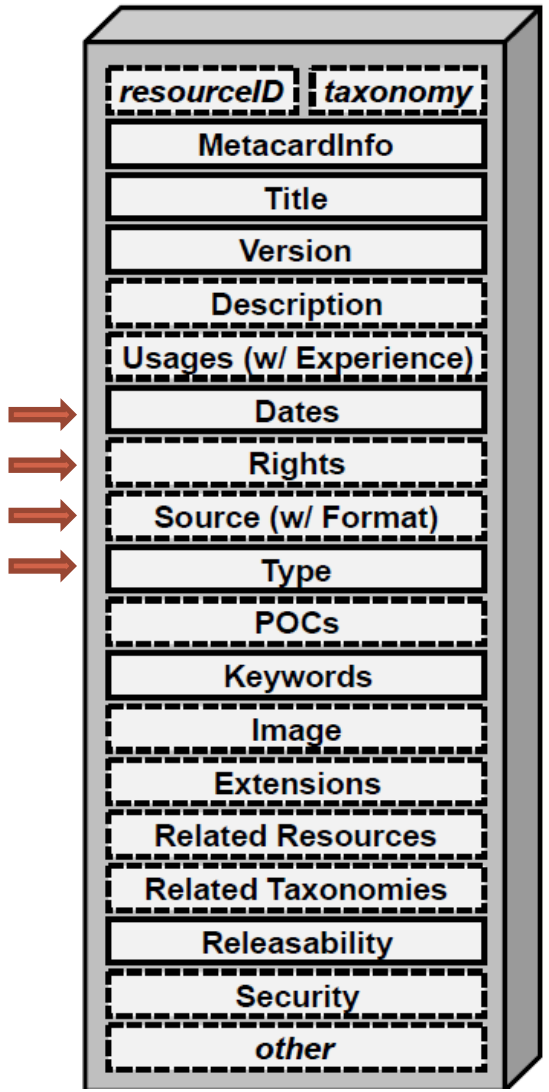


Illustration of Discovery Metadata Application Using the MSC-DMS Resource Metacard (3 of 4)

- POCs
  - Role – e.g., *owning organization*, *technical POC*
  - POC.Organization – e.g., contact info for owning organization
  - POC.Person – e.g., contact info for technical POC
- Keywords
  - e.g., *missile defense* for a capability document for an interceptor
- Related Resources
  - e.g., specifies that *length* of a component "is a part of" a CAD model dataset for that component
- Releasability
  - e.g., *Distribution D. DoD and DoD Contractors Only*

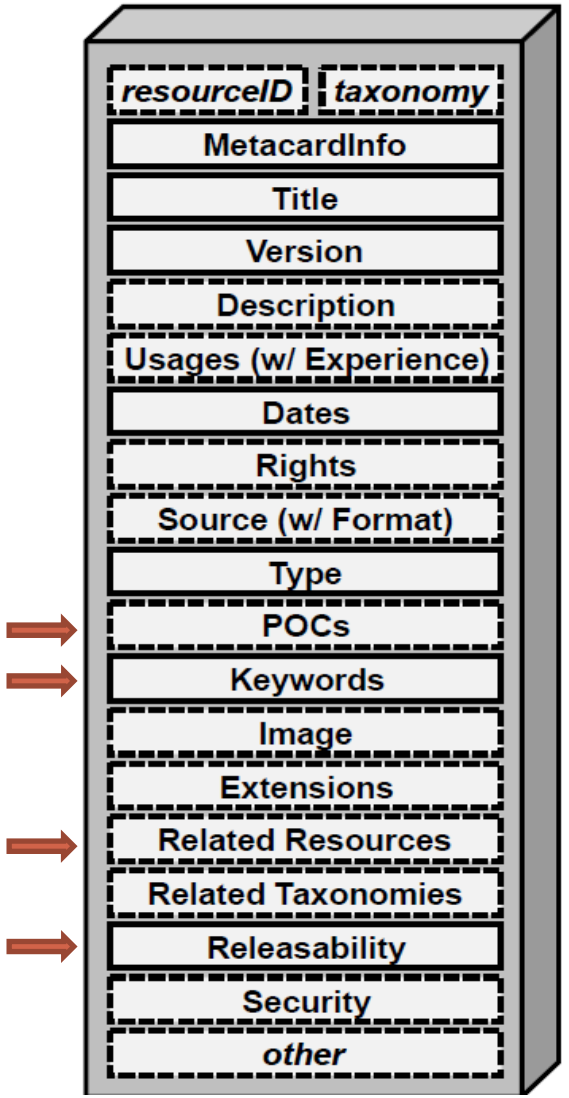
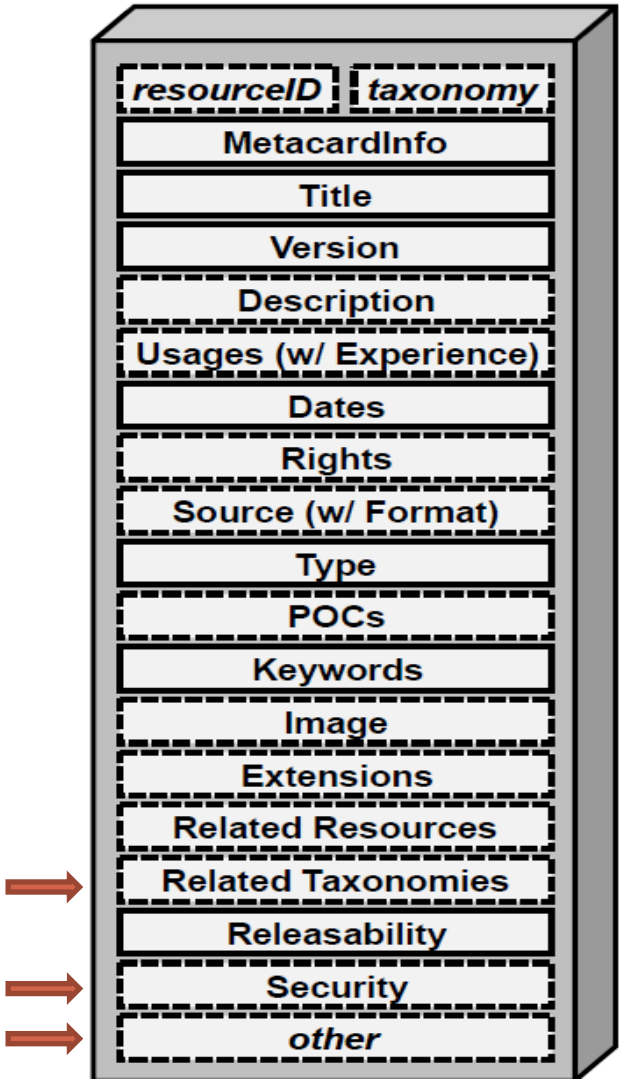


Illustration of Discovery Metadata Application Using the MSC-DMS Resource Metacard (4 of 4)

- Security
  - e.g., the security classification (e.g., *Secret*) and classification authority
- Other
  - e.g., *units of measure* for contents of a dataset
- Related Taxonomies
  - e.g., a title (e.g., *M&S glossary*) and description



Summary

- Formulation of a Discovery Metadata Repository for a major system's digital engineering artifacts will aid stakeholders in a Digital Engineering Collaborative Environment for a major system to discover and access those artifacts.
- The MSC-DMS (v1.5, 2012) provides a good current starting point for discovery metadata definition and creation for varied applications.
- The DMS-MSR standard that is in progress in SISO has the promise to be a *sustainable* successor to the MSC-DMS.
  - DMS-MSR Product Development Group (PDG) in-progress work, along with a copy of the MSC-DMS, can be accessed at https://www.sisostds.org/StandardsActivities/DevelopmentGroups/DMS-MSRPDG.aspx
  - New members can join the DMS-MSR PDG at the above web site.

ManTech
Securing the Future



Securing the Future

Taking Authority Over Your Modeling Enterprise: ManTech's Elastic Model Governance Approach

Dr. Heidi Davidz, Intelligent Systems Engineering SME
Dr. Douglas Orellana, VP of Intelligent Systems Engineering
Rebekah Pak, A3 Data Governance

Safe Harbor Statement

This presentation contains "forward-looking statements," within the definition of the Private Securities Litigation Reform Act of 1995. These statements are subject to numerous assumptions, risks, and uncertainties, many of which are outside of our control, and include the risks and uncertainties that are identified in the Risk Factor section in our Annual Report on Form 10-K (filed with the SEC on February 19, 2021), and in other periodic and current reports we file with the SEC. While the forward-looking statements herein reflect our current expectations, no assurance can be given that the results or events described in such statements will be achieved, and our actual results may differ materially from the results we anticipate.

We undertake no obligation to revise or update any of these forward-looking statements (whether as a result of new information, subsequent events or circumstances, changes in expectations or otherwise) that may arise after the date of this presentation.

****

Executive Summary

Model Governance Guide

As Digital Engineering (DE) employs a digital thread with a broad range of interconnected models, it can be difficult to govern linked models across disciplines and contractual boundaries. This approach includes:

GUIDANCE – Model-based guidance with in-model work instructions,

INTEGRATION – Integration of the overall model governance system, DE Ecosystem (DEE) infrastructure, individual models, and composite models,

PURPOSE – Traceability of model purpose and resolution of technical debt,

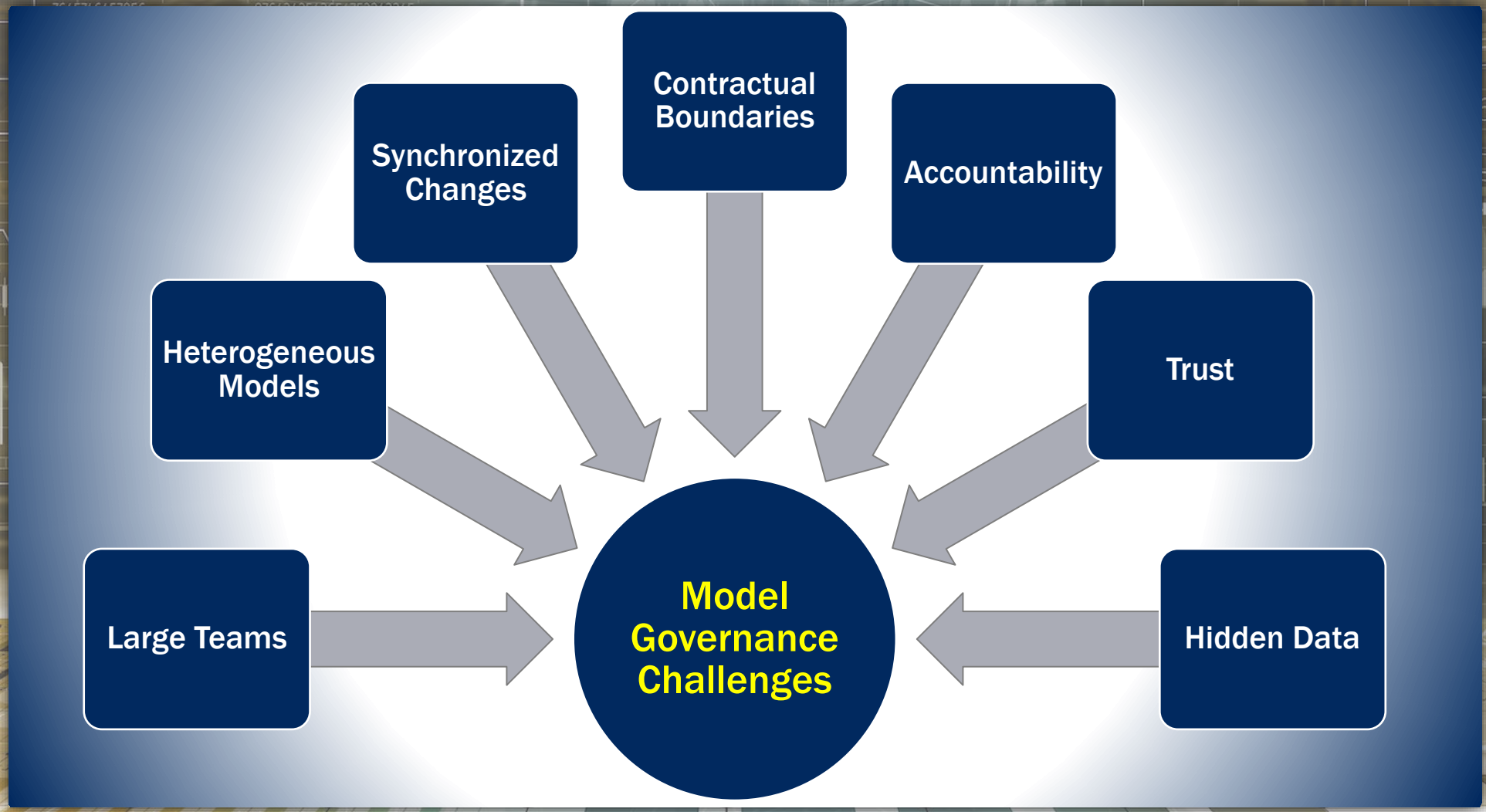
VALIDATION – Automated validation for insight on compliance,

FLEXIBILITY – Customization for flexibility and tailoring (fleX-engineering™).

Agenda

Model Governance Challenges

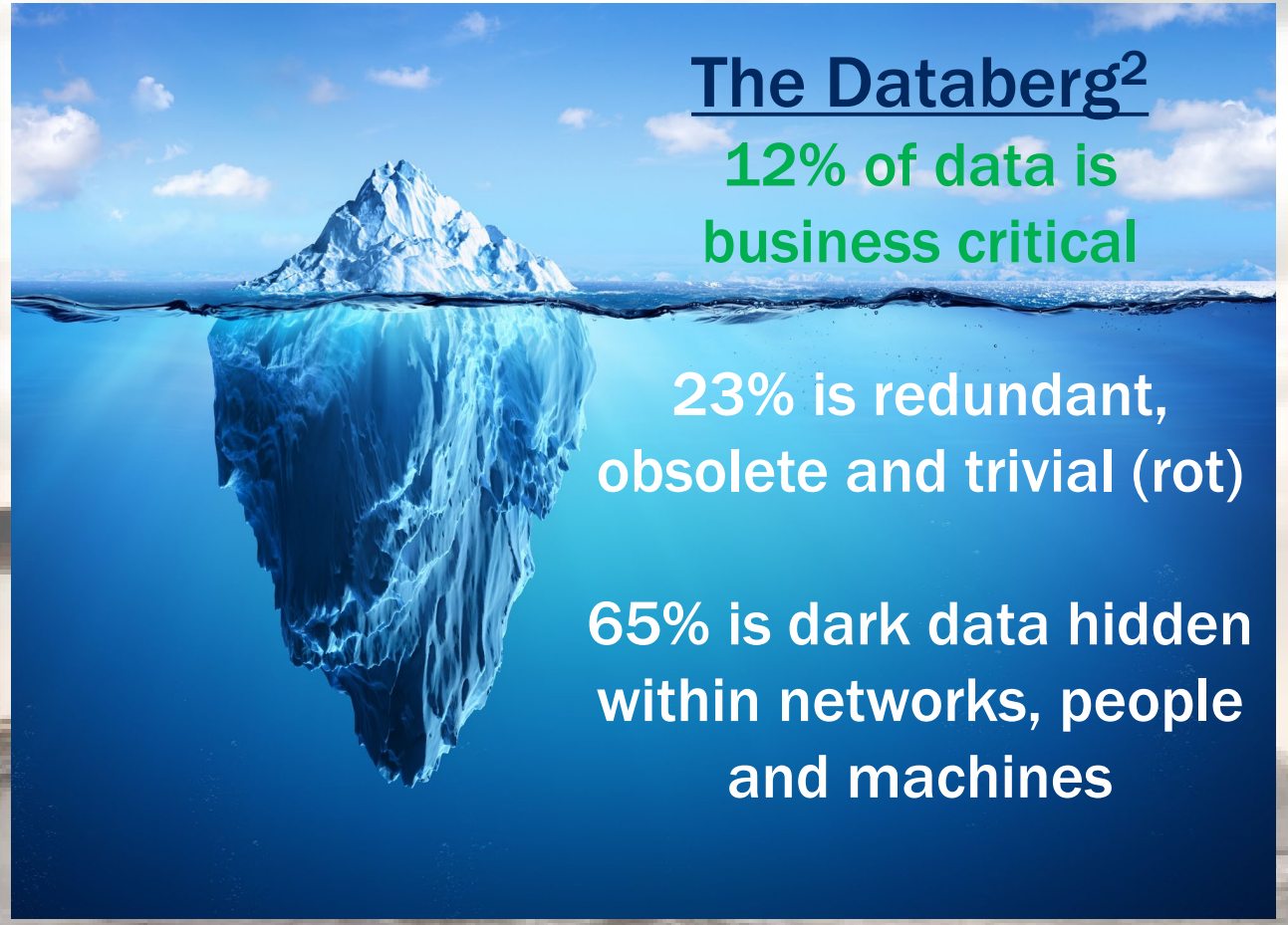
Challenges


Contractual Boundaries
Synchronized Changes
Accountability
Heterogeneous Models
Trust
Large Teams
Model Governance Challenges
Hidden Data

Data on Challenges

Need[1]

- Organizations score low on “Model Management” capabilities when assessed by the INCOSE Model-Based Capabilities matrix
- SERC SE Survey cited “Model Management” as a significant area of improvement
- Acquirers routinely ask for model management work and responding bidders have a range of responses

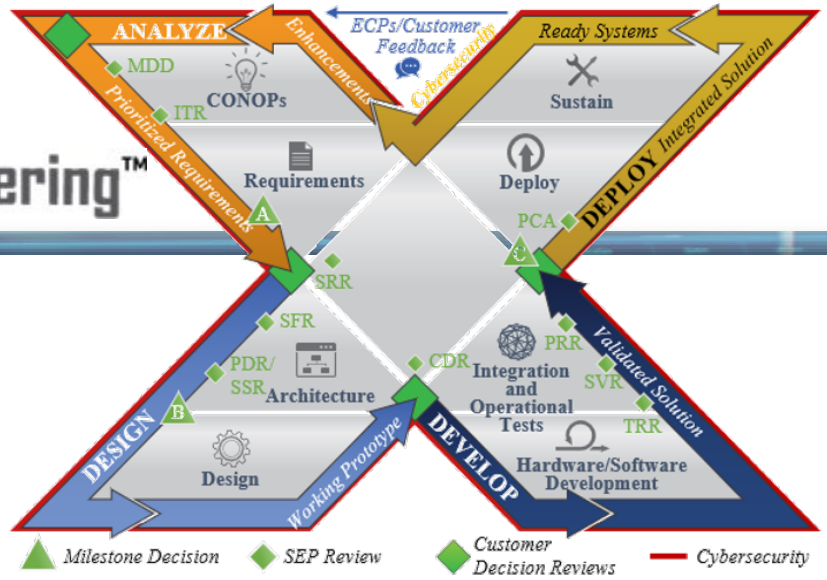


Model Governance is a Recognized Need

ManTech Approach

Approach to Problem

fleX-engineering™



1. **Harvest information**
   - ❑ Review existing literature and practice
2. **Develop process and address desired features**
   - ❑ Use model lifecycle and guidelines from NASA-STD-7009[3,4]
   - ❑ Expand on International Council on Systems Engineering model lifecycle management[5] and configuration management[6], OpenMBEE[7,8], model curation[9,10], digital curation[11], data governance[12], Model Portfolio Management Guide[13], Model-Based Capabilities Matrix[14]
   - ❑ Structure process to be flexible per DoDI 5000.02[15] "Operation of the Adaptive Acquisition Framework" and ManTech's fleX-engineering™
   - ❑ Utilize established SysML model validation practices[16]
   - ❑ Involve ManTech Data Governance expertise to update approach
3. **Obtain feedback and update**
   - ❑ Update using feedback from stakeholders, users, presentations

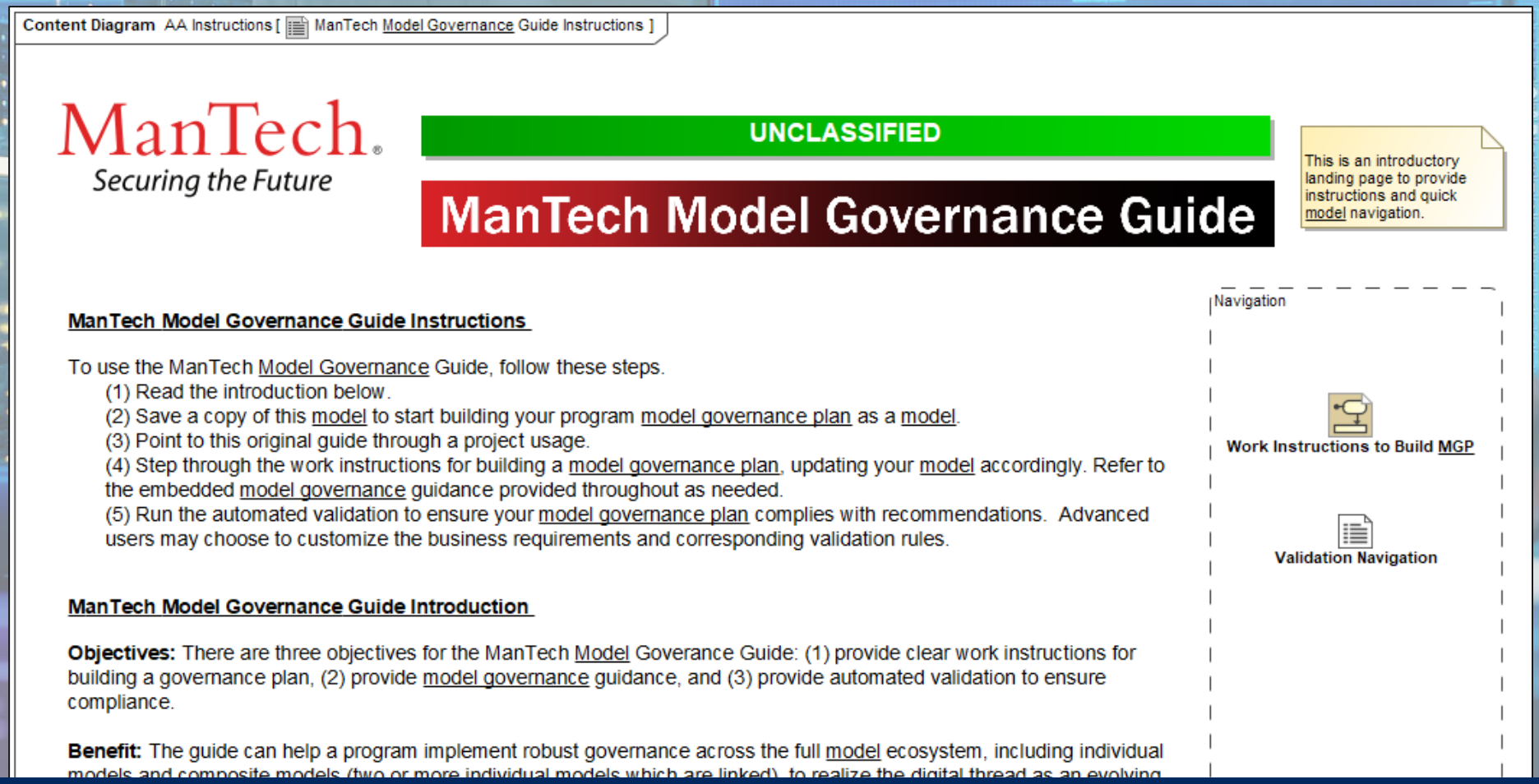
Build from Existing Model Governance Work

Solution Features with Corresponding Value

Features	Value
Provide model-based guidance with in-model work instructions	Enhance usability and demonstrate model-based methods promoted
Establish explicit governance system	Ensure veracity of authoritative source of truth
Include interacting elements – model governance system, DEE infrastructure, individual models, composite models	Improve integration, since elements can be referenced, linked, checked
Trace model purpose through needs addressed, questions answered, technical debt resolved	Establish transparency into system development status
Automate validation for insight on compliance	Enable synchronized data structuring for analytics applications to enhance outcomes
Structure for customization	Provides flexibility and tailoring for context

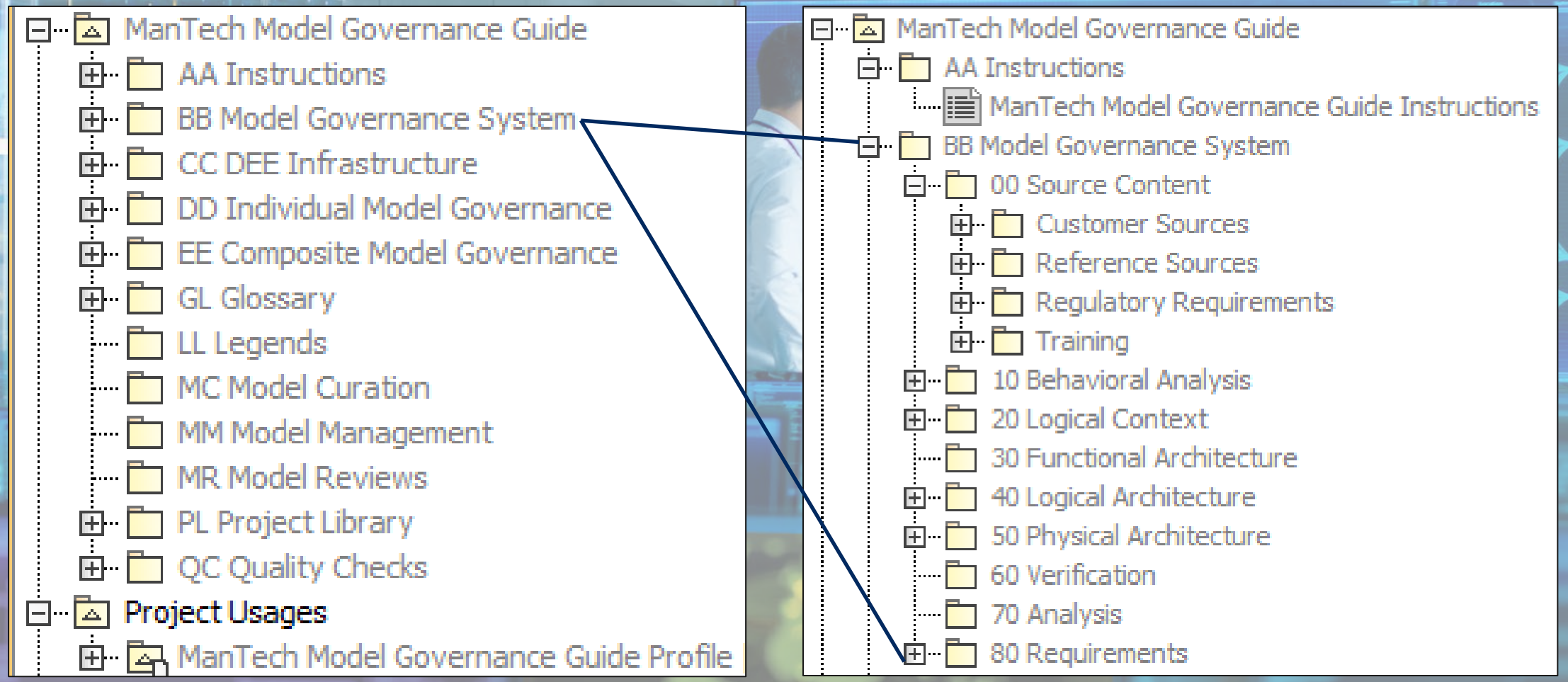
Model Governance Guide Profile and Model

Welcome and Navigation



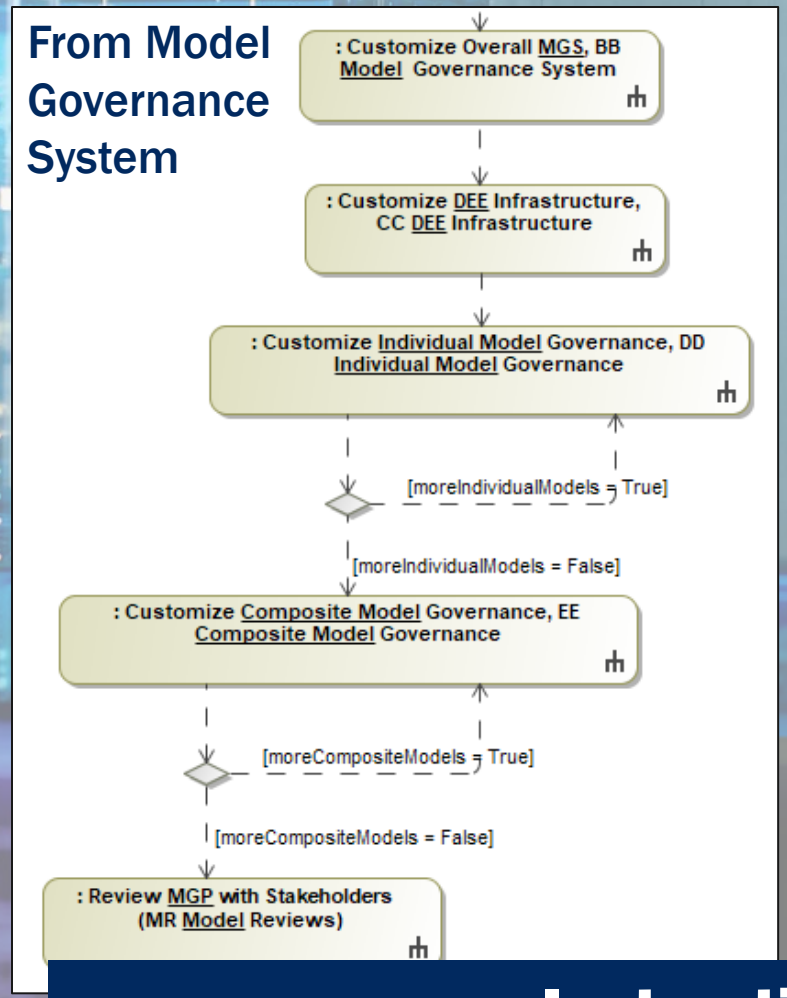
Navigation Aids and Embedded Explanation Provided

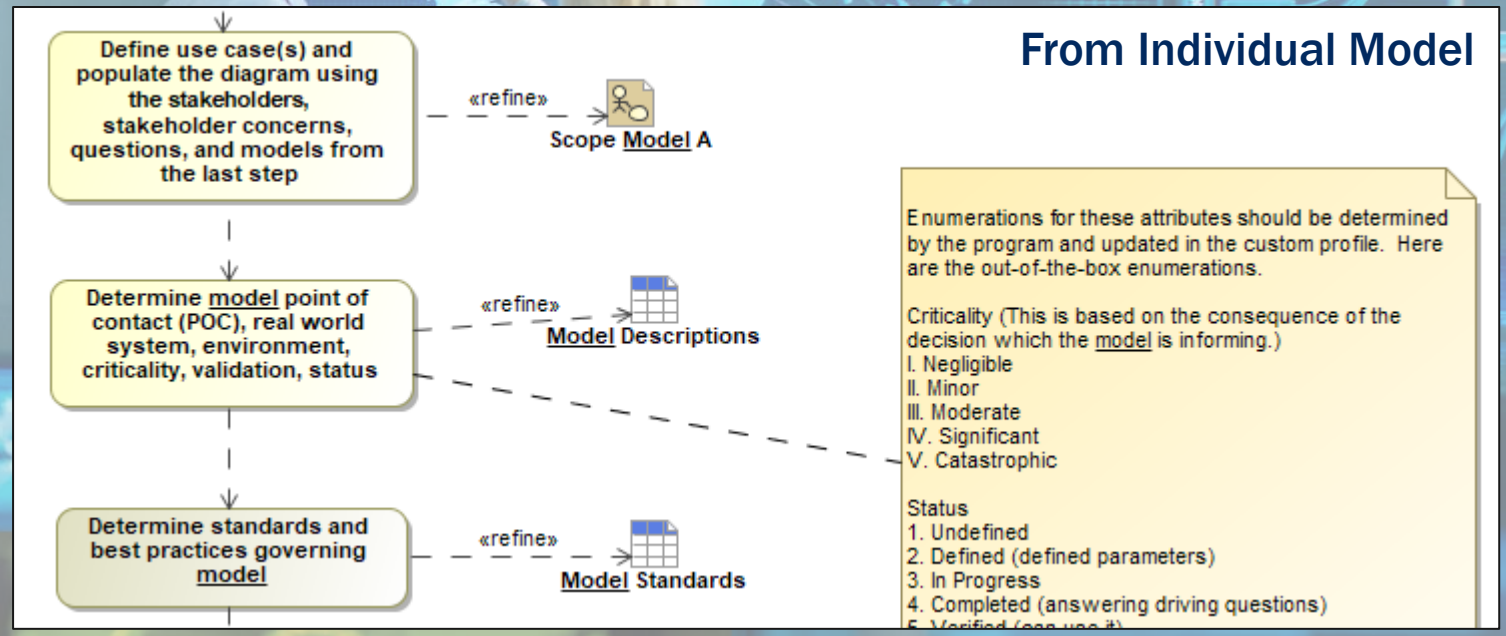
Structure



Repeatable Structure to Easily Find Information

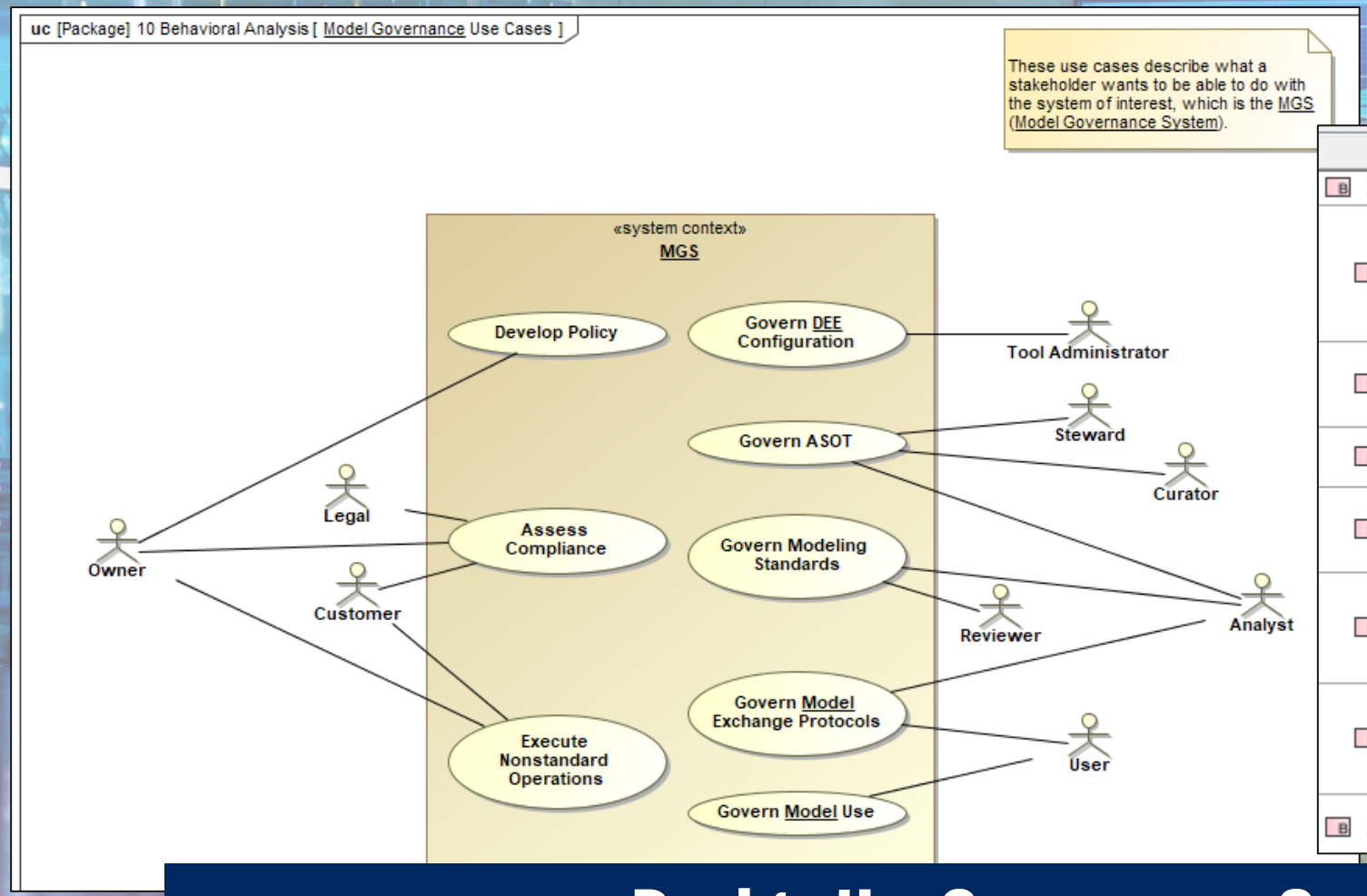
Work Instructions





Instructions Provided at Point of Need

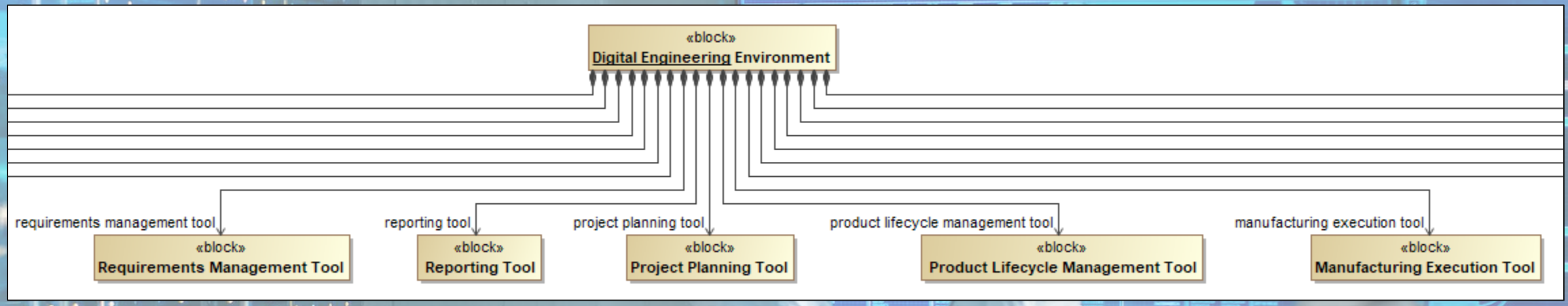
Model Governance System

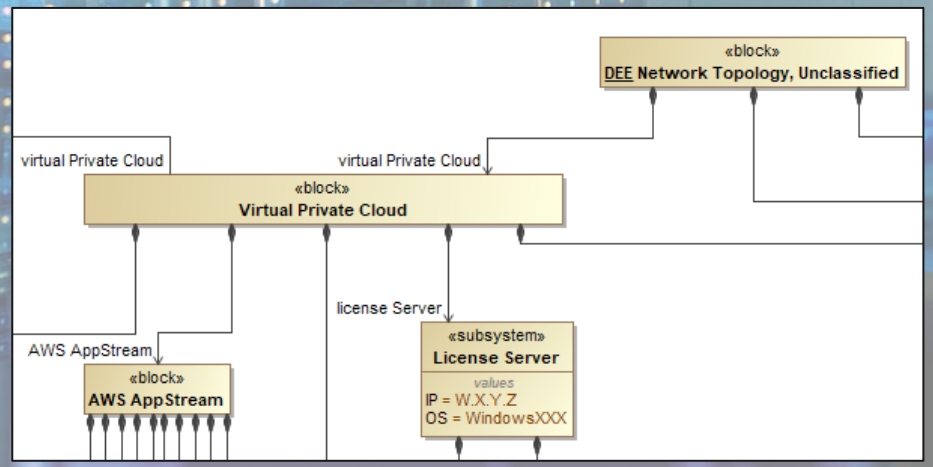


Name	Text	Traced To
26 MGS Services		
26.1 Different Kinds	The MGS services shall include models of different kinds including geometric, analysis, and logical models (refer to model taxonomy in SEBoK Part 2 'Representing Systems with Models').	Fisher, Amit, M. Nol
26.2 Results	The MGS services shall include artifacts that result from the execution of models such as simulation and analysis results.	Fisher, Amit, M. Nol
26.3 Inputs	The MGS services shall include needed inputs to stimulate the models.	Fisher, Amit, M. Nol
26.4 Views	The MGS services shall include artifacts that are generated as views of the models including documents and reports.	Fisher, Amit, M. Nol
26.5 Environments	The MGS services shall include the tools and environments used to create, review, update and delete the models and related artifacts.	Fisher, Amit, M. Nol
26.6 Metadata	The MGS services shall include metadata about the models, the related artifacts, the tools and environments, and the users of the models and related artifacts.	Fisher, Amit, M. Nol
27 Model Content Modification	The MGS shall not modify the model content (excluding its metadata).	Fisher, Amit, M. Nol

Design the Governance System Itself

DEE Infrastructure

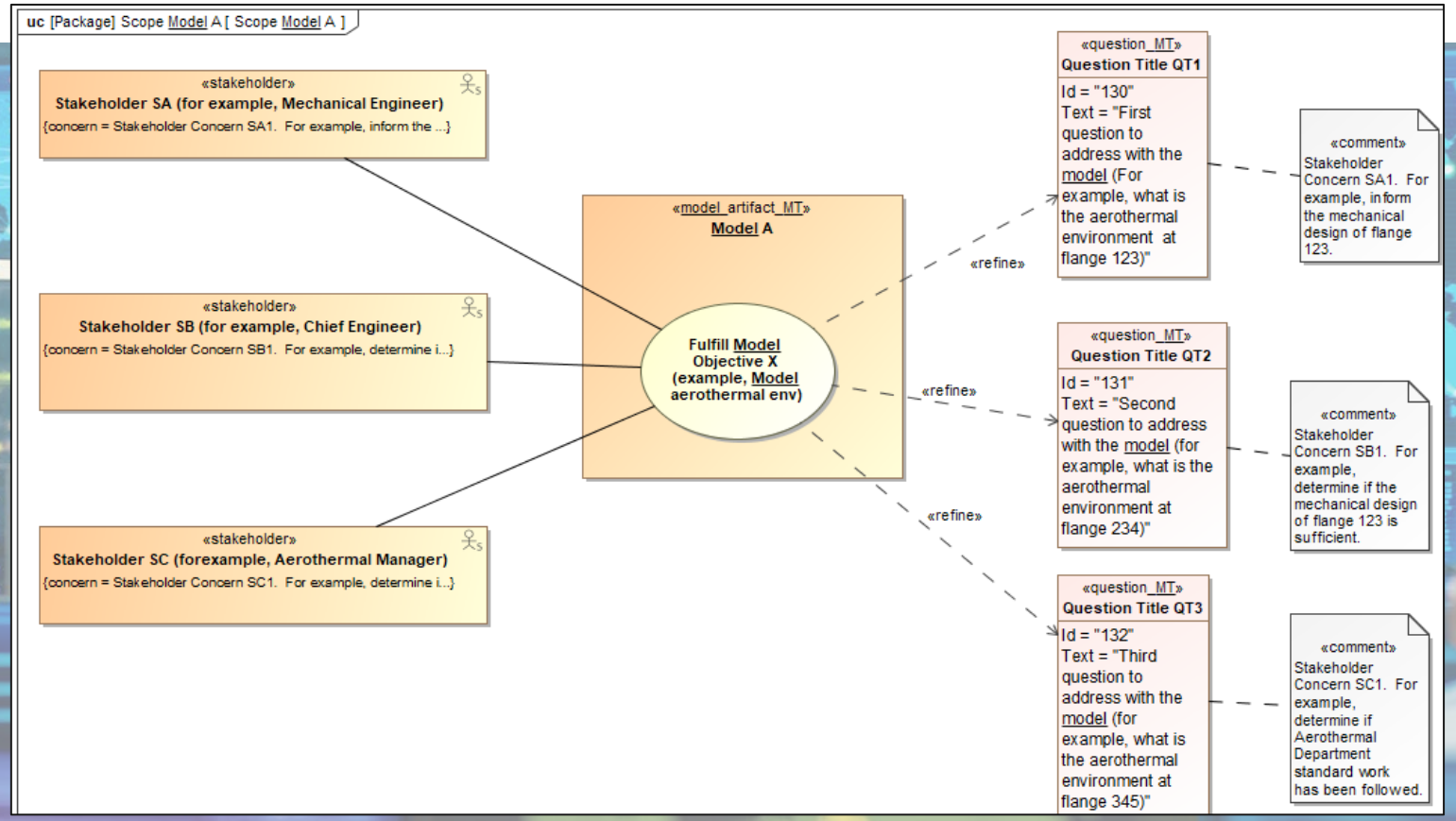




Name	Documentation	Realizes	Associations
Cameo Enterprise Architecture	Dassault Cameo is a model-based systems engineering tool.	Architecture Tool Verification Management T	Teamwork Cloud FlexNet Publisher Cameo Collaborator AWS AppStream
Matlab	Matlab is an analytical tool.	Analytical Tool	Computer A AWS AppStream
ModelCenter	ModelCenter is a tool which enables trades and multi-disciplinary optimization.	Analytical Tool Trades and Optimization T	FlexNet Embedded AWS AppStream

Include DEE Infrastructure Details and Relationship to Models

Individual Models



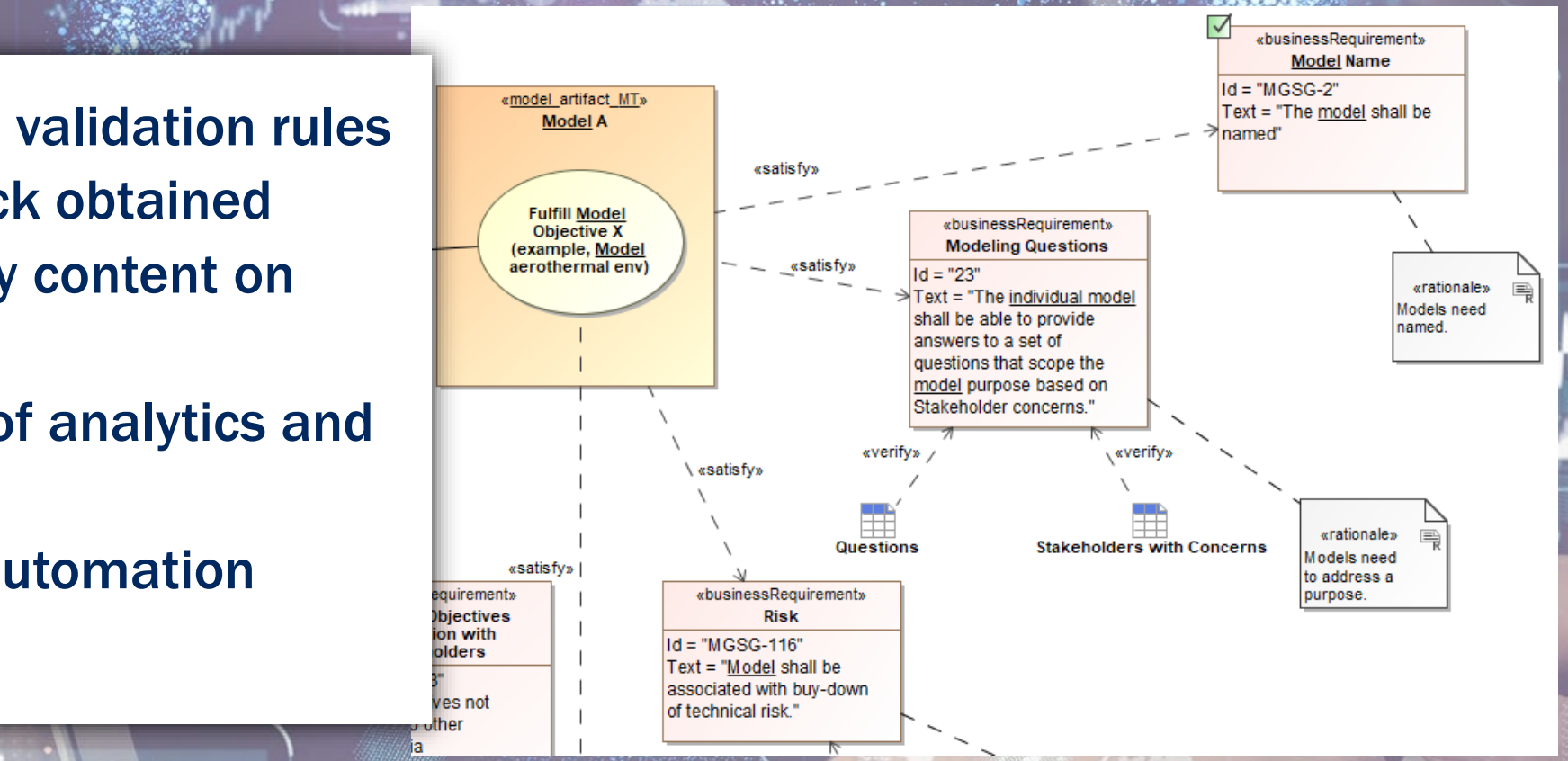
#	Name	Documentation	Associated Assumptions	Associated Risks	Traced to Standards	Use Cases	Questions2	Satisfies	Allocated To	Location
1	Model A	This is the description of Model A...	Assumption B Assumption A	Risk R1	Standard 1 (for example, I Best Practice 3 (for examp Standard 2 (for example, (	Fulfill Model Objective X (e	Question Title QT1 Question Title QT2 Question Title QT3	23 Modeling Questions MGSG-116 Risk MGSG-2 Model Name	ansys : ANSYS	AWS AppStream

Scoping and Traceability for Models to Address Stakeholder Needs

Next Steps

Next Steps

- Add more automated validation rules
- Update using feedback obtained
- Add more explanatory content on customization steps
- Enhance integration of analytics and automation
- Explore governance automation across digital thread



Enhance Automation and Analytics for Digital Thread Integration

Summary

Model Governance Guide

As Digital Engineering employs a digital thread with a broad range of interconnected models, it can be difficult to govern linked models across disciplines and contractual boundaries. This approach includes:

GUIDANCE – Model-based guidance with in-model work instructions,

INTEGRATION – Integration of the overall model governance system, DE Ecosystem infrastructure, individual models, and composite models,

PURPOSE – Traceability of model purpose and resolution of technical debt,

VALIDATION – Automated validation for insight on compliance,

FLEXIBILITY – Customization for flexibility and tailoring (fleX-engineering™).

Thank you

For more information contact:

Dr. Heidi Davidz, Heidi.Davidz@ManTech.com

Dr. Douglas Orellana, Douglas.Orellana@ManTech.com

References

1. Hoheb, Al, M. Zetilyan, A. Chang, J. Howie, “Model Portfolio Management (MPM) Guide: A Guide to Defining the Scope, Purpose, Tasks and Products of Model Portfolio Management,” The Aerospace Corporation Systems Engineering Forum, May 11, 2021, available at, https://custom.cvent.com/CDB22CFE0C9E4A08A08CC433A7A4E713/files/db524a94cefc48909a659d4304496cb7.pdf, accessed November 2021.
2. Pathrose, Shijin, “Why Organizations Need to Leverage Data Governance on Dark Data,” SG Analytics, published in Data Aggregation & Management, blog archives, October 2019, available at, https://us.sganalytics.com/blog/why-leverage-data-governance-on-dark-data/#:~:text=The%20dark%20data%20is%20a%20huge%20chunk%20of,cost-effective%20than%20managing%20its%20storage%20without%20a%20cause, accessed November 2021.
3. National Aeronautics and Space Administration (NASA), NASA-STD-7009A w/Change 1, “Standard for Models and Simulations,” Approved 2016-12-07, available at, https://standards.nasa.gov/standard/nasa/nasa-std-7009, accessed November 2021.
4. NASA, NASA-HDBK-7009A, “NASA Handbook for Models and Simulations: An Implementation Guide for NASA-STD-7009A,” approved 2019-05-08, available at, https://standards.nasa.gov/standard/nasa/nasa-hdbk-7009, accessed November 2021.
5. Fisher, Amit, M. Nolan, S. Friedenthal, M. Loeffler, M. Sampson, M. Bajaj, L. VanZandt, K. Hovery, J. Palmer, L. Hart, “Model Lifecycle Management for MBSE,” International Council on Systems Engineering (INCOSE) International Symposium, July 2014.
6. INCOSE Configuration Management Working Group, “Configuration Management in the Context of a Model-Based Enterprise,” white paper revision B, accessed November 2021.
7. Open Model Based Engineering Environment (OpenMBEE), available at, https://www.openmbee.org/, accessed November 2021.
8. Karban, Robert, C. Delp, YouTube video, "OpenMBEE Intro @MODELS’20,“ January 2021, available at, https://www.youtube.com/watch?v=ofKgcDrBFZQ, accessed November 2021.
9. Rhodes, Donna, “Investigating Model Credibility within a Model Curation Context,” Conference on Systems Engineering Research (CSER) 2020.
10. Rhodes, Donna, “Model Curation: Requisite Leadership and Practice in Digital Engineering Enterprises,” CSER 2019.
11. Digital Curation Centre, DCC Publications, available at, https://www.dcc.ac.uk/publications/research-publications, accessed November 2021.
12. Pak, Rebekah, “A^3 Data Governance: Data Governance Introduction and General Process,” May 2021.
13. Hoheb, A., A. Chang, M. Zetilyan, J. Howie, “Model Portfolio Management Guide,” Aerospace Corporation Technical Operating Report TOR-2020-01577, September 2020.
14. Hale, Joe, A. Hoheb, “INCOSE Model-Based Capabilities Matrix and User’s Guide,” Version 1.0, January 2020.
15. United States Department of Defense, “DoD Instruction 5000.02, Operation of the Adaptive Acquisition Framework,’” https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093.
16. SAIC, “Digital Engineering Validation Tool,” available at, https://www.saic.com/digital-engineering-validation-tool, accessed November 2021.

NDIA

Booz | Allen | Hamilton®

INTELLECTUAL PROPERTY CONSIDERATIONS IN DIGITAL ENGINEERING IMPLEMENTATION FOR ACQUISITION IN THE DEPARTMENT OF DEFENSE (DOD)

NDIA 2021 Systems & Mission Engineering Conference

Systems and Mission Engineering Transformation and Modernization

John Daly

Booz Allen Hamilton Systems Engineering Community of Practice

DECEMBER 2021

Abstract

Rapidly advancing Digital Engineering (DE) capabilities being adopted by the Department bring some unique challenges, and possibilities. In a move from paper-based acquisition to digital systems engineering (fueled by adoption of Model Based Systems Engineering (MBSE) methodology and tools), re-thinking of Intellectual Property (IP) is stimulated in an effort to be more efficient and agile in DoD acquisition. Additionally, the Adaptive Acquisition Framework (AAF) is accelerating the move to a more efficient and timely acquisition processes, and digital MBSE capabilities and frameworks can be leveraged to meet the DoD "speed of relevance" goals in acquisition. This evolving change in the process of acquisition, systems engineering, and program management will be discussed in the presentation, as well as the IP challenges and possibilities that can result in their adoption.

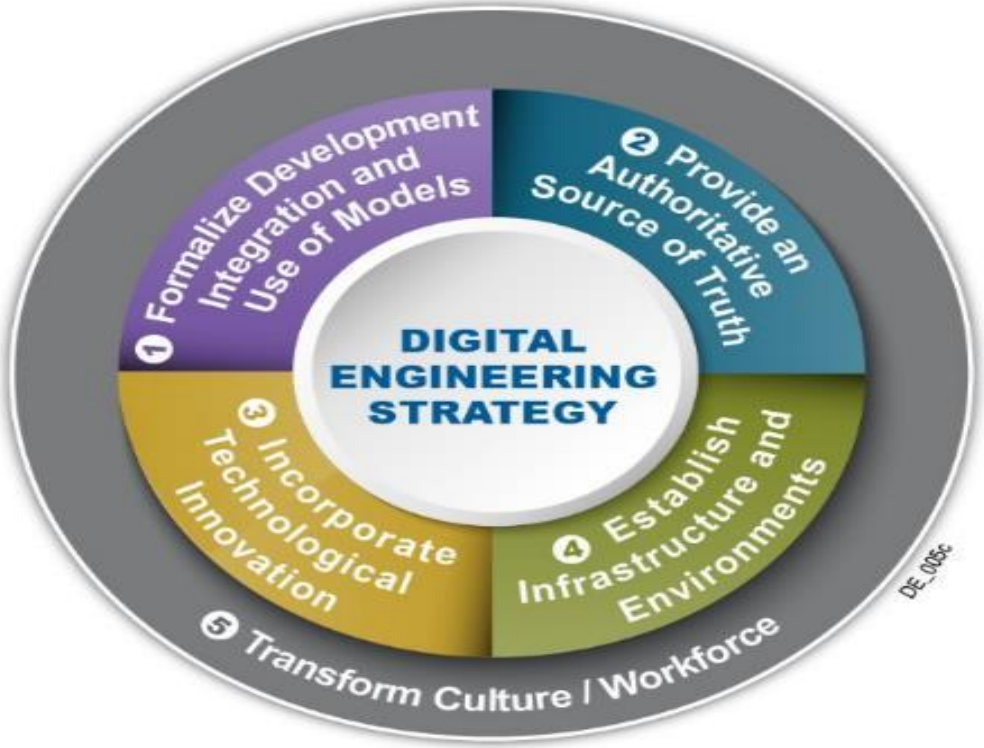
Agenda

- What is Digital Engineering
- What is Model Based Systems Engineering?
- The Digital Engineering/ MBSE Puzzle
- What is Intellectual Property in the DoD?
- What is the IP SE/Business Process?
- How do we protect and use IP in a DE environment ?
- Some MBSE IP Considerations
- Summary
- Recommendations for NDIA SE Division

What is Digital Engineering?

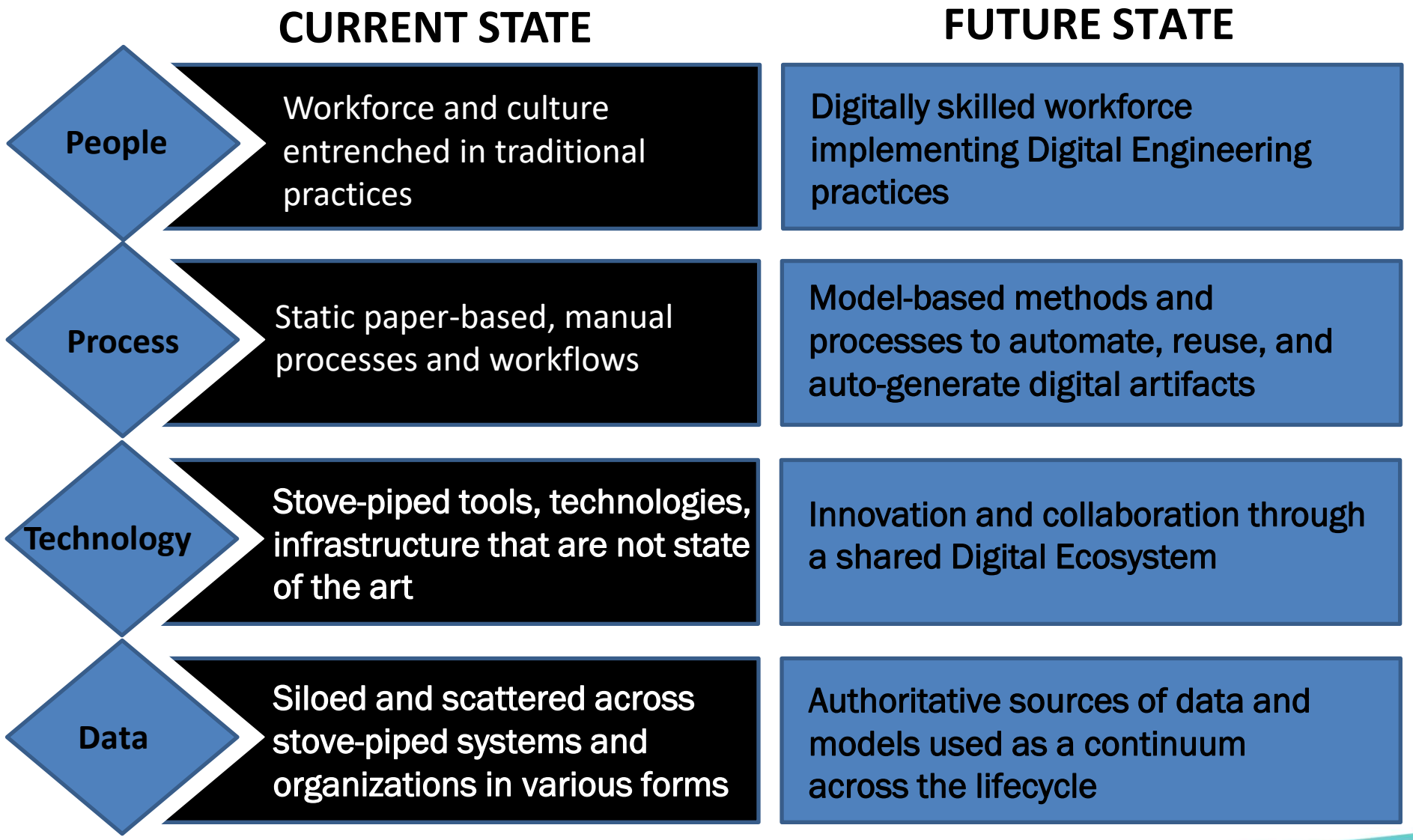
"An integrated digital approach that uses <u>authoritative sources of systems' data and models as a continuum across disciplines</u> to support life cycle activities from concept through disposal " ***(DoD Definition)***

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 link digital models of the actual system with the physical system in the real world
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



Distribution Statement A: Approved for public release DOPSR# 20-S-0306. Distribution is unlimited (USD(R&E)).

Digital Engineering Transformation



What is Model-Based Systems Engineering

"Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases[1]."

1. Ref: INCOSE SE Vision 2020

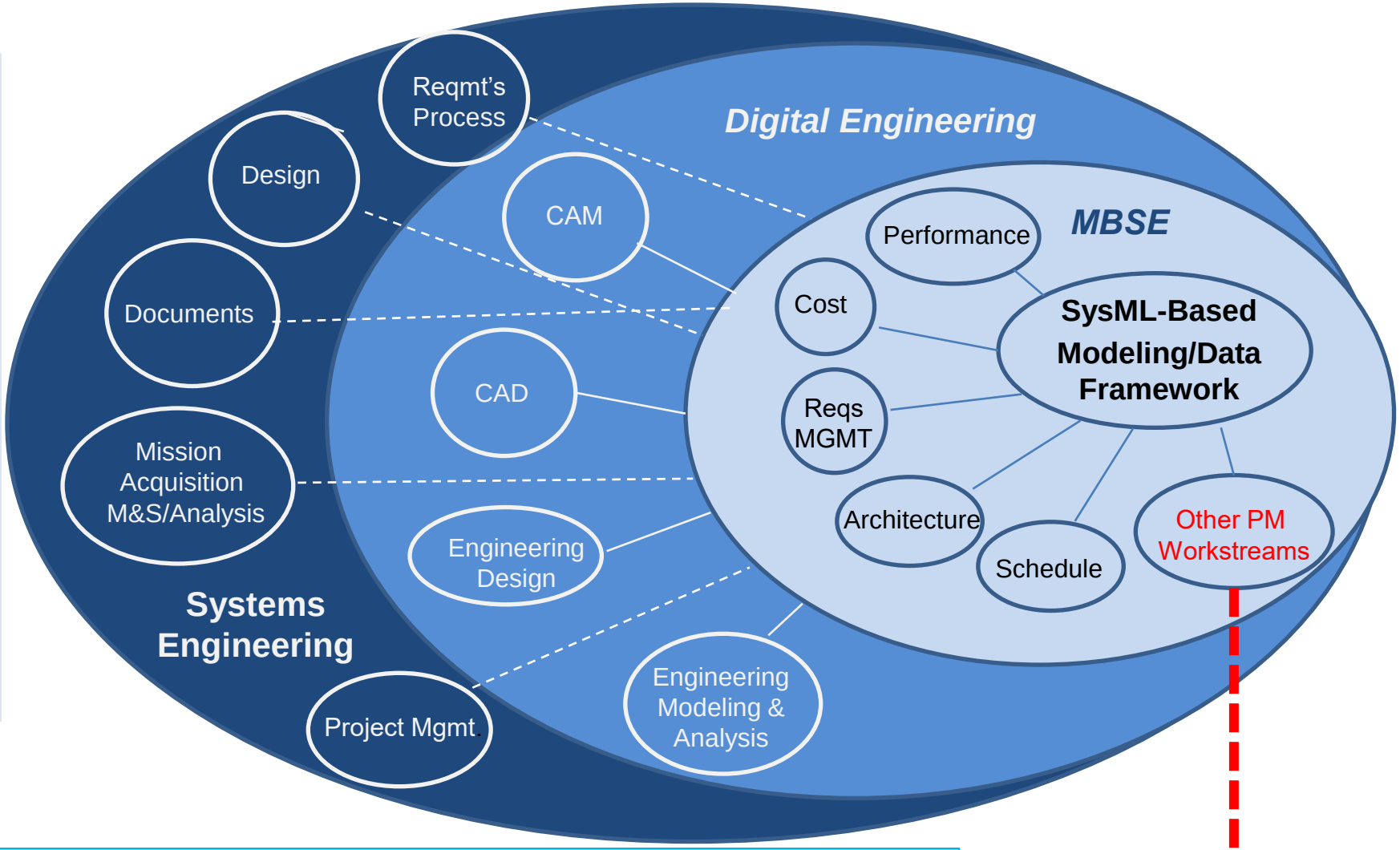
Model Based Systems Engineering

- Model-based systems engineering (MBSE) is a systems engineering methodology that focuses on creating and exploiting domain models as the primary means of information exchange between engineers, rather than on document-based information exchange
- MBSE provides a method to organize data to function / purpose over a program's lifecycle via a limited number of major tools (MagicDraw Cameo, Rational Rhapsody,Visual Paradigm…., etc.)
  - Since an MBSE approach is inherently robust and contains the data required to model the processes intrinsic in a system development, it:
    - Requires/enforces a structure "baked into the tools" for the data that it organizes into a systems engineering process
    - Has the prerequisite digital structure to link to the data produced/consumed by engineering-level engineering analysis and design framework tools(e.g. ANSYS, COMSOL, Autodesk, CATIA, Simula … etc.)
    - Can provide the interoperability link to Mission Simulations, especially if they are reconstituted in UML friendly modern modeling frameworks, or in an MBSE application itself
- If we view an acquisition lifecycle as a process, with many sub processes also model-able.. then the use of a scalable conceptual framework (MBSE) to organize data is attractive- and provides a digital link to other SE processes – **like Intellectual Property management**.

The Digital Engineering/ MBSE Puzzle

Our View

- Digital Engineering and MBSE support the systems engineering process of developing a capability. Digital Engineering includes much more than MBSE – all engineering processes
- MBSE is a process tool that instantiates systems engineering and engineering processes in a digital construct
- MBSE is the "glue" that integrates all these activities digitally, and "stores" the digital data associated with these SE/ENG/PM processes and contains the system architecture and all its attributes



Other PM workstreams can include other business processes such as:
Intellectual property (IP) /license management

MBSE and Acquisition
(and Intellectual Property)

- MBSE provides a method to organize data to function / purpose over a program's lifecycle
  - Since an MBSE approach is inherently robust and contains the data required to model the processes intrinsic in a capability development, it:
    - Requires a structure for that data that organizes a process with often disparate data into an organized entity
    - Has the prerequisite digital structure to **support modeling any systems engineering process**

- MBSE can be used to help objectively model an acquisition programs macro capability in performance terms and as the Systems of Systems level

- MBSE can provide clarity on requirements and insight on trades between both functional and performance requirements

- If we view an acquisition lifecycle as a process, with many sub processes also "model-able".. then **we can use MBSE to model a "process of processes" where the Intellectual Property business process is part of our overall mix and included in all our "trade-space" and optimization analysis - as well as an integral part of our digital thread of the acquisition**

What is Intellectual Property in the DoD?

- ***Intellectual Property (IP):*** *Information, products, or services that are protected by law as intangible property, including data (e.g., technical data and computer software), technical know-how, inventions, creative works of expression, trade names.*

- ***IP deliverables:*** *Products or services (including information products and services) that are required to be delivered or provided to the U.S. Government by contract or other legal instrument and that include or embody IP (e.g., technical data and computer software).*

- ***IP rights:*** *The legal rights governing IP, including ownership as well as license or other authorization to engage in activities with IP (e.g., make, use, sell, import, reproduce, distribute, modify, prepare derivative works, release, disclose, perform, or display IP).*

1. Ref: DOD INSTRUCTION 5010.44 INTELLECTUAL PROPERTY (IP) ACQUISITION AND LICENSING; https://www.esd.whs.mil/dd/dod-issuances/

What is IP Policy in DoD Acquisition?

It is DoD policy (DODI 5010.44) to acquire, license, and manage IP to[1]:

(1) Enable coordination and consistency across DoD Components in developing and implementing strategies for acquiring and licensing IP and communicating with industry.

(2) Ensure that program managers are aware of the rights and obligations of the Federal Government and contractors in IP, and that program managers fully consider and use all available techniques and best practices for acquiring and licensing IP early in the acquisition process.

(3) Encourage customized IP strategies for each system based on, at a minimum, the unique characteristics of the system and its components, the product support strategy for the system, the organic industrial base strategy of the military department concerned, and the commercial market.

Clearly, this puts the IP business process as a key responsibility of PM's and that an acquisition needs to have an IP strategy… BUT this is a systems engineering responsibility as all systems engineering activities have an IP attribute/dependency - overt or implied

1. Ref: DOD INSTRUCTION 5010.44 INTELLECTUAL PROPERTY (IP) ACQUISITION AND LICENSING; https://www.esd.whs.mil/dd/dod-issuances/

What is the IP SE/Business Process?

Need look no further than DODI 5010.44 *"additional core DoD IP Principles"*[1]:

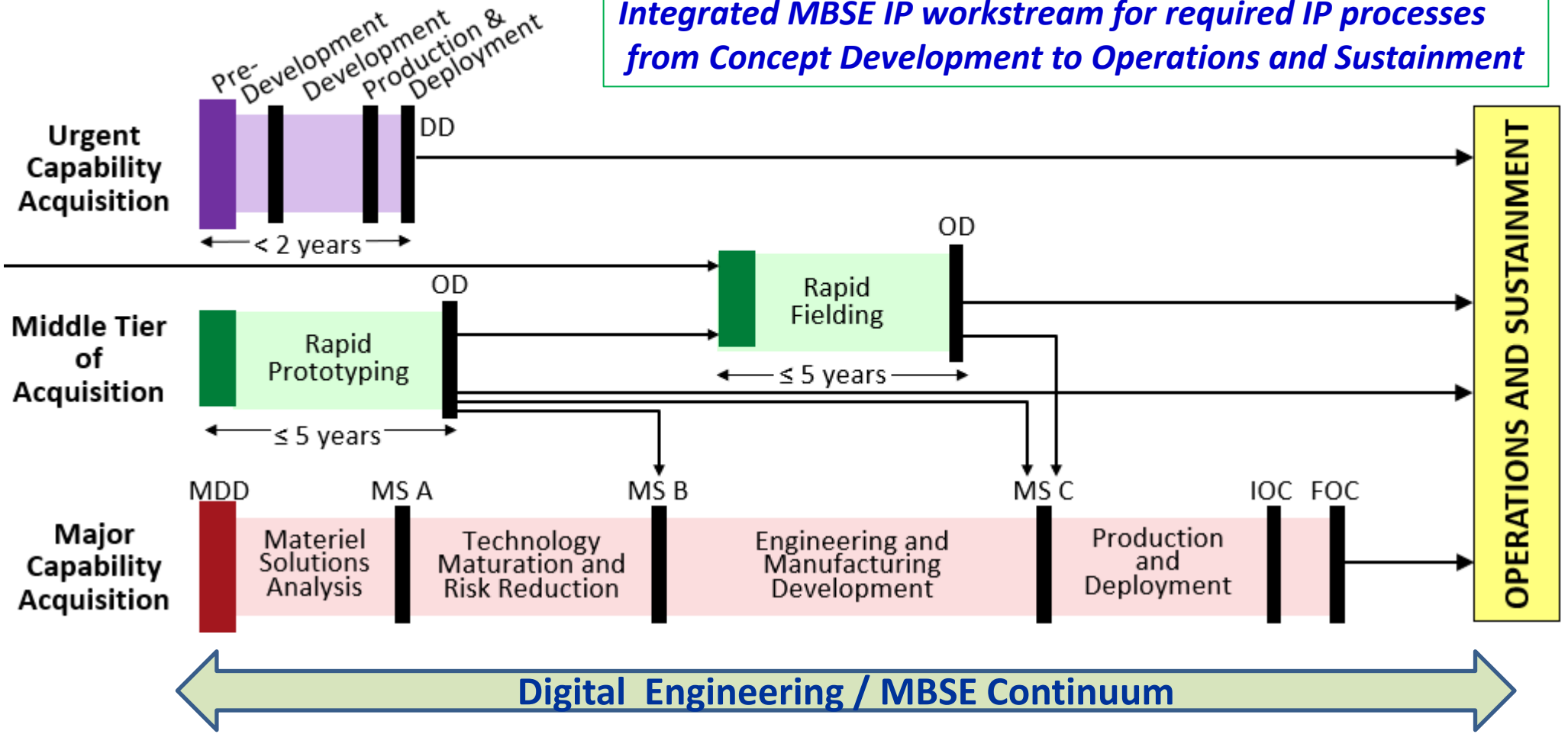
- **Integrate IP planning** fully into acquisition strategies and product support strategies to protect core DoD interests over the entire life cycle. **Seek to acquire only those IP deliverables and license rights necessary** to accomplish these strategies, bearing in mind the long-term effect on cost, competition, and affordability.
- **Negotiate specialized provisions for IP deliverables and associated license rights** whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights. **This is most effective early in the life cycle, when competition is more likely.**
- **Respect and protect IP** resulting from technology development investments by **both the private sector and the U.S. Government**.
- **Clearly identify and match data deliverables with the license rights** in those deliverables. **Data or software deliverables are of no value unless and until the license rights to use it are attached, and the U.S. Government actually obtains and accepts those deliverables**

OK.. A lot of IP processes… needs implementation materials, training and management to implement… but what if this is an included workstream in an MBSE Digital engineering environment??

1. Ref: DOD INSTRUCTION 5010.44 INTELLECTUAL PROPERTY (IP) ACQUISITION AND LICENSING; https://www.esd.whs.mil/dd/dod-issuances/

IP and MBSE Across Acquisition

Integrated MBSE IP workstream for required IP processes from Concept Development to Operations and Sustainment



Use of MBSE can put these IP/SE processes in a digital construct, modeling the processes, archiving their digital data, linking the IP process to other SE processes, and making data and models accessible and consumable from stage to stage

How do we protect and use IP in a DE environment ?

What are some key differences from a document –centric systems engineering environment and MBSE from an IP perspective?*:*

	Traditional	Digital	Issues
IP deliverables	Data delivered physically	Data delivered digitally, as part of a modeling environment	How does the USG "obtain and accept" Data? (Delivery, Access, "Renting" etc.…)
IP (trade secrets etc..)	IP is protected by inclusion/exclusion in documents	IP in data/models included and required in MBSE model/ process	How do we protect IP if it needs to be included in an MBSE representations of our acquisition?
IP rights	Rights to use IP are negotiated and tracked for each instance of use	Rights to use IP are an integral attribute of each dependent process	How does MBSE increase our visibility of the impact of IP rights and assist us in licensing?

MBSE implementation increases the visibility and traceability of IP, but also requires more IP to make model representations vs. paper representations of SE processes
If you can model it, you have completely described it!

Some MBSE IP Considerations

(1) ***IP Deliverables*** *As we move to an* ***MBSE environment, data is an integral part of models*** *that may or may not be part of the deliverable. Access to that data is an important digital concept and "access, delivery, and use" are important in DoD IP. In a traditional document-centric environment we just don't include data we don't want to. In an MBSE environment it's all inclusive:*

- *How do we provide "access and use" of that data/information in an MBSE environment ("rental")?*
- *What constitutes "delivery"? Physical delivery or negotiated access and for how long?*
- ***What about negotiated access to an MBSE environment of a producer and/or a "mirror' environment ?***

(2) ***IP Rights*** *are handled traditionally in a document-centric set of agreements. These may be integrated together across the acquisition, but is difficult without structure.* ***MBSE can enable an IP Rights process for the acquisition where IP rights are key attributes of SE processes*** *– and interrelations and dependencies are identified and modeled:*

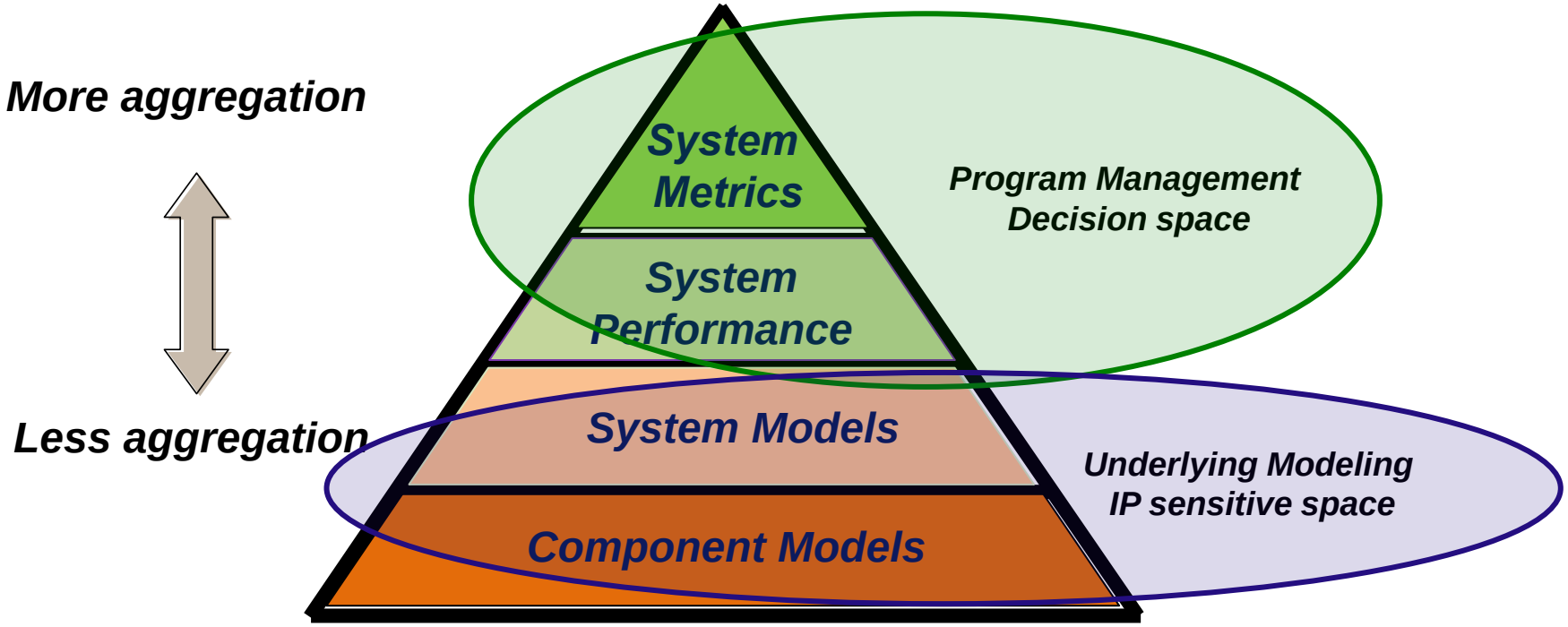
- *How do we build an "IP Strategy" workstream in an MBSE PM environment?*
- ***Why can't we link IP Rights to elements in an MBSE representation of the entire acquisition?***

(3) ***IP (Trade Secrets etc..)*** *are handled traditionally similarly to data- we just don't include in a document what we don't want to expose it in (business decision). In an* ***MBSE environment we need that information or a surrogate to create the model in the first place****:*

- *How do we model and entity/process completely without including IP sensitive data and representations?*
- ***This is a hard problem and a key stumbling block in MBSE and Mission modeling environments!***

Aggregation/Abstraction a modeling solution?

Aggregation. The process of grouping entities while preserving the salient effects of entity behavior and interaction while grouped[1]:

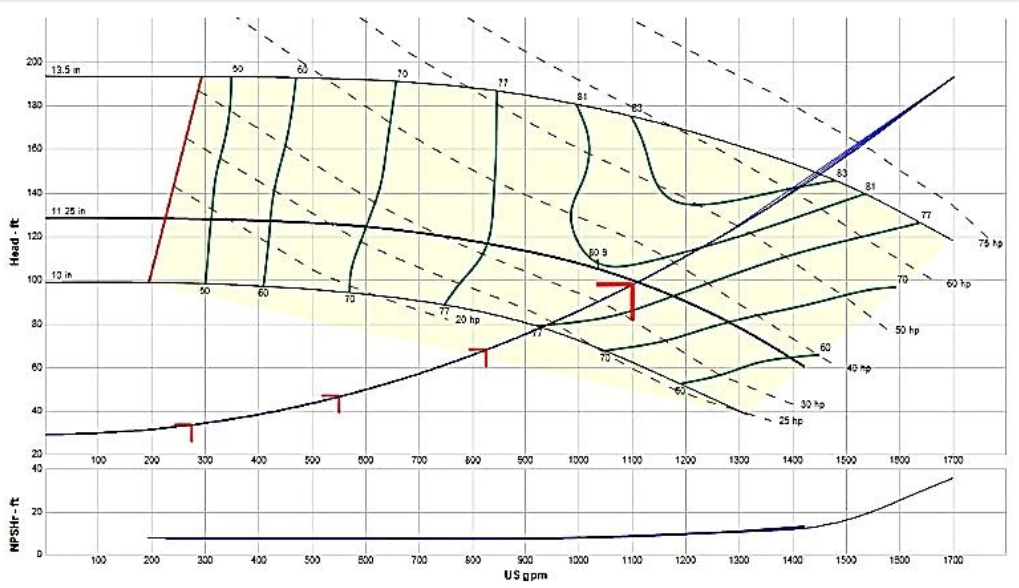


- As we move **up the pyramid the information is broader and more important** to the PM/Decision-maker – more abstraction from the underlying detailed models
- As we go **down it is more granular and focused**; becomes very descriptive of the system and components
- **PM's and Decision-makers need the outputs from modeling at the upper levels**, details below are not as important

If we want to "mirror" a manufacturer proprietary MBSE modeling environment for PM purposes.. Why not surrogate (Black Box) the sensitive models in the lower end of the pyramid?

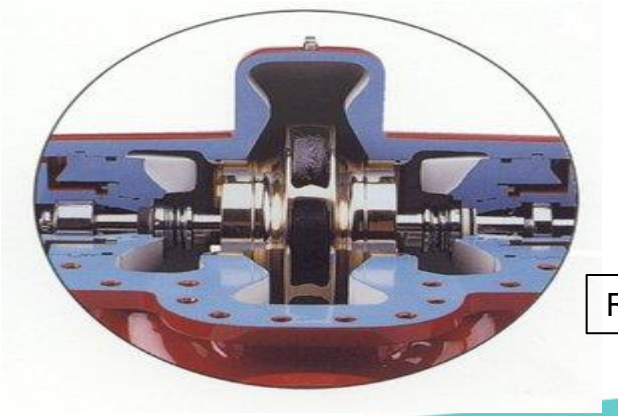
Example: Choosing a Centrifugal Pump -Traditional

- A manufacturer traditionally provides a picture of the pump, specifications, and a pump performance curve:



- They generally do not provide detailed construction details or specifics outside what the user needs for implementation; This is a business decision

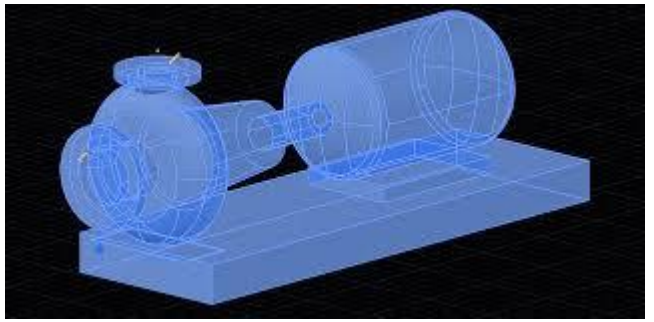
- The manufacturer does not disclose any details they regard as their IP or trade secrets unnecessary for their user to make an informed selection and use of their product – informed trade-off

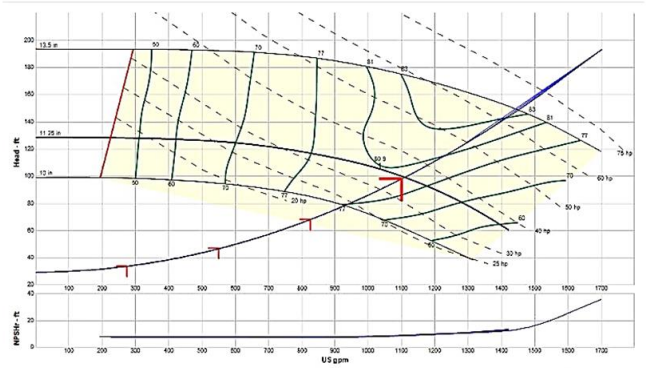


Ref: https://jmpcoblog.com

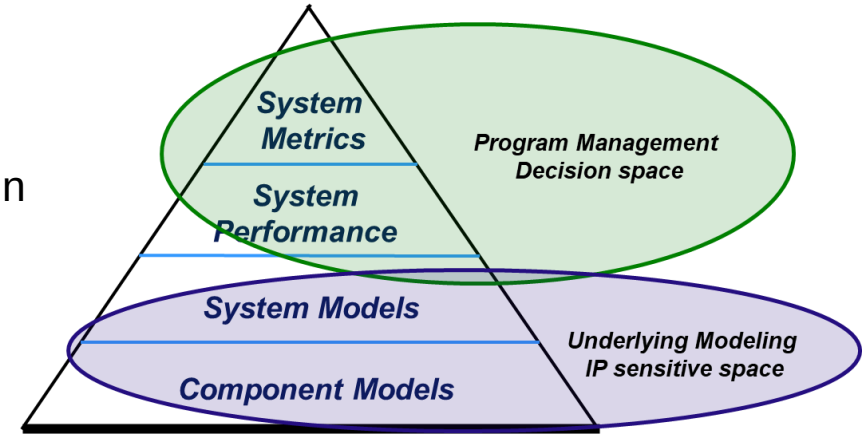
Example: Choosing a Centrifugal Pump - MBSE

- A manufacturer may provide a picture of the pump, specifications, and pump performance as an MBSE digital model:





- They do not have to provide all the underlying IP sensitive modeling in their "public" MBSE model, just surrogate models sufficient to produce the overall system performance at the top level;
  <u>This is a "black box" approach</u>



Ref: https://jmpcoblog.com
https://forums.autodesk.com/

Summary

(1) IP Deliverables:

- *How do we provide "access and use" of that data/information in an MBSE environment ("rental")?*
- *What constitutes "delivery"? Physical delivery or negotiated access and for how long?*

Explore negotiated access to an MBSE environment of a producer and/or a "mirror' environment

***(2) IP Rights**:*

- *How do we build an "IP Strategy" workstream in an MBSE PM environment?*

Link IP Rights to elements in an MBSE representation of the entire acquisition

*(3) IP (Trade Secrets etc..) are handled traditionally similarly to data- we just don't include in a document what we don't want to. In an **MBSE environment we need that information or a surrogate to create the model in the first place**:*

- *How do we model and entity/process completely without including IP sensitive data and representations?*

Use Abstraction/Aggregation techniques to "Black Box" the detailed Trade Secrets out of the delivered MBSE

Recommendations for NDIA SE Division

(1) Engage with the NDIA corporate IP initiative and NDIA members to look at these problems in Digital Engineering/MBSE adoption and potential solutions from the industry perspective

(2) Engage with the DoD IP Cadre[1] on the implementation of Digital Engineering/MBSE in systems engineering of Defense capabilities and meeting the requirements of DODI 5010.44

(3) Develop technical approaches to implementing IP workstreams into MBSE and system engineering baselines

1. Codified in Section 4, DOD INSTRUCTION 5010.44 INTELLECTUAL PROPERTY (IP) ACQUISITION AND LICENSING; https://www.esd.whs.mil/dd/dod-issuances/

Questions?

NORTHROP GRUMMAN

A View of the Digital Engineering Process.

A simple definition of the problem DE is solving, how DE can be used to solve the problem, and an overview of the needed technologies required to implement the solution.

NDIA 2021 Virtual Systems & Mission Engineering Conference

Jeff Bryson
Sr. Principal Engineer Systems

December 2021

NORTHROP GRUMMAN

Presentation Introduction

- Digital Engineering is a methodology that can be used to solve many different kinds of problems.
- In this presentation we will discus:
  - **What is the problem the DoD is trying to solve?**
  - **How can Digital Engineering support the effort to create the solution.**
  - **What is require for a Digital Engineering environment to be successful in solving the DoD's problem**

What is the problem the DoD is trying to solve?

- I have seen the following goals identified:
  - "Our customers are looking for faster cycle times and more affordable systems to counter rapidly evolving threats with a need to maintain capability and capacity." – Northrop Grumman
  - "we must modernize our defense systems and **prioritize speed of delivery**"-DoD National Defense Strategy of 2018
  - "In our industry, success isn't just about speed on the battle-field, but speed to the battlefield" *Wes Kremer : National Defense Magazine*
- I believe the statements above will not provide the DoD with the solutions they need.
- I believe the problem the DoD has, should be made clearer:
- We need to **"Reduce the time to solve problems of high complexity by an order of magnitude"**.
  - I have not seen this statement in any DoD, Northrop Grumman, or MBSE documentation.
  - If you can provide evidence that I am wrong, please let me know
  - If you can provide evidence that I am correct, please let me know
- For problems of "High Complexity":

If you don't define the problem that needs to be solved, you will not produce a solution to that problem.

What's the difference between these two statements

NORTHROP GRUMMAN

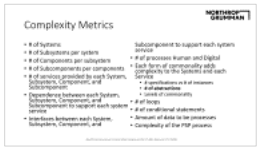
- **Deliver solutions with the speed, agility and affordability**
  - Move my current processes to a digital environment
  - At best, this statement says if I use a digital environment, I may be able to improve my current processes
  - The actions above imply that we just need to update out processes
- ***Reduce the time to solve problems of high complexity by an order of magnitude***
  - **We must change the way that we solve problems in a significant way**
    - If this statement does not make this clear, then a statement that makes clear the significance of the problem needs to be defined

NORTHROP GRUMMAN

Nothing yet says
‘Use Digital Engineering’

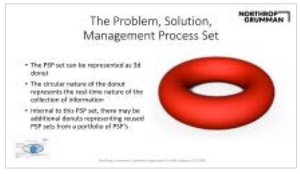
Concepts that need to be Clarified

- Commonality (Commonality is a paper/presentation by itself)
  - Commonality = A single source of record
- Complexity (this definition is a paper/presentation by itself)
  - Complexity is what drive up cost and time in solving problems.
  - There needs to be a standard way to identify, measure, and justify complexity
- Minimizing complexity
  - To ensure that the solution is not over complexity there should be an effort to ensure the complexity of the problem definition is close and directly related to the complexity of the solution definition and solution implementation



More Concepts

- **Problem Definition, Solution, Process** (PSP) set
  - The basic three actions required to solve a problem of high complexity are:
    - Define the problem
    - Create the solution (this includes verification)
    - Manage the process
- **Extendibility** = a single system of partial record. The single source is definition for a common ‘type’ of problem and is expected to have additional information/data/definition defined for a specific problem



What is a problem of High Complexity

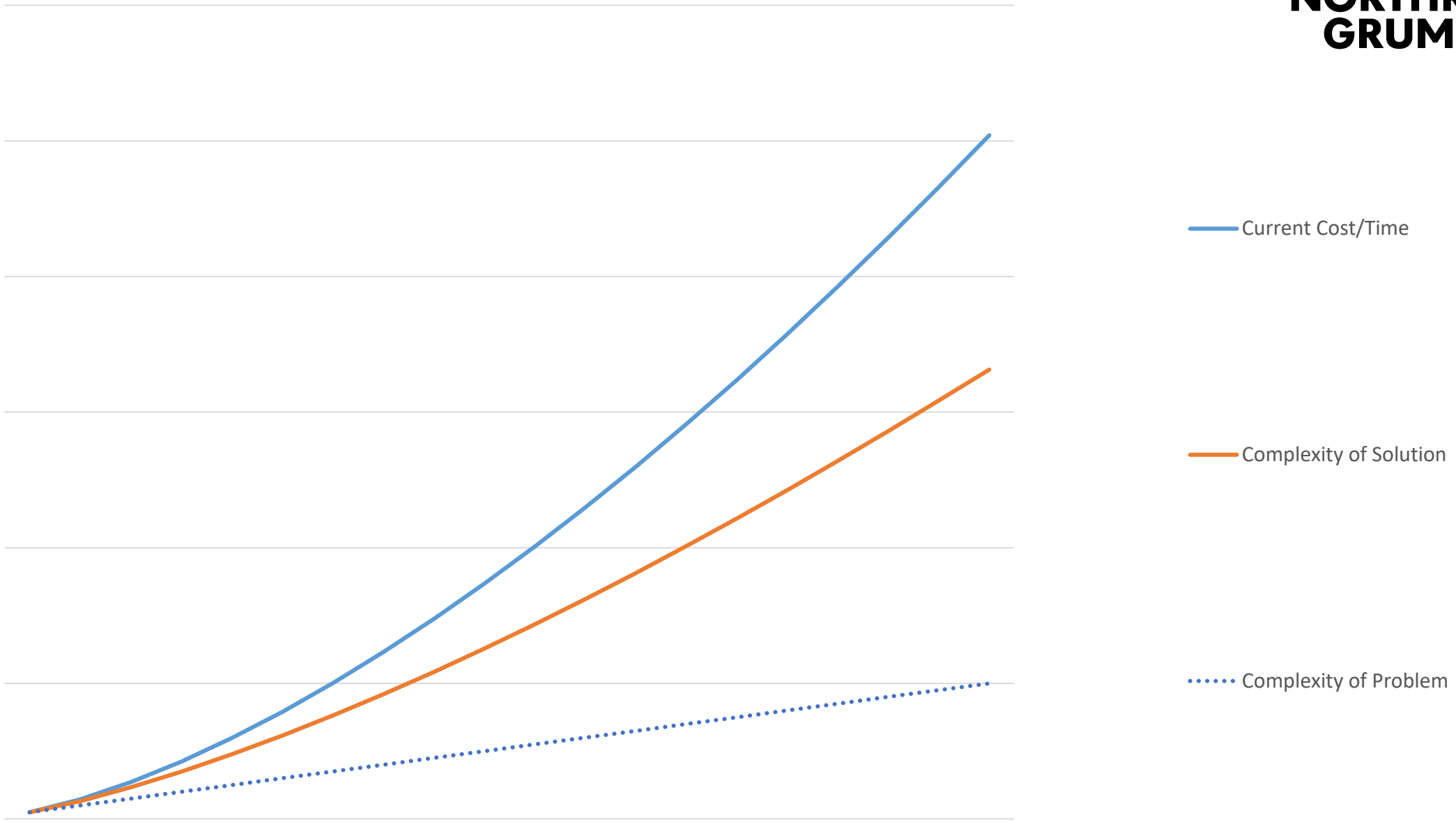
- From Chaos theory, there are four types of problems identified:
  - Ordered
  - Complex
  - Chaos
  - Disordered
- When we analyze the four types it can be argues that there are really only two forms of problems
  - Static
  - Dynamic (Complex, Chaos, Disordered)
- From this analysis it can be argued that a complex problem is a problem where the definition of the problem and the implementation of the solution are expected to change over time.
- A problem of high complexity is a problem that contains 2 or more internal problems of complexity
- The problem to '**Reduce the time to solve problems of high complexity by an order of magnitude**' is itself a problem of high complexity

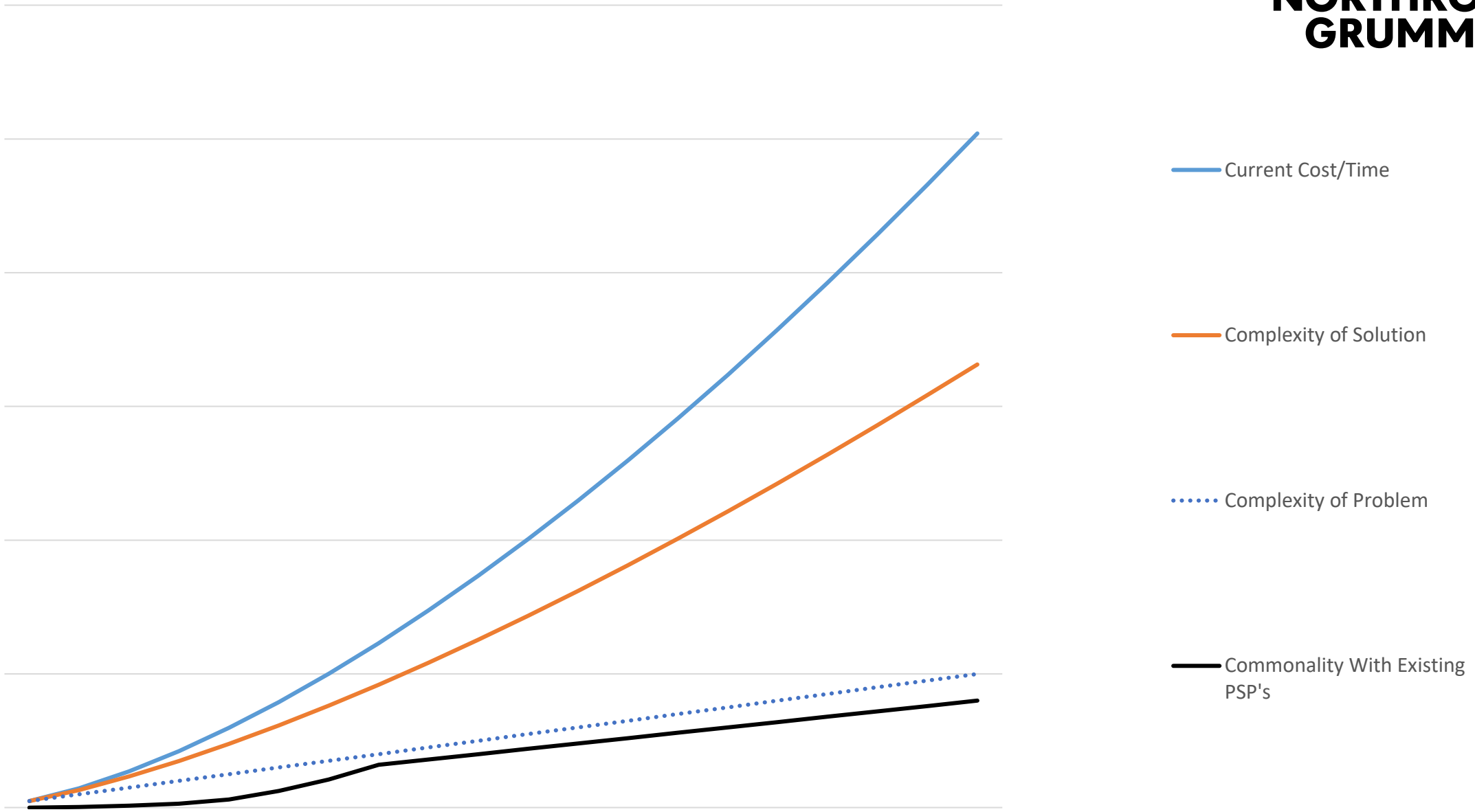

Complexity of the solution

NORTHROP GRUMMAN

How can we solve the time reduction problem

- There are many ways to try to reduce the time to solve these complex problems
- But we can't get there by reducing the time by 5% or 10%.
- We need a path/vision that allows us to solve problems that currently take 10 year, now in 1 year (Order of Magnitude)
- How? What is the vision?
    1. **Minimize the complexity of the Problem Definition, Solution, Process (PSP) set <u>that must be solved</u> by maximizing the commonality of the parts of the PSP that have <u>already been solved</u>**
    2. I need to ensure that the complexity of the solution is minimized

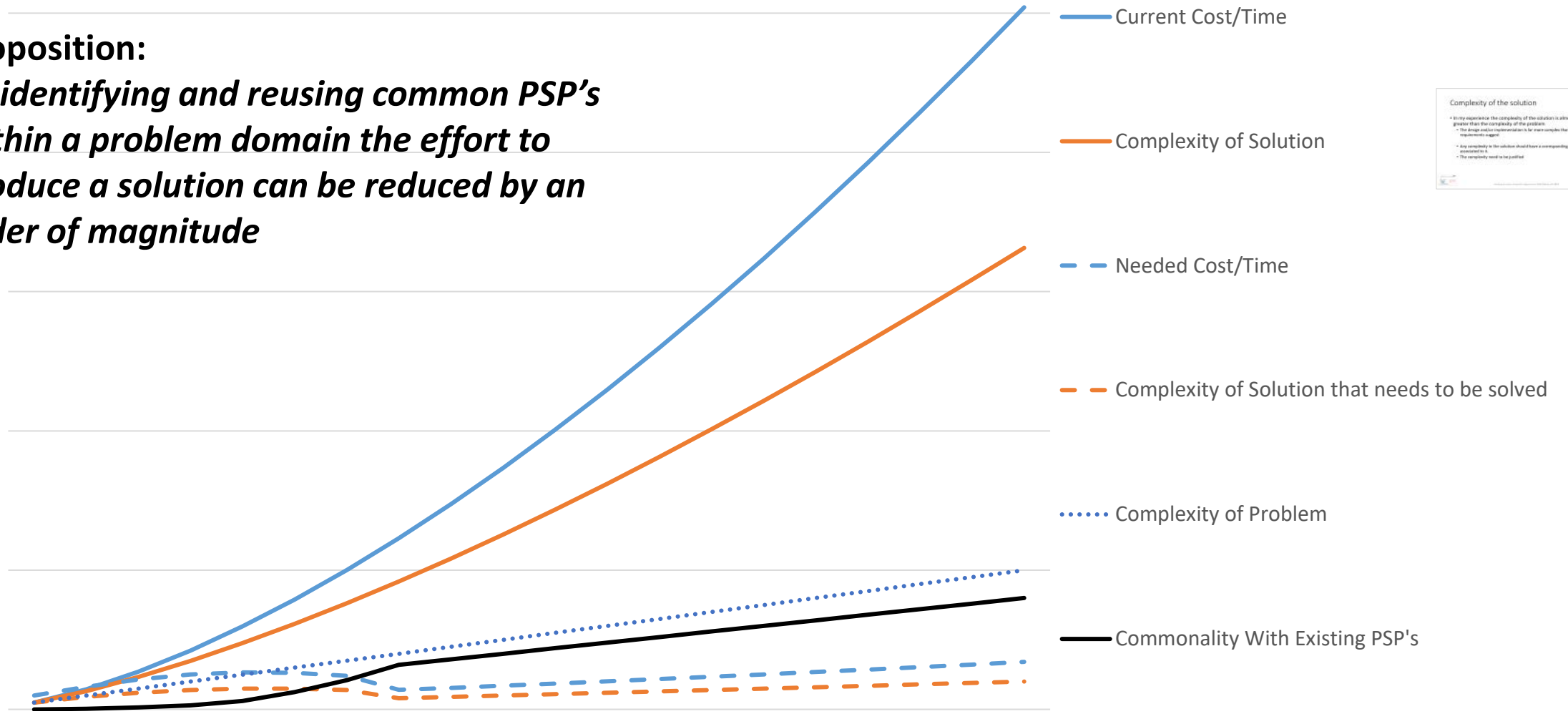




NORTHROP GRUMMAN

Proposition:

By identifying and reusing common PSP's within a problem domain the effort to produce a solution can be reduced by an order of magnitude



NORTHROP GRUMMAN

Nothing yet says
‘Use Digital Engineering’

Forms of Commonality and types Reuse

NORTHROP GRUMMAN

Reuse Type\Commonality Form		False	Reference	Pattern	Variable Pattern	Static Design	Dynamic Design
Copy & Paste		X					
Reference			X				
Recursion			X				
Pattern/Encapsulation	Service or Capability via Specification/Instantiation			X			
Service (parameterized)	Configurable			X	X		
Template (parameterized)	Configurable			X	X	X	
Extendable (Inheritance)	Extendable			X	X	X	
Overloading (Static Polymorphism)	Extendable			X	X	X	
Abstraction (RunTime Polymorphism)	Extendable			X	X		X

Now we see a clear need for a Digital Engineering Environment

NORTHROP GRUMMAN

- A Digital Engineering Environment can provide a means of defining, creating, linking and managing these common engineering artifacts in a problem domain centered portfolio
- This Digital Engineering Environment can also add additional benefits
  - Identification of the impact of change
  - A portfolio's history of commonality and reuse
  - An automated way of identify and compare complexity
  - An automated way of insuring consistency
  - An automated way of insuring commonality

What is require for a Digital Engineering environment to be successful in solving the DoD's problem

- First - Clearly identify the problem that we are trying to solve is.
  - **Reduce the time to solve problems of high complexity by an order of magnitude**
- Second - There need to be a clear understanding on why Digital Engineering is being used to solve this problem (The vision needs to be clear). What are the goals of using Digital Engineering.
  - **Minimize the complexity of the Problem Definition, Solution, Process (PSP) set that needs to be solved by maximizing the commonality of the parts of the PSP that have already been solved**
- Third - All types of reuse and commonality need to be clearly understood.
- Fourth - **The Digital Engineering Environment needs to support all forms of commonality.**

The current Digital Engineering Environment does not support all forms of commonality

- The DEE's I have seen are dependent (or should be) on a relational database.
  - All the artifacts, links, data mining activates justify the usage of an underlying database.
- There are current efforts to attempt to link and share model artifacts across models and tools.
  - These databases are all based on different designs making a translation effort the only viable means of sharing information

Translation if not a form of commonality

NORTHROP GRUMMAN

We need a new type of Database Environment

- We need a database environment that allows us to utilize all forms of commonality.
- At a minimum, the database environment would need to encapsulate the database schema, rules, and query logic (SQL) into a single **Database Specification** that then can have all forms of commonality applied to it.
- The basic forms of commonality (reference, recursion, encapsulation) support all the advance forms of commonality.
  - A foundation database specification might define a common modeling language (CML).
  - That CML database specification might then be extended with different forms of commonality to define more specific modeling language databases
  - Because there is a common database specification some data, analysis, and/or behavior would be common to all version of these models regardless of how the tools are implemented.

Summary

- **The DOD need to clearly identify the problem needs to be solved.** *"Reduce the time to solve problems of high complexity by an order of magnitude"*
- **The DOD needs to identify and documentation their 'Vision' of how Digital Engineering should be used to solve this problem.**
- *"Minimize the complexity of the problem (PSP) that must be solved by maximizing the commonality of the parts of the problem (PSP) that have already been solved"*
- **The industry need to migrate form a start/stop (Linear) engineering process's to engineering process's that are based on Finite State Machines (Cyclic)**
- **An environment that allows for the utilization of all forms of commonality need to be created and used**

An Elastic Approach to Digital Engineering

Matthew Taylor
Intelligent Systems Engineering SME

Safe Harbor Statement

This presentation contains "forward-looking statements," within the definition of the Private Securities Litigation Reform Act of 1995. These statements are subject to numerous assumptions, risks, and uncertainties, many of which are outside of our control, and include the risks and uncertainties that are identified in the Risk Factor section in our Annual Report on Form 10-K (filed with the SEC on February 19, 2021), and in other periodic and current reports we file with the SEC. While the forward-looking statements herein reflect our current expectations, no assurance can be given that the results or events described in such statements will be achieved, and our actual results may differ materially from the results we anticipate.

We undertake no obligation to revise or update any of these forward-looking statements (whether as a result of new information, subsequent events or circumstances, changes in expectations or otherwise) that may arise after the date of this presentation.

****

Agenda


Digital Engineering
Optimizing Digital Engineering
fleX-engineering™ Approach
Future Work

What is Digital Engineering? [1]

- Digital Engineering (DE) is defined as ‘‘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”
- DE combines model-based techniques, digital practices, and computing infrastructure to enable delivery of high pay-off solutions to the end users at the speed of relevance.
- DE modernizes how the scientists and engineers conceive, design, operate, and sustain capabilities to outpace adversaries.
- DE incorporates technological innovation into an integrated digital model-based approach to transform the state of engineering practice in support lifecycle activities.

DE Accelerates Missions – It is Not, Itself, the End Goal

Applying DE Capability for Customers is Complex… (but let's look closer here)

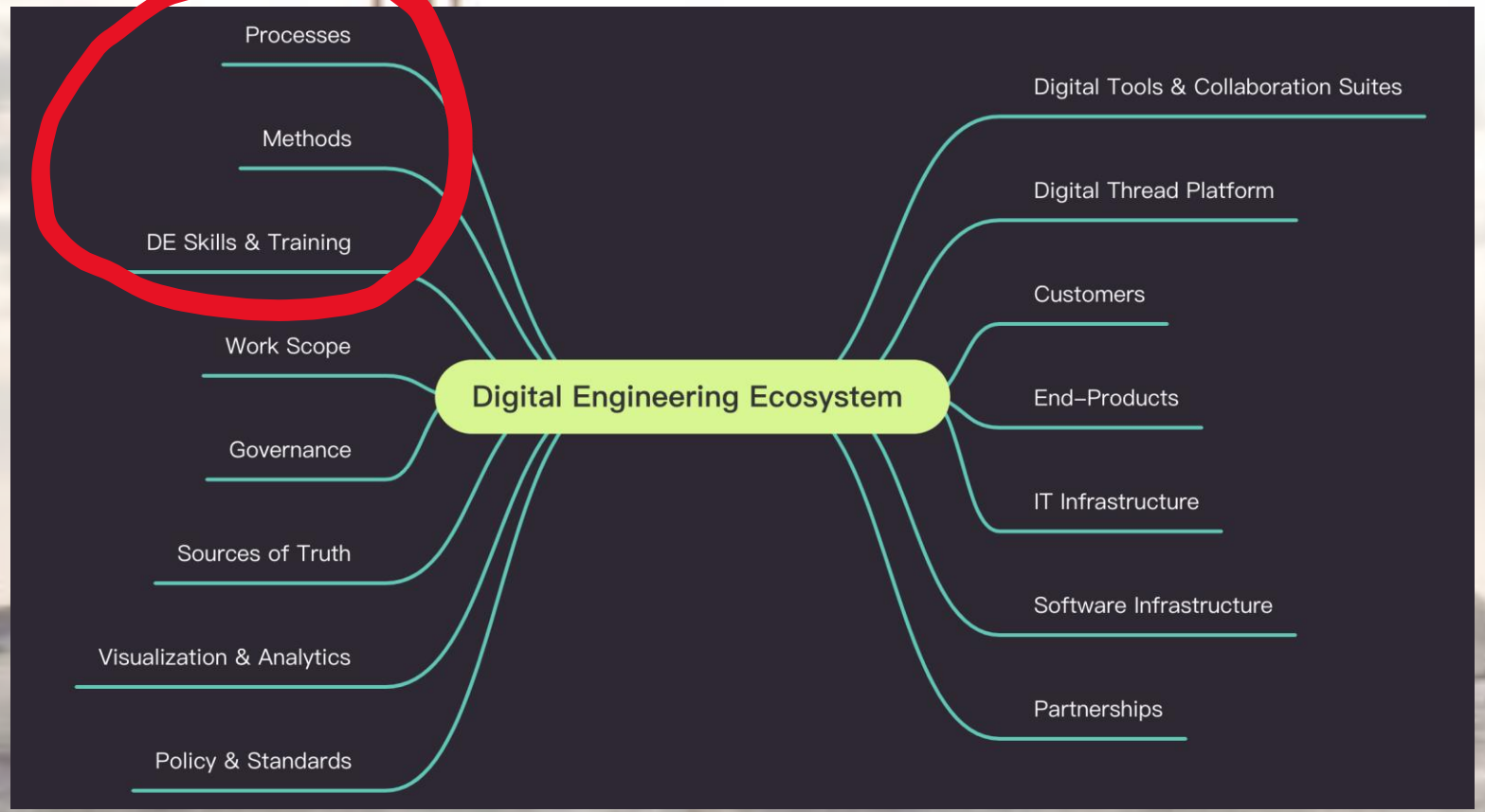
Challenges

- Methods and processes in use by orgs typically not 'born digital'
- Orgs possess varying mix of DE competency

Our Approach

flex-engineering™

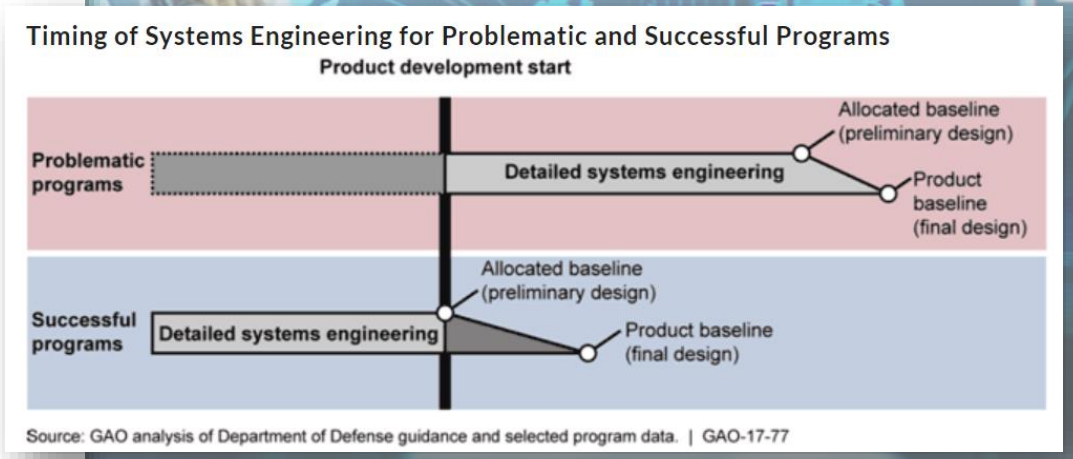
ManTech UNIVERSITY



Analogy: Optimizing Size of SE Effort

Return on Investment (ROI) and sizing Systems Engineering effort is a well-studied problem:

- http://www.hcode.com/seroi/ (SE ROI)
- INCOSE SE Handbook[2], Section 2.8.1
- GAO-17-77[3]
- GAO-15-469[4]



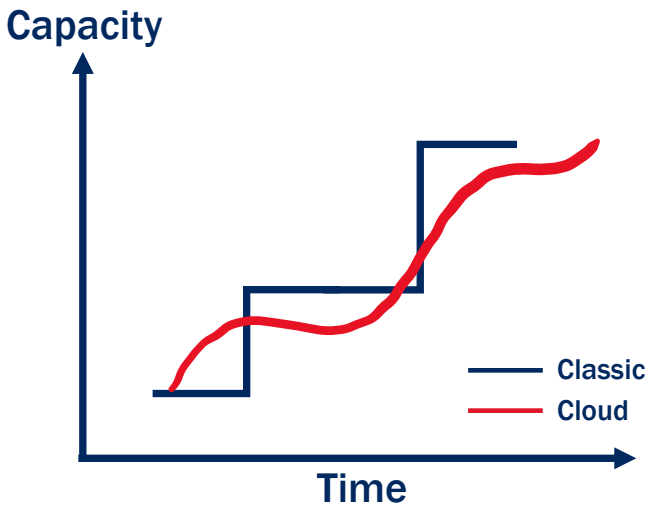
There Are Also 'Right Amounts' and 'Right Times' for DE Effort… It's Different for Every Project.

Analogy: Elasticity in Cloud Computing

Acquire resources as you need them, and release resources when you no longer need them. In the cloud you want to do this automatically, and dynamically.

The DE approach should be optimally sized for the needs of the project at each point in time. You also want to do this dynamically; predicting it all at project inception is difficult:

- The project evolves
- Technology evolves
- DE capabilities mature and evolve

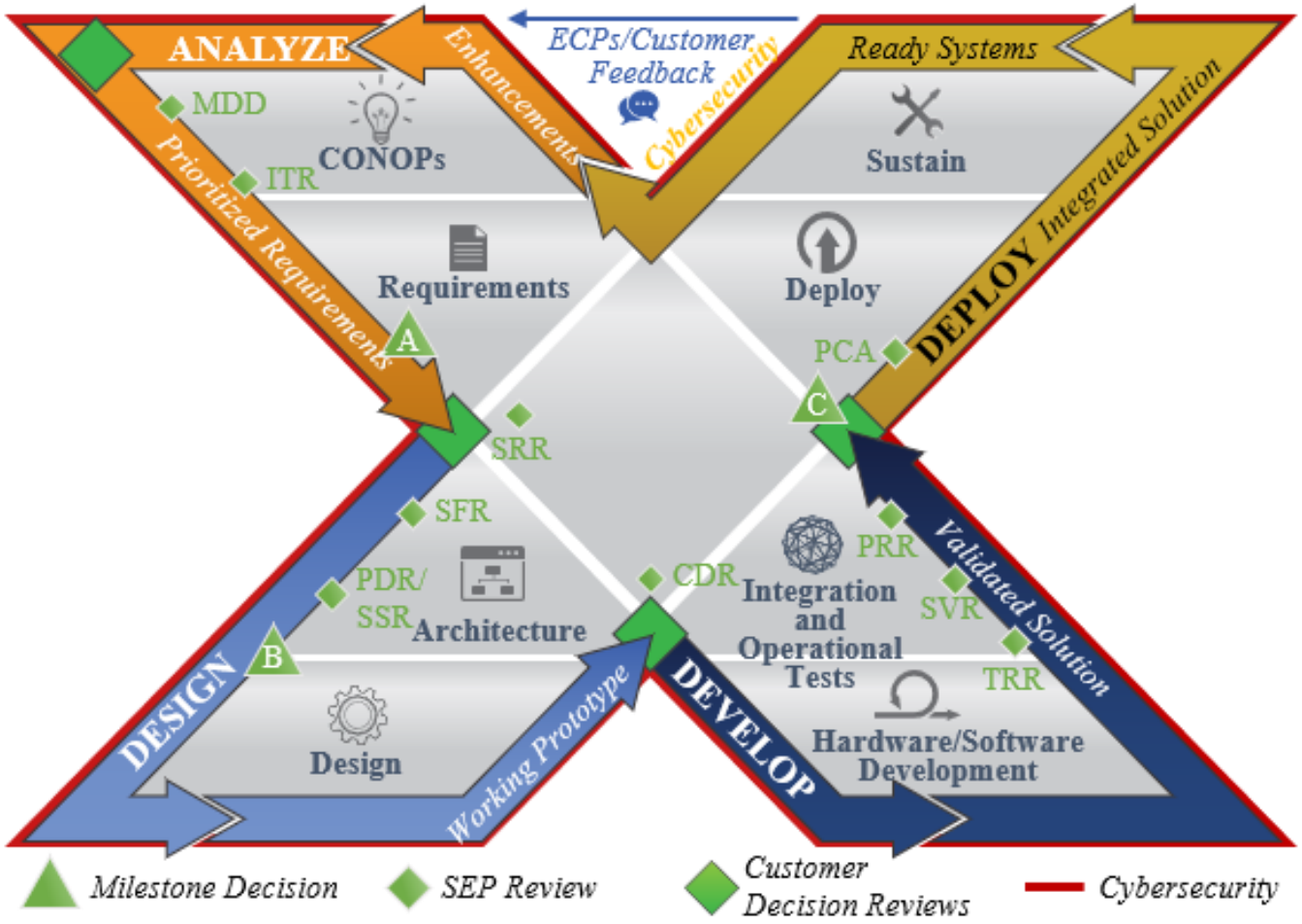


DE is Not 'Set, and Forget'…
Inspect the DE Approach, Expand/Contract as Needed.

Toaster Image: © 2021 Breville USA, Inc.

Finger Image: https://pixabay.com/vectors/pointing-finger-pointing-hand-3170418/

fleX-engineering™ Approach



ISO/IEC/IEEE 15288 Technical Processes Mapped by X 'leg'

ANALYZE
- 6.4.1 Business or mission analysis process
- 6.4.2 Stakeholder needs and requirements definition process
- 6.4.3 System requirements definition process

DESIGN
- 6.4.4 Architecture definition process
- 6.4.5 Design definition process
- 6.4.6 System analysis process

DEVELOP
- 6.4.7 Implementation process
- 6.4.8 Integration process
- 6.4.9 Verification process

DEPLOY
- 6.4.10 Transition process
- 6.4.11 Validation process
- 6.4.12 Operation process
- 6.4.13 Maintenance process
- 6.4.14 Disposal process

fleX-engineering™

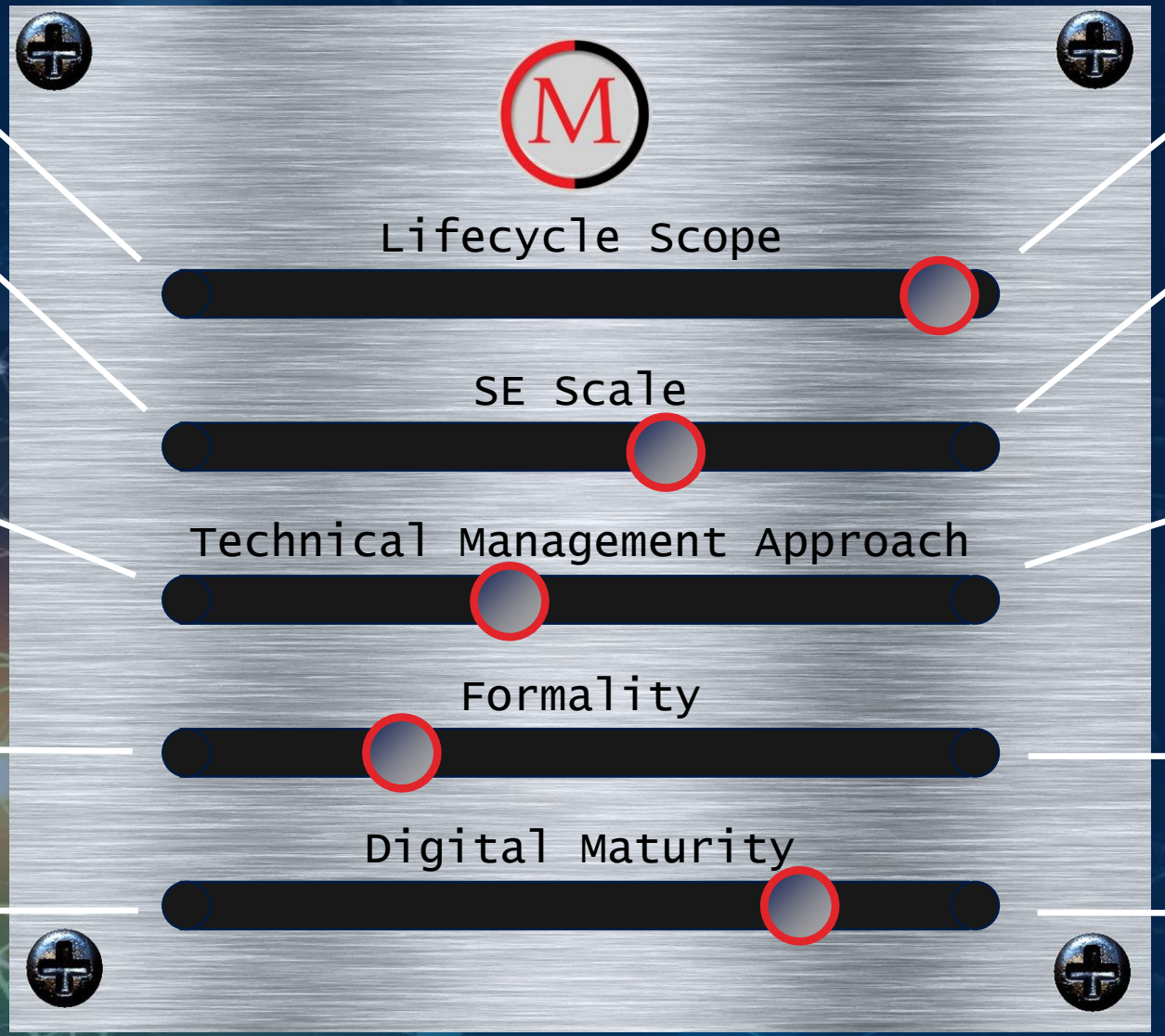
Single SE Process
- One 15288 outcome
- Partial fleX “X”

Very Small Entity
- Lightweight process & work products reflect ISO 29110 – Entry profile

Waterfall
- Sequential, planning focused, full system scope advanced linearly

Low Ceremony
- Continuous or informal review, focused meetings & artifacts

Document-based
- Documentation-centric, ad-hoc threading of info



All SE Processes
- All 15288 outcomes
- Full flex “X”

Large Organization
- Heavyweight process & work products reflect full ISO/IEC/IEEE 15288

Iterative
- Continuous planning & adjustment, system scope advanced via threads

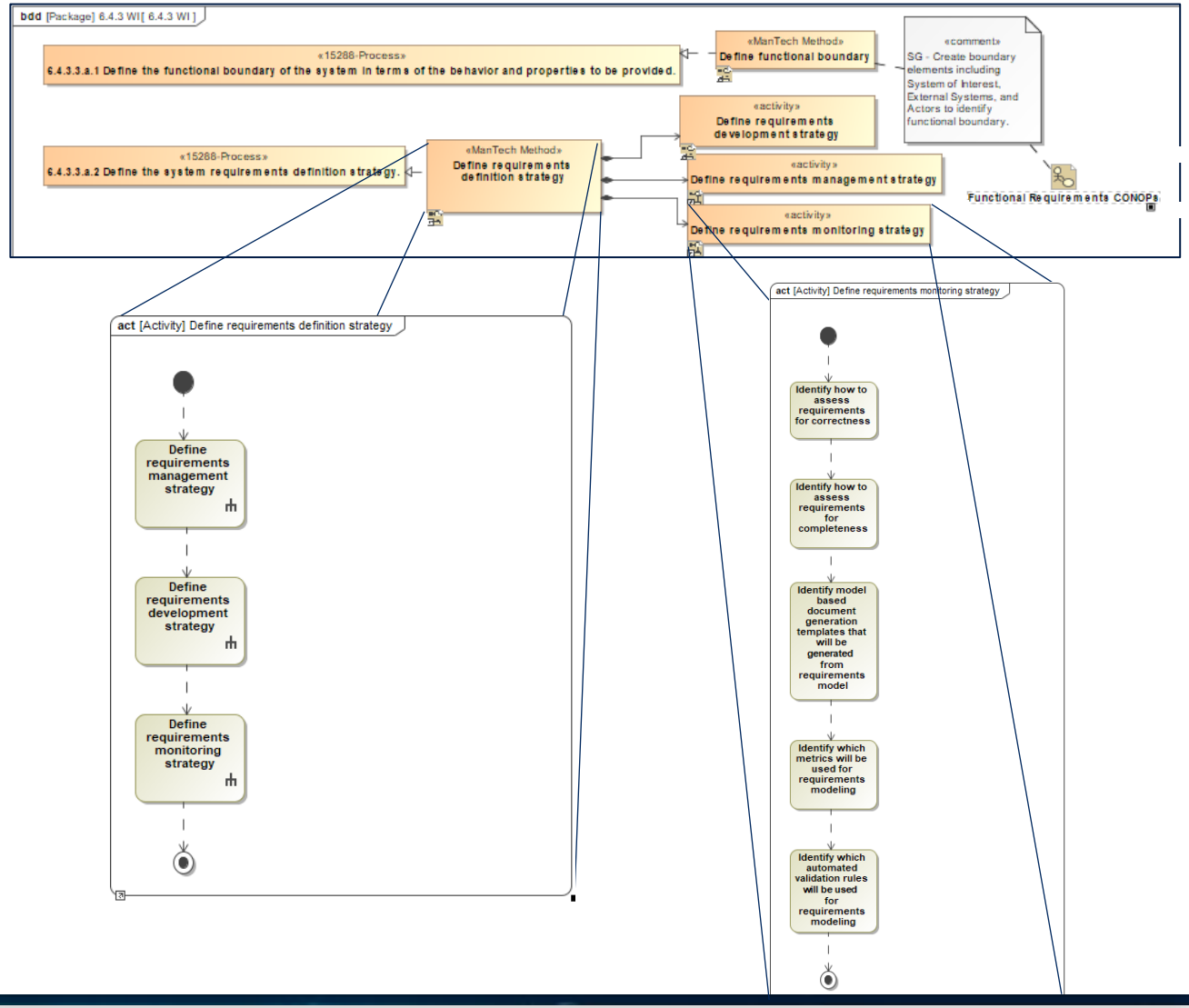
High Ceremony
- Stage-gate reviews, high meetings, high artifacts

Model-based
- Architecture-centric, self-documenting models, digital threading of info

Model-Based Work Instruction

- Work instructions architected in Cameo help with the creation of a Systems Engineering Management Plan
- Work Instructions accompanied with style guides and validation rules to provide quality control of artifacts and methodology described
- ManTech methods and associated activities are ‘micro-processes’ that are tailored in or out at higher levels

Example SysML Work Instruction in Cameo



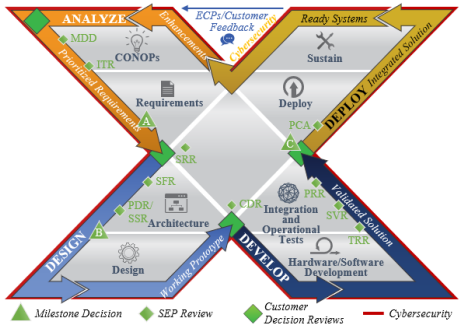
Flexibility with Discipline (Process Owner)

fleX-engineering™ Users

methodpark by UL stages

DASSAULT SYSTEMES
Teamwork Cloud
CAMEO COLLABORATOR

Process Owners



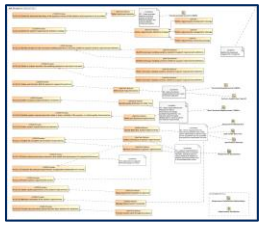
What

- Value Streams
- Workflows & Activities
- Phases & Milestones
- Work Products
- Guidance
- Roles

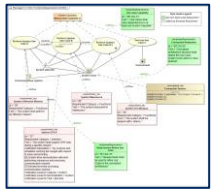
- Establish & maintain processes
- Control and view versioning
- Structure tailoring
- Compliance/Reference tracing

Links To

How



Work Instructions



Style Guide Validation

Training Videos

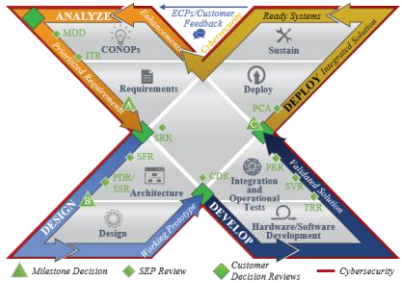
Flexibility with Discipline (Process Customer)

fleX-engineering™ Users

methodpark by UL stages

DASSAULT SYSTEMES Teamwork Cloud CAMEO COLLABORATOR

Program A



Program B

Tailoring

Value Streams
Workflows & Activities
Phases & Milestones
Work Products
Guidance
Roles

Program-specific

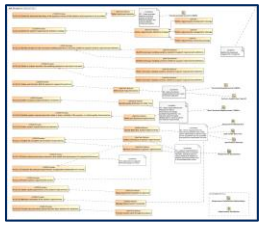
Tailoring

Value Streams
Workflows & Activities
Phases & Milestones
Work Products
Guidance
Roles

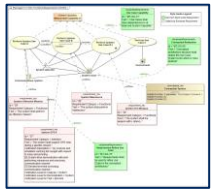
Program-specific

Links To

Links To



Work Instructions



Style Guide Validation

Training Videos

Final Thoughts

- DE approaches should be elastic in nature and adapt to the work at hand.
- Work to enable speed and flexibility, with discipline.
- Connect information to eliminate process islands, support DE knowledge management in the enterprise.

Future Work

- Mature and evolve process, work instruction, style guide models.
- Incorporate recent work on governance of models into processes and methods
- Evaluate fleX-engineering™ approaches against DE competency[5,6], maturity frameworks, customer efforts[7].
- Explore synching modeled process and modeled work instruction.

References

1. United States Department of Defense, “Digital Engineering Strategy,” June 2018, available at, https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf, accessed July 2021.
2. Walden, David, G. Roedler, K. Forsberg, R. Hamelin, T. Shortell, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, Fourth Edition, John Wiley & Sons, Inc. 2015.
3. https://www.gao.gov/products/gao-17-77
4. https://www.gao.gov/products/gao-15-469
5. https://sercuarc.org/serc-programs-projects/project/86 for the DE competency study
6. https://www.incose.org/products-and-publications/competency-framework
7. https://www.afmc.af.mil/Digital/

Thank you

For more information contact:

Matthew Taylor, Matthew.Taylor@ManTech.com

Dr. Douglas Orellana, Douglas.Orellana@ManTech.com

Dr. Heidi Davidz, Heidi.Davidz@ManTech.com

Updating DoD Policy and Guidance for Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)

Philomena Zimmerman
Director, Engineering Tools and Environments

Joseph Carnell
Senior Analyst, Engineering Policy & Systems / Engineering Tools & Environments

Office of the Deputy Director for Engineering
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems and Mission Engineering Conference
Virtual
December 2021

https://www.CTO.mil *@DoDCTO*
https://ac.cto.mil/engineering

Abstract

The Department of Defense (DoD) and the military services recognize the value of modeling and simulation for many aspects of their operations and have prepared directives and guidelines to provide general instructions on how, when, and under what circumstances to employ formal Verification, Validation, and Accreditation (VV&A) procedures. VV&A incorporates three interrelated processes to gather and evaluate evidence to determine whether the capabilities, accuracy, correctness, and usability of a model or simulation are sufficient to support its intended uses. An accreditation recommendation reflects the degree to which the verification and validation (V&V) evidence supports using the model or simulation.

The Department's instruction for DoD Modeling and Simulation (M&S) VV&A (DoDI 5000.61) establishes policy, assigns responsibilities, and prescribes procedures for the VV&A of models, simulations (including distributed simulations), and their associated data. The current policy was approved December 9, 2009, with an interim change approved October 15, 2018. Supplemental guidance exists to support DoD- and Service-level M&S Communities in the effective and efficient implementation of VV&A Policy.

The Policy and Guidance for M&S VV&A are undergoing a comprehensive review and revision that reflect a decade's worth of changes in expanded use and consideration of models and simulations. The purpose of this VV&A Policy update is much more than the simple reissuance of a DoDI. The goal is to enhance the state of practice of modeling and simulation VV&A and establish a comprehensive framework for modeling and simulation credibility that operates within a suitable DoD Policy and the best practices and documentation standards that facilitate its implementation.

The review scope includes the VV&A processes as captured in the current policy; the notion of risk of use and the potential for policy and guidance to improve applications of risk-based concepts; current terminology and the need to address modern concepts such as trustworthiness and credibility; and the possible expansion of VV&A techniques in either policy or guidance. Consideration is also given to the position of the current policy as the basis for Service and Agency instructions, policy and guidance.

What is VV&A?

Three interrelated processes

to gather and evaluate evidence

to determine whether the capabilities, accuracy, correctness, and usability

of a model or simulation

are sufficient to support its intended uses

- **Verification** – Did I build the thing right?
- **Validation** – Did I build the right thing?
- **Accreditation** – Is it believable enough to be used?

An accreditation recommendation reflects the degree to which the V&V evidence supports *using* a model or simulation

VV&A Policy Overview

- OUSD(R&E) is responsible for the Department's Policy for DoD Modeling and Simulation VV&A
  - DoD Instruction (DoDI) 5000.61
  - Associated guidance on best practices
  - Documentation standards

VV&A Website
(https://vva.msco.mil)
- VV&A Templates
- MIL-STD-3022
- Recommended Practices Guide

VV&A Policy and Guidance

"Policy" relates to DoD Issuances (e.g., Directives & Instructions)
"Guidance" is about technical implementation

Policy

- DoDI 5000.61 – DoD Modeling & Simulation VV&A

Guidance

- Mil-STD-3022 – Documentation of VV&A for Models and Simulations
- Recommended Practices Guide

Key Features of DoDI 5000.61

- Establishes DoD policy for VV&A of M&S
  - Requires VV&A of models, simulations and data used to support DoD processes, products and decisions
  - Directs VV&A results be documented and made accessible
  - Assigns Components and PAS* Officials as final validation authority for representations in their areas of responsibility
- Establishes standards for documentation and accessibility of VV&A results

* OSD Presidentially Appointed, Senate-confirmed (PAS)

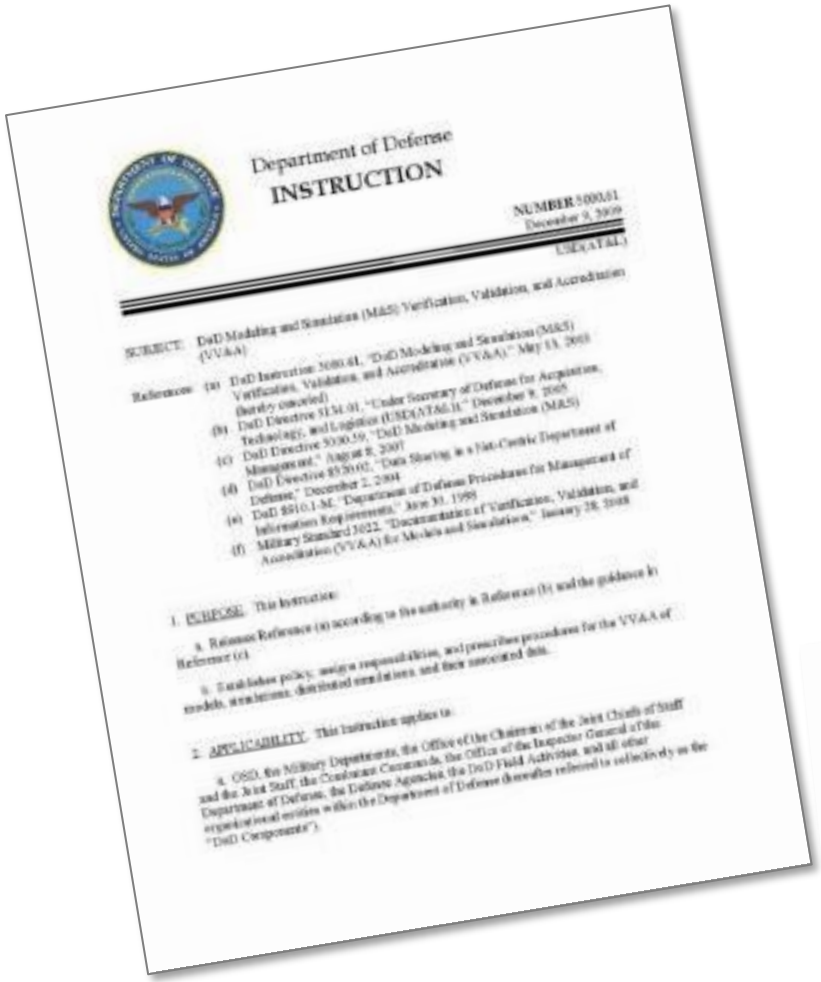
DoDI 5000.61 Sets Overarching VV&A Policy

*"**Heads of the DoD Components and OSD Presidentially Appointed, Senate-confirmed (PAS) officials** are authorized to provide, within their areas of responsibility, VV&A procedures and guidance as appropriate and in accordance with this Instruction." (DoDI 5000.61 draft, para 1.2.e.)*

*"The Heads of the DoD Components and the OSD Presidentially Appointed, Senate-confirmed (PAS) Officials shall… **Establish VV&A policies, practices, and procedures for models, simulations, and associated data**, within their areas of responsibility." (DoDI 5000.61 draft, para 2.4.)*

*"VV&A Recommended Practices Guide (RPG). The RPG is intended to **facilitate the application of DoD-specified directives and guidelines, and to promote the effective application of VV&A**. The guidance contained within this RPG is generally applicable to the full spectrum of M&S products employed for military and defense applications." (DoDI 5000.61 draft, para 3.2.b.)*

Status of VV&A Policy & Its Interdependencies


Department of Defense
INSTRUCTION

NUMBER 5000.61
December 9, 2009
USD(AT&L)

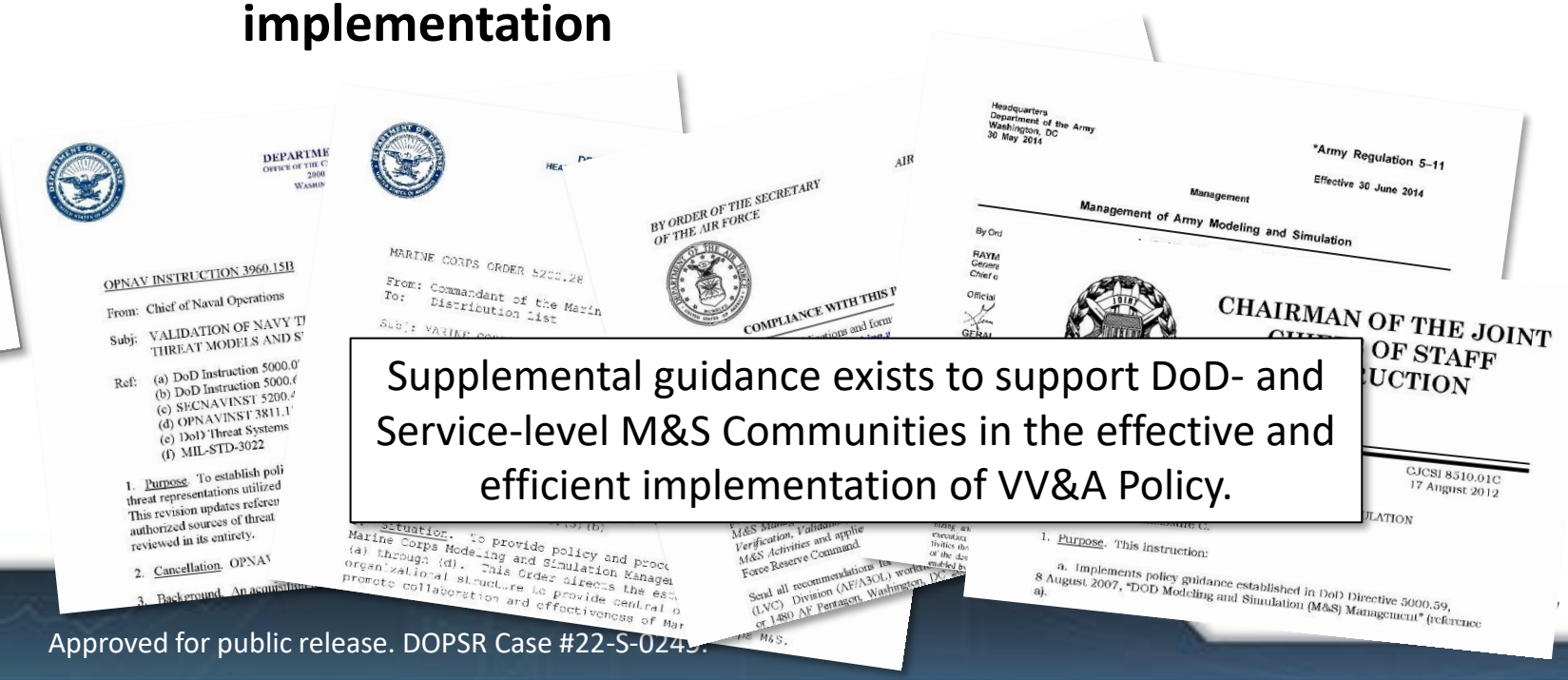
SUBJECT: DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)

1. PURPOSE. This Instruction:

2. APPLICABILITY. This Instruction applies to:

DoDI 5000.61, DoD M&S VV&A

- Issued: Dec 9, 2009 w/ Ch 1 Oct 15, 2018
- Currently undergoing review and update
  - Concepts and terminology consistent with current practices (e.g. Digital Engineering Strategy)
  - Templates for documentation
  - Additional guidance needed for effective, efficient implementation


OPNAV INSTRUCTION 3960.15B

From: Chief of Naval Operations

Subj: VALIDATION OF NAVY TH
THREAT MODELS AND S

Ref: (a) DoD Instruction 5000.0
(b) DoD Instruction 5000.
(c) SECNAVINST 5200.
(d) OPNAVINST 3811.1
(e) DoD Threat Systems
(f) MIL-STD-3022

1. Purpose. To establish poli
threat representations utilized
This revision updates referen
authorized sources of threat
reviewed in its entirety.

2. Cancellation. OPNAV

MARINE CORPS ORDER 5200.28

From: Commandant of the Marin
To: Distribution list

BY ORDER OF THE SECRETARY
OF THE AIR FORCE

COMPLIANCE WITH THIS P

Headquarters
Department of the Army
Washington, DC
30 May 2014

*Army Regulation 5–11

Effective 30 June 2014

Management

Management of Army Modeling and Simulation

CHAIRMAN OF THE JOINT
OF STAFF
UCTION

CJCSI 8510.01C
17 August 2012

1. Purpose. This instruction:

a. Implements policy guidance established in DoD Directive 5000.59, 8 August 2007, "DOD Modeling and Simulation (M&S) Management" (reference a).

Supplemental guidance exists to support DoD- and Service-level M&S Communities in the effective and efficient implementation of VV&A Policy.

ModSim Community of Practice & Pain Points

Pain Points nominated, consolidated, prioritized by MS CoP WG Core members

- Lack of a current DoD strategy for simulation interoperabilty
- Lack of adequate standards program
- Lack of a common lexicon of technical, functional, programmatic, and acquisition terms related to DoD Enterprise modeling and simulation
- Insufficient agile/responsive RMF process (permissions) to quickly stand up LVC simulation events
- Insufficient Multi-Level Security guidance for simulation events
- **Inadequate V&V policy and guidance to support new rapid acquisition, test, analysis, and training capabilities**
- Insufficient authoritative data sources, insufficient ability to discover and share
- **Lack of V&V techniques for M&S supporting cloud environment, AI and Autonomy**
- Lack of guidance and tools to better integrate all M&S with Digital Engineering Infrastructure
- **Lack of automated V&V tools to speed process**
- **Lack of validation methods for small data sets for T&E**
- Lack of an integrating infrastructure to facilitate Discovery, Accessibility, and Reuse of Models and Simulations to better support the M&S community
- Lack of a DoD-wide repository for models and simulations
- Insufficiently trained and knowledgeable M&S Workforce
- Insufficient collaborative body for M&S resource decision making and problem solving
- Lack of a resourced and empowered centralized organization that can make tangible decisions / develop interoperability solutions for implementation across the Services
- Lack of cyber / EMS / space models
- Insufficient environmental representations
- Lack of accurate human representations (digital human)
- Insufficient understanding of human / machine interface
- Insufficient threat representation
- Inadequate support and correlation for Multifidelity Representation
- Lack of cloud-enabled models and simulations
- Current simulations are not rapidly composable in containerized, modular methods from remote locations-M&S as a Service
- Lack of simulations compatibility for distributed simulation in the cloud
- Lack of modeling frameworks that enable rapid simulation composition to better support rapid combat capability development processes
- Insufficient collaborative M&S environment for both US and International Partners

DoD VV&A Workshop – A First Step

- Policy and Guidance must reflect a decade's worth of changes
  - VV&A concepts and terminology
  - Documentation templates for evolving VV&A responsibilities
  - Breadth and depth of recommended practices
- R&E convened a workshop on April 14, 2021
  - Reviewed the current policy and associated guidance
  - Presented VV&A challenges across Services and Communities
  - Identified common areas to address in DoD policy and guidance

Focus Areas for Review/Update

- Generality
  - Should the V&V process be more general to support uses beyond the original intended use?
  - If so, how do we capture them in policy and/or guidance?
- Risk of use
  - The notion is implicit in policy and guidance, but is it understood?
  - How do we improve understanding and applications of risk-based concepts?
- Terminology
  - How do the ideas of Trustworthiness and Credibility differ from Accreditation?
  - Should we define those in policy or guidance?
- V&V techniques
  - Which acceptable/encouraged/preferred V&V techniques are captured/maintained by OSD?
  - Should DoD level policy or guidance address this?
  - Is this functional-area (community) or Service- specific?
  - Should subordinate policies and guidance be stored or referenced in a DoD-level repository?

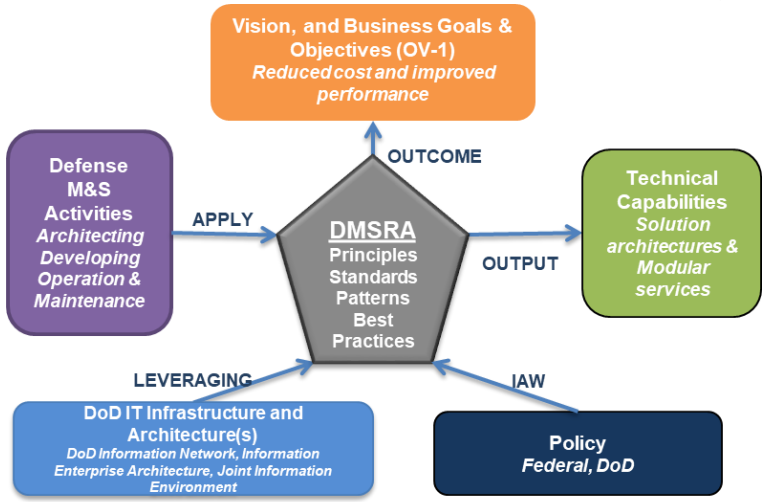
Initial Update Activities

- Service Coordination
  - Service-led M&S VV&A Working Groups
  - Service reviews of policies and dependency to DoD issuance
- Digital Engineering
  - “Fit for use” – validation needs if not original intended use
  - Understanding data/info from a model or simulation, decision to trust and use it
  - Digital artifacts – explore specifications for use of metrics
  - Address critical areas like Cyber modeling and Digital Twins
- Test & Evaluation
  - M&S is critical to delivering relevant capabilities faster; V&V is vital to testing
  - Testing requires a consistent M&S framework, standards, best practices at different levels of modeling
  - Develop Use Case on (earlier) use of models & simulations, specify in T&E Master Plans
- Threat Modeling
  - Joint Threat Modeling Program – incorporating IC models, cost for developing trust
  - Variation in blue, threat behavior and rapidly emerging threats can invalidate the validation assessment
  - Maintain link to end users so IC gets useful feedback on models
  - Develop Use Case on how a threat representation is validated, quantification of uncertainty

Beyond DoD Policy and Guidance Updates

- Partnership with Simulation Interoperability Standards Organization
  - Product Steering/Development Group on VV&A
  - Paper review at the February 2022 Simulation Interoperability Workshop
  - Focus on Use Cases in the RPG and recommend changes, additions
  - Include international VV&A standards, particularly, consistent terminology

SISO
Simulation Interoperability Standards Organization
"Simulation Interoperability & Reuse through Standards"



- DoD M&S VV&A Framework
  - Enhance the state of practice of modeling and simulation VV&A and establish a comprehensive framework for credibility
  - Common guidance to improve effectiveness and efficiency of joint and combined VV&A
  - Foster innovation in processes that improve credibility of models and simulations for proper use, enhanced interoperability, reuse, and trust

Contact

Philomena Zimmerman
Director
Engineering Tools and Environments
OUSD(R&E)
philomena.m.zimmerman.civ@mail.mil
571-372-6695

Joe Carnell
Modeling and Simulation Validation & Credibility Lead
Engineering Tools and Environments
OUSD(R&E)
joseph.a.carnell.ctr@mail.mil
571-372-6672

Model Portfolio Management (MPM): A Guide for Best Practices

Misak Zetilyan, Jordan Howie, Al Hoheb, Alexander Chang
The Aerospace Corporation

December 2021

Cleared for Public Release OTR 2022-00118

Agenda

MPM Guide Presentation Topics

- **Background**
  - *Problem/Solution*
  - *Implementation*
  - *Definitions*
  - *Use Cases*
  - *Approach*
  - *Deliverables*
  - *Roles and Responsibilities*
- **Life Cycle** (Goals, Work Products, and Activities)
  - *Initiation*
  - *Planning*
  - *Execution*
  - *Monitoring and Control*

Problem/Solution

Bottom Line Up Front (BLUF)

- **Problem**
  - *Acquirers that routinely ask for "Model Management" work and get large variance of responses*
  - *"Model Management" scored low by organizations – INCOSE Model-Based Capabilities Matrix*
  - *"Model Management" as a significant area of improvement – SERC SE Survey*
  - *No prior guide or standard that addresses managing a collection of models*

- **Solution**
  - *The Aerospace Corporation wrote the "Model Portfolio Management (MPM) Guide" technical operating report TOR-2021-01577, cleared for public release to serve organizations that would like to manage their collection of models and to serve as a solicitation reference document*
  - *The TOR is already been used as a reference for US government acquisitions*
  - *INCOSE is in the process of adopting the guide*

Implementation

Where does the MPM Guide fit in

Define "what" needs to be done

- DE Strategy
- DE Implementation
- MBSE Implementation
- Model Portfolio Management Guide

Address the "how" and "how well"

- Model Life Cycle Management Guide
- Model Requirement Guide
- Model Security Guide
- Model Integration Guide
- Model Metrics Guide
- Model Configuration Management Guide
- Model Style Guide
- Model Verification & Validation Guide
- Model Development Plan

Source: MPM Guide Figure 2. Model-Relevant Tree

Definitions

Key Definitions in MPM Guide

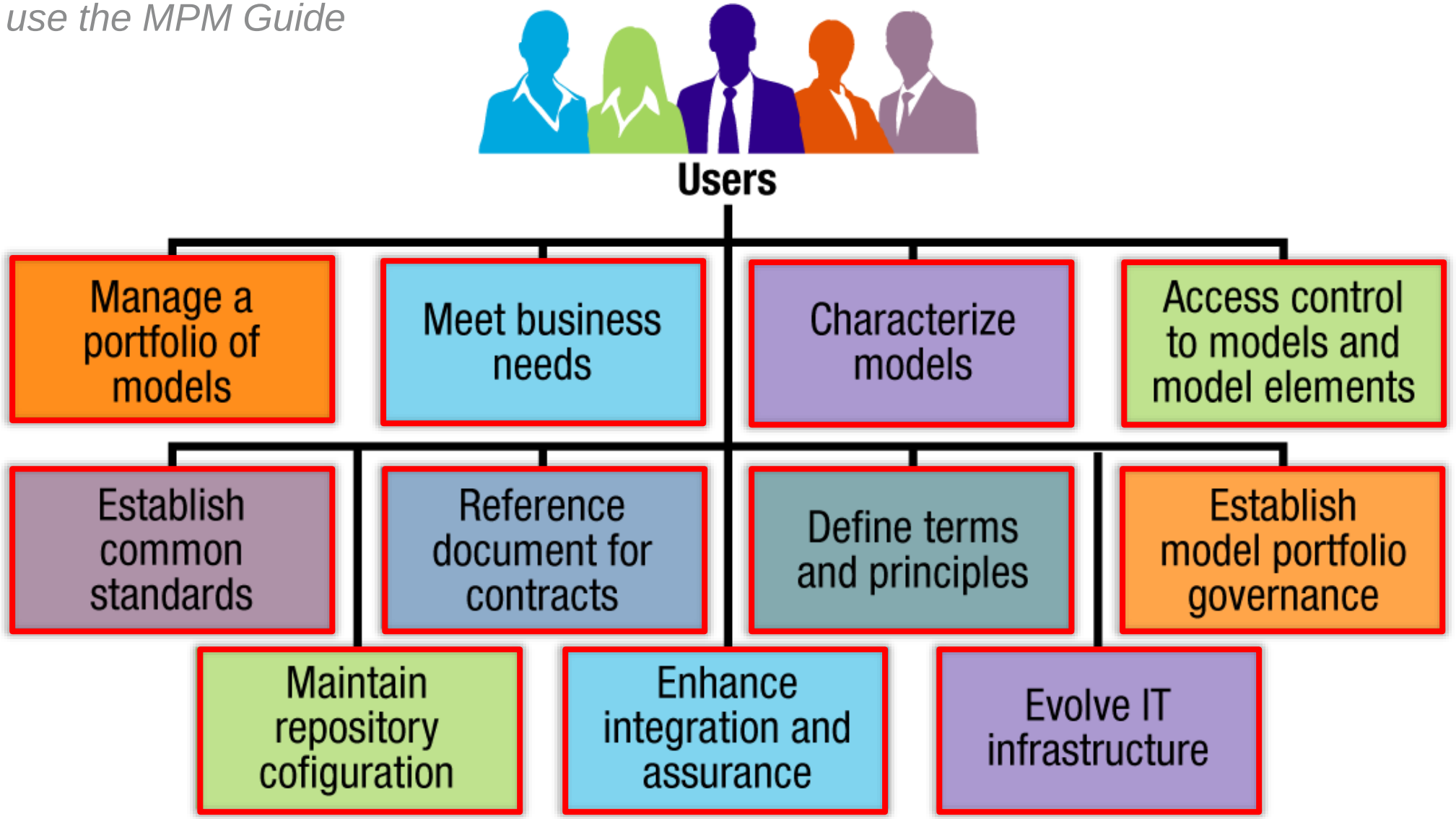
Term	Definition
Portfolio	*A collection of **projects** grouped together to facilitate effective management of work to meet strategic business objectives. (Mathur, 2006)*
Model Portfolio	*A collection of **models** grouped together to…*
Model Portfolio Management	*The administration of a collection of models to achieve strategic objectives…*
Model Portfolio Management Life Cycle	*A continuous set of activities to be performed for the Model Portfolio Management process to be successful.*

Full definitions to these terms and many others can be found in the MPM Guide

Source: "The Standard for Portfolio Management," Project Management Institute (PMI).

Use Cases

How to use the MPM Guide



Full definitions to these Use Cases and many others can be found in the MPM Guide

Approach

Approach for Contracting

Acquisition Strategy

- Select MPM as a needed Digital Engineering feature

Request for Proposal

- Contractor shall perform model portfolio management (SOW)
- MPM Guide as a reference document

Proposal

- Define the MPM related work (CSOW)
- Estimate MPM tasks/subtasks (BOEs, Cost Volume)
- MPM Plan (CDRL)

Contract

- Defined Role
- MPM Plan
- Governance
- Standards
- Repositories
- Model component libraries
- Metrics
- Management reports

MPM Guide as an RFP Reference Document to ensure government insight, access, and use.

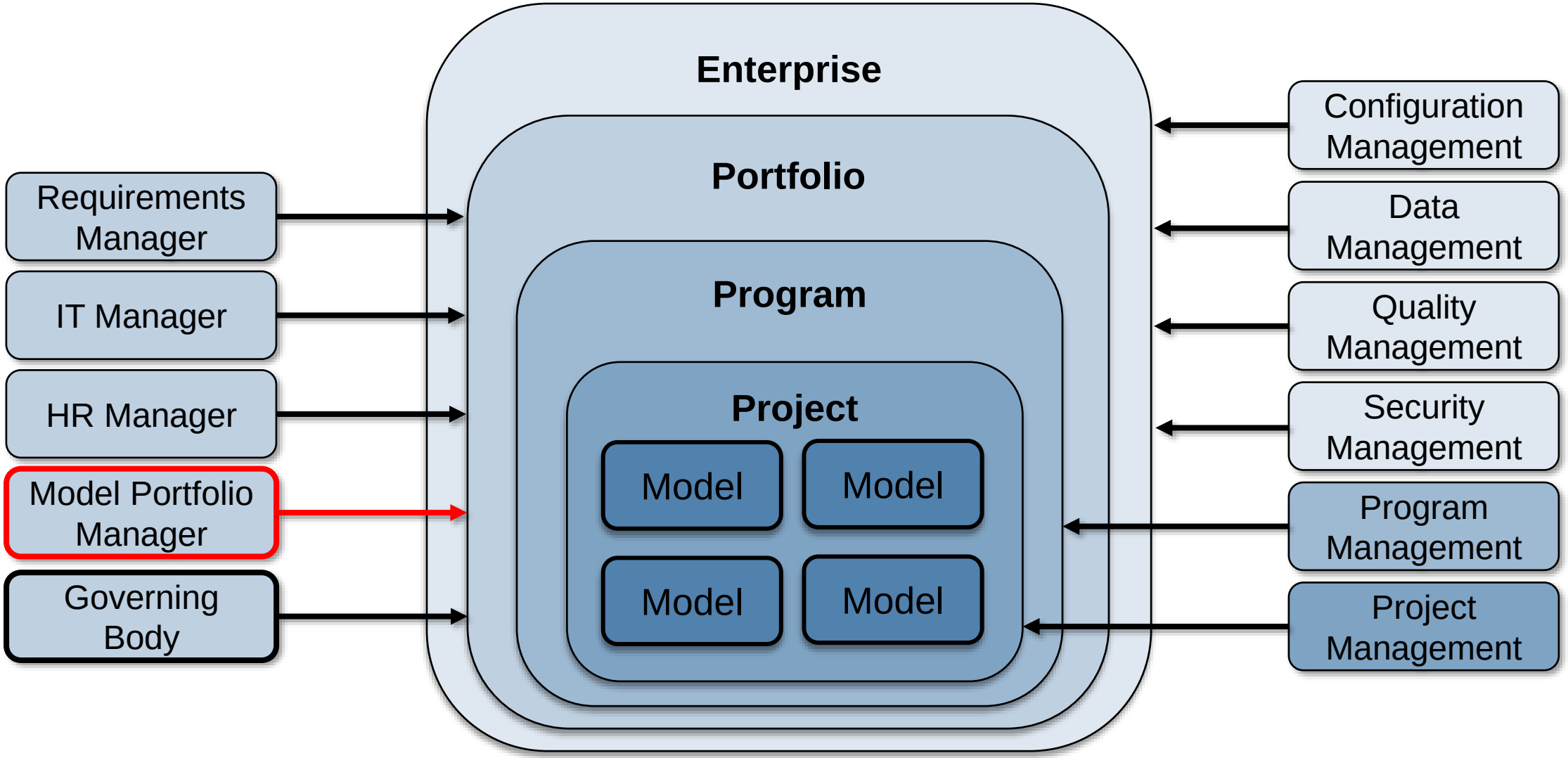
Deliverables

Recommended Deliverables from Contractors to Government

Name	Description
MPM Plan/Model	Defines the key components in the MPM Life Cycle (resources, structure, hierarchy, processes, users, scope, etc..
Governance Plan/Model	The governance plan may be a stand-alone view (documented or modeled) or may be a subsidiary to the MPM Plan.
Model Accession List	An index of working models made readily available for review by model integrators.
Model Data Accession List	An index of working data items accessible to relevant stakeholders to review model data.
Model View Accession List	An index of digital views accessible to relevant stakeholders to review model views.
MPM Risks Register	An index of risks and mitigation plans impacting the model portfolio.

Full Description to these deliverables and many others can be found in the MPM Guide

Roles and Responsibilities



Life Cycle

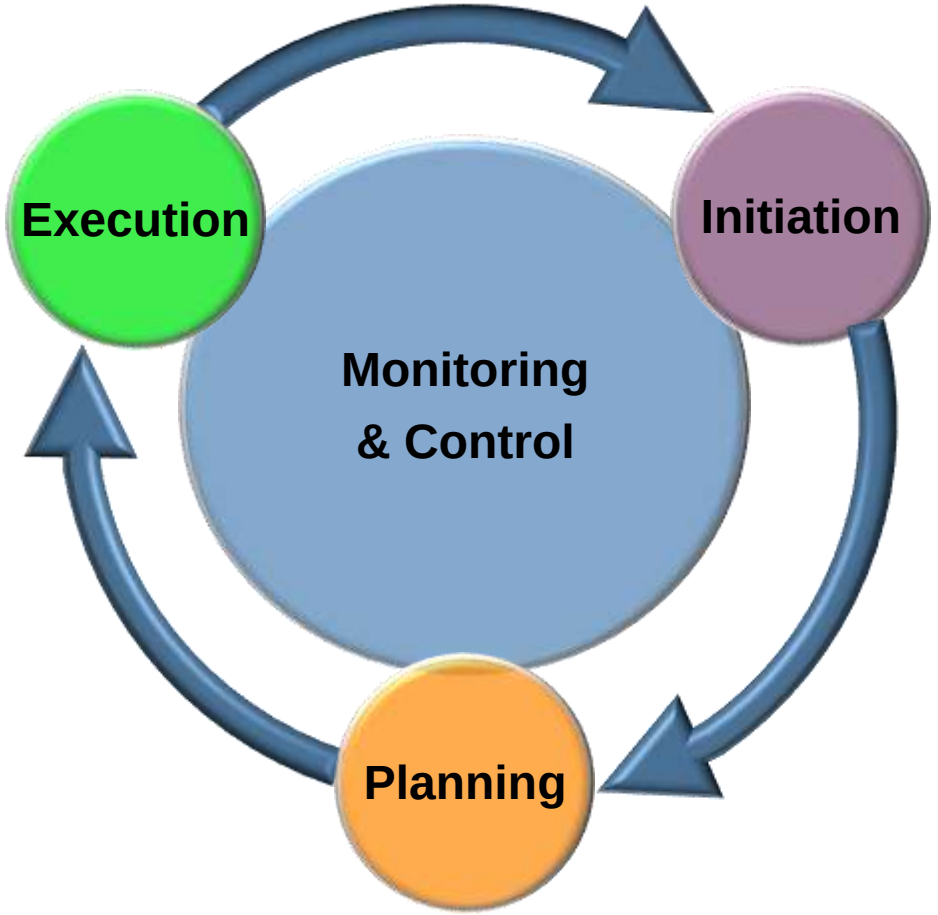
Model Portfolio Manager (MPM)

Performs

Coordinates with

Model Management

- Model Acquisition
- Model Integration
- Configuration Management of Portfolio
- Model Management Access
- Modeling Quality
- Model Products



Model Portfolio Governance

- Business Strategy
- Operational Strategy
- Roadmap
- Scope Management
- Process Optimization
- Performance Metrics
- Sponsorship

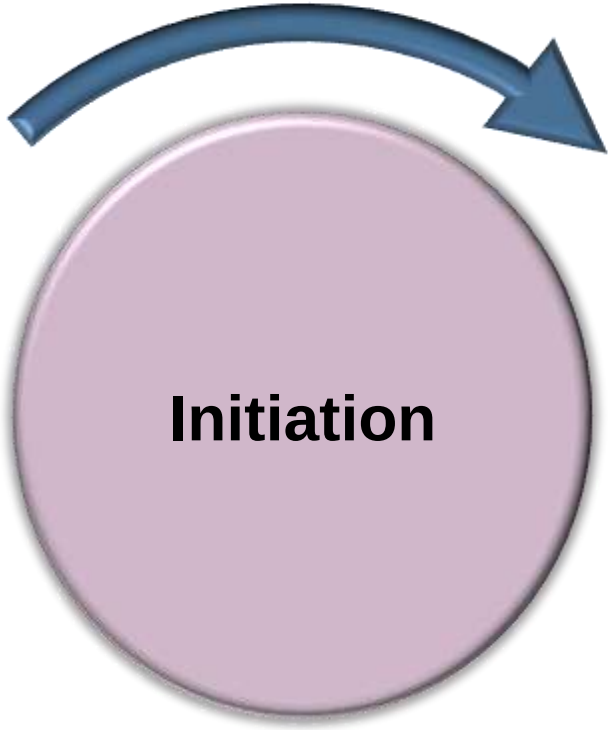
MPM roles of Management and Governance across the MPM Life Cycle

Source: "The Standard for Portfolio Management," Project Management Institute (PMI)

MPM Initiation

GOALS

- Business/Operational Strategy
- Portfolio Components
- Financial Goals
- Performance Metrics
- Communication
- Governance
- Stakeholders' Definition & Roles
- Ongoing Management Plans



ACTIVITIES

- MPM Strategy
- Model Management CONOPS
- Prioritization Criteria
- Stakeholders' Definition & Roles
- Communications Planning
- Model Portfolio Manager
- MPM Roadmap

Examples

- ***Stakeholders' Definition & Roles***
- *Strategy*
- *Modeling Guidelines*
- *Intellectual Property Rights*
- *IT Infrastructure*

Table 1. Stakeholder Roles, Interest and Expectation

Stakeholder	Roles	Interests	Expectations
Sponsor or Organizational Executive	Provide funding and resources	Alignment with goals	Informed regularly of key portfolio decisions and milestones
Model Portfolio Manager	Provides the management of the portfolio of models needed by the organization	Portfolio of models meets the organizational goals and objectives	At the sponsor's request, performs portfolio model management with the Portfolio Governing Body and model managers
Portfolio Governing Body	Oversees the portfolio priorities, manages spending, and manages timely delivery of value	Portfolio level risks and issues that require key decision and change management	Informed regularly of developments, change needs, and progress
Model Managers	Ensures model life cycle management	Mitigates portfolio level risks and issues impacting their model	Adheres to MPM agreements and is informed of portfolio changes, risks and issues

MPM Planning

GOALS

- MPM Plan
- MPM Scope
- Budgeting
- Model/Data Interdependencies
- Risks & Issues
- Resourcing
- Prioritization
- Sponsor/Stakeholder Accountability
- Portfolio Metrics
- Scope of Components
- Product/Service Requirements

Planning

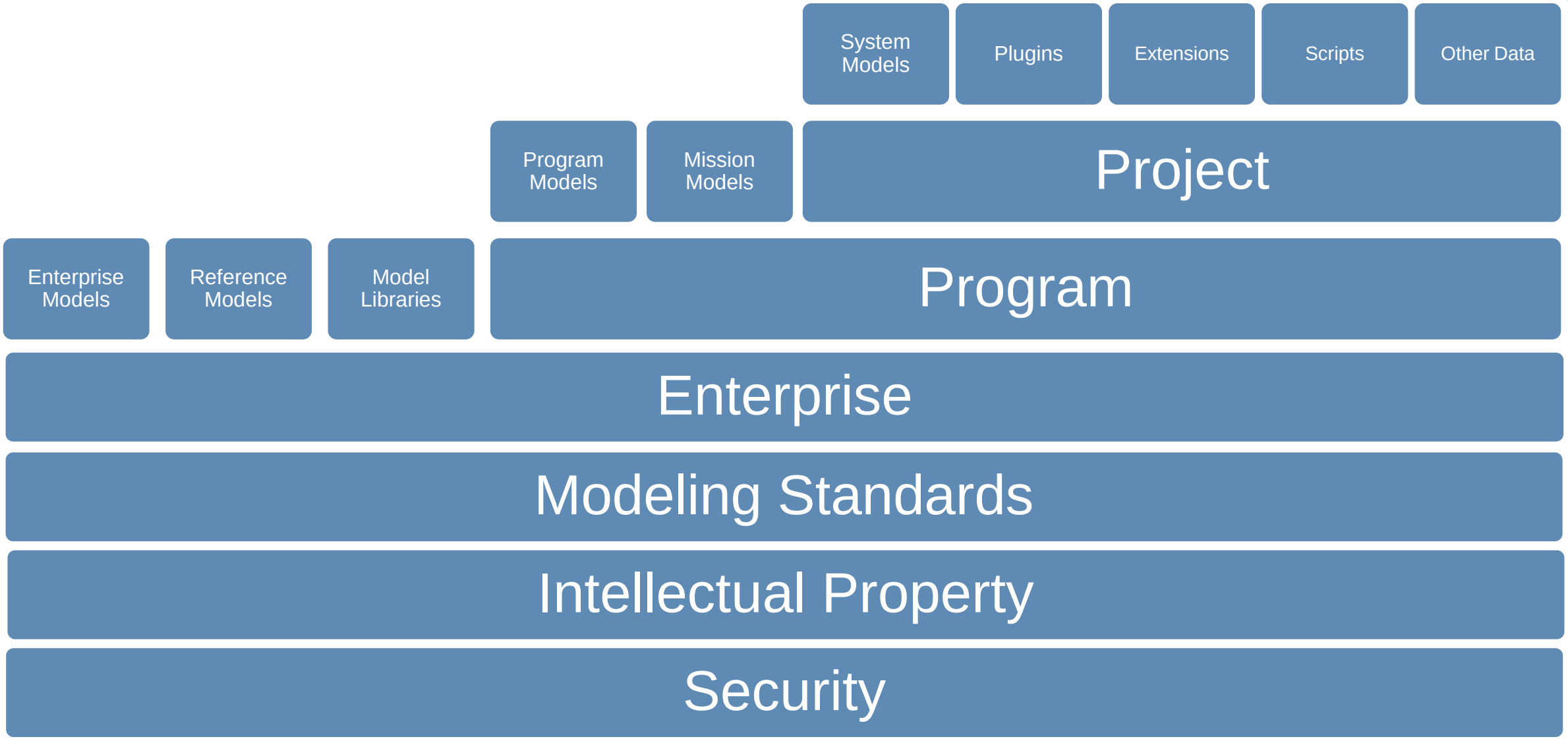
ACTIVITIES

- MPM Scope Plan
- MPM Plan
- Modeling Resources

Examples

- ***Portfolio Components***
- *Model & Data Registries*
- *Accession Lists*
- *Modeling Software*
- *Model Libraries*

Figure 3. Portfolio Components



MPM Execution

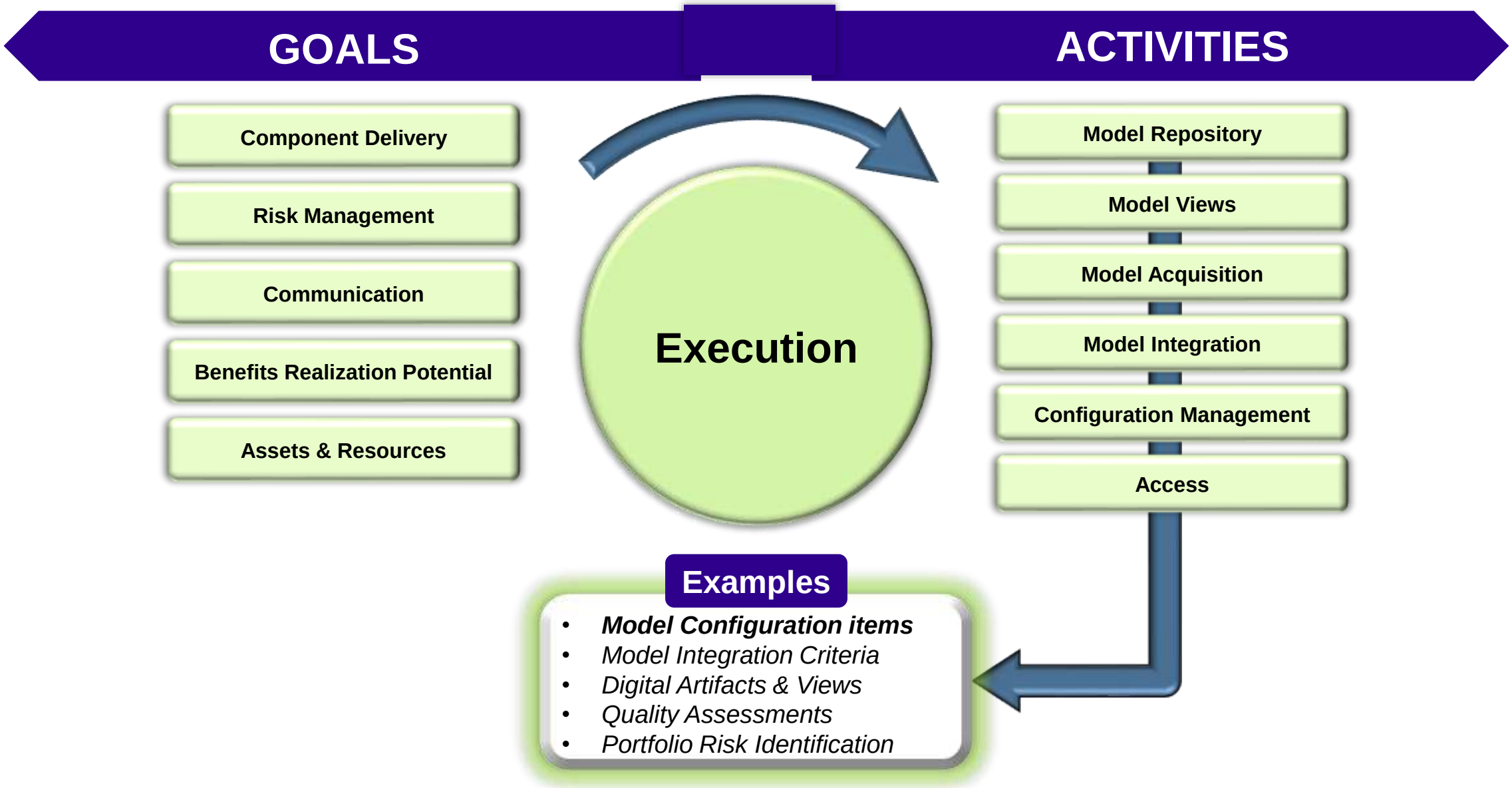
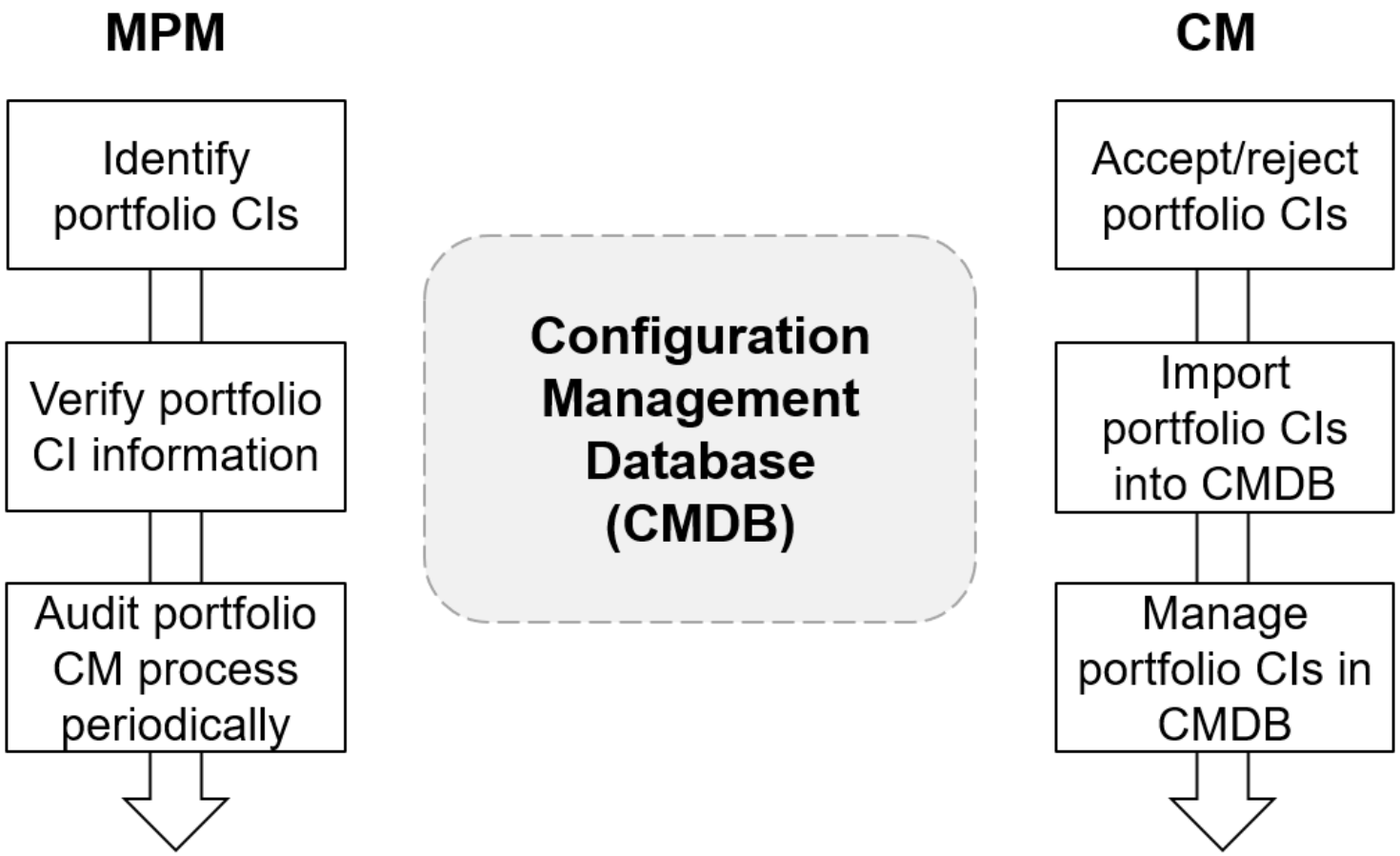


Figure 5. Responsibilities of Portfolio CM



MPM Monitoring & Control

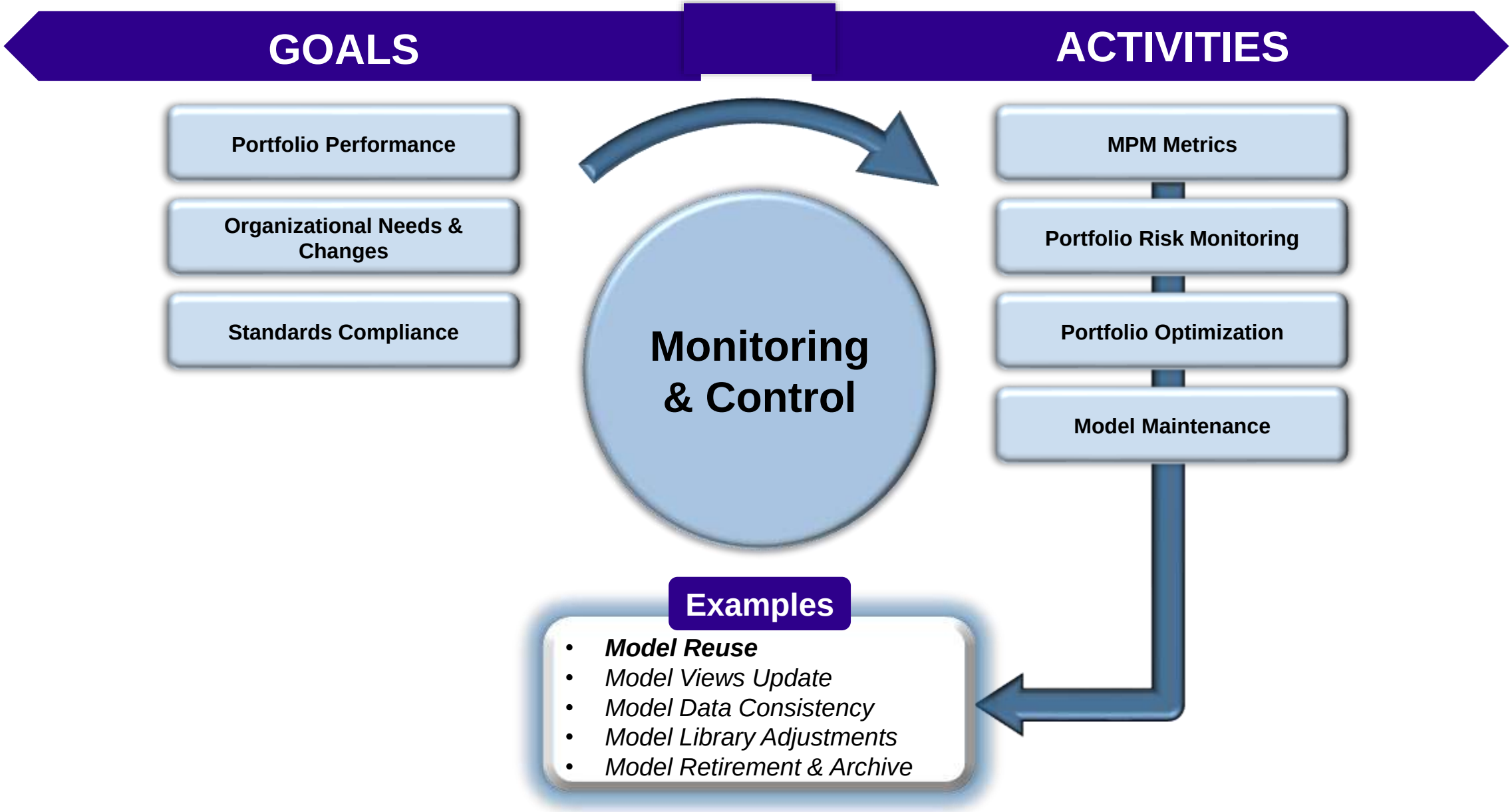
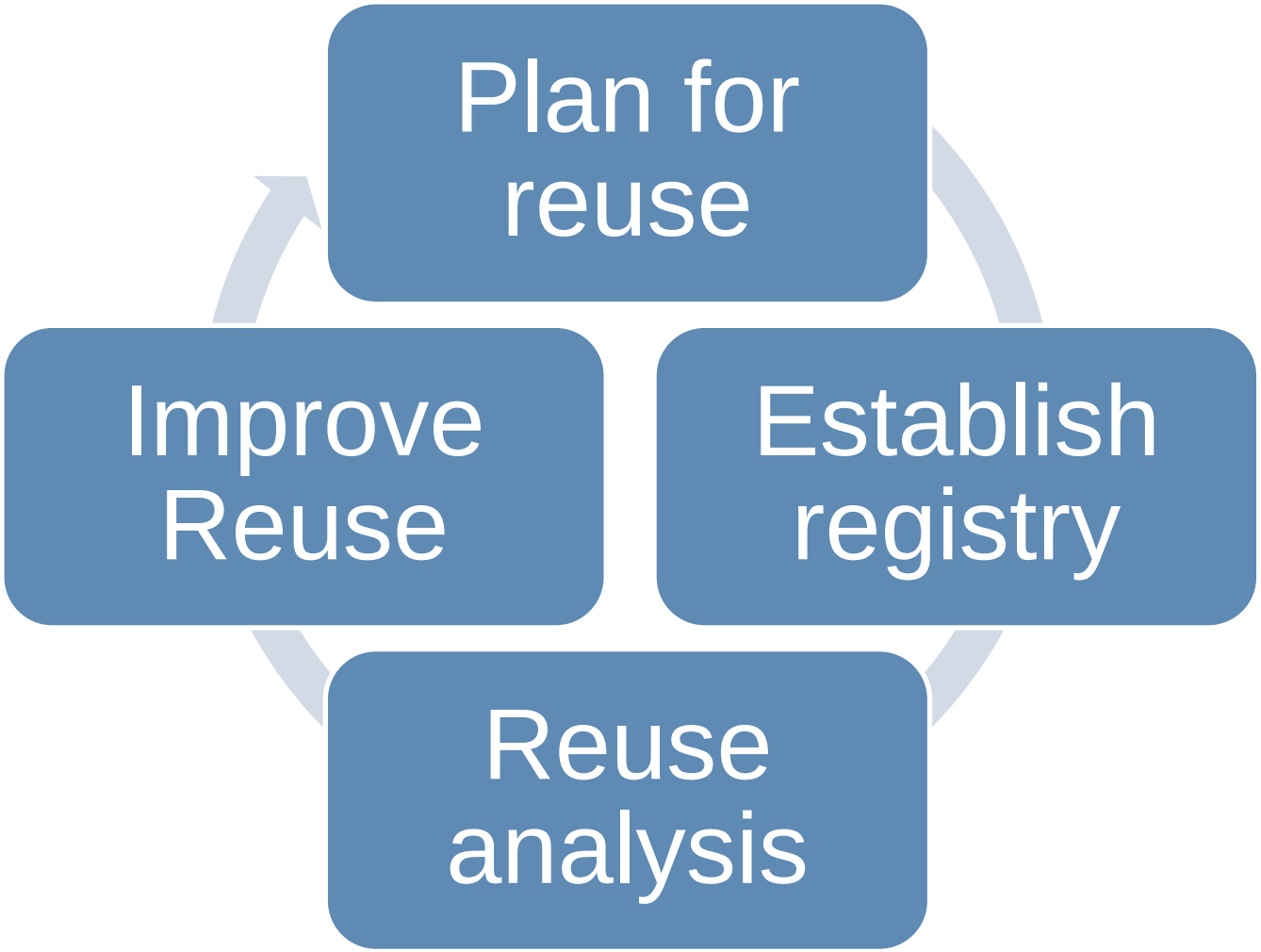


Figure 6. Model Portfolio Reuse



Summary

The Model Portfolio Management Guide:

- Solution to not having a common definition of what is “Model Management”
- Tailorable to choose what is most important to an organization
- Serves as a reference document for model-based acquisition to ensure government insight, access, and use
- Already being used by US government
- Cleared for public release
- Being adopted by INCOSE

Questions

References

1. INCOSE, "Model-Based Capabilities Matrix and User's Guide," INCOSE, 2020.
2. D. o. Defense, "DoD Digital Engineering Strategy," DoD, 2018.
3. The Standard for Portfolio Management, Fourth Edition ed., Pennsylvania: Project Managment Institute, Inc., 2017.
4. The Standard for Program Management, Fourth Edition ed., Pennsylvania: Project Management Institute, Inc., 2017.
5. "Systems and software engineering – Methods and tools for Model-based systems and software engineering (Draft)," International Organization for Standardization, Geniva, 2020.
6. "ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary," Geneva, 2018.
7. A. M. a. R. S. Sanford Friedenthal, A Practical Guide to SysML: The Systems Modeling Language, Thir Edition, San Francisco: Morgan Kaufmann Publishers, 2015.
8. "Systems and software engineering -- Architecture description ISO/IEC/IEEE 42010".
9. a. I. C. S. INCOSE Systems Engineering Research Center, "Guide to the Systems Engineering Body of Knowledge (SEBoK)," 31 October 2019. [Online]. Available: www.sebokwiki.org.
10. OMG, "Primary use cases of MBSE libraries," OMG, https://www.omgwiki.org/MBSE/lib/exe/fetch.php?media=mbse:incose_usability_libraries_2pg_v4.pdf.
11. A guide to the Project management Body of Knowledge, Pennsylvania: Project management Institue, Incorporated, 2017.
12. Julie S Fant, PhD, Myron Hecht, Robert Pettit, PhD, and Peggy Hwu,, "ATR-2020-00232 System Engineering Model Assurance Levels (MALs) Detailed Criteria," The Aerospace Corporation, distribution may be requested, El Segundo, 2020.
13. Julie S Fant, PhD., Karen E. McShane, Vineet Velmurugan, Ronald Nussbaum, PhD., Robert G. Pettit, PhD, "ATR-2020-00806 Overview of Model Assurance Levels (MALs) for Systems and Software Models," The Aerospace Corporation, distribution may be requested, El Segundo, 2020.

References (Continued)

14. "Draft ISO/IEC CD 24641 Methods and Tools for Model-Based Systems and Software Engineering (MBSSE)," 29 April 2020.
15. "Criteria," [Online]. Available: https://www.lexico.com/en/definition/criterion.
16. J. Coleman, "DEIX Topical Encyclopedia Entries," Object Management Group (OMG), 28 December 2018. [Online]. Available: https://www.omgwiki.org/MBSE/doku.php?id=mbse:topical_encyclopedia_for_digital_engineering_information_exchange_deixpedia. [Accessed 28 August 2020].
17. R. E. Giachetti, Design of Enterprise Systems: Theory, Architecture, and Methods, Boca Raton, FL: USA: CRC Press, Tayloar and Francis Group, 2010.
18. "Governing Body," [Online]. Available: https://www.lexico.com/definition/governing_body.
19. "Manager," [Online]. Available: https://www.lexico.com/en/definition/manager.
20. "Metric," [Online]. Available: https://www.lexico.com/en/definition/metric.
21. J. P. Siegel, "Terms and Acronyms," 7 September 2005. [Online]. Available: https://www.omg.org/gettingstarted/terms_and_acronyms.htm#M.
22. S. Mathur, "Project portfolio management techniques," in PMI Global Congress 2006, Bangkok, Thailand. Newton Square, PA, USA, 2006.
23. "Practice," [Online]. Available: https://www.lexico.com/en/definition/practice.
24. "Principle," [Online]. Available: https://www.lexico.com/en/definition/principle.
25. "Process," [Online]. Available: https://www.lexico.com/en/definition/process.
26. "DOD Dictionary of Military and Associated Terms," January 2020. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-01-24-100230-123.
27. P. Weaver, "Understanding programs and projects--oh, there's a difference!," in PMI Global Congress 2010, Melbourne, Victoria, Australia. Newtown Square, PA, USA, 2010.

Related Publications

- Model Portfolio Management Guide
  - *A. Hoheb, A. Chang, M. Zetilyan, J. Howie – TOR-2020-01577*
- Model Portfolio Management Guide Overview
  - *A. Hoheb, M. Zetilyan – 2021 INCOSE International Workshop (OTR 2021-00292)*
- Model Portfolio Management (MPM) Guide: A Guide to Defining the Scope, Purpose, Tasks and Products of Model Portfolio Management
  - *A. Hoheb, M.Zetilyan, A. Chang, J. Howie (OTR 2021-00592)*
- Defeat Entropy: A Guide To Managing Your Model Portfolio
  - *June 2021 issue of Getting It Right*
  - *https://aerospace.org/story/defeat-entropy-guide-managing-your-model-portfolio*

Modeling and Analysis of Standard Operating Procedures

Presented by Steven H. Dam, Ph.D., ESEP

NDIA Systems and Mission Engineering Conference

December 10, 2021

SPEC INNOVATIONS

Agenda

- PROBLEM
- SOLUTION
- NEW SOP ANALYSIS PROCESS
- NEXT STEPS

SPEC INNOVATIONS

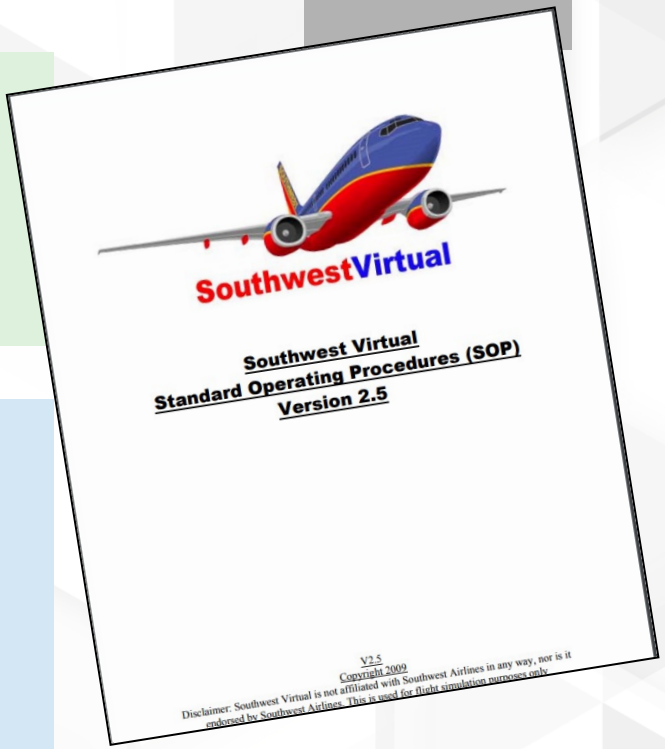
PROBLEM

Standard Operating Procedures

- What must be accomplished/Tasks?
  - Each Operator Action that must be executed in a sequence
- When (under what conditions)?
- Who is responsible for each step?
- How each step is performed/Functions?
- How to confirm?

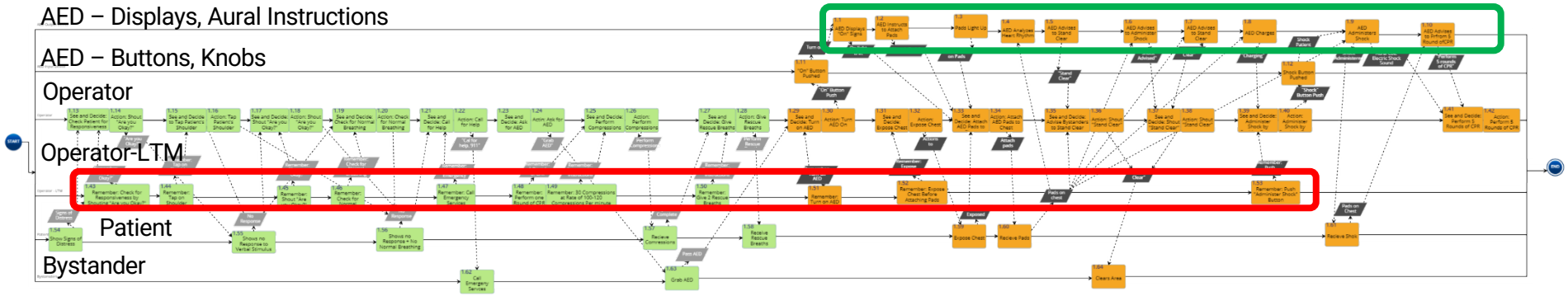
Procedures define:
- Human-Machine Interaction
- Human Automation Interaction
- Human-Human Interaction
- Human-External Actors Interaction

Types of Operator Actions:
- Info gathering
- Info processing
- Conditional branching
- Decision-making
- Waiting/Timing
- Action
- Verification
- Validation



GMU Center for Air Transportation Systems Research

Operator Tasks to Complete an SOP Are Complex



Operator Actions = 15

Actions prompted by visual/aural cues = 8

Actions rely on Long-term Memory *only* = 8

An AED is a type of computerized defibrillator that **automatically analyzes the heart rhythm** in people who are experiencing cardiac arrest. When appropriate, it delivers an electrical shock to the heart to restore its normal rhythm.

SPEC INNOVATIONS

The Problem with SOPs

1. Missing imperative steps in the SOPs due to automatic level of consciousness
2. WHAT must be done is specified, but not WHEN - *TK1951*
3. Information required to perform next step is not available
4. Race conditions – information not available in timely manner
5. Procedure cannot be completed in time (i.e., before hazardous event) - *Egypt Air 990*
6. Procedure difficult to learn due to user-interface cues - *OZ 214*
7. Poor procedural training
8. No procedure for the scenario *AF447*?
9. Procedures across System-of-Systems are not compatible - *SQ 237 – Runway Excursion*

SPEC INNOVATIONS

Need

There is a burgeoning need to improve aviation safety following recent airliner accidents. The following areas are candidates for improved SOPs:

NASA APPLICATIONS

A short-list of general areas includes:

- Mission Control
  (International Space Station, satellites)
- Launch procedures
- Extravehicular Activities (EVA) procedures
- Space and aircraft maintenance procedures
- Medical procedures

NON-NASA APPLICATIONS

Some of the organizations that have expressed interest in this kind of digital assistant include:

- Swiss International Air Lines
- Southwest Airlines
- United Airlines
- Boeing Commercial Aircraft Group (BCAG)
- Honeywell Technology Center
- Rockwell Collins
- U.S. Navy - Strategic Warfare Systems

SOLUTION

The Solution:

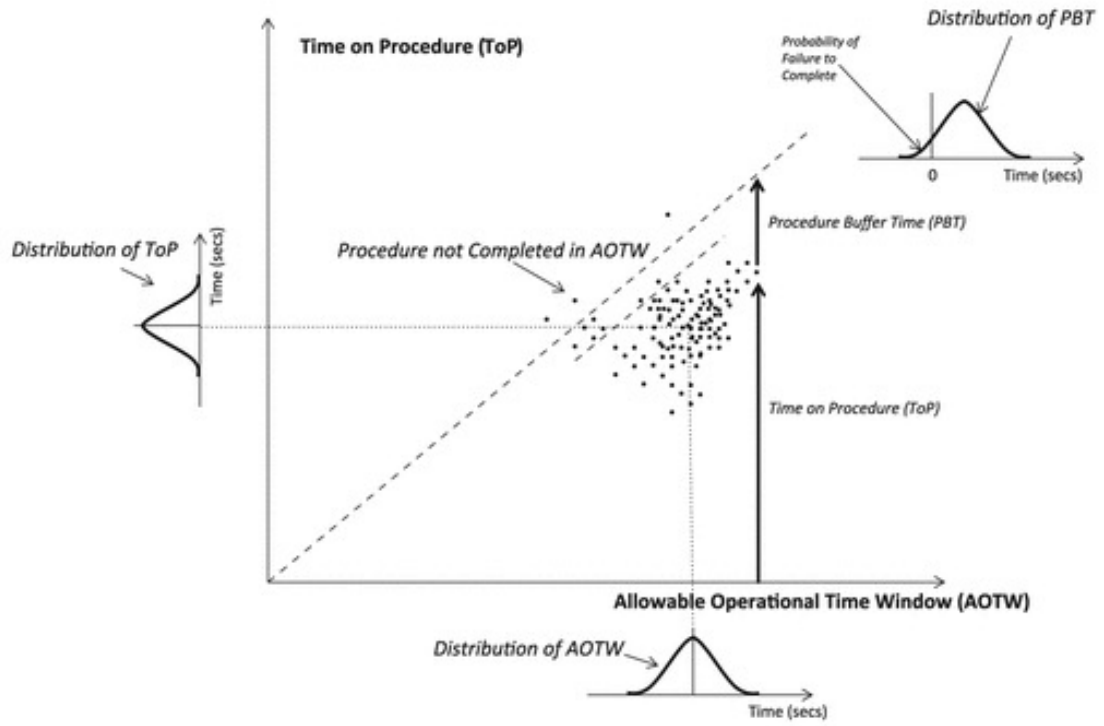
Use Modeling and Simulation to Identify SOP Problems Early

Detailed model of Perception/Cognition/Motor tasks performed to complete an SOP for Airlines Engine-out Above Maximum Altitude

SPEC INNOVATIONS

The Solution:
Measure Procedure Performance

- Allowable Operational Time Window (AOTW)
  - Time before something bad happens
- Time of Procedure (ToP)
  - Time it takes to perform procedure
- Procedure Buffer Time (PBT)
  - AOTW – ToP
  - If < Zero, then Procedure not completed on time



But this is a fair complicated set of metrics to develop and analyze

The Solution: Develop a Digital Assistant to Support SOP Analysis

Research supported through
NASA Phase I STTR
80NSSC-20-C-0579

We designed Sopatra with the overall goal to demonstrate the improved creation of Standard Operating Procedures (SOPs) by the automated creation and verification of SOPs using a digital assistant (DA)

Sopatra

Use Natural Language Processing (NLP) for interacting with the MBSE development environment (i.e. creating the LML/SysML model)
Provides configuration management and revision management of massive models
Develops executable simulation of the MBSE model

Sopatra is a digital assistant that will convert text to an LML Action Diagram and execute the simulation automatically to check all possible paths through the procedure.

SPEC INNOVATIONS

The Solution: Goal – A Modern Digital Assistant Using AI and Mixed Reality Technologies

The figure shows our vision for Sopatra

- Automated Text Entry and Analysis (Phase I)
- Automated Voice Recognition Entry and Analysis (Phase II)
- Automated Mixed Reality Entry and Analysis (Phase II)
- Simulation and Analysis of Standard Operating Procedures (Phase I)

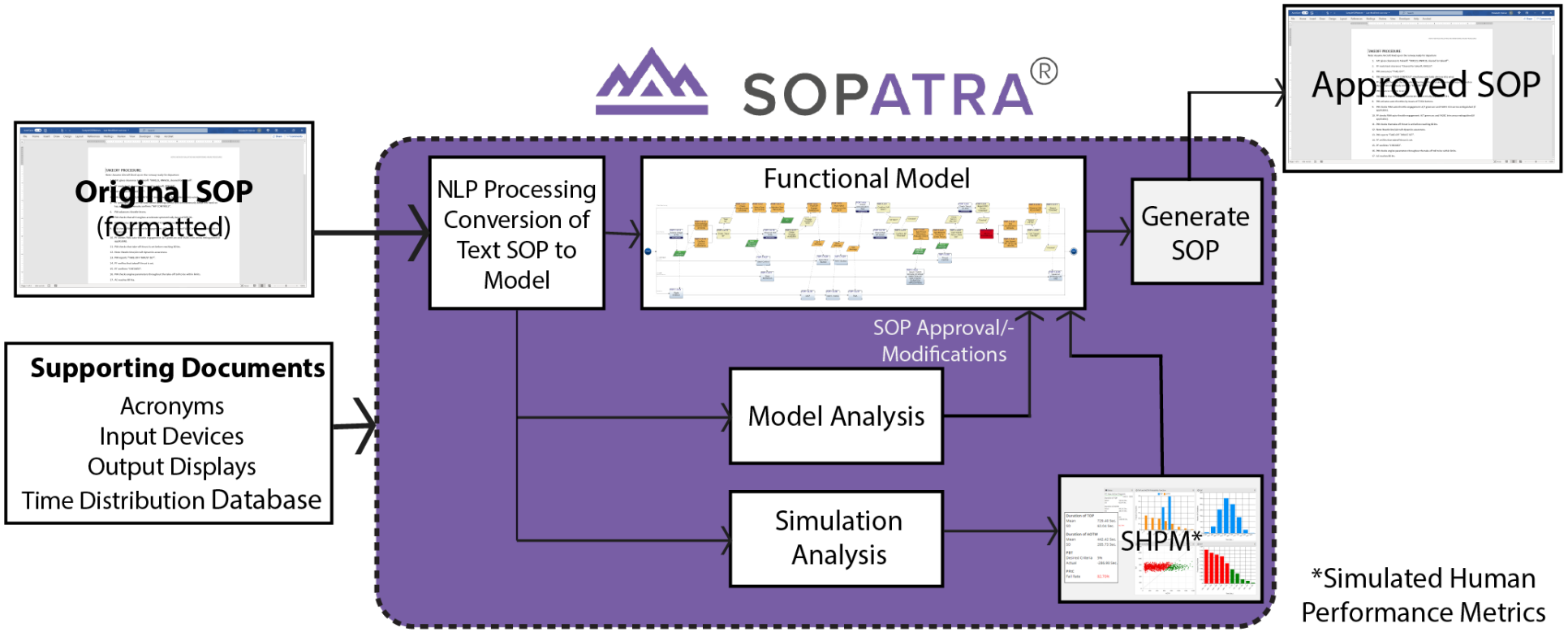
SPEC INNOVATIONS

The Solution: Approach

- Adapt a state-of-the-technology MBSE tool to provide the basis for the digital assistant
  - Innoslate® was chosen as it already had the diagramming and simulation capabilities needed. It also already uses AI/NLP extensively
- Develop requirements and a prototype under the NASA STTR Funding
  - Prototype software, requirements and documentation delivered to NASA within 6 months of contract start
- Productize using SPEC Innovations IR&D
- Introduce version 1.0 of the product for further research making it available for other researchers to advance the practice

SPEC INNOVATIONS

NEW SOP ANALYSIS PROCESS


SOPATRA®
Original SOP
(formatted)
Supporting Documents
Acronyms
Input Devices
Output Displays
Time Distribution Database
NLP Processing Conversion of Text SOP to Model
Functional Model
Generate SOP
Approved SOP
SOP Approval/-Modifications
Model Analysis
Simulation Analysis
SHPM*
*Simulated Human Performance Metrics

Formatted SOP

NLP rules derived from a provided SOP to consider:

- Actors
- Actions for Operators
- Actions resulting from cues from:
  - Output Displays
  - Environments
- Input Device and Operator Responses

TAKEOFF PROCEDURE:

Note: Assume Aircraft lined up on the runway ready for departure

1. Air Traffic Control gives clearance to Takeoff: "XXX123, RNW16, cleared for takeoff".
2. Pilot Flying reads back clearance "Cleared for takeoff, XXX123".
3. Pilot Monitoring announces "TAKE-OFF".
4. Pilot Monitoring announces "YOUR CONTROLS" simultaneously holds ailerons into wind.
5. Pilot Flying puts right hand on the nose wheel steering control and simultaneously keeps left hand on lap, and simultaneously confirms "MY CONTROLS".
6. Pilot Monitoring advances throttle levers.
7. Pilot Monitoring checks that all 4 engines accelerate symmetrically beyond 50% N1.
8. Pilot Monitoring activates auto throttles by means of TOGA buttons.
9. Pilot Monitoring checks FMA auto-throttle engagement: A/T green arc and FADEC trim arrow extinguished (if applicable).
10. Pilot Flying checks FMA auto-throttle engagement: A/T green arc and FADEC trim arrow extinguished (if applicable).
11. Pilot Monitoring checks that take-off thrust is set before reaching 80 kts.
12. Note: Needs time/aircraft dynamics awareness.
13. Pilot Monitoring reports "TAKE-OFF THRUST SET".
14. Pilot Flying verifies that takeoff thrust is set.
15. Pilot Flying confirms "CHECKED".
16. Pilot Monitoring checks engine parameters throughout the take-off toll to be within limits.

SPEC INNOVATIONS

Supporting Formatted Documents

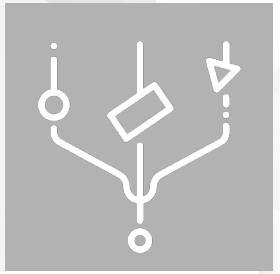
- Acronym, Output Display, and Input Device Files are all in simple list formats
- All text and word files are created with expert industry knowledge and can be easily edited
- Files will be supplied by SPEC Innovations/GMU

```
A/T = Autothrottle
A/THR = Autothrust
AAL = Above Aerodrome Level
AC = Advisory Circular
ADIRS = Air Data Inertial Reference System
ADIRU = Air Data Inertial Reference Unit
AFDS = Autopilot Flight Director System
AFE = Above Field Evelvation
AFM = Airplane Flight Manual
AGL = Above Ground Level
AI = Altitude Indicator
ALT = Altimeter
AOTW = Allowable Operational Time Window
AP = Autopilot
APU = Auxilary Power Unit
ASI = Airspeed Indicator
C = Captain
Capt = Captain
CB = Circuit Breaker
CDL = Configuration Deviation List
```

```
ADF Bearing Indicator
Airspeed Indicator
Airspeed Trend Indicator
Airspeed Tape
Altitude Indicator
Altimeter
Approach Verificatio Light
Artificial Horizon
Avionics
Barometric Altimeter
Circuit Breaker
Direction Finder
Engine Instruments
Flaps Position Indicator
Fuel Gauge
Fuel Quantity Gauges
GPS
G.P.S.
GPWS Warning
Heading Indicator
Hobbs Meter
Indicated Airspeed Tape
Landing Gear Position Indicator
```

```
Alternate Flap Selector
Alternating Static Source
Altitude Set Switch
Auto Pilot
Auto-throttle
Auto-thrust
Autopilot
Autopilot Engage Button
Autopilot Disengage Button
Autothrottle
Autothrottle Arm Switch
Auto Thrust
Autothrust
Battery Switch
Brake Pedal
Brake Pedals
Circuit Breaker
Climb thrust
Control Column
Control Stick
Control Wheel
Control Yoke
Electrical Switch
Engine Thrust Lever
Engine Thrust Levers
Flap Control Lever
```

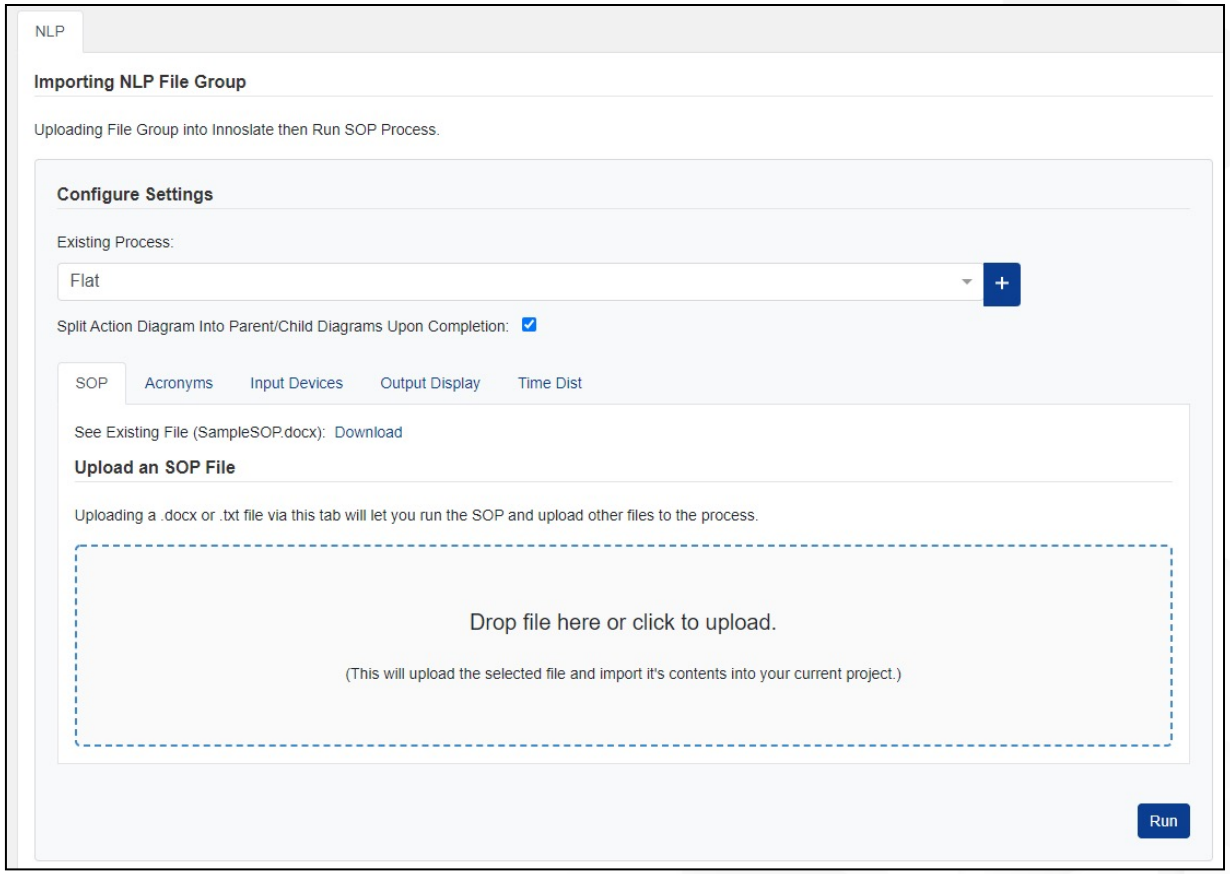
Supporting Formatted Documents



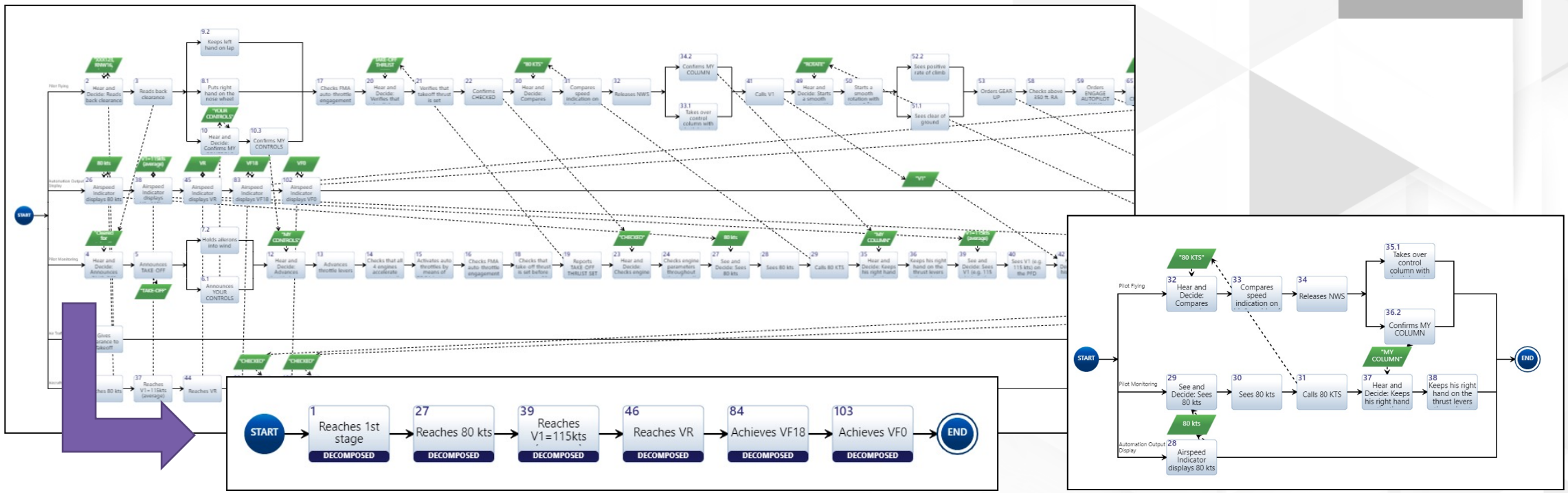
- Formatted Time Distribution Databases can be read in or manually inputted and adjusted through ASOPDA's Database view
- Also provided by SPEC Innovations/GMU

				Distribution Parameters:			Cue Evaluation:						
Distribution Class	Name	Description	Distribution Type: Triang	Min	Mode	Max	No Cue (LTM)	Not in FOV	In FOV, Not Salient (i.e. Cluttered /Lost in Noise)	In FOV, Salient, Ambiguous Semantics	In FOV, Salient, Unambiguous Semantics	Frequency (Every Flight, Frequent, Infrequent, Rare)	
AOTW	Takeoff Roll: 80 Knots to V1		Triang	3	7	17	N/A	N/A	N/A	N/A	N/A	N/A	
AOTW	Takeoff Rotate: V1 to VR		Triang	1	4	9	N/A	N/A	N/A	N/A	N/A	N/A	
AOTW	Takeoff Climbout: VR to VF18		Triang	4	6	60	N/A	N/A	N/A	N/A	N/A	N/A	
AOTW	Takeoff Retract Flaps 24 to 18		Triang	20	90	240	N/A	N/A	N/A	N/A	N/A	N/A	
ToP	Generic: Recall from LTM		Triang	0.03	0.05	5	X					Every Flight, Freq	

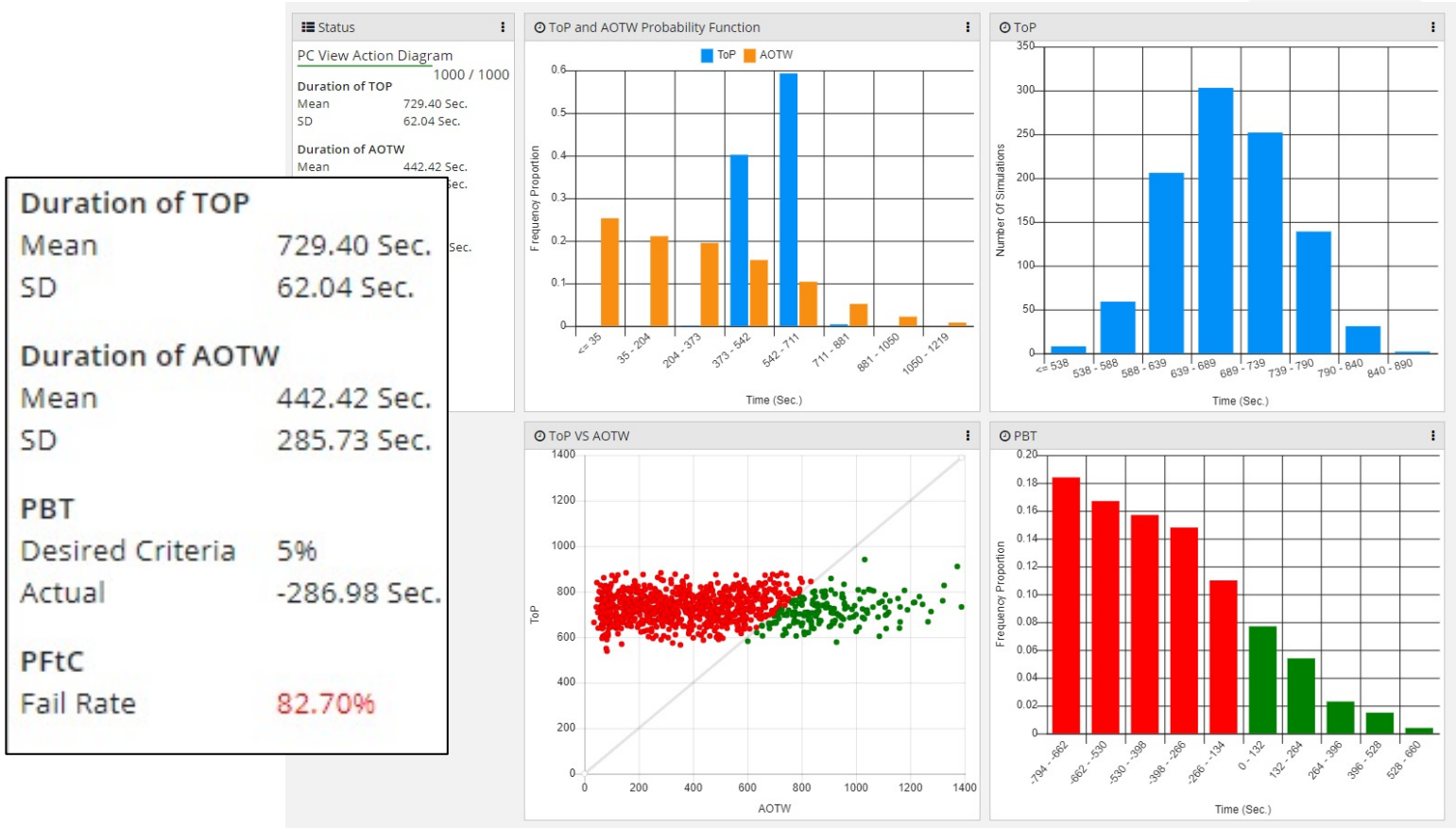
Importing SOP and Supporting Documents



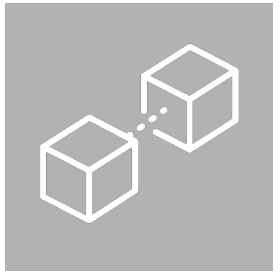
Resulting Action Diagrams



Monte Carlo Simulation to Identify SOP Problems



Innoslate + Sopatra



- Innoslate provides an end-to-end system lifecycle solution
  - Database Management with bulk editing, advanced query search, rollup, labels, customized reports, and more.
  - Schema Editors to allow customization and flexibility.
  - Modeling – Full SysML, LML, DoDAF and more with complete coverage of cost, schedule, performance, and risk.
  - Test Management with full reports, status updates, results, and more.

- Sopatra and Innoslate can work together seamlessly

INNOSLATE®

SOPATRA®

BETTER TOGETHER

SPEC INNOVATIONS

NEXT STEPS

Next Steps – NASA STTR Phase II Objectives

- Enhance Natural Language Processing (NLP) for interacting with the MBSE development environment (i.e. creating the LML/SysML model) with more complex models
- Develop configuration management and revision management of massive models and apply Machine Learning to enhance modeling using this data set
- Continue improving executable simulation of the MBSE model by aiding user to select an appropriate number of iterations for the model's complexity
- Integrate SOPs with system (i.e. machine) model for digital engineering
- Generate SOP in industry standard formats, such as NASA's Procedure Reference Language (PRL)

Questions and Answers

Use the panel on the right to ask your questions

More Resources

SPEC Innovations offers training, books, videos, documentation, trials, and more

Training: specinnovations.com/training

Books: “Real MBSE” textbook and lab manual available on Amazon

Videos: Visit the SPEC Innovations YouTube channel

LinkedIn: Innoslate and Systems Engineers User Group

Documentation: help.Innoslate.com

Trial: cloud.Innoslate.com

SPEC INNOVATIONS

Thank you.

Engineer
Your
Competitive
Advantage

Product Line Engineering in the New Age of Digital Engineering

NDIA 2021 Virtual Systems & Mission Engineering Conference
December 6-8, 2021

Charles Krueger, PhD, CEO
BigLever

onePLE

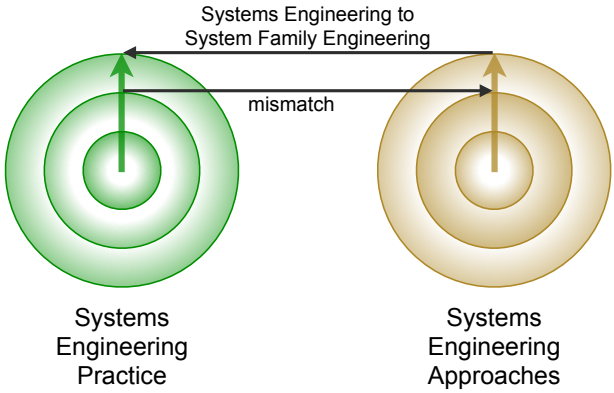
Confronting Engineering Complexity

*"The **top driver** of operational **complexity** in complex engineering organizations, as identified by surveys of hundreds of business leaders, is the **number of product and system configurations** engineered, manufactured, deployed, and sustained."*

- Michelle Boucher, VP of Research for Engineering Practices,Tech-Clarity

From Systems Engineering to System Family Engineering

- Product lines are ubiquitous
  - Almost every engineering organization builds their systems as a family of similar systems
  - Nobody builds just one
- But conventional systems engineering practice focuses on a single *System of Interest*
- With Digital Engineering, this has become a profound mismatch with staggering risks and unintentional complexity
- Successful Digital Engineering requires the *System Family* to be a System of Interest



System Family Engineering with modern Feature-based PLE

ISO 26580 Methods and Tools for Feature-based PLE

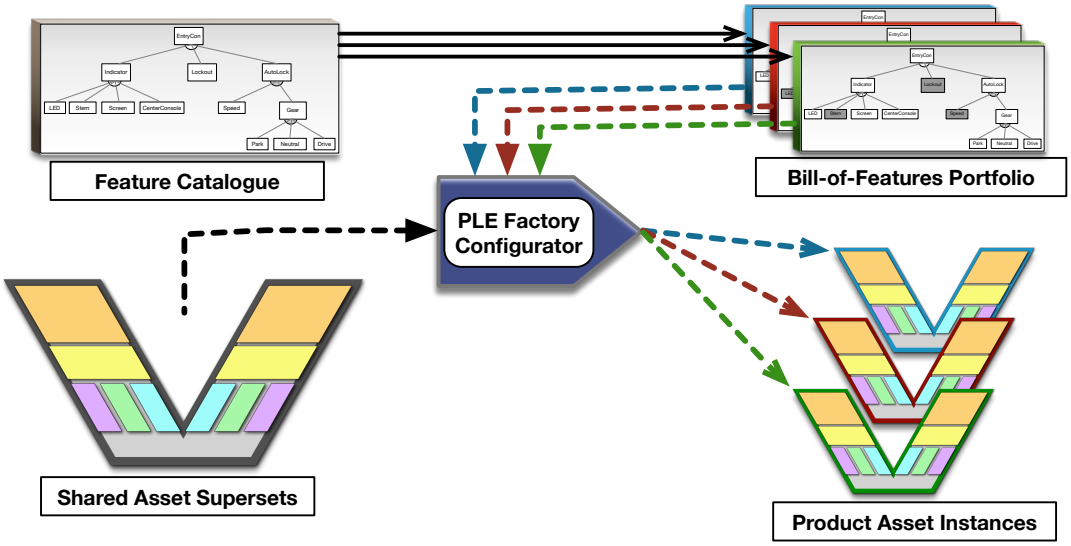
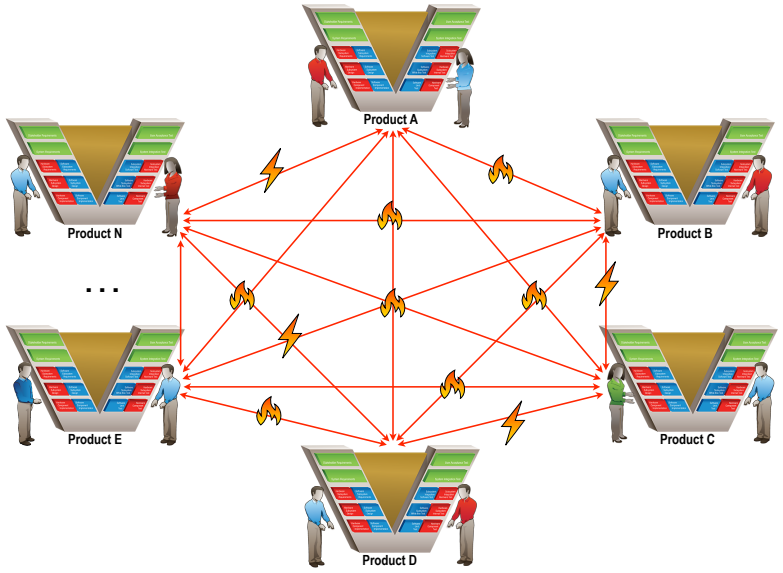


Figure from ISO/IEC 26580
Copyright © ISO/IEC 2021
https://www.iso.org/standard/43139.html

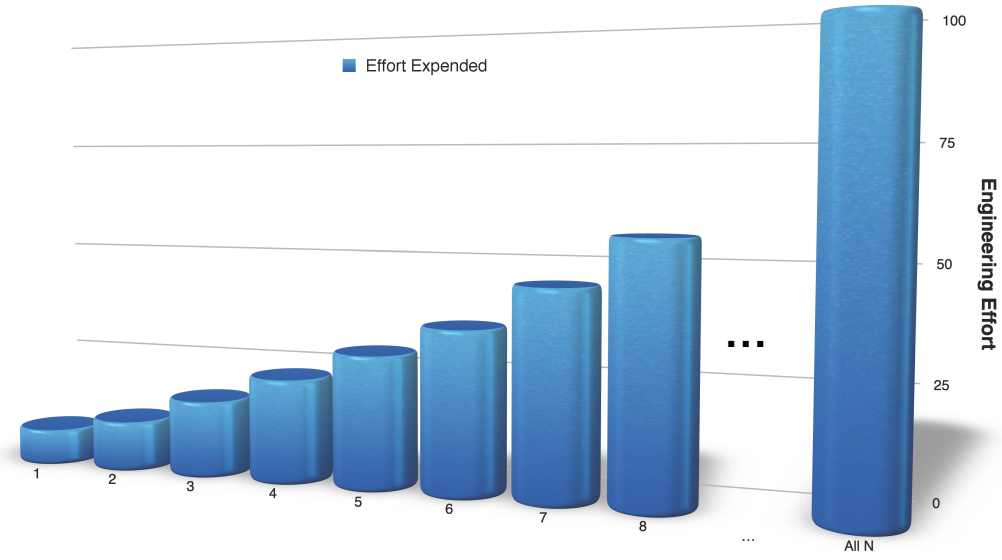
PLE is a Move Away from Product-centric Engineering

- Duplication, branch-and-merge, clone-and-own, self-inflicted N^2 complexity, …
- Informality introduces significant risks in the form of defects, errors, and omissions
- Leads to delays, budget overruns, recalls, system failures, and opportunity losses



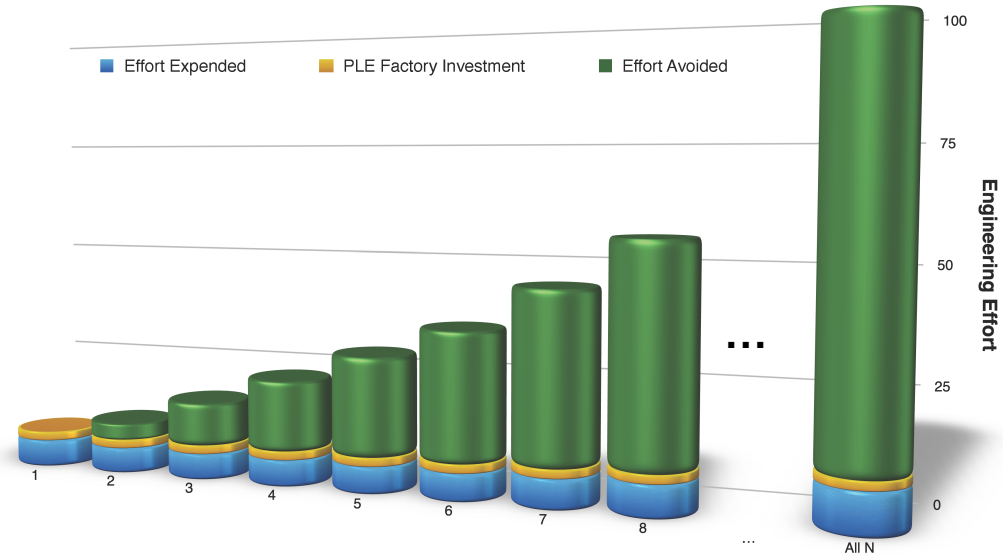
Product-centric Engineering Effort

- Dominated by low-value, mundane, replicative work
- Deprives teams of time and energy better spent on high-value innovative work that advances business objectives



Feature-based PLE Effort Avoidance

- What if your engineers could do their normal day's work before lunch?
- What would you have them do in the afternoon?
- Feature-based PLE can address engineering staff shortages by multiplying effectiveness of existing resources

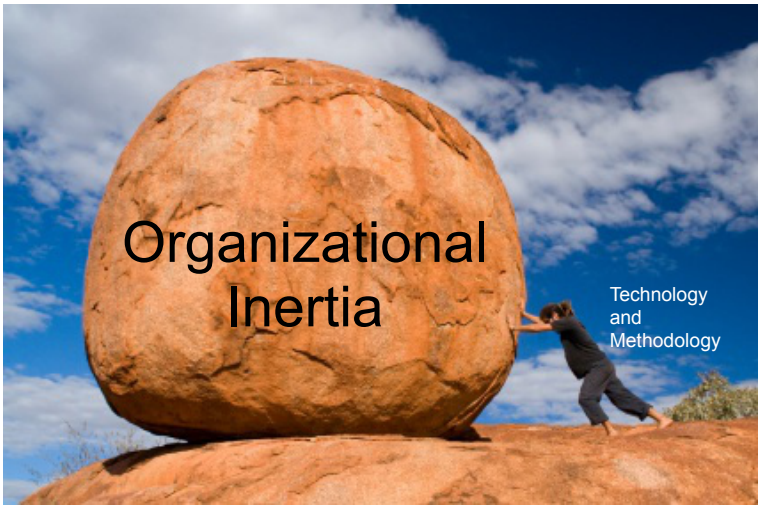


Number of Products Impacted by a Change

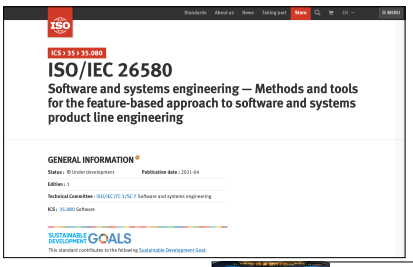
LOCKHEED MARTIN	GENERAL DYNAMICS	gm	Raytheon Technologies	GE Aviation
AEGIS Weapon System for US and International Navies	Live Training Transformation: US Army, Air Force, Marines. Plus enterprise initiative.	One of the largest and most complex product lines, comprising millions of instances per year	Rapidly growing and evolving portfolio of the world's most advanced missile systems	Helicopter engines for all configurations of the new US Army Future Vertical Lift (FVL) program
High cost of old approach threatened loss of entire contract	Innovative low-cost solution essential to win and retain major contracts	Significant challenges to provide suppliers with a family of complex specs for electronic controller unit families	Traditional methods of creating and testing prototypes are too slow, imprecise, expensive to meet mission demands	Demand to maximize sharing and reuse to prevent multiplicative costs for flight certification
Feature-based PLE Results with BigLever				
Turned an at-risk program into an enthusiastic long-term relationship by eliminating low-value redundant effort	**Grew a $2B+ business from scratch with the US DoD. Delivering 3x more capability within budget, to the delight of the customer**	**Digital transformation to a digital supply chain by applying PLE to MBSE**	**Using Feature-based PLE to proliferate best candidate simulations to find optimal solution within a trade space**	**Using a single Feature-based PLE Factory with a single collection of shared engineering assets for the full engineering lifecycle**

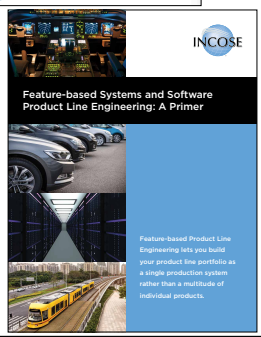
Technology and Methodology are critical, but not enough

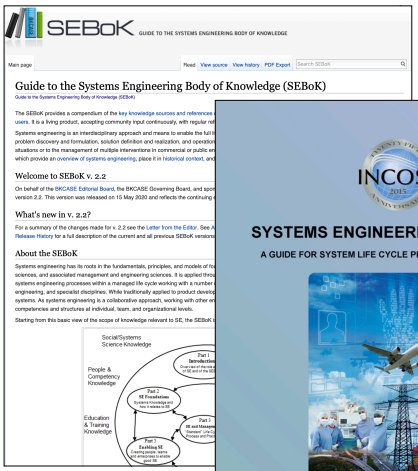
- Proven technology, methodology, and successful practice exists today
- Where is everybody?
- Broader awareness and adoption are lagging significantly
- Organizational Change impediments
  - technology is easy, people are hard
  - change is good, you go first
  - too busy to save time, can't afford to save money

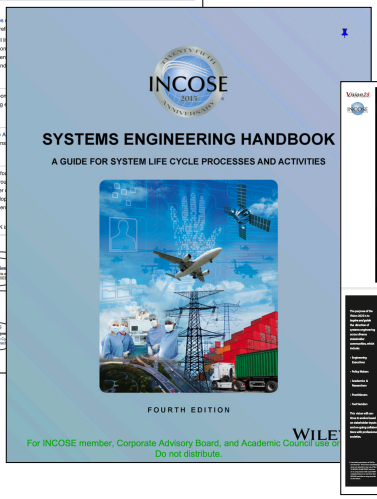


Lowering the risk of organizational change by elevating Product Line Engineering to a standard practice in the industry









Managing Supply Chain Complexity with the Acquisition Security Framework (ASF)

Dr. Carol Woody (presenter)
Christopher Alberts
Charles Wallen

December 7, 2021

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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

DM21-0435

Topics

Describing the Context

Acquisition Security Framework Overview

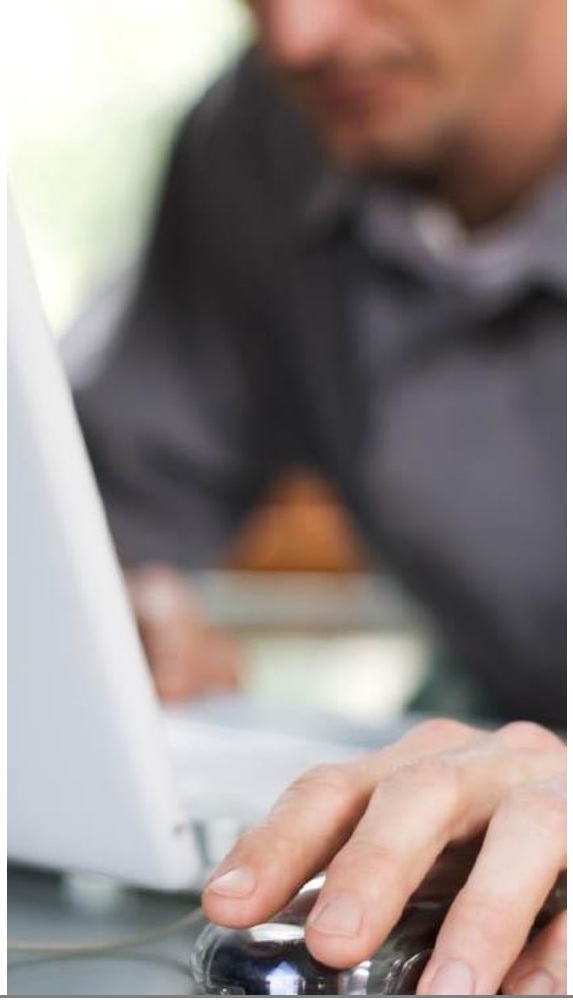
Current Framework Details

Applying the Framework

Summary

Acquisition Security Framework (ASF)

Describing the Context



Challenge: Software is Everywhere

You think you're building (or buying, or using) a product such as:

car or truck	satellite	mobile phone	development tools
home security system	aircraft	pacemaker	security tools
home appliance	financial system	bullets for a gun	

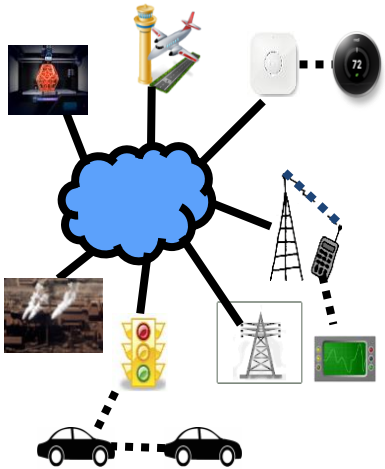
You are getting ***a software platform:***

- Software is a part of almost everything we use.
- Software defines and delivers component and system communication.
- Software is used to build, analyze and secure software.

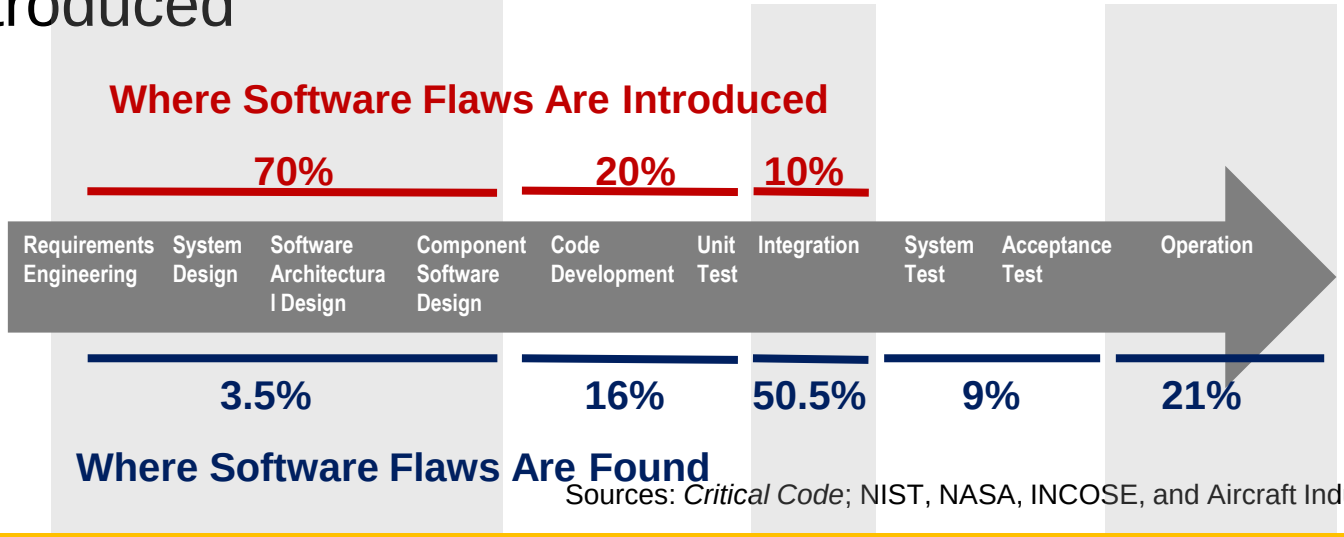
All software has defects:

- Best-in-class code has <600 defects per million lines of code (MLOC).
- Good code has around 1000 defects per MLOC.
- Average code has around 6000 defects per MLOC.

(based on Capers Jones research http://www.namcook.com/Working-srm-Examples.html)



Challenge: Most Software Defects Are Found Long After They Are Introduced



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

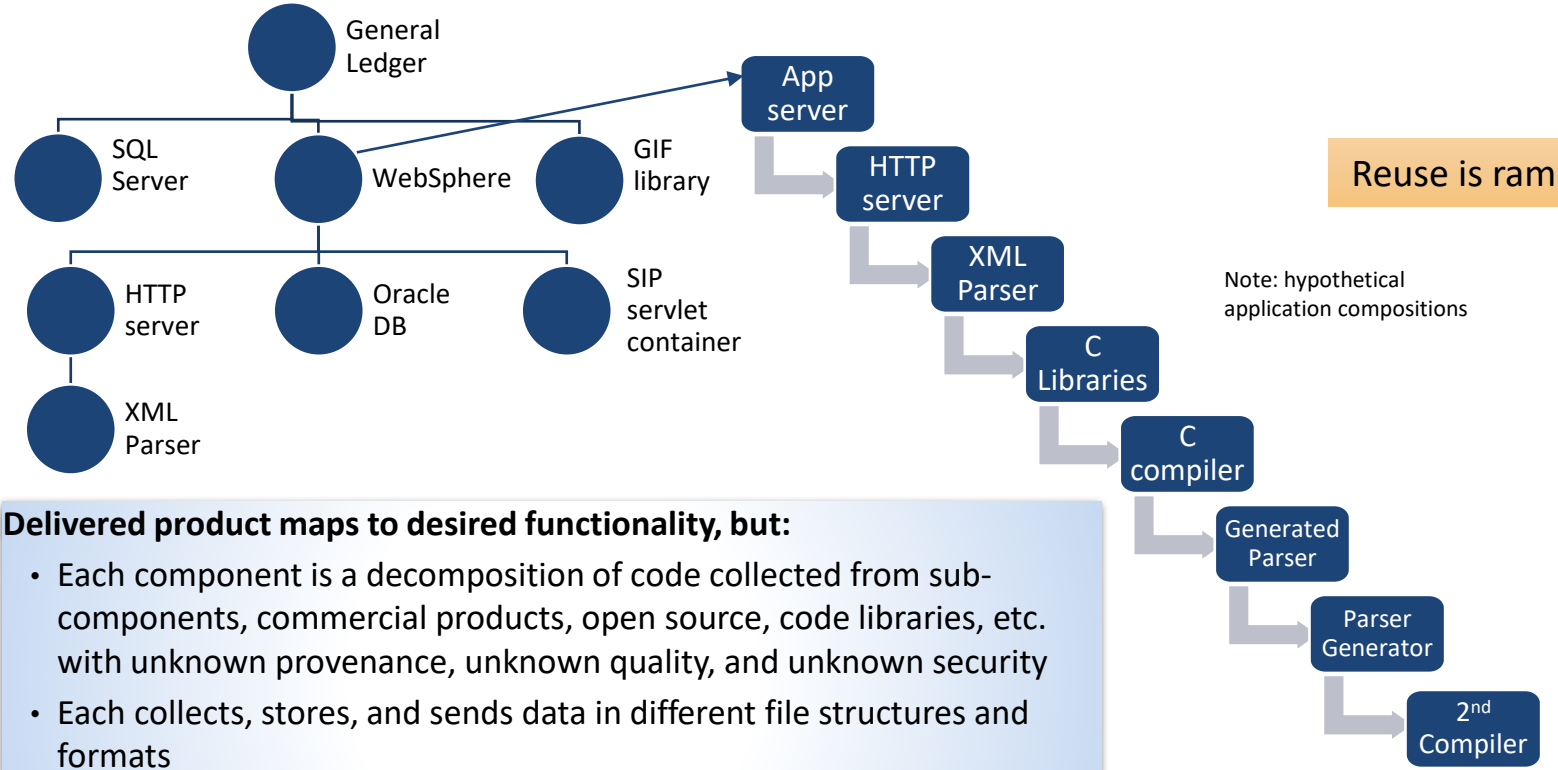
All software code contain defects; up to 5% are vulnerabilities

ref: Woody, Carol et al. *Predicting Software Assurance Using Quality and Reliability Measures* http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=428589)

Hundreds of thousands of known software vulnerabilities exist in operations

ref: NIST National Vulnerability Database, https://nvd.nist.gov/general/nvd-dashboard

Software Development is Now Module Assembly



Reuse is rampant!

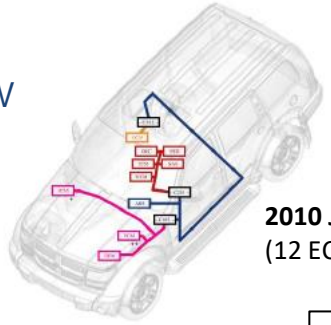
Note: hypothetical application compositions

Delivered product maps to desired functionality, but:

- Each component is a decomposition of code collected from sub-components, commercial products, open source, code libraries, etc. with unknown provenance, unknown quality, and unknown security
- Each collects, stores, and sends data in different file structures and formats
- No one person, team, or organization knows how all the pieces work

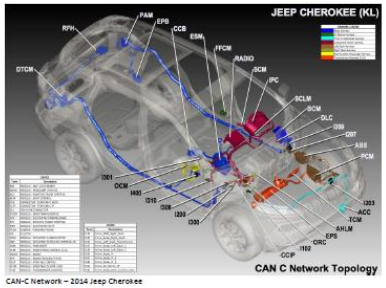
Assembly from 3rd Party Components Reduces Construction Cost/Schedule and Increase Flexibility

Example:
Vehicles are now Assembled from Engine Control Units (ECUs)



2010 Jeep Cherokee
(12 ECUs)

2014 Jeep Cherokee
(32 ECUs)



Supply Chain Risk Increases Exponentially

ECUs are prefabricated, software-driven components addressing select functionality and tailorable to a specific domain.

Modern high-end automotive vehicles have software and connectivity:

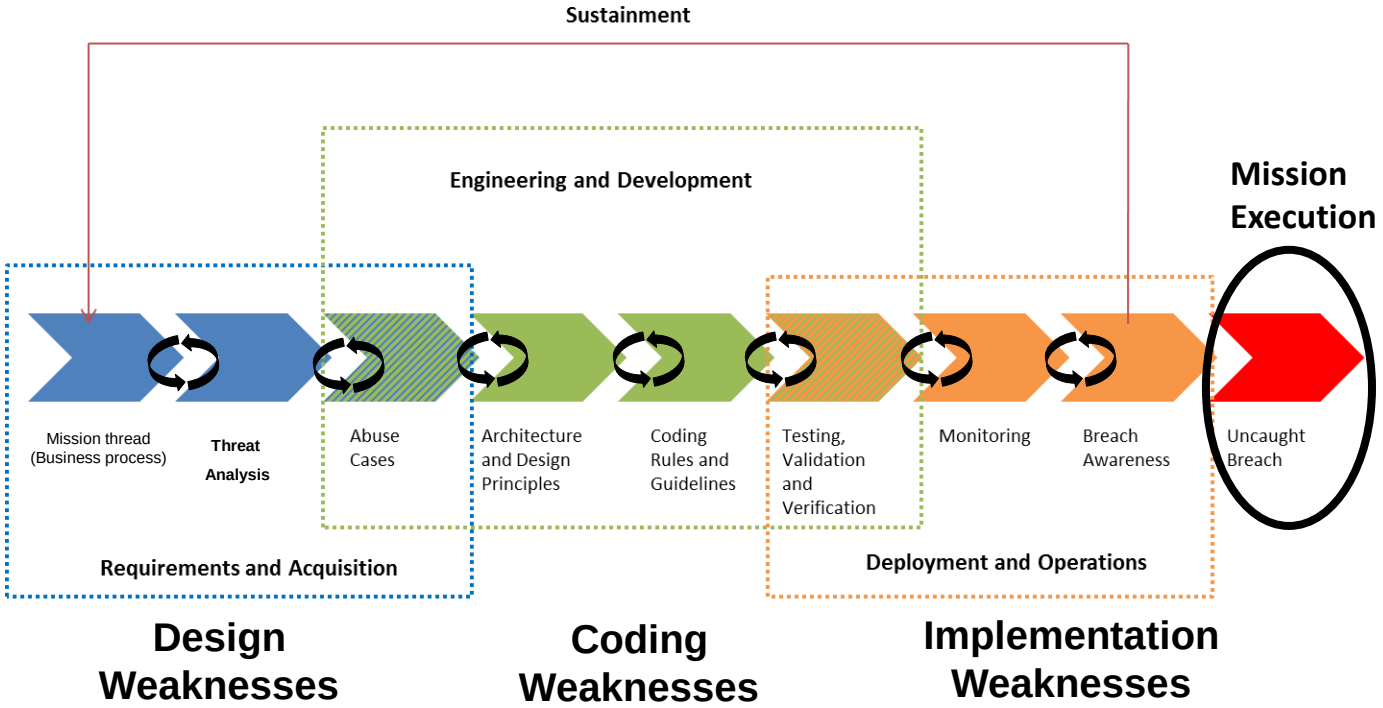
- Over 100 million lines of code
- Over 50 antennas
- Over 100 ECUs

Sources: Miller and Valasek, A Survey of Remote Automotive Attack Surfaces, http://illmatics.com/remote%20attack%20surfaces.pdf; https://www.cst.com/webinar14-10-23~?utm_source=rfg&utm_medium=web&utm_content=mobile&utm_campaign=2014series
https://en.wikipedia.org/wiki/Electronic_control_unit

Challenge: Major Shifts in Technology Adds Cybersecurity Risk

From…	To…
Hardware-based solution	Software-intensive system
Waterfall methodology	Agile at scale approach
Organization owned infrastructure	Shared infrastructure (e.g. Cloud)
Compliance verification upon completion before fielding (e.g. ATO)	Continuous integrated monitoring (e.g. cATO)
Systems developed from requirements and architectural designs	Systems assembled primarily from reused (often 3rd party) components that map to requirements
Development life cycle tailored to the system under development	DevSecOps Development Factory using 3rd party tools and automation

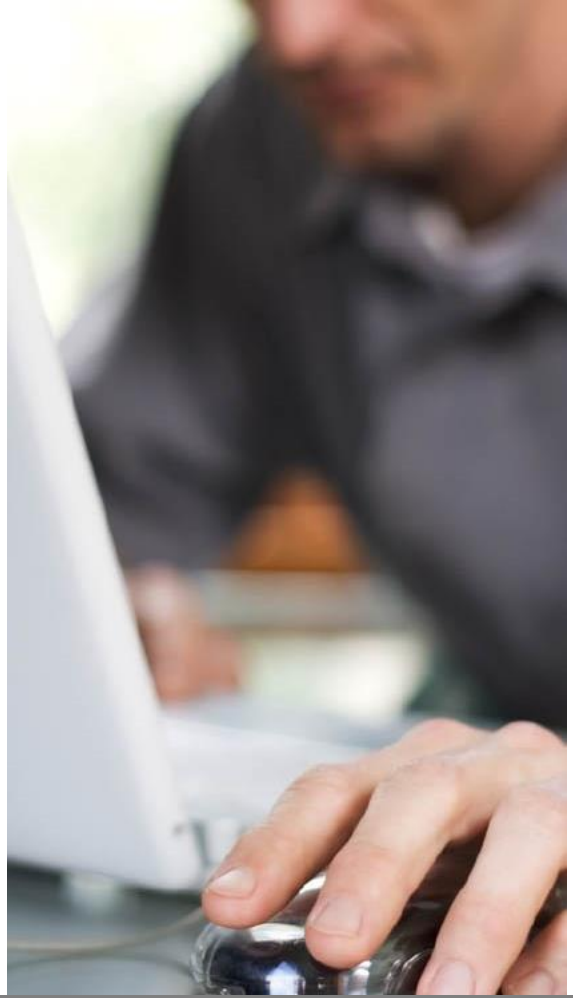
Cybersecurity and Supplier Risk are Lifecycle Concerns



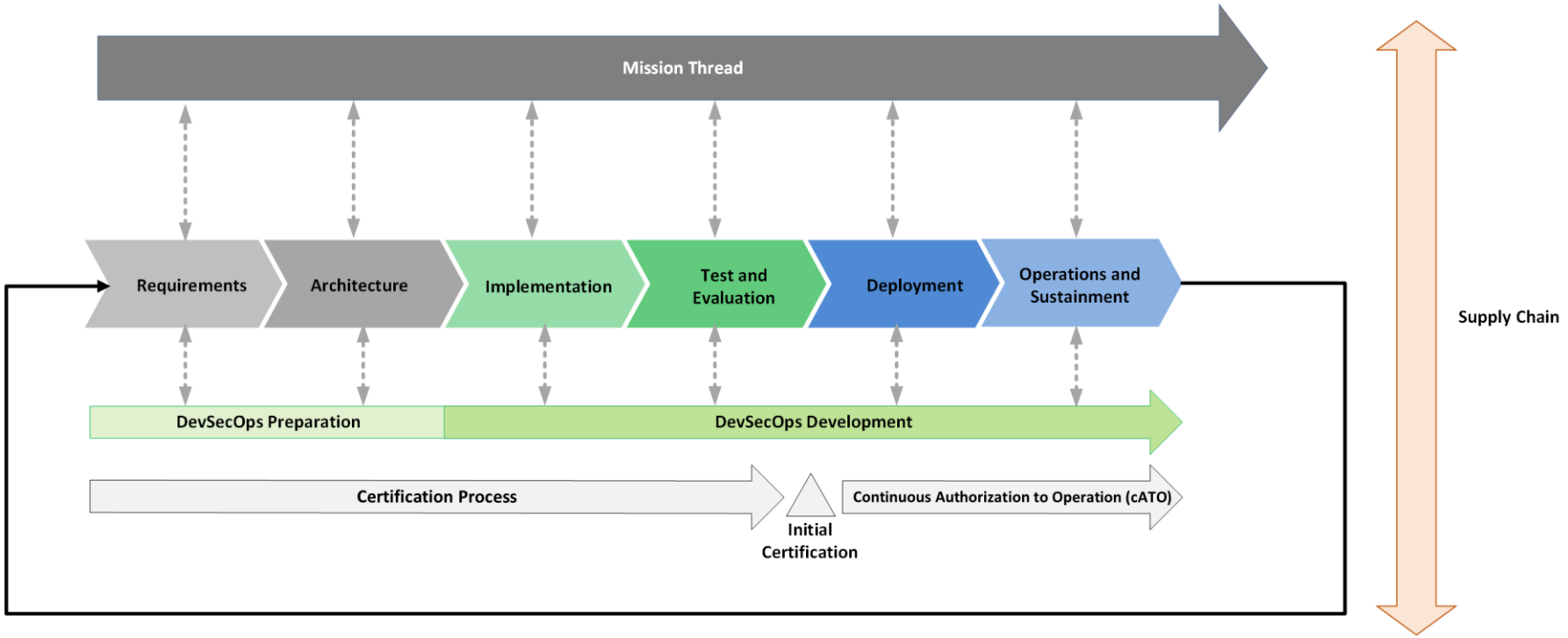
Key Gaps Impacting Cybersecurity and Supply Chain Risk

- **System Engineers** frequently decompose the system into its technology components and delegate risk and requirements management
- **Systems Engineers** are not learning from current operational experience
- **System Engineers** often accept risks without understanding the potential mission impacts over the system's lifecycle
- **Program Managers** have not focused on acquisition oversight in the face of growing third party service and product dependencies
- **Program Managers** can define acquisition requirements using standards, guidelines, and controls as a substitute for effective system security requirements

Acquisition Security Framework (ASF) Overview



Acquisition Security Framework (ASF) Problem Space



ASF Problem Space -2

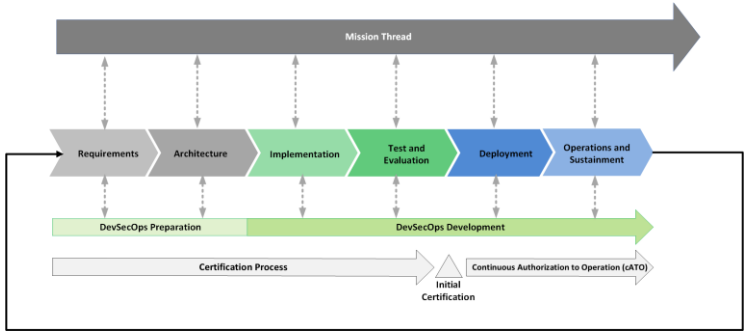
Cybersecurity practices need to be integrated with engineering activities across the systems lifecycle to

- Mitigate acquisition-related security risks
- Implement resilient architectures

Cybersecurity risks must be managed continuously during operations to ensure that evolving security and resilience requirements are met, effectively and efficiently.

- Update software, hardware, and firmware to address security vulnerabilities
- Manage operational security processes to produce consistent results over time

DevSecOps components must be integrated into the systems lifecycle via collaborative process management.



Integrated Security Risk Management

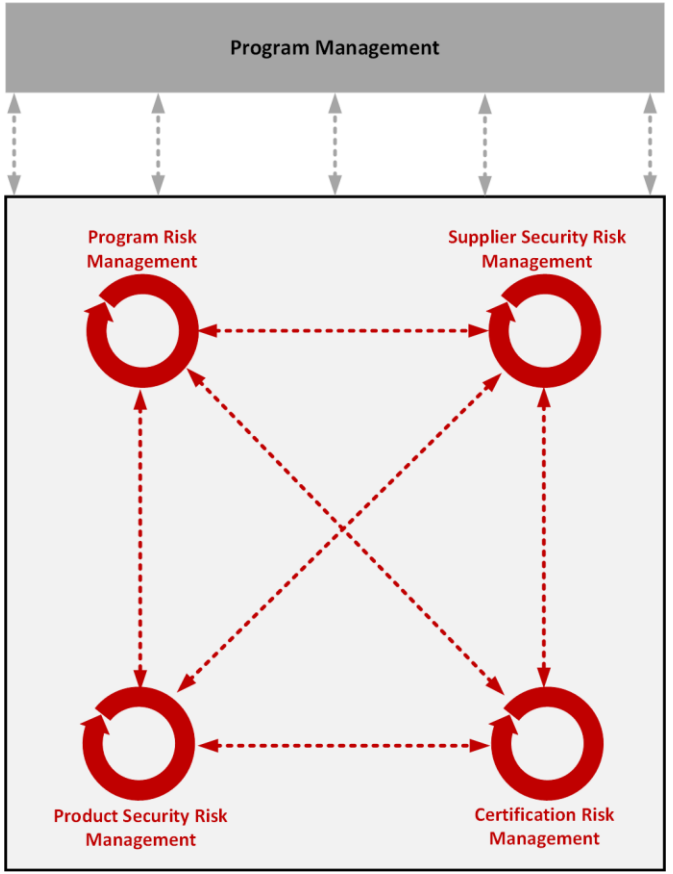
Security risk is managed from multiple perspectives across an acquisition program.

Leadership roles and coordination points change and evolve throughout the lifecycle.

Risk identification, prioritization, and escalation must be ongoing by all areas From all perspectives

The program's risk management strategy defines how

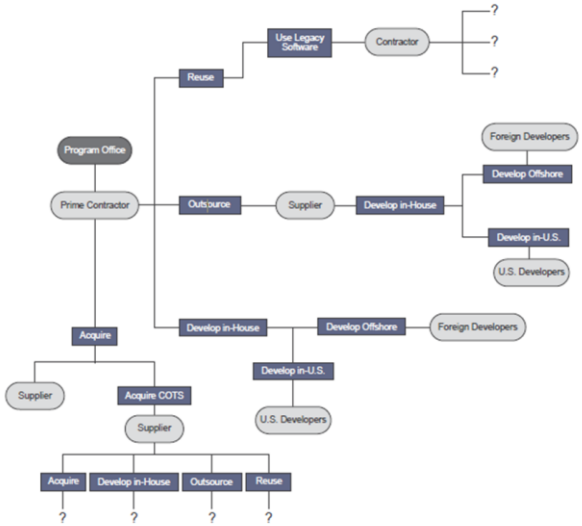
- Groups manage risk collaboratively
- Technology and security gates support security risk objectives



Aligning and Managing Security Objectives -1

Each organization/program unit addresses security from a different perspective:

- Mission Thread
  - Focus: Assuring mission success
- Acquisition and Development
  - Focus: Build security into the software-reliant system
- Operations and Sustainment
  - Focus: Protection and sustainment of the system
- Certification
  - Focus: Certify systems for deployment

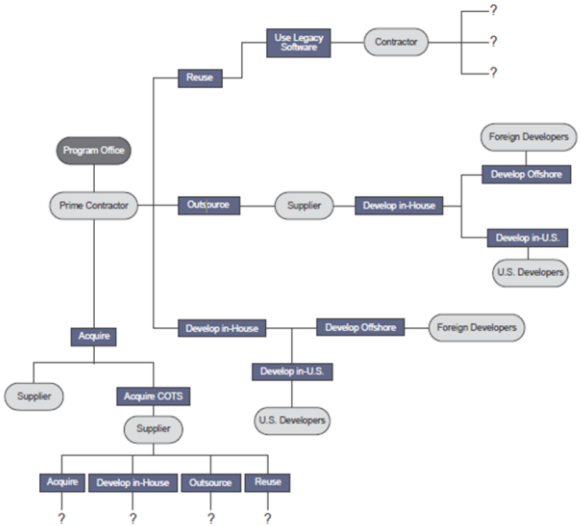


Security objectives across organizations/program units need to be aligned and managed.

Aligning and Managing Security Objectives -2

ASF facilitates the alignment of shared foundational program objectives to support:

- Governance of program management, suppliers, controls, compliance, and certification
- Process management and improvement to monitor a
  - Ongoing changes in security posture
  - Program security effectiveness and efficiency
- Risk management and disposition strategies



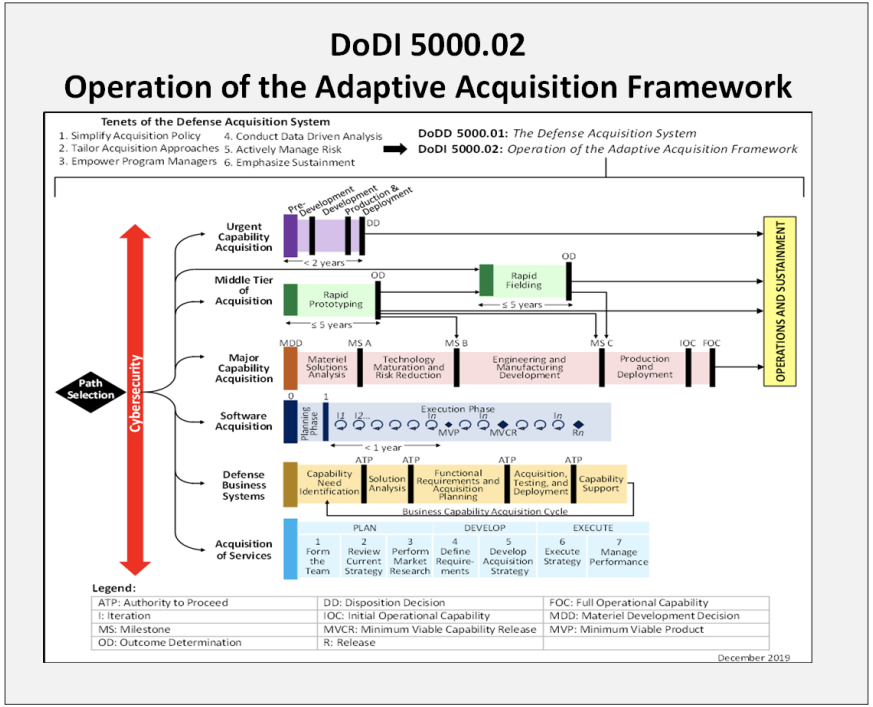
Integrating Security into Acquisition and Engineering

Security practices (management and technical) need to be integrated into a program's existing acquisition and engineering practices.

Security practices and processes (management and technical) need to scale to multiple types of acquisitions, including

- Major capability acquisition
- Software acquisition
- Defense business systems
- Acquisition of services

Security practices and processes must scale to specific development approaches, such as DevSecOps.



Process Management and Improvement

Higher degrees of process management translate to more stable environments that

- Produce consistent results over time
- Are able to achieve their missions during times of stress

Each organization/program unit must manage the maturity of its security practices.

Security practices do not need to be at a uniform level of maturity to be sufficient.

Acquisition Security Framework (ASF) Task: Goals

Integrate software security engineering practices into the acquisition lifecycle

- Define a risk-based framework that supports
  - Security engineering across the lifecycle and supply chain
  - Complexity through integrated process management
- Integrate lessons learned from successful supply chain attacks (e.g., malware, ransomware, denial of service)
- Incorporate DevSecOps concepts and principles[1]
- Adapt system and software engineering measurement activities to include security where appropriate, especially in early lifecycle activities
- Ensure consistency with DoD policies, such as DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*.

1. As defined in Woody, C.; Chick, T.; Reffett. A.; Pavetti, S.; Laughlin, R.; Frye, B.; & Bandor, M. “DevSecOps Pipeline for Complex Software-Intensive Systems: Addressing Cybersecurity Challenges.” *Journal of Systemics, Cybernetics and Informatics*. Volume 1. Number 5. (ISSN: 1690-4524) 2020. pp. 31-36.

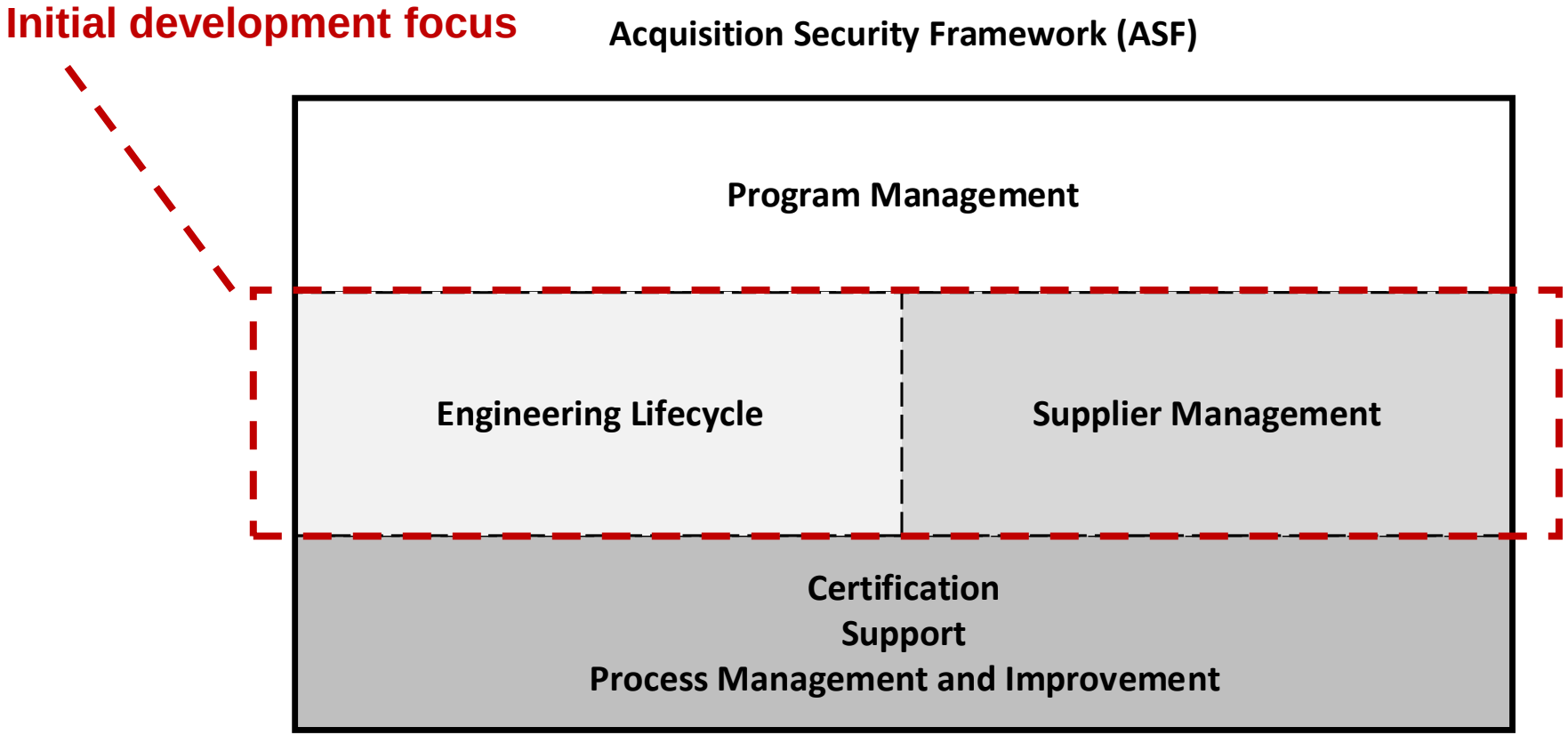
What is the ASF?

The ASF structures a collection of cybersecurity practices that an acquisition program should perform when acquiring a secure and resilient software-reliant system into the areas that need to ensure they are performed:

- Program Management
- Engineering Lifecycle
- Supplier Management
- Certification
- Support
- Process Management and Improvement

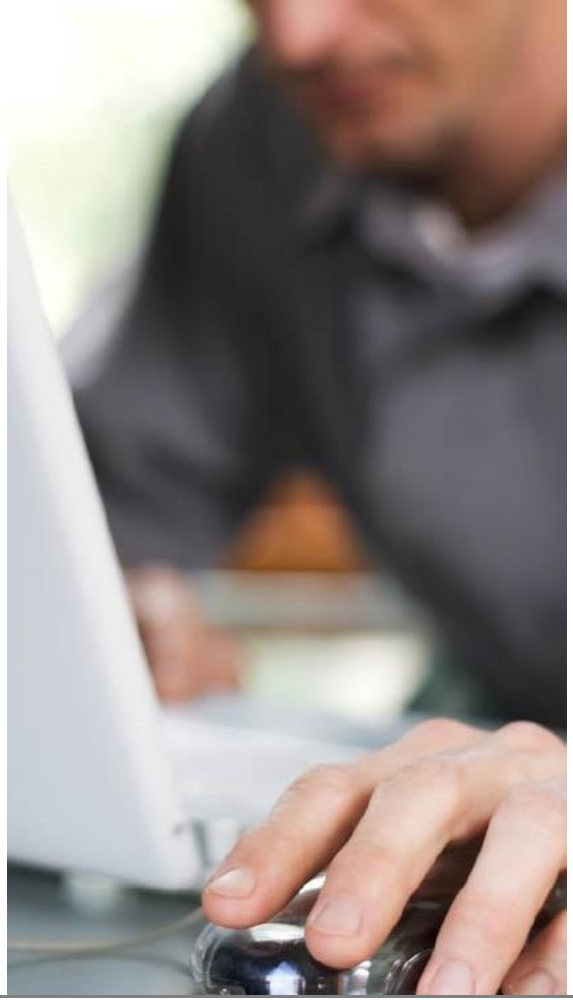
The framework enables programs to identify gaps when acquiring, engineering, and operating secure, resilient software-reliant systems.

ASF Structure



Acquisition Security Framework (ASF)

Current Framework Details



Engineering Lifecycle

Domain	Key Concepts
Engineering Infrastructure	Infrastructure Development Infrastructure Operation and Sustainment
Engineering Activities	Product Risk Management Requirements Architecture Third-Party Components Implementation Test and Evaluation Transition Artifacts Deployment Secure Product Operation and Sustainment

Example: Architecture

Goal—Cybersecurity risks in the architecture and design are identified and mitigated.

The purpose of this goal is to identify and mitigate security risks resulting from in the system's architecture and detailed design.

1. Is a process for performing security risk analysis of the architecture and detailed design defined?
2. Are identified security risks in the architecture and detailed design addressed?
3. Has an architecture tradeoff analysis of quality attributes, including security, been performed?
4. Have security risks resulting from architecture tradeoffs been communicated to stakeholders?
5. Has the architecture's attack surface been minimized based on the results of an attack-path analysis?
6. Is a cross check of the architecture and detailed design performed to resolve any issues or inconsistencies in security features?
7. Are security requirements updated periodically to reflect security changes to the architecture or detailed design?
8. Are reviews conducted with stakeholders to ensure that security risks in the architecture and detailed design are mitigated sufficiently?

Example: Third-Party Components

Goal—Security vulnerabilities in third-party components (TPCs) are identified and mitigated.
The purpose of this goal is to develop a bill of materials (BOM) for a product and ensure that operational security risks in the third-party software, firmware, and hardware are managed over time.

1. Are engineering relationships with third parties based on standards, guidelines, and policies?
2. Is an identification scheme that uniquely identifies each third-party component (TPC) implemented?
3. Is a repository to track TPC usage in products implemented and maintained?
4. Is a process defined for identifying the TPCs used in a product to create a bill of materials (BOM)?
5. Are suppliers evaluated and selected for their use of secure development practices?
6. Is a process defined for assessing a TPC's operational risk?
7. Are TPCs monitored for vulnerabilities and available patches?
8. Are TPCs prioritized for patch application based on operational risk?

Example: Implementation

Goal—Vulnerabilities in software code are identified, managed, and tracked.

The purpose of this goal is to identify and address vulnerabilities and security issues in the code base.

1. Is an appropriate suite of security tools integrated into the software development environment?
2. Are secure coding standards and practices applied?
3. Are code reviews (e.g., peer reviews) performed to identify weaknesses and vulnerabilities?
4. Is source code in critical components analyzed using white-box testing (e.g., static code analysis) during coding and unit testing to identify weaknesses and vulnerabilities?
5. Is software in critical components analyzed using black-box testing (e.g., dynamic code analysis, vulnerability scanning) during integration testing to identify weaknesses and vulnerabilities?
6. Are coding weaknesses and vulnerabilities remediated and tracked to resolution?

Supplier Dependency Management

Domain	Key Concepts
Relationship Formation	Establishing supplier relationships is planned Formal agreements include resilience requirements Supplier are evaluated Managing supplier risk
Relationship Management	Suppliers are identified and prioritized Supplier performance is governed and managed Supplier risk management is continuous Change and capacity management are applied to suppliers Supplier access to program or system assets is managed Infrastructure and governmental dependencies are managed Supplier transitions are managed
Supplier Protection and Sustainment	Disruption planning includes suppliers Planning and controls are maintained and updated Situational awareness extends to suppliers

Supplier Dependency Management – Example - 1

Domain 1. - Relationship Formation

Goal 1– Establishing supplier relationships is planned.

The purpose of this goal is to assess whether processes are in place to enter into relationships and formal agreements with suppliers.

1.	Does an established process exist for entering into formal agreements with suppliers? [EXD:SG3.SP3]*

Goal 2 – Formal agreements include resilience requirements.

The purpose of this goal is to assess whether supplier agreements include resilience/security requirements.

1.	Are resilience requirements included in formal agreements with suppliers? [EXD:SP3.SP4]

* References the CERT Resilience Management Model. The naming format is: Domain:Goal:Practice.

Supplier Dependency Management – Example - 2

Domain 3. - Supplier Protection and Sustainment

Goal 1 – Disruption planning includes suppliers.

The purpose of this goal is to assess whether the program or system accounts for suppliers as part of its incident management and service continuity processes.

2.	Have incident declaration criteria that support the program or system been established and communicated to relevant suppliers? [IMC:SG3.SP1, IMC:GG2.GP7]

* References the CERT Resilience Management Model. The naming format is: Domain:Goal:Practice.

Next Steps

Preparing two areas of practice for broader distribution and review:

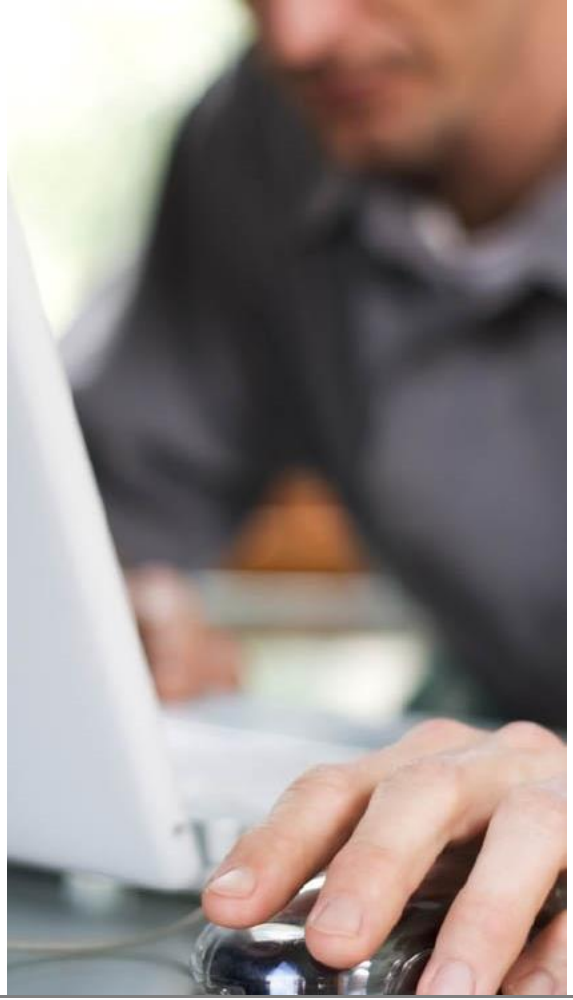
- Engineering Lifecycle
- Supplier Management

Drafting next area: Program Management

Exploring pilot opportunities with DoD programs to apply published practices for gap analysis

Acquisition Security Framework (ASF)

Summary



Barriers to Effective Management

Complexity

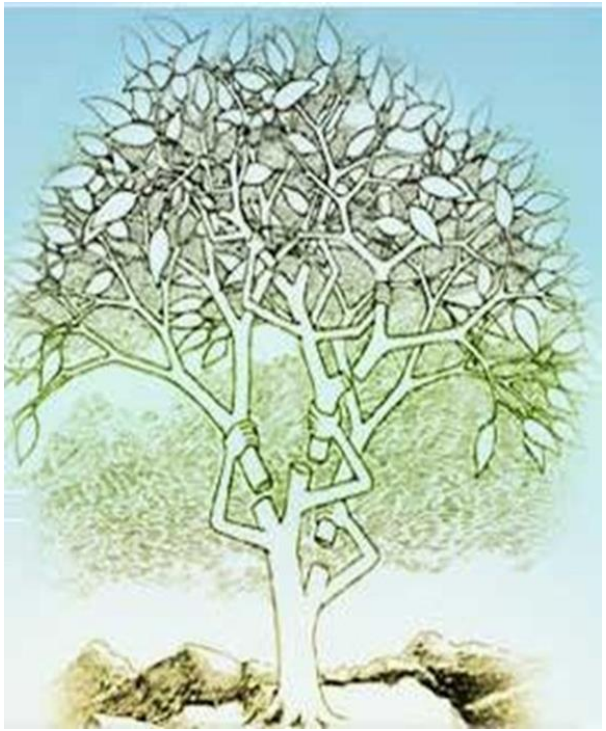
Siloed departments operating under different requirements

- Procurement/acquisitions
- Operations
- Incident management

Vagueness or limitations in formal agreements

Changing requirements across system lifecycles

Incomplete or narrow risk management processes



Acquisition Security Framework Approach

Integrate cybersecurity practices with engineering activities across the systems lifecycle to

- Mitigate acquisition-related security risks
- Implement resilient architectures

Continuously manage cybersecurity risks during operations

Integrate DevSecOps components into the systems lifecycle via consistent and collaborative process management

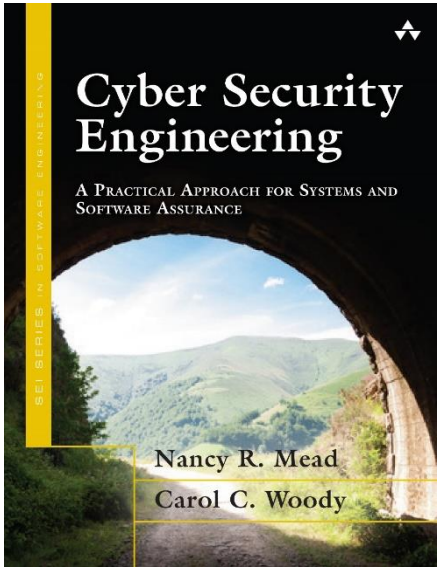
Ensure consistency with DoD policies, such as

- DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*
- DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*

Opportunities to Learn More

Textbook

Cybersecurity Engineering



SEI Book Series

Professional Certificate

CERT Cybersecurity Engineering and Software Assurance

https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881

Online training in five components

- Software Assurance Methods in Support of Cybersecurity Engineering
- Security Quality Requirements (SQUARE)
- Security Risk Analysis (SERA)
- Supply Chain Risk Management
- Advanced Threat Modeling

Contact Information

Carol Woody, Ph.D.

cwoody@cert.org

Web Resources

Building security into application lifecycles

https://sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=48574

CMU SEI Home Page

https://sei.cmu.edu/

Joint Federated Assurance Center Software Assurance Strategy

Bradley Lanford
Software Assurance Lead, Contractor Support
Office of the Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems & Mission Engineering Conference
December 6-8, 2021

Introduction

- **The Joint Federated Assurance Center (JFAC) was established to ensure the security of software and hardware developed, acquired, maintained, and used by the Department of Defense (DoD) through the federation of existing DoD software and hardware assurance resources, expertise, and capabilities.**

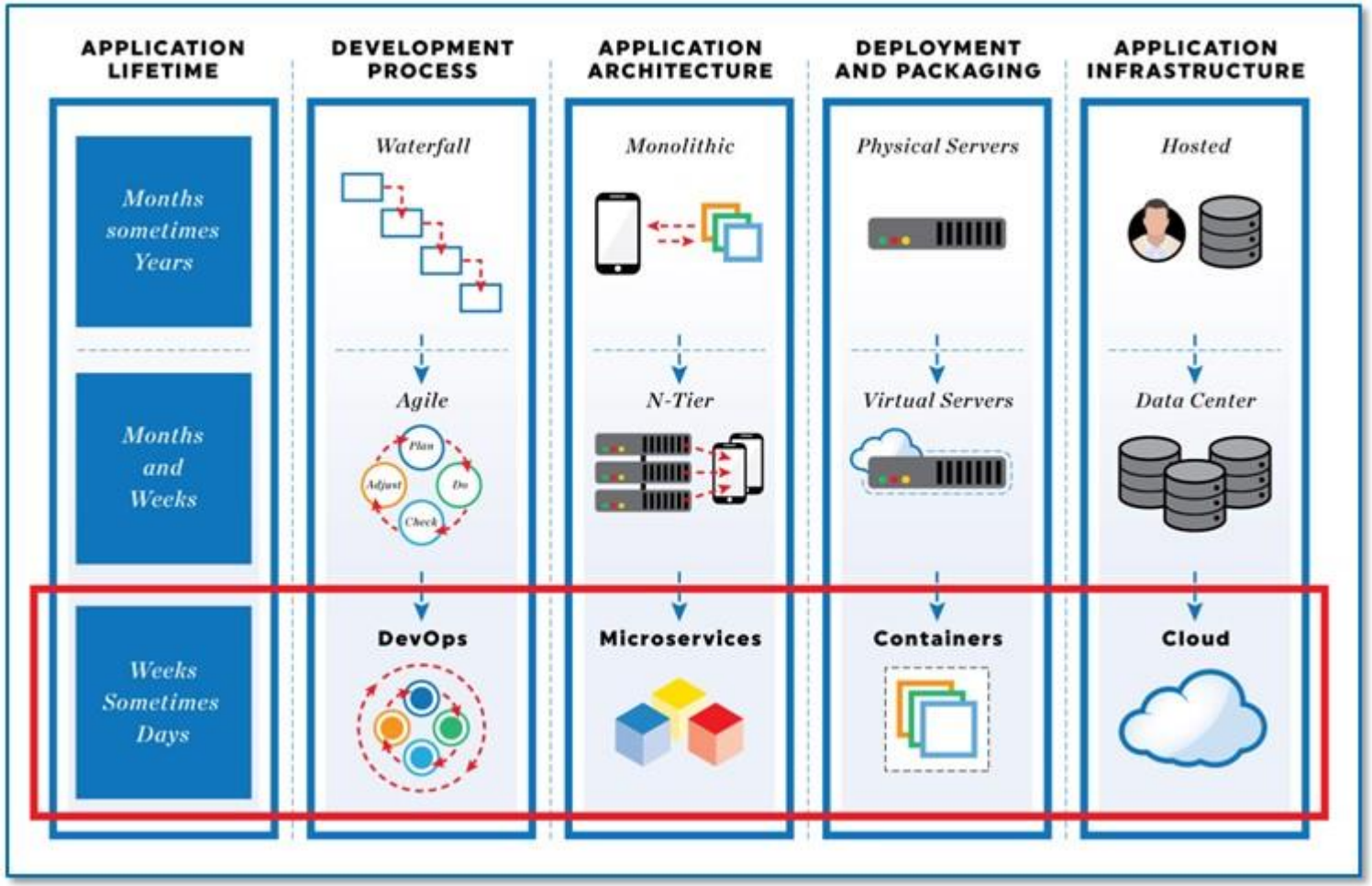
- **Federal and Department initiatives are revolutionizing application of software assurance tools, practices, and techniques:**
  - Development, Security, and Operations (DevSecOps)
  - Zero Trust Architecture
  - DoD Adaptive Acquisition Framework Software Acquisition Pathway
  - Executive Order 14028 – Improving the Nation's Cybersecurity

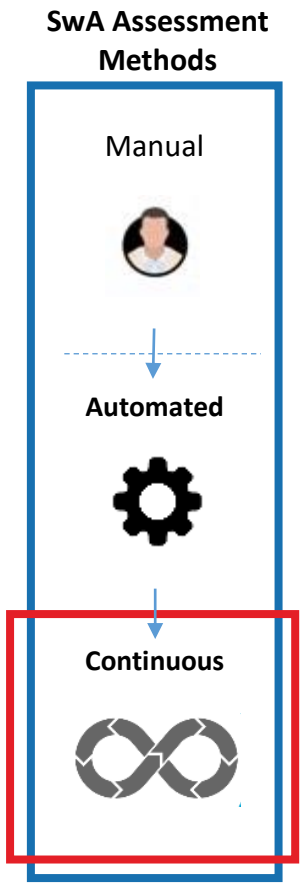
- **The JFAC Modernization Strategy for Software Assurance was developed to support the software assurance initiatives:**
  - Focus on opportunities to overcome resource limitations to provide capabilities and expertise directly to DoD programs
  - Leverage existing DoD software initiatives to modernize JFAC infrastructure and capabilities
  - Transition culture away from the development of capabilities to the federation and maturation of existing tools and resources

JFAC Historical Overview

Growth of JFAC		State of Software Assurance (SwA)
National Defense Authorization Act (NDAA) Section 933 required the establishment of a baseline for SwA in policy	FY 2013	Estimated 27% of known vulnerabilities remediated by government, Veracode '13-15
NDAA Section 937 established JFAC as a federation of capabilities	FY 2014	Government spending on Information Technology (IT) defenses vs. SwA analysis 23:1, Gartner '14
JFAC Charter signed by Deputy Secretary of Defense	Q2 2015	84% of breaches exploit vulnerabilities in the application, Forbes '15
JFAC Concept of Operations (CONOPS) approved establishing JFAC Coordination Center	Q3 2015	Common Vulnerability Scoring System (CVSS) Version 3 published for SW vulnerability evaluation
JFAC Portal (Army.mil) and Coordination Center (SEI) capability established	FY 2016	NDAA FY16 Section 1647 requires the evaluation of cyber vulnerabilities for all weapons systems
Consolidation of Portal and Coordination Center Hosting (NSERC)	FY 2017	NDAA FY17 Section 1650 requires the evaluation of cyber vulnerabilities for critical infrastructure
Increase in Coordination Center support for tool metrics, AKB, SIPR/JWICS portal	FY 2018	DSB identifies opportunities to address SW vulnerabilities with iterative development and tool chains

Software Evolution





SwA Modernization Roadmap

FY 2019 - FY 2021

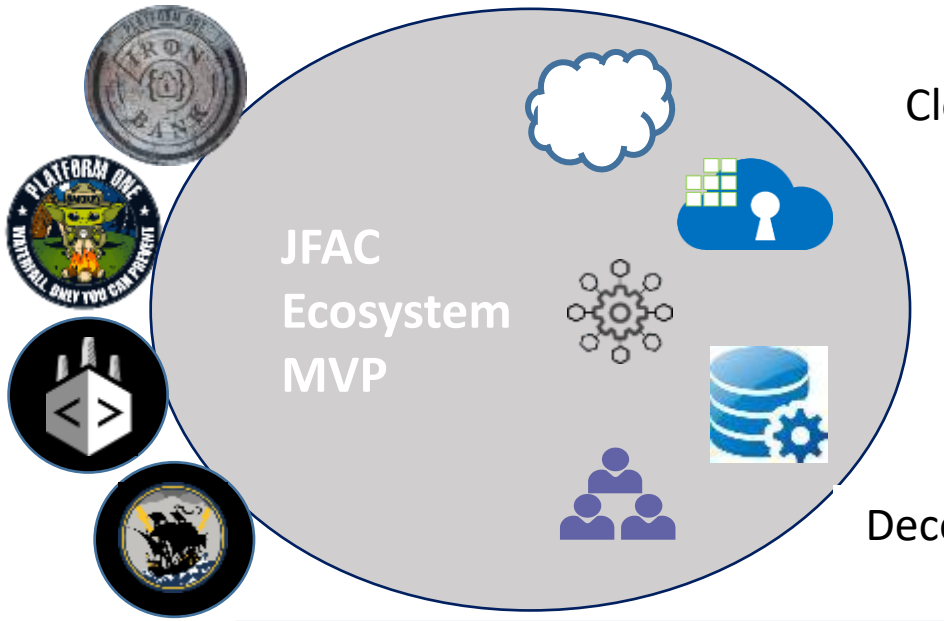
Capabilities that Deliver Tangible Value across DoD

- #1 Guidance and Training
- #3 Software Assurance Tools/Licenses
- #2 Knowledge Base of Tools, use, and Components
- #4 JFAC Support Services
  - JFAC Portal
  - Assurance Knowledge Base
  - Licenses Distribution

FY 2021 Efforts Pilot initial capabilities and performance measures	FY 2022 Develop Infrastructure	FY 2023 Establish Capabilities	FY 2024 Capabilities Deploy to Service Providers and Programs
MITRE Technology & Innovation Roundtable™ Assurance Lab Pilot	Identify cloud provider and core services		• Platform as a Service (PaaS) • Integrated/Swappable Tools • Risk Categorization Engine
Red Hat Enterprise Linux & kubernetes			• Software as a Service (SaaS) • Automated SwA Analysis • Secure Artifact Repository
DoD/NNSA Malware Discovery Exercise (MDX)			• Software as a Service (SaaS) • Packaged tool solution • Secure, SBOM, & POA&M
JFAC Tools & License Distribution	Streamline Infrastructure	Modernization	• Streamlined information to programs • Modernized Approach (EO 14028) • Inform procurement (NDAA 1655)
JFAC Technical Working Group	• Development S&T Roadmap • Identification Hard Problems • Prioritization SwA Gaps and Performers		Iterate

Modernization Strategy for Software Assurance

Goal: Assurance as a Service
Create an environment, leveraging existing Software Factories, to provide tools and capabilities available to SwA Service providers and programs.



Cloud Native Assessment Environment

Assured Pipeline and Repository

Technology Maturation and Transition

Software Assurance Toolkit and License

Decentralized Assessments/Automation of Alerts

Key enablers to drive maturity
Standardization of processes to enable automation
Science & Technology investment to mature assurance capabilities
Education of service providers to transition culture

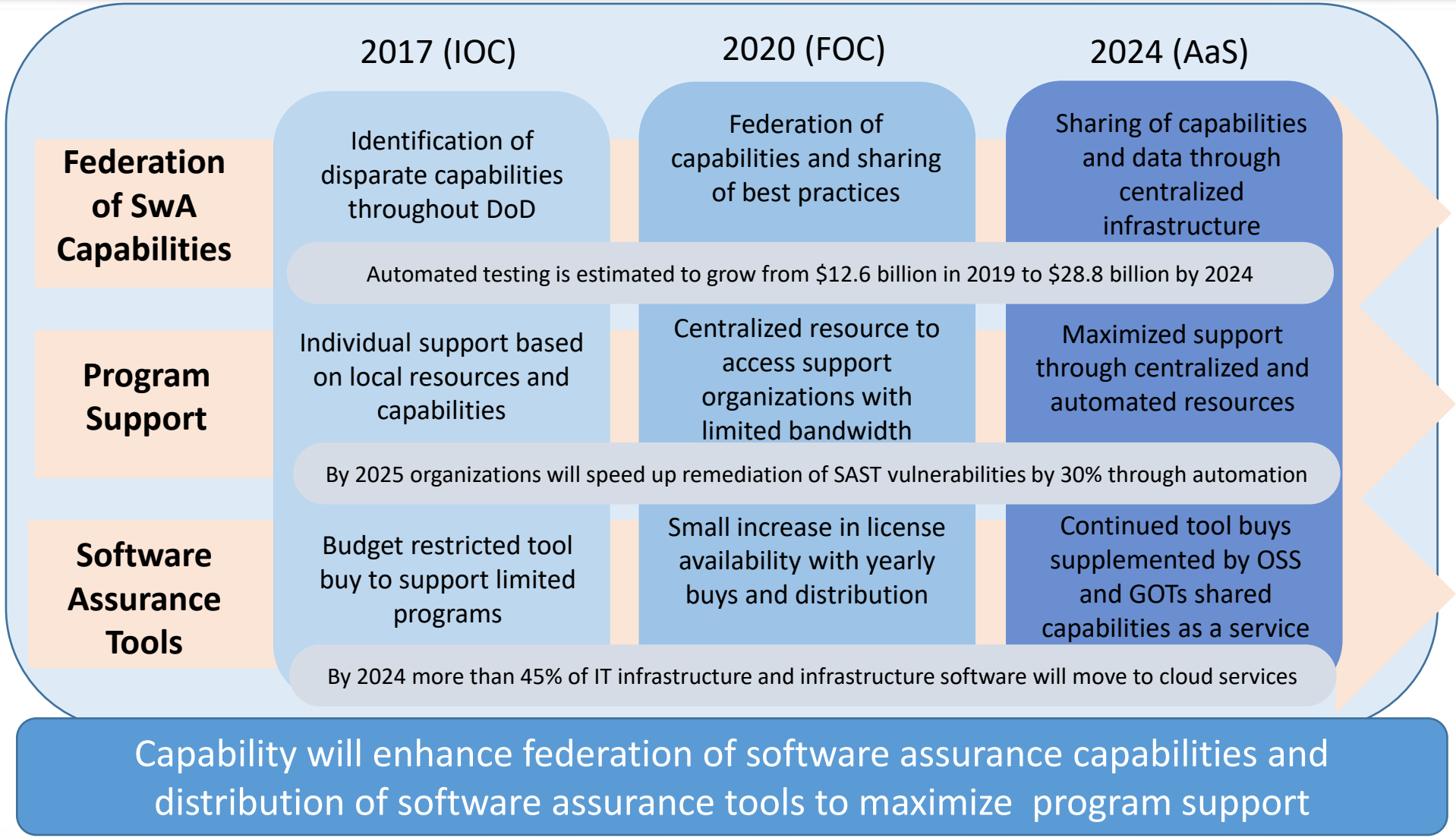
Software Assurance as a Service

- **Transition away from the federation of self-hosted assurance capabilities towards existing cloud native assurance services.**

- **Minimum Viable Product ecosystem will include:**
  - Platform-as-a-Service environment allowing remote access to automated assurance pipelines
  - Software-as-a-Service assurance capabilities available to all DoD programs
  - DoD accessible repository for access to assured tools, components, and S&T
  - Toolkit for access to assurance resources in offline environments

- **Roadmap Overview:**
  - FY21: JFAC Modernization Strategy for Software Assurance developed
    - Incorporates lessons learned and adoption of new practices
  - FY22: Streamline existing JFAC infrastructure; identify cloud capabilities to support transition
  - FY23-24: Create a collaborative ecosystem to promote and make available tools and capabilities for program use
    - Leverages JFAC SwA Technical Working Group recommendations, maturation of S&T, and federation of existing capabilities into the cloud native environment

Advancement of Software Assurance

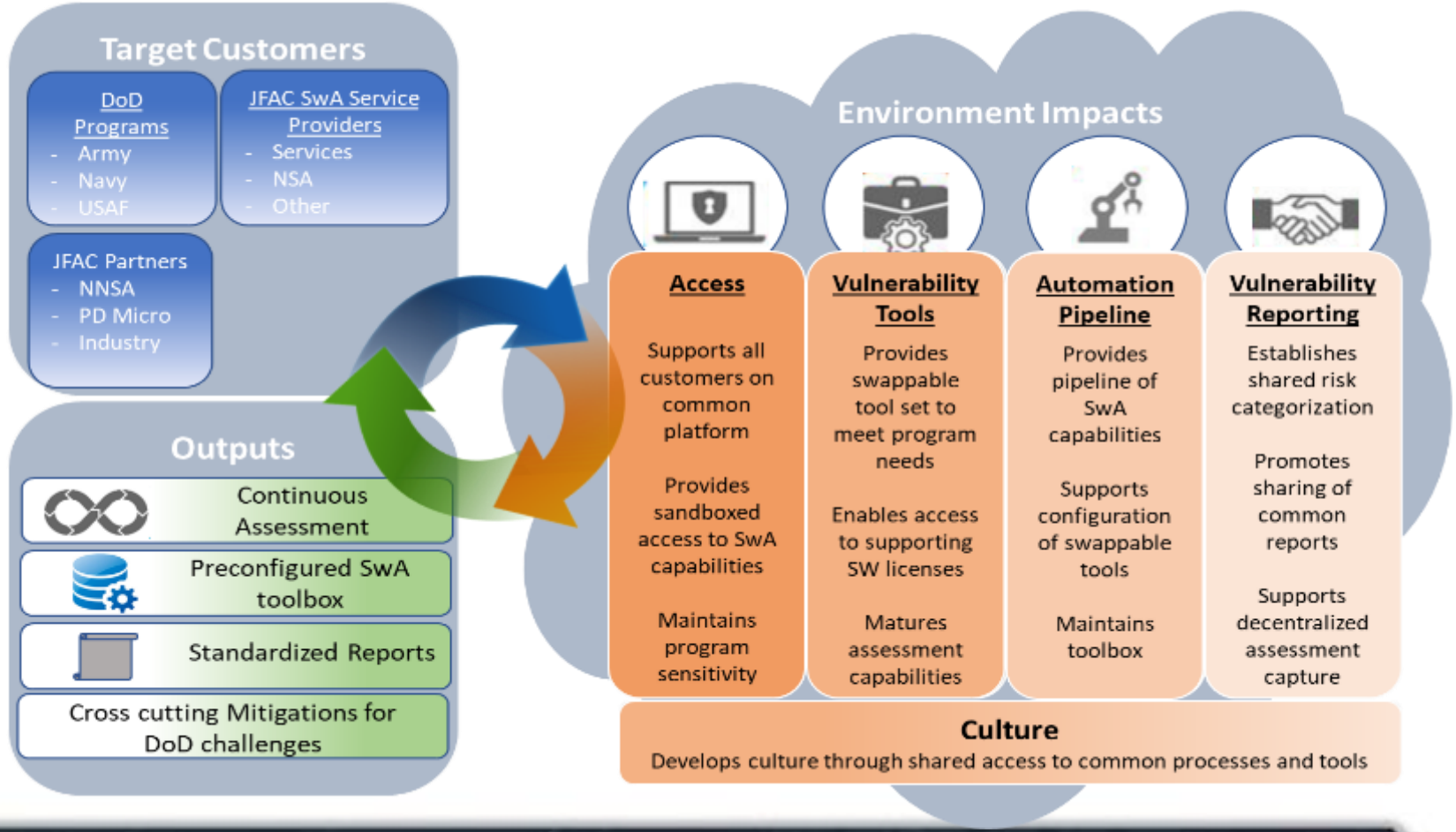


Capability will enhance federation of software assurance capabilities and distribution of software assurance tools to maximize program support

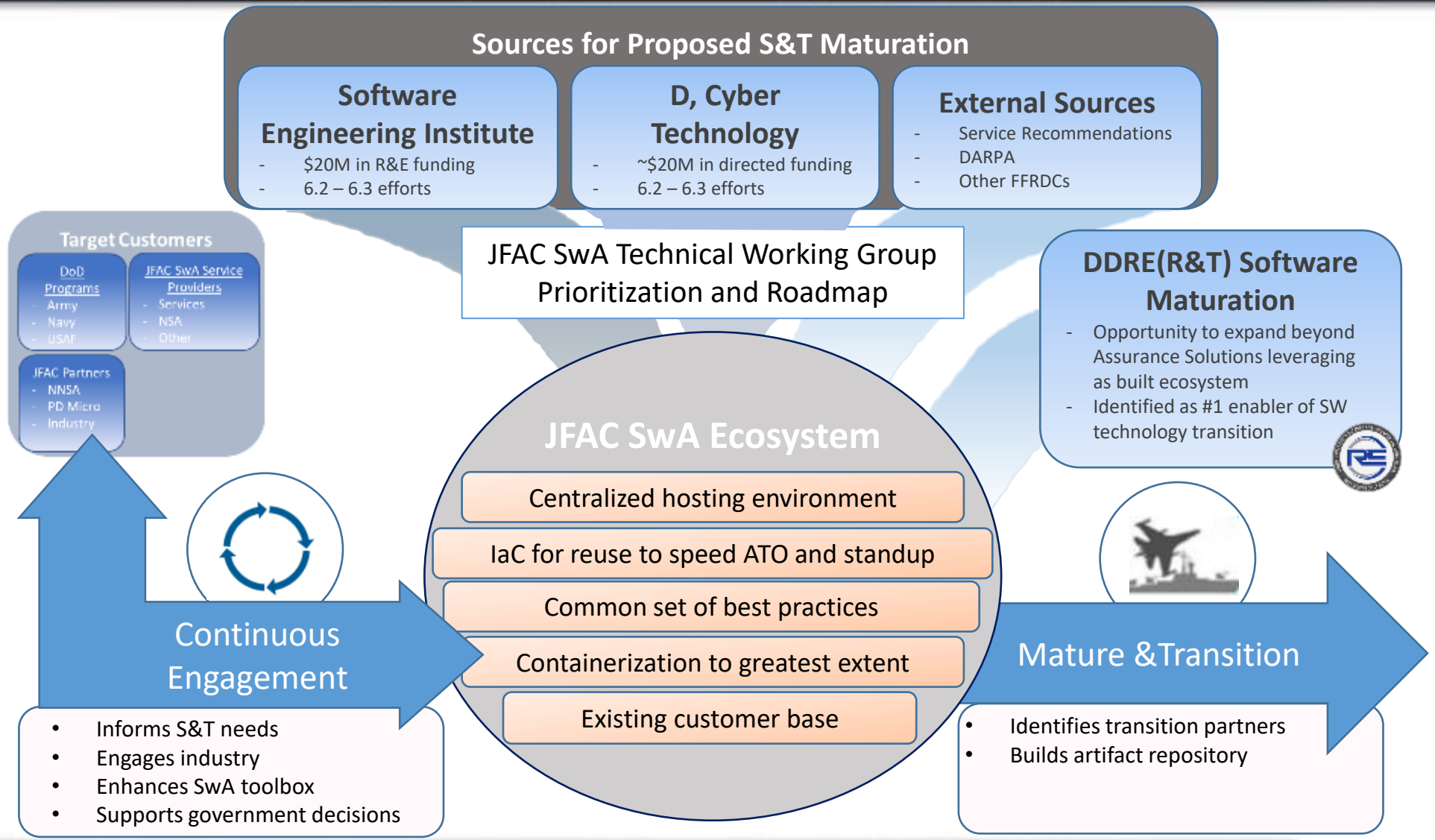
JFAC Environment Capabilities

Provide a centralized resource for DoD programs that offers:

- Consolidation of effective assurance capabilities
- Common risk categorization and reporting
- Increased assurance rigor through automation



Software Assurance Technology Transition Opportunities



JFAC SwA Technical Working Group
Way Ahead

Gap Analysis Prioritization

Review and update of 2017 capability gap analysis

- Prioritize of gaps based on risk and value
- Inform JFAC Strategy implementation

S&T Roadmap

Develop SwA Science and Technology Roadmap

- Lead identification of efforts for proposed investment
- Recommend performers and steps for maturation

Hard Problem Analysis

Make available mitigations directly impacting program

- Identify future SwA gaps and mitigations
- Support service providers and programs through federation of knowledge

JFAC Infrastructure Transition

Software Licensing

Program Support

Body of Knowledge

Procurement Support

Streamline infrastructure to support critical needs (MVP)

COTS Licenses Distribution

- SaaS containerized tool offerings
- BOAs for licensing
- Utilization of GOTS/FOSS tools

Support Services

- Software Service Provider use of PaaS solutions
- Access to SaaS toolkit

Document Repository

- Access to enterprise cloud services
- Link to existing services to strengthen BoK

Assessment Capture

- Partner with JFAC HwA
- Automation of alerts and assessment findings

Modernization to operate in cloud native environment

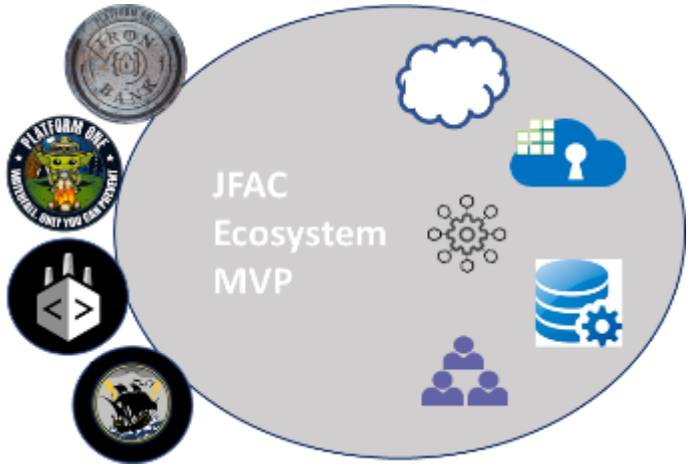
Partnerships

- **DoD DevSecOps Initiative**
  - Coordination of Assurance Platform with DoD SW factories to promote adoption and support DSO efforts
  - Alignment of JFAC Enterprise Software Licenses with platform centralized contract vehicle
  - Recognition for JFAC as leader in technical assessment capabilities through support to DSO initiatives
- **Principle Deputy for Microelectronics Office**
  - Centralized JFAC infrastructure to support HwA and SwA cloud service offerings
  - Single source of assessment information with distributed capabilities and tracking
- **National Nuclear Security Administration (NNSA)**
  - Utilization of Operational Technology and Software Engineering Lifecycle Assurance Guide
  - Promotion of NNSA capabilities as SaaS offerings
  - Coordination with NNSA labs and plants through PaaS and SaaS offerings
- **Military Services and DoD Agencies**
  - Maturation of COTS solutions and distribution to DoD organizations through cloud service offerings
  - Support for existing service providers with PaaS and SaaS capabilities
  - Investment in S&T and identification of partners to advance SwA capabilities

FY22 Planning

Goal: Enhance federation of SwA capabilities and distribution of SwA tools to maximize program support

- **Standardization and advancement of existing JFAC capabilities**
  - Kubernetes / Redhat Phase 3
  - Acquisition and assurance lab pilot
  - Risk categorization
- **Identification of software and platform service offerings**
  - Software factory capabilities
  - Centralized artifact repositories (IronBank)
  - Container hardening processes
- **Recommendations for maturation and transition of S&T capabilities**
  - Investment of 6.4 funding to mature 6.2 / 6.3 efforts
  - Advancement of assurance tools and capabilities
  - Integration of assurance into cybersecurity S&T
- **Respond to Congressional and Executive Orders**
  - Recommendations for JFAC SwA procurement
  - Assessment and identification of mitigations supporting FY19 NDAA Section 1655
  - Testing and SBOM standards supporting Executive Order 14028



Performance Metrics

- Collaborate with partners to develop metrics that measure outcomes
  - Promote successes
  - Enable change

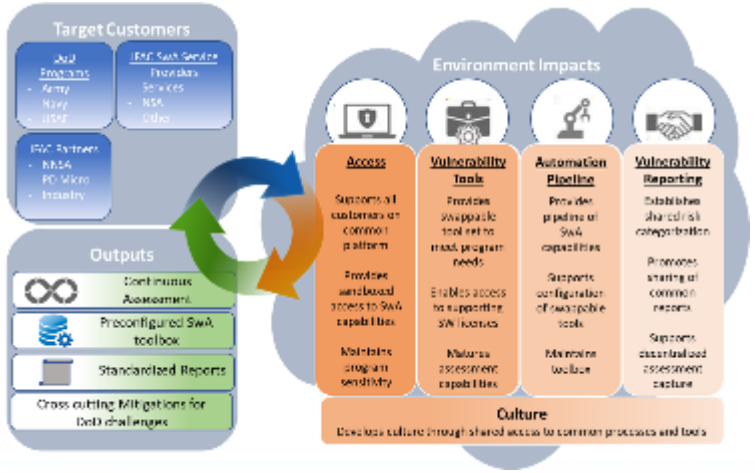
Efforts	Proposed Metrics
Cloud Native Assessment Environment	# of utilized JFAC PaaS offerings, # of downloads, # of capabilities made available through cloud environment
Assured Pipeline and Repository	# and involvement of partner organizations supporting JFAC efforts, # of products assessed, % adoption of JFAC services across DoD
Software Assurance Toolkit	# of programs/service providers utilizing SaaS offerings, # of tools available in SwA toolkit
Tools and License Distribution	# of assessments identified, # of federated organizations, # of licenses distributed, # of programs supported
Technical Working Group	# SwA gaps identified/resolved, # of technology transitions, completion of S&T Roadmap

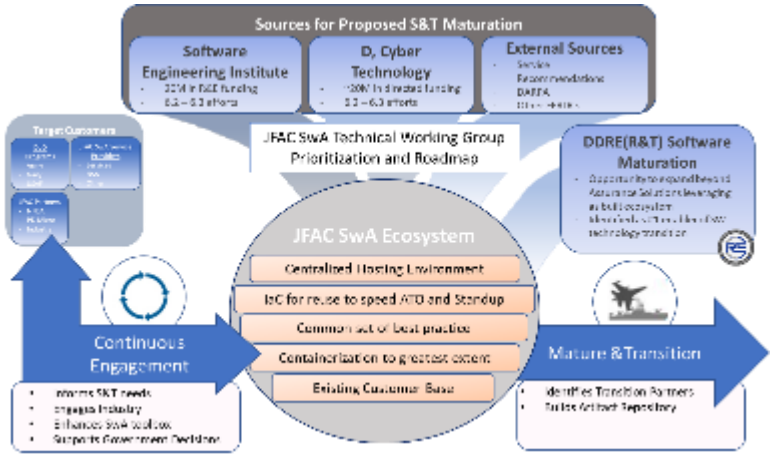
Summary

- **DoD transition to a DevSecOps ecosystem, adoption of modern architecture patterns, and adherence to DevSecOps best practices drives the need for modernization of JFAC infrastructure and program support.**

- **JFAC FY 2022-2024 SwA Strategy provides means to proactively increase mitigation of software vulnerabilities. Strategy includes:**
  - Instantiation of JFAC ecosystems to support platform and SwA services
  - Emphasis on JFAC SwA Technical Working Group expertise to guide project decisions
  - Renewed focus on performance metrics to support Department growth

- **OUSD(R&E) JFAC ecosystem facilitates federated DoD software and assurance capabilities:**
  - Provides access to assessment capabilities for all DoD programs
  - Creates a platform for maturation and transition of S&T efforts





Questions

Backup

References

Automated testing growth:
https://www.marketsandmarkets.com/Market-Reports/automation-testing-market-113583451.html#:~:text=What%20is%20the%20market%20size,18.0%25%20during%20the%20forecast%20period

Increase in SaaS :
https://www.forbes.com/sites/forbescommunicationscouncil/2021/02/24/saas-trends-to-watch-in-2021/?sh=18cb87565385

Application Security Testing Automation:
https://www.gartner.com/doc/reprints?id=1-1YADS6J8&ct=200206&st=sb

Transition to the Cloud:
https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/

2021 Virtual Systems & Mission Engineering Conferenc

Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts

December 7, 2021

Presentation: Rick Dove

Authors: Rick Dove, Keith Willett, Tom McDermott, Holy Dunlap, Cory Ocker, Delia MacNamara

The Future of Systems Engineering (FuSE)

A multi-organization INCOSE-led initiative pursuing the systems engineering Vision.

To accomplish this the FuSE initiative encompasses a number of topic areas with active projects to shape the future of systems engineering.

INCOSE's Systems Security Engineering working group is addressing the FuSE System Security topic area and has identified a roadmap of eleven foundational concepts appropriate for near-term attention.

A brief overview of the eleven concepts follows.

INCOSE FuSE

Future of Systems Engineering

FuSE Collaborative Community

FuSE Road Map (~January 2020)

INCOSE Vision 2025 on Security

The principle purpose of FuSE is to realize the vision

for the future of systems engineering.

“Systems engineering routinely incorporates requirements to enhance systems and information security and resiliency to cyber threats early and is able to verify the cyber defense capabilities over the full system life cycle, based on an increasing body of strategies, tools and methods. Cyber security is a fundamental system attribute that systems engineers understand and incorporate into designs.”

Vision 2035 will be published in January 2022

FuSE System Security

**2020 Activity: Identify foundation gaps appropriate to fill in the near term future,
ie, a roadmap of the next part of the security journey,
not a road atlas of every point of interest.**

**2020 was about concept identification, not a handbook of practice mastery,
i.e., we need new starting points to fill some capability gaps.**

What is impeding the practice of system security that could be rectified now?

FuSE System Security Charter (2020)

Systems Security in the Future of Systems Engineering
(a FuSE initiative project)

Team:
- DoD – Keith Willett
- INCOSE – Rick Dove (Project Lead)
- ISSS – Delia Pembrey MacNamara
- NDIA – Holly Dunlap, Corey Ocker
- SERC – Tom McDermott

What will good look like when we use FuSE to deliver systems?
1. All stakeholders share common security vision and respect.
2. Security is embedded in systems.
3. Security agility is in practice.
4. Systems are built for trust.
5. System and component behavior is monitored for anomalous operation.
6. System components are self protective.

Objectives

What is stopping us from doing this now?
1. SE relates to SSE as an independent specialty practice.
2. Security is viewed as a non-functional cost and ROI value is difficult to verify.
3. Security standards compliance is considered sufficient.
4. Actionable research is in early stages.
5. Contracts and projects detail features and requirements up front rather than desired capabilities that allow innovative solutions.

What will good look like in 2023-2025?
1. Security responsibility and expertise is integrated in the SE-team.
2. Security is viewed as a functional requirement.
3. Security agility will have some effective working patterns in practice as an early base line.
4. Strategies for shared security vision and respect in early practice.

What will good look like by end of 2020?
1. Multi-organization collaboration is active.
2. Initial foundation concepts for FuSE Security identified.
3. Projects to develop and publish some of the foundation concepts are active.

2020 Action Plan
1. IS20 initial foundation papers:
   - Techno-Social Contracts for Security Orchestration.
     www.parshift.com/s/200718IS20-FuSETechnoSocialContracts.pdf
   - Contextually Aware Agile Security.
     www.parshift.com/s/200718IS20-FuSEAgileSecurity.pdf
   - Toward Architecting the Future of System Security.
     https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2020.00717.x
2. Mid 2020: Periodic web workshops in process identifying additional foundation areas.
3. Ongoing: Recruit foundation developers.
4. Late 2020: Additional foundation papers in process.

Objectives

1. **All stakeholders share common security vision and respect.** Many types of stakeholders are involved in the development, usage, and sustainment of a system designed for purpose. That purpose can be compromised by the weakest security link among the stakeholders, which may stem from insufficient security respect or unresolved priority conflicts.
2. **Security is embedded in systems.** Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.
3. **Security agility is in practice.** The attack community is agile in method innovation and target selection. System security needs a response capability equally agile, architected for proactive composability and reactive resilience.
4. **Systems are built for trust.** Trust is accepted dependence on the system, by both stakeholders and other systems. The reasons for trusting a system need to be built in and evident to all stakeholders.
5. **System and component behaviors are monitored for anomalous operation.** Adversaries innovate new attack methods to evade known-pattern detection screening. System and component behavior outside of normal expectations is a method-agnostic telltale.
6. **System components are self protective.** System componentry is augmented, upgraded, and replaced over time by methods and personnel that cannot be unequivocally trusted.

TRL Framework (Technology Readiness Level)

Level	Definition	DoD DAG Description
1	Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4	Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5	Technology validated in relevant environment	
6	Technology demonstrated in relevant environment	
7	System prototype demonstration in operational environment	
8	System complete and qualified	
9	Actual system proven in operational environment	

2020 FuSE System Security project focused on identifying concepts to start work on in 2021.

Foundation Concept – Criteria

Concept can provide new and useful value to the state of practice.

Concept has relevance to systems engineering considerations.

Concept value proposition can be articulated in SE terms.

Concept can be supported by notional examples.

Concept doesn't yet have sufficient published exposure for broad SE consideration.

Concept could (or might) be prototyped now.

Concept is principally about why and desired outcome (strategic intent), rather than what and how (prescriptive tactics), though examples of how lend credence.

Purpose of foundation concept papers is to inspire and instigate pursuit in the systems engineering security communities.

Development of concept papers is encouraged and open to anyone, individually or in collaboration.

TRL 1, 2, 3, 4

Eleven Concept Descriptions – One Per Page

Security Proficiency in the Systems Engineering Team

Table 1. Synopsis: Security Proficiency in the Systems Engineering Team

Problem	Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.
Need	System security and its evolution effectively enabled by systems engineering activity.
Intent	Integrate socially-sensitive system-level security expertise in the SE team; specify roles and responsibilities across the SE team.
Value	Security sensitive and knowledgeable systems engineering.
Metrics	Security engineering SE-level competencies present; evidence of effective competency application; evidence of accepted roles and responsibilities across the team.
Notions	(Gelosh 2014); (Nejib, Beyer & Yakabovicz 2017).

The professional side of the system adversary community is highly skilled, innovative, and relentless. Targeted systems cannot prevail with fixed defenses against a determined and intelligent attacker. This produces a need for an intelligent defense, one that is highly sensitive to adversarial actions, capable of rapid innovative countermeasures, and equally relentless. All of which is constrained or enabled by early systems engineering decisions that establish system requirements, architecture. and design strategy.

Vision 2025 sees system security as a "fundamental system attribute that systems engineers understand and incorporate into designs." Guidance in this direction can be found in (Nejib, Beyer & Yakabovicz 2017). Understand and incorporate is a minimal and necessary expectation that falls short of proficiency: "a high degree of competence or skill; expertise.[1]" Proficiency is unlikely to be found in systems engineers that haven't spent considerable career time developing breadth and depth in security.

This argues for installing system security engineering proficiency in the systems engineering (SE) team, with key competencies in system security architecture, strategy, and empathy. Security strategy is a process to analyze vulnerabilities and to select protection features that provide acceptable assurance levels to system stakeholders. Empathy is a social attribute that understands how and why to leverage security acceptance and appreciation by all stakeholders who interact with system security, and to balance usability and risk. One of the roles of security proficient personnel in the SE team is to elevate the understandings of others on the team and promote design and architecture strategies relative to security.

Concept development might explore means for finding and embedding appropriate proficiency in the SE team, the nature of SE team interaction and collaboration on security system engineering, or how appropriate proficiency might address each of the FuSE Security objectives and foundation concepts.

Descriptions focus on strategic intent, leaving ample room for various approaches.

The metrics row suggests general methods for measuring concept-employment success.

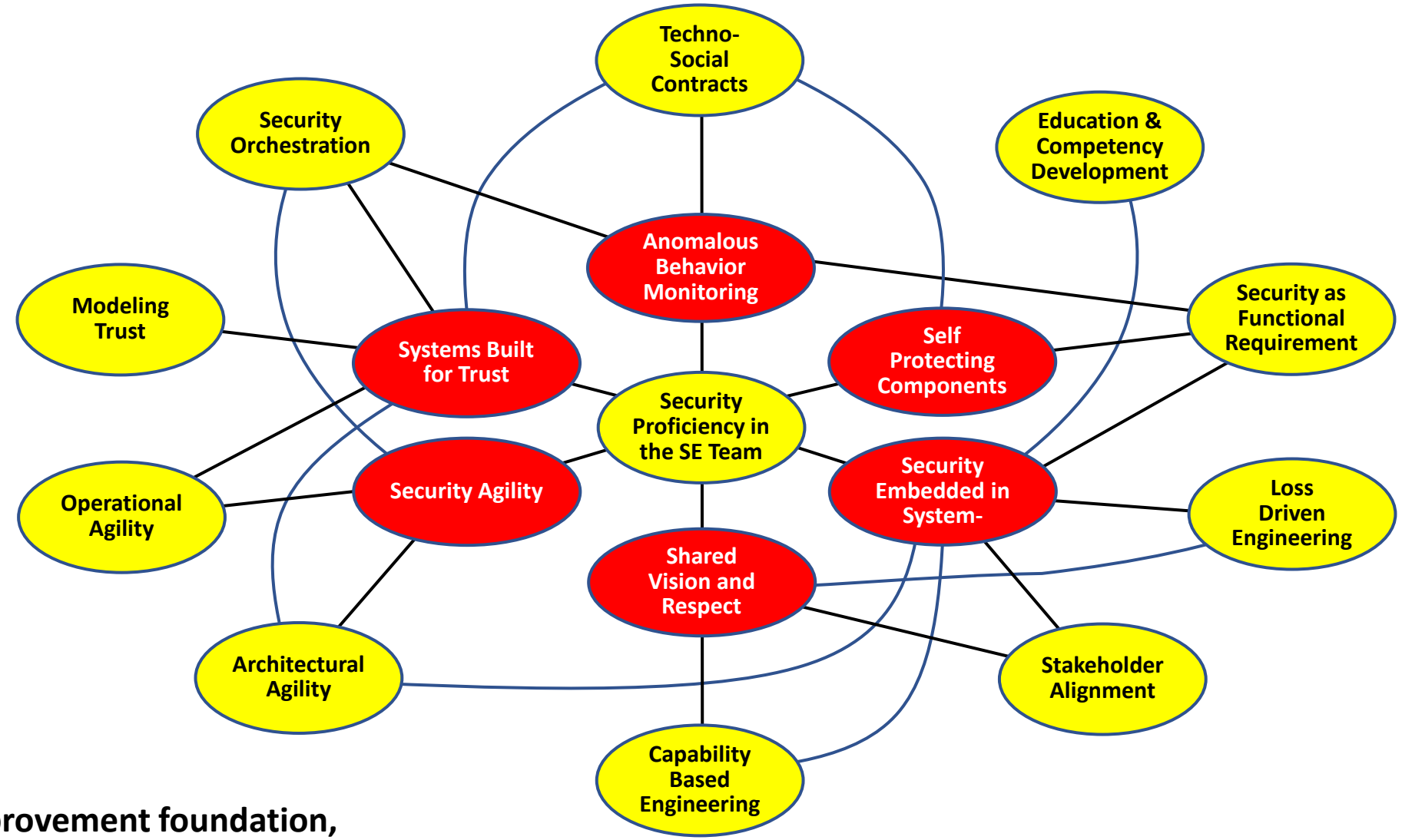
The notions row provides relevant ideas for inspiring thought without intending to constrain a solution path.

www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Concept Title	General Problem to Address	General Needs to Fill	General Barriers to Overcome
1. Security Proficiency in the SE Team	Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.	System security and its evolution effectively enabled by systems engineering activity.	Disrespect between SE and Sec people; perception of security as non-functional requirement; finding high level security expertise (architecture/strategy/empathy).
2. Education and Competency Development	Security education is not well integrated with engineering education, creating a skills gap.	Education at all levels focused on security of cyber-physical systems (CPS).	Perception of insufficient scientific/technical rigor for inclusion in engineering programs; engineering faculty security knowledge gap.
3. **Stakeholder Alignment**	Misalignment of security vision among stakeholders. Inconsistent appreciation for security among stakeholders.	Common security vision and knowledge among all stakeholders.	Stakeholder willingness to engage in collaborative convergence.
4. **Loss-Driven Engineering**	Traditional vulnerability assessments and risk/consequence models for security, safety, and related 'ilities occur too late in the SE process.	Standard metrics and abstractions relevant to all system lifecycle phases.	Cross domain vocabulary/taxonomy differences; insufficient respect for potential leverage; solution- rather than problem-dominant security thinking.
5. **Architectural Agility**	Enabling effective response to Innovative threats and attacks.	Readily composable and re-composable security with feature variants.	Comfort with and acceptance of a dynamic security profile.
6. **Operational Agility**	Timeliness of detection, response, and recovery.	Ability for cyber-relevant response to attack and potential threat; resilience in security system.	Comfort with and acceptance of a dynamic response and recovery capability.
7. **Capability-Based Security Engineering**	Security strategies based on available solutions rather than desired results.	Top-down approach to security starting with desired results/value.	Difference between capability and features; solution-dominant thinking; trust that the outcome will be satisfactory.
8. **Security as a Functional Requirement**	As a non-functional requirement, systems security does not get prime SE attention.	Systems engineering responsibility for the security of systems.	Cultural inertia that prioritizes system purpose over viability.
9. **Modeling Trust**	Systems Security has moved away from traditional focus on trust to a more singular focus on risk.	Reinvigorate formal modeling of system trust as a core aspect of system security engineering; address issues of scale with model-based tools and automation.	Entrenched risk-based practices and education; simplicity of communicating and comparing risk metrics; perception of security as a non-functional requirement.
10. Security Orchestration	Disparate security solutions operate independently with little to no coordination.	Tightly coupled coordinated system defense in cyber-relevant time.	Independent stovepipe solution tools; multiple disparate stakeholders; hesitation to explore interdependencies
11. Techno-Social Contracts	Insufficient detection capability for innovative attack methods [with dedicated purpose security components].	Augmented detection & mitigation of known and unknown attacks [with components collaborating for mutual protection].	Trust in the security of the approach; trust in the emergent result.

FuSE System Security

Synergy Linkage Between 11 Foundation Concepts and 6 Objectives



A near-term improvement foundation, not a comprehensive strategy web.

FuSE System Security Project – 2022+

Goals for 2022

1. Multi-organization collaboration is active.
2. All foundation concepts have publishable development
3. Foundation concept practice development is in early-stage process.

Action Plan 2022+

1. Late Jan: Review article drafts for June 2022 INSIGHT Magazine on all FuSE Security concepts.
2. Instigate & inspire foundation concept development.
3. Find and publish in-practice case examples.
4. Conduct 2-Hr. virtual workshops on individual concepts (Architectural Agility might be mid-Jan)
5. Plan transition of concepts to practice.
6. Evolve roadmap as appropriate.

If you are interested in active participation,
contact rick.dove@parshift.com

www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Closing the Systems to Silicon Gap: MBSE-Enabled Digital Electronics Verification

Lisa Murphy, Siemens Digital Industries Software
Mark Malinoski, Siemens EDA

NDIA Systems and Missions Engineering Conference
December 2021

Approved for Public Release

SIEMENS

Toward Trustworthy Microelectronics

A long journey, as yet not completed

NDIA’s first Trusted Microelectronics Workshop held in 2015

Siemens acquisition of Mentor Graphics in 2017 creates new opportunities

SIEMENS

We don’t have trustworthy electronics today

Hard to get electronics failure data for DoD, so look at autos

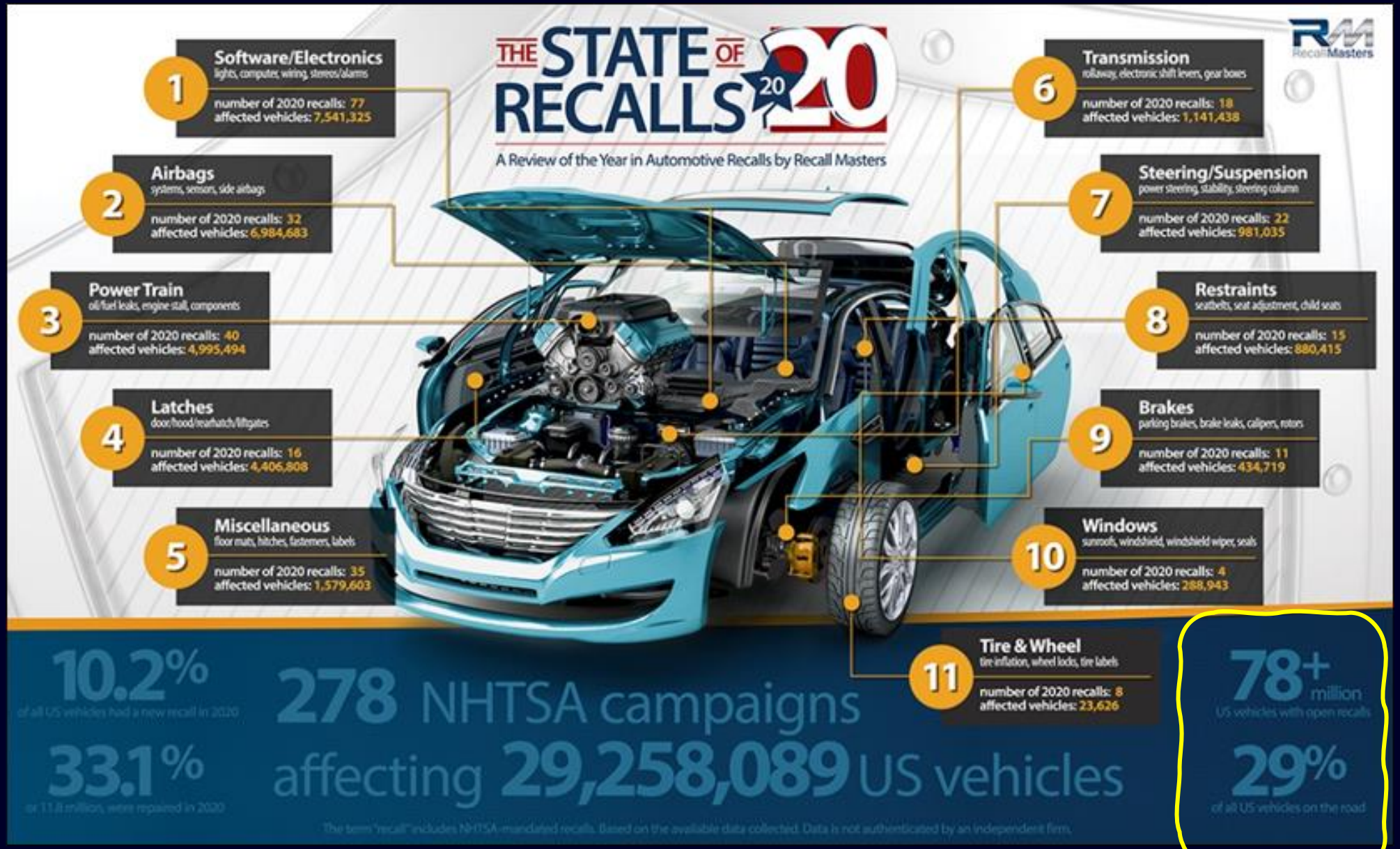
In 2020, there were **29 million** auto recalls per National Highway Traffic Safety Administration (about 2 vehicles recalled for each vehicle sold)

Almost 25% were faulty software or electronics, up from about 6% in 2016; **increasing frequency in integrated electronics**

At $500 average direct cost of about $36 BILLION

Many of you are aware of critical applications experiencing this problem in the defense space

[For comparison, both auto and military are around 3-4% of GDP]


THE STATE OF RECALLS 2020
A Review of the Year in Automotive Recalls by Recall Masters
RecallMasters
1 Software/Electronics
lights, computer, wiring, stereos/alarms
number of 2020 recalls: 77
affected vehicles: 7,541,325
2 Airbags
systems, sensors, side airbags
number of 2020 recalls: 32
affected vehicles: 6,984,683
3 Power Train
oil/fuel leaks, engine stall, components
number of 2020 recalls: 40
affected vehicles: 4,995,494
4 Latches
door/hood/rearhatch/liftgates
number of 2020 recalls: 16
affected vehicles: 4,406,808
5 Miscellaneous
floor mats, hitches, fasteners, labels
number of 2020 recalls: 35
affected vehicles: 1,579,603
6 Transmission
rollaway, electronic shift levers, gear boxes
number of 2020 recalls: 18
affected vehicles: 1,141,438
7 Steering/Suspension
power steering, stability, steering column
number of 2020 recalls: 22
affected vehicles: 981,035
8 Restraints
seatbelts, seat adjustment, child seats
number of 2020 recalls: 15
affected vehicles: 880,415
9 Brakes
parking brakes, brake leaks, calipers, rotors
number of 2020 recalls: 11
affected vehicles: 434,719
10 Windows
sunroofs, windshield, windshield wiper, seals
number of 2020 recalls: 4
affected vehicles: 288,943
11 Tire & Wheel
tire inflation, wheel locks, tire labels
number of 2020 recalls: 8
affected vehicles: 23,626
10.2%
of all US vehicles had a new recall in 2020
278 NHTSA campaigns
33.1%
affecting 29,258,089 US vehicles
78+ million
US vehicles with open recalls
29%
of all US vehicles on the road

SIEMENS

Challenges to achieving high levels of assurance for microelectronics

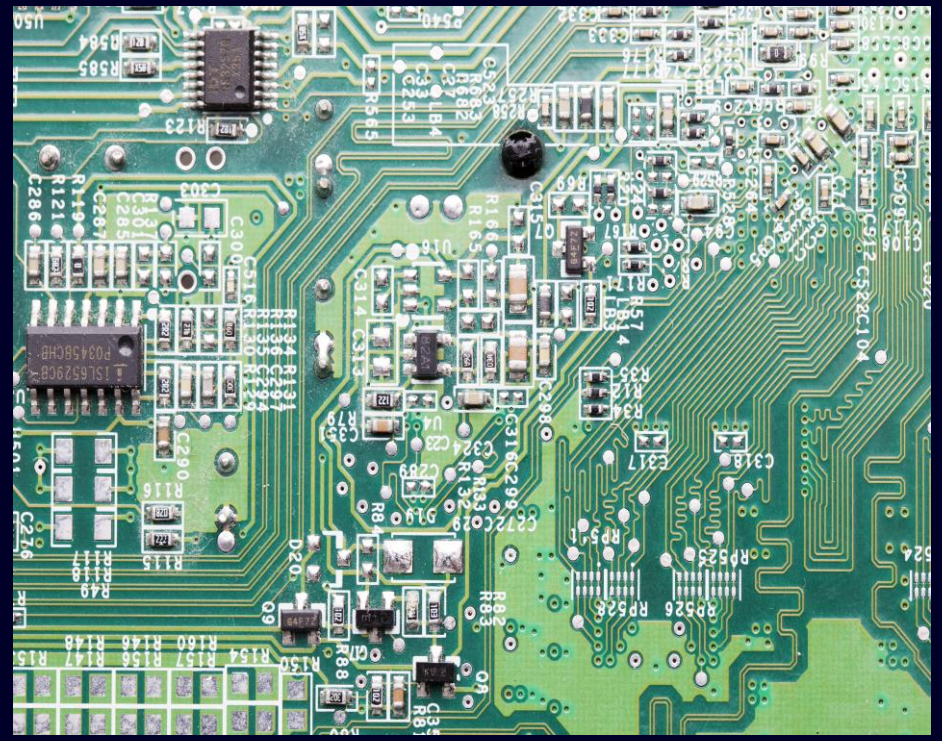
Electronics continue to evolve to produce higher performance in smaller and smaller packages

Not uncommon for a System on a Chip (called SoC or ASIC) to have 10 billion gates

The electronics industry has pioneered use of highly abstract models to drive automated verification (before any silicon is laid down)

But there's a gap that keeps that intense verification work from being sufficient to achieve high levels of assurance we desire and need – there is no direct linkage between requirements and design verification

So, what would help?



Microelectronics cannot (yet) be trusted

Reliance on sophisticated custom-build electronics in critical applications

Unintentional performance issues increasingly likely

Let’s shift focus to the left and close the loop with requirements

Not quite to the “easy button” stage but making progress

Let us share our journey starting with a little background

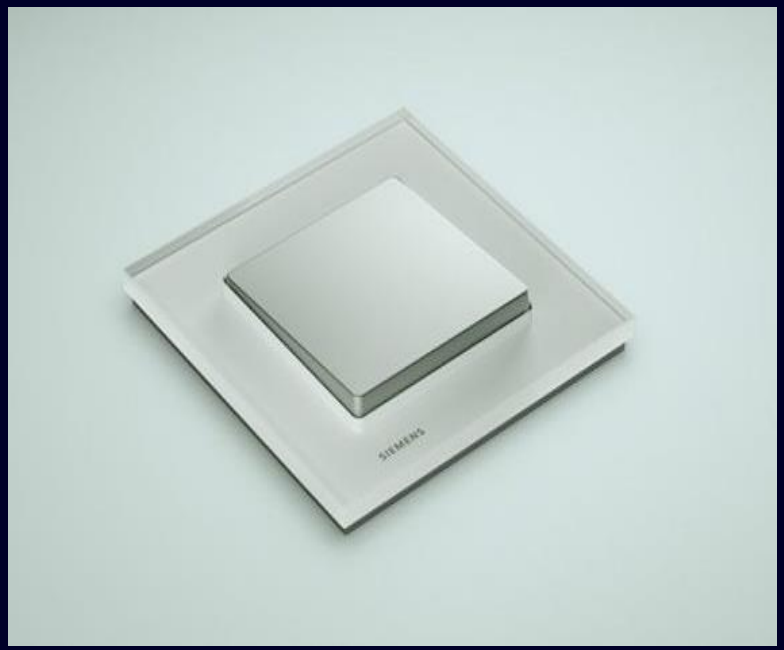
Siemens is now one of the top ten software companies in the world

We’ve been involved in product design and systems engineering for quite a while, including standards efforts

Today, initiatives are underway at Siemens to

- Deliver next-generation MBSE that is SysML V2 compliant*
- Connect electronics verification to systems engineering via MBSE
- Enable a major step forward for trustworthy microelectronics

We call this “Closing the Systems to Silicon Gap”



* *Called Systems Modeling Workbench with Arcadia/Capella*

SE Vision: Connected Engineering of Systems Across the Lifecycle

REQUIRED BEHAVIORAL STRUCTURAL AS DESIGNED AS ORDERED AS BUILT AS DELIVERED AS SERVICED

Systems Engineering

- Begins at the conceptual design phase, continuing throughout the life cycle
- Defines and validates requirements to meet user needs
- Designs, analyzes and verifies a system to meet the requirements

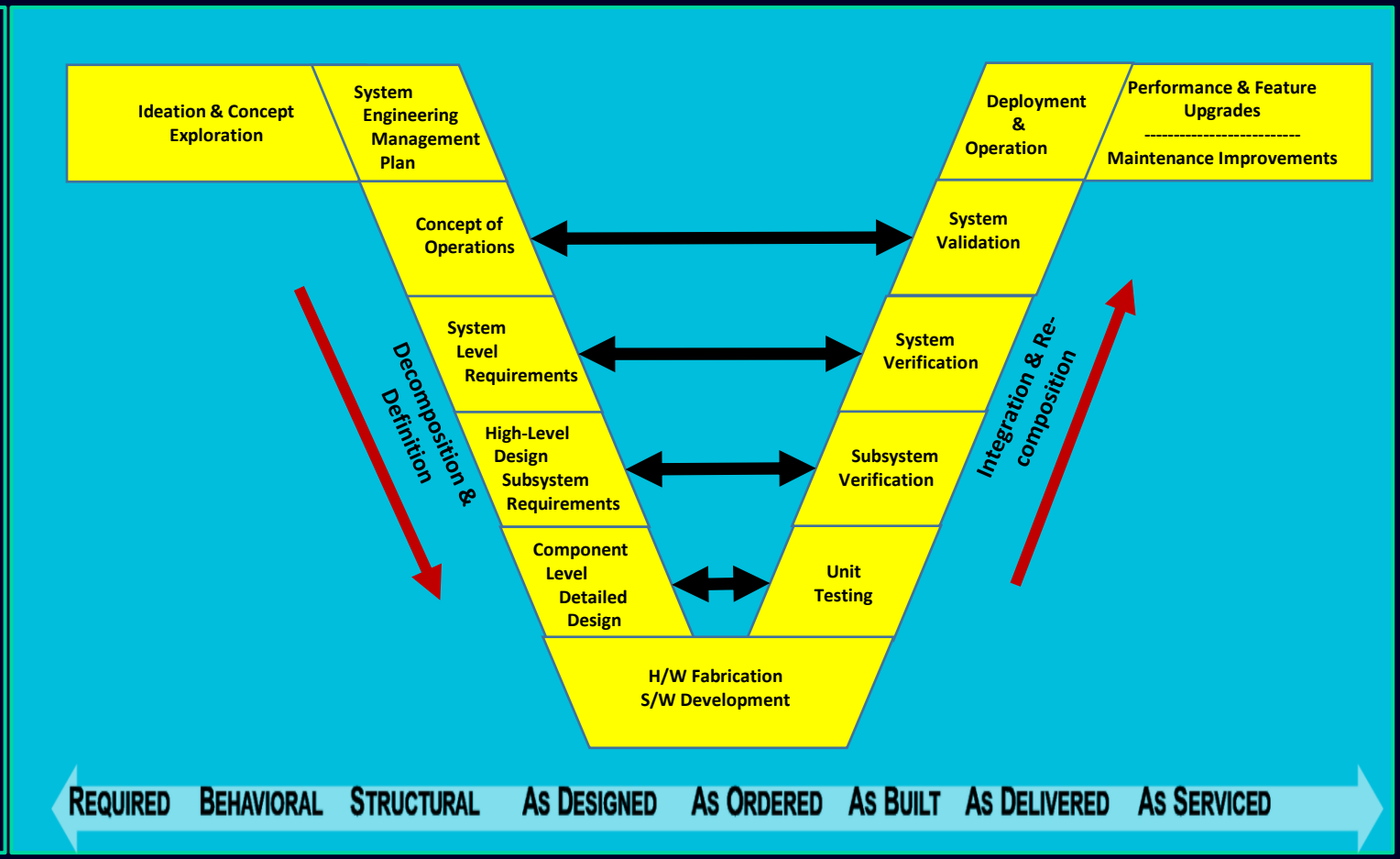
Before there was CAD/CAE, there was Systems Engineering. Many types of SE documents and diagrams were produced, maintained and shared manually.

If MBSE is to be CAD/CAE for SE, are we there yet?

SIEMENS

Engineering “V” – Emphasis on Continuous Verification Levels

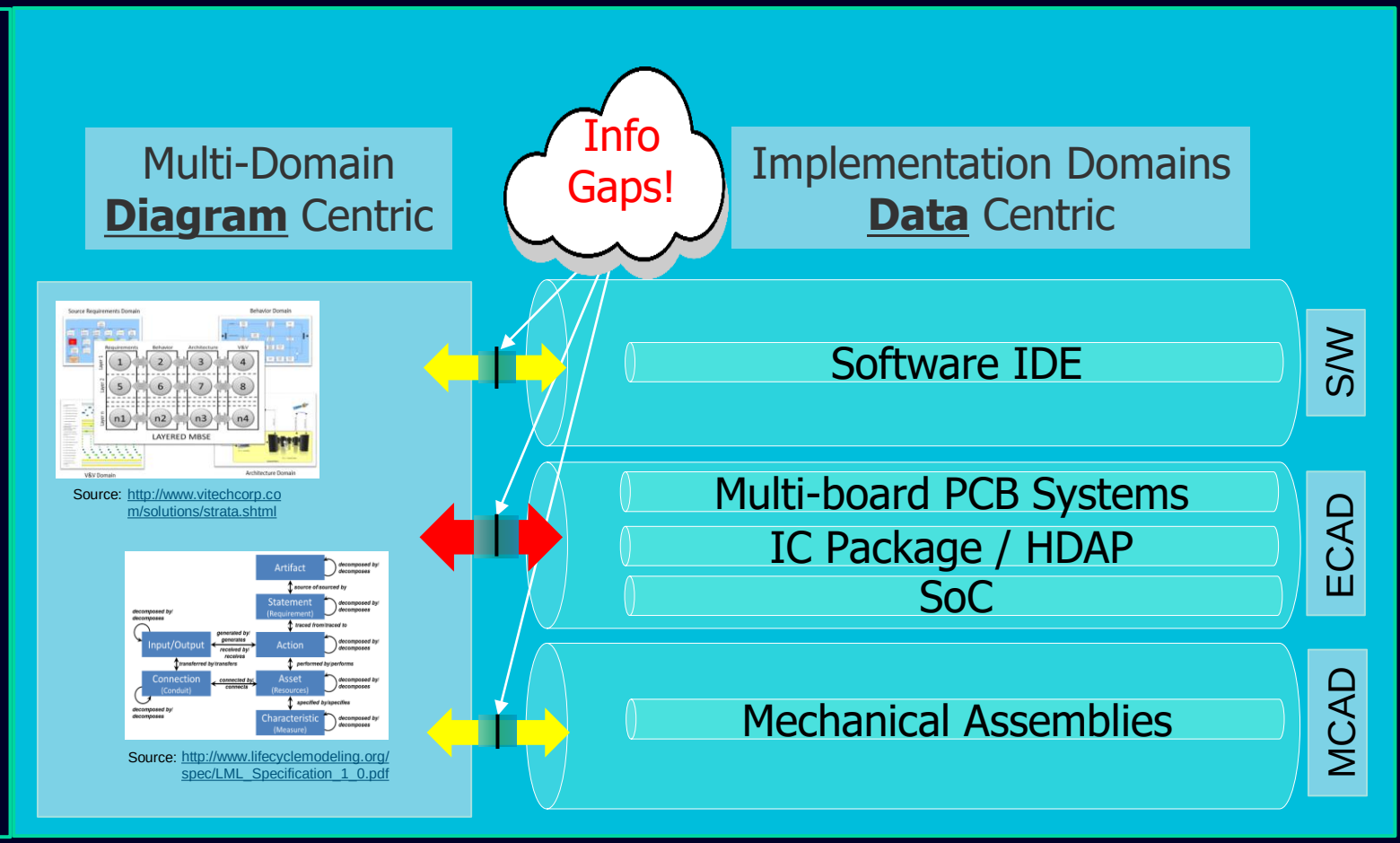
- Verification requires feedback loops in the life cycle timeline
- The engineering “V” diagram emphasizes verification feedback and detail layers
- Requirement verification plans MUST be continuously refined and then performed EARLY
- SE work-products must share architecture info to express requirements to be verified



SIEMENS

Current Electronics Status: MBSE-driven Architecture is NOT SHAREABLE

- Most SE diagrams are not intuitive, and Domain engineers are not fluent in them
- Most diagrams are not stored as data elements in enterprise level database repositories
- Gaps exist which restrict the flow of information and the ECAD gap is the most severe
- ECAD has sub-domain decomposition layers and the deepest verification challenge

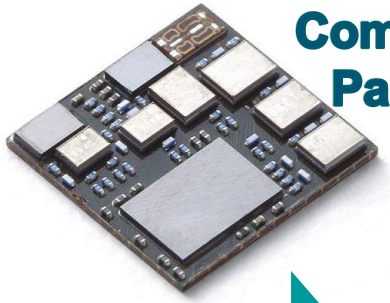


SIEMENS

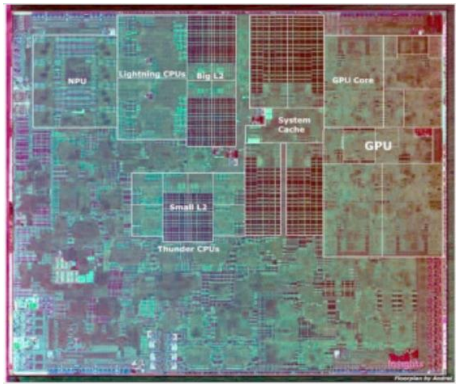
Electronics Requires Continuous Decomposition and Verification to Realize "System-to-Silicon" Verification

Multi-PCB System Enclosure

Printed Circuit Board



Component Package



SoC / ASIC

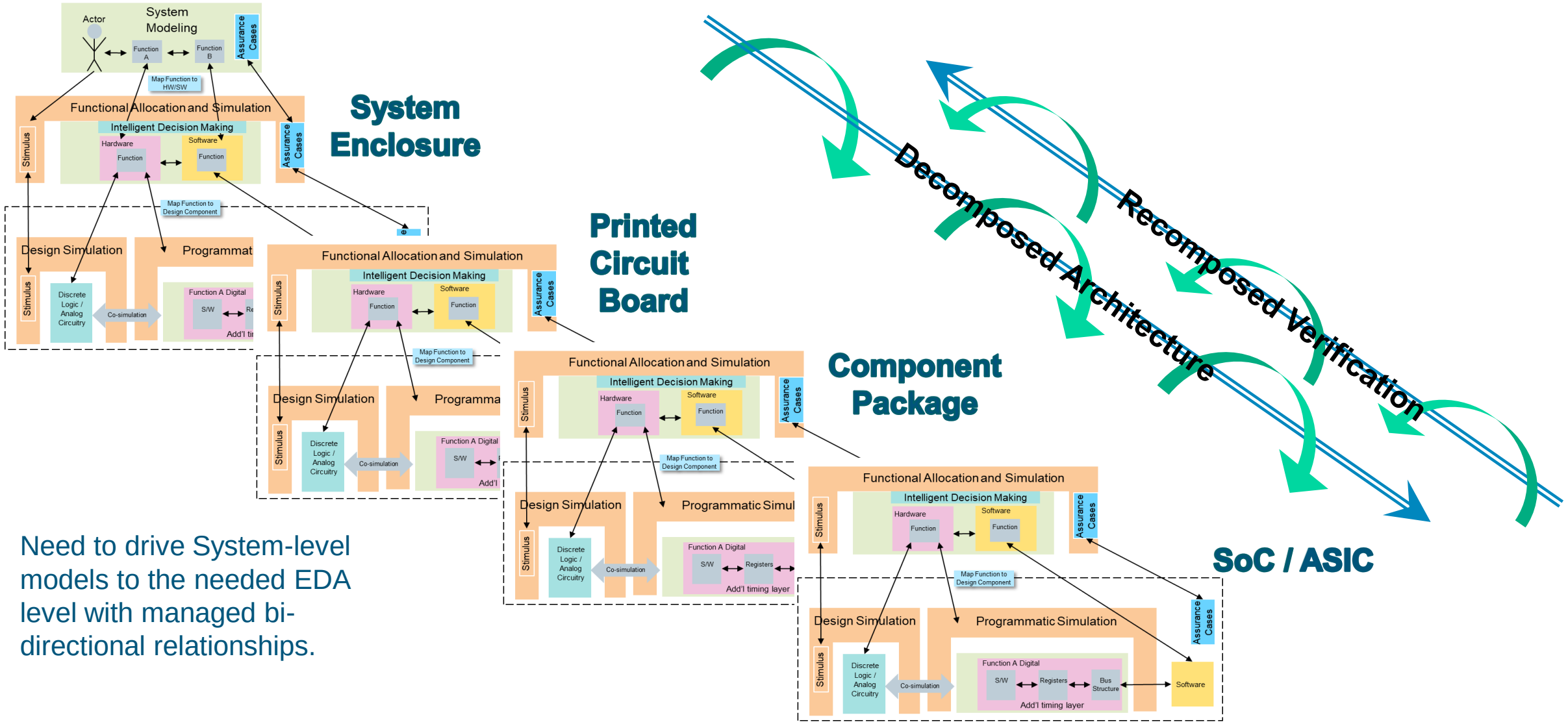
Decomposed Architecture

Recomposed Verification

The epicenter of the complexity explosion: SoCs executing embedded software

SIEMENS

Future State: Commonality Across Workflows, System-to-Silicon

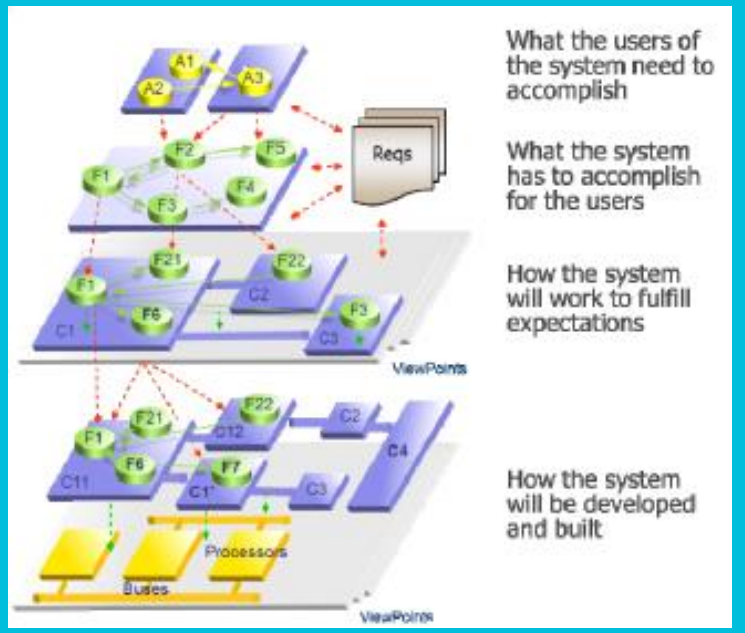


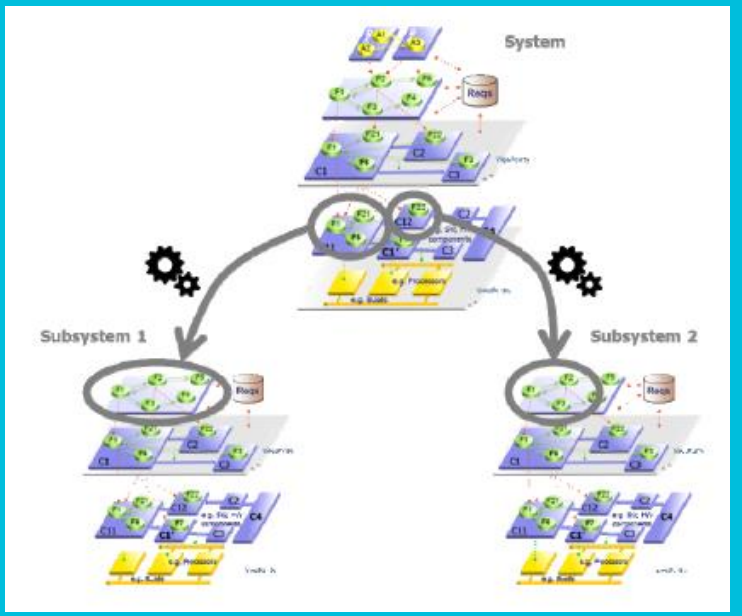
Need to drive System-level models to the needed EDA level with managed bi-directional relationships.

SIEMENS

ARCADIA/Capella Uniquely Addresses Continuous Decomposition

- Focused on Arcadia/Capella as the capability set for continuous decomposition
- Most modern method and tooling with most advanced refinement capabilities
- CAD/CAE style of underlying data model
- Guides the user to assure models are complete and consistent
- Advanced model management via SMW link to Teamcenter

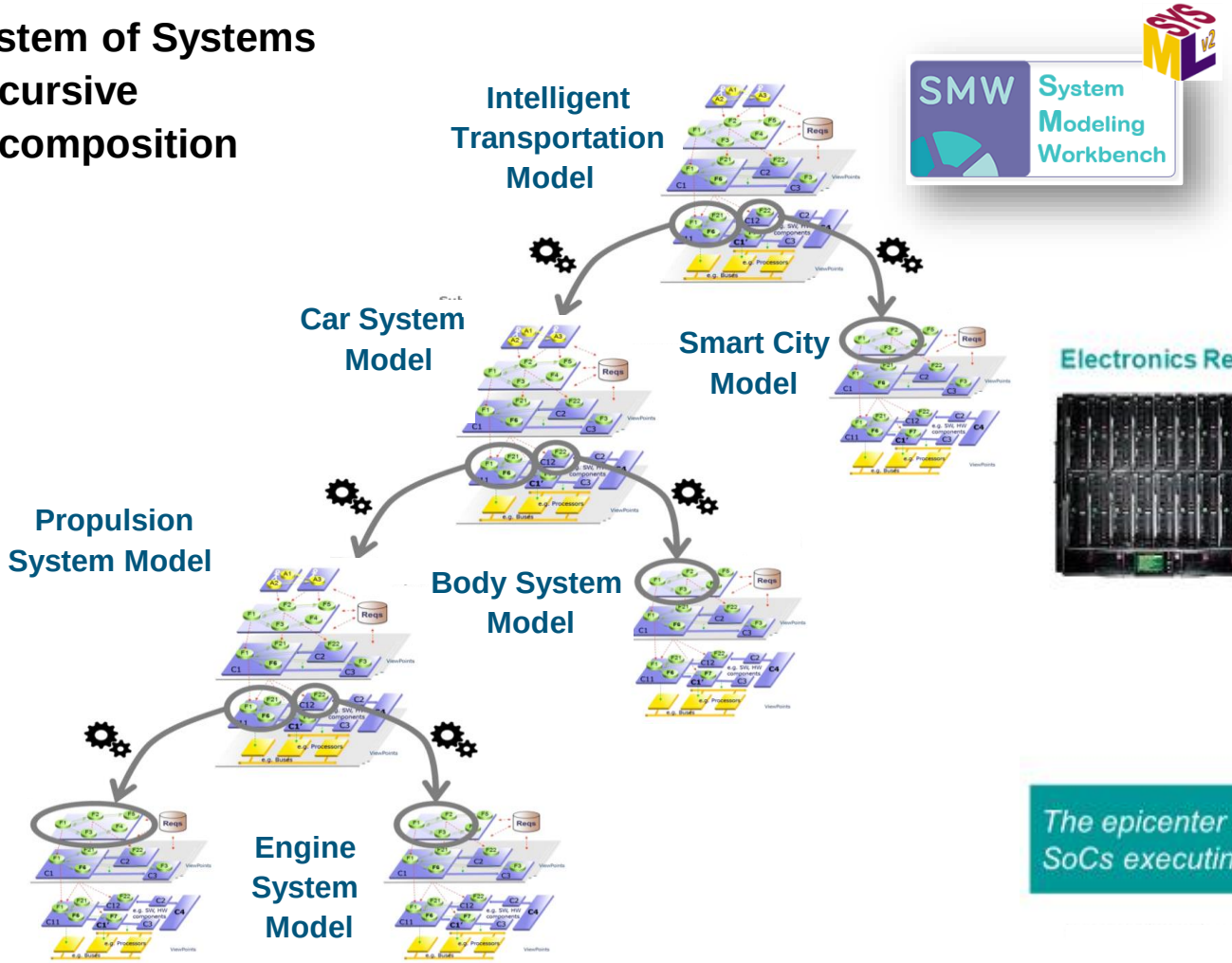




SIEMENS

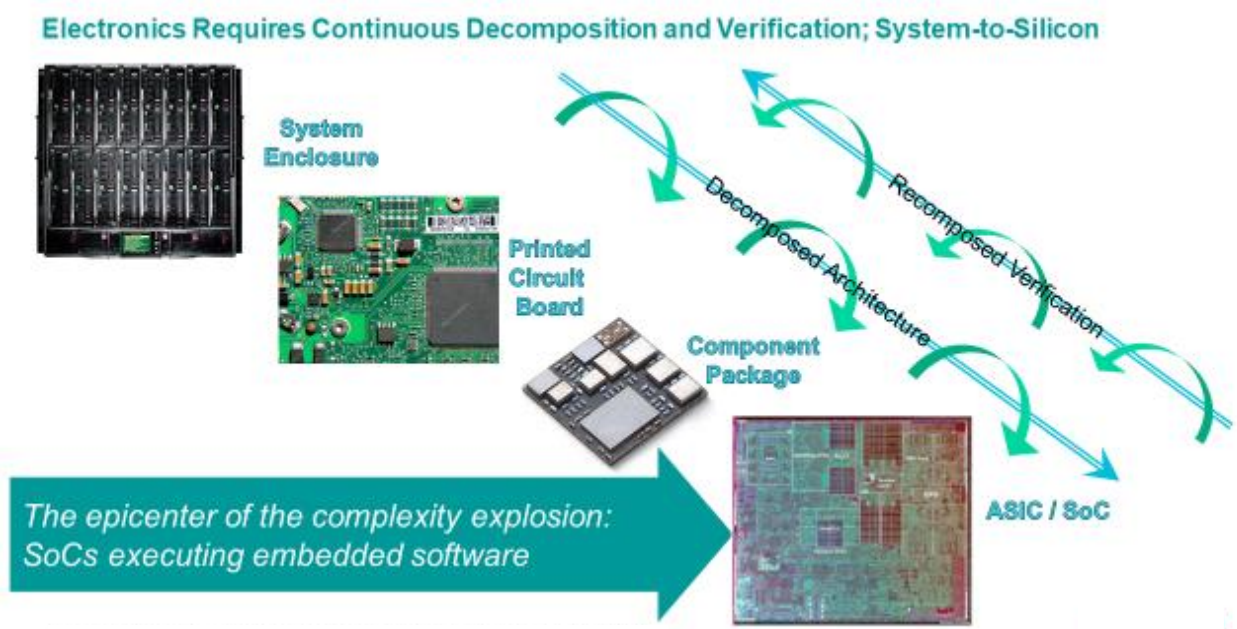
System-to-Silicon Engineering is Now Realizable

System of Systems Recursive Decomposition



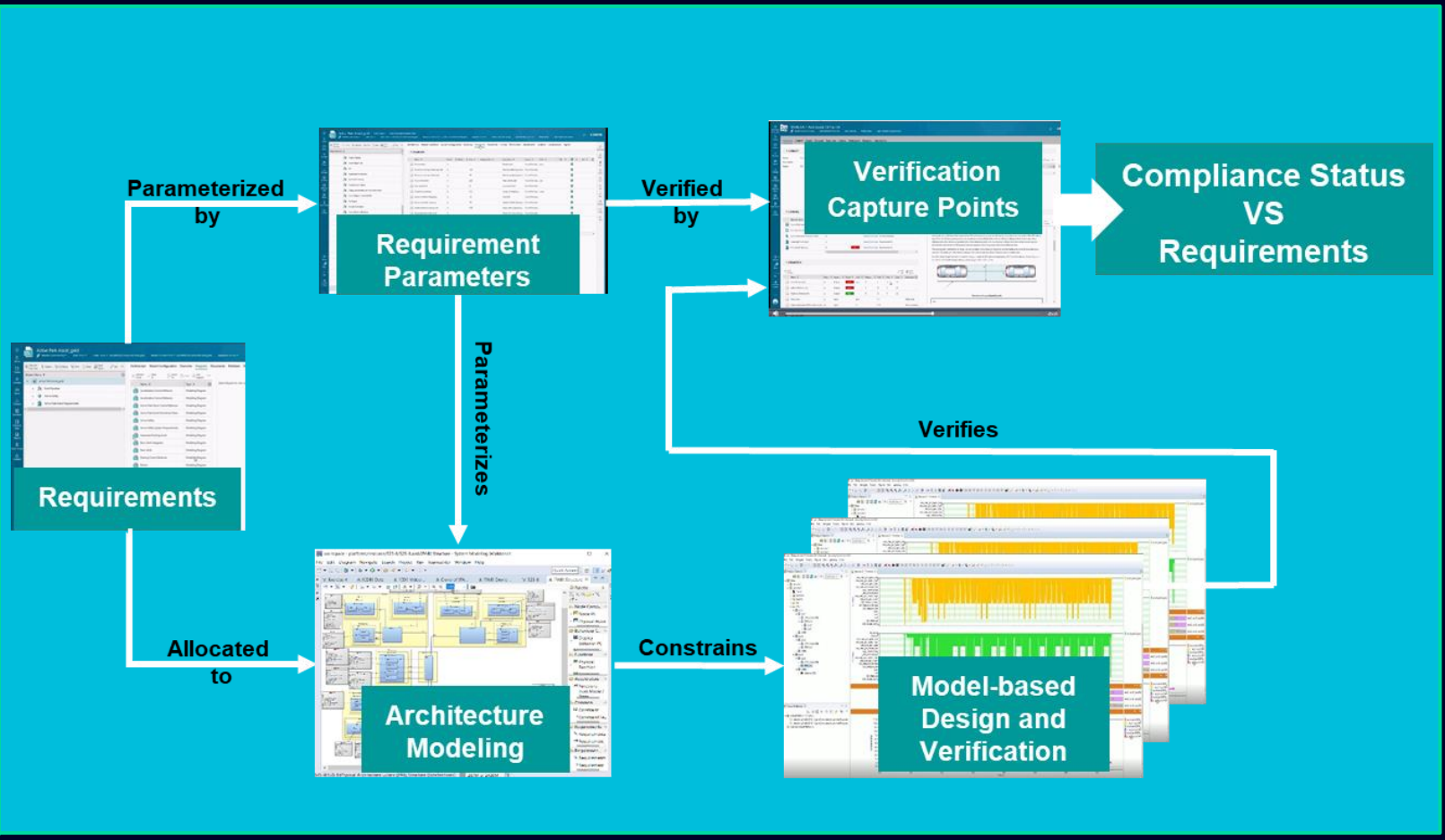
SMW System Modeling Workbench

The decomposition models and their relationships need to be tracked and managed, preferably in one Authoritative Source of Truth.



Proposed: A Solution Pattern for Electronics Verification in an MBSE Context

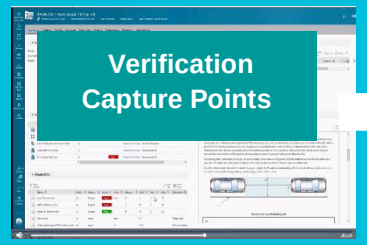
- Requirements are maintained, parameterized, allocated & verified in an ASoT manner
- Design simulation results are compared to parameter values and completes the VCP
- Verification conformance & compliance can be assessed based on total VCP status
- Design/implementation team owns requirement verifiability and refinement



SIEMENS

Verification Capture Points: “Do the Math”

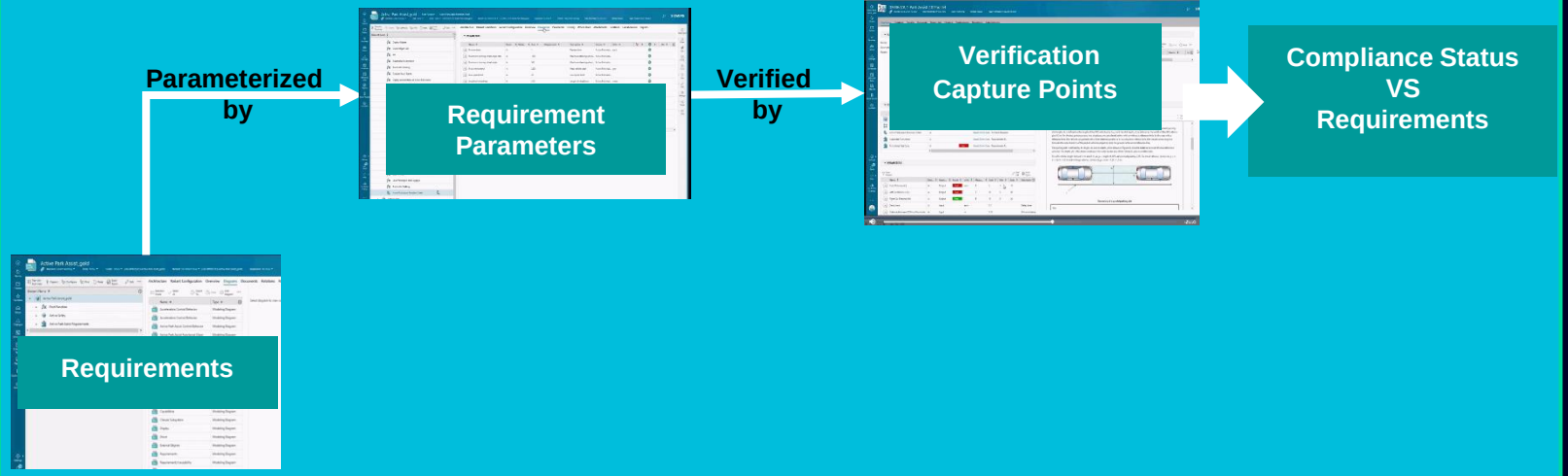
- We must digitalize verification with VCPs
- Implicit requirements currently outweigh explicit parameterized requirements
- Domain specific knowhow will determine what to verify and how to verify it
- Best known methods must be reviewable for escapes and organizational learning



Compliance Status VS Requirements

Requirements must be parameterized

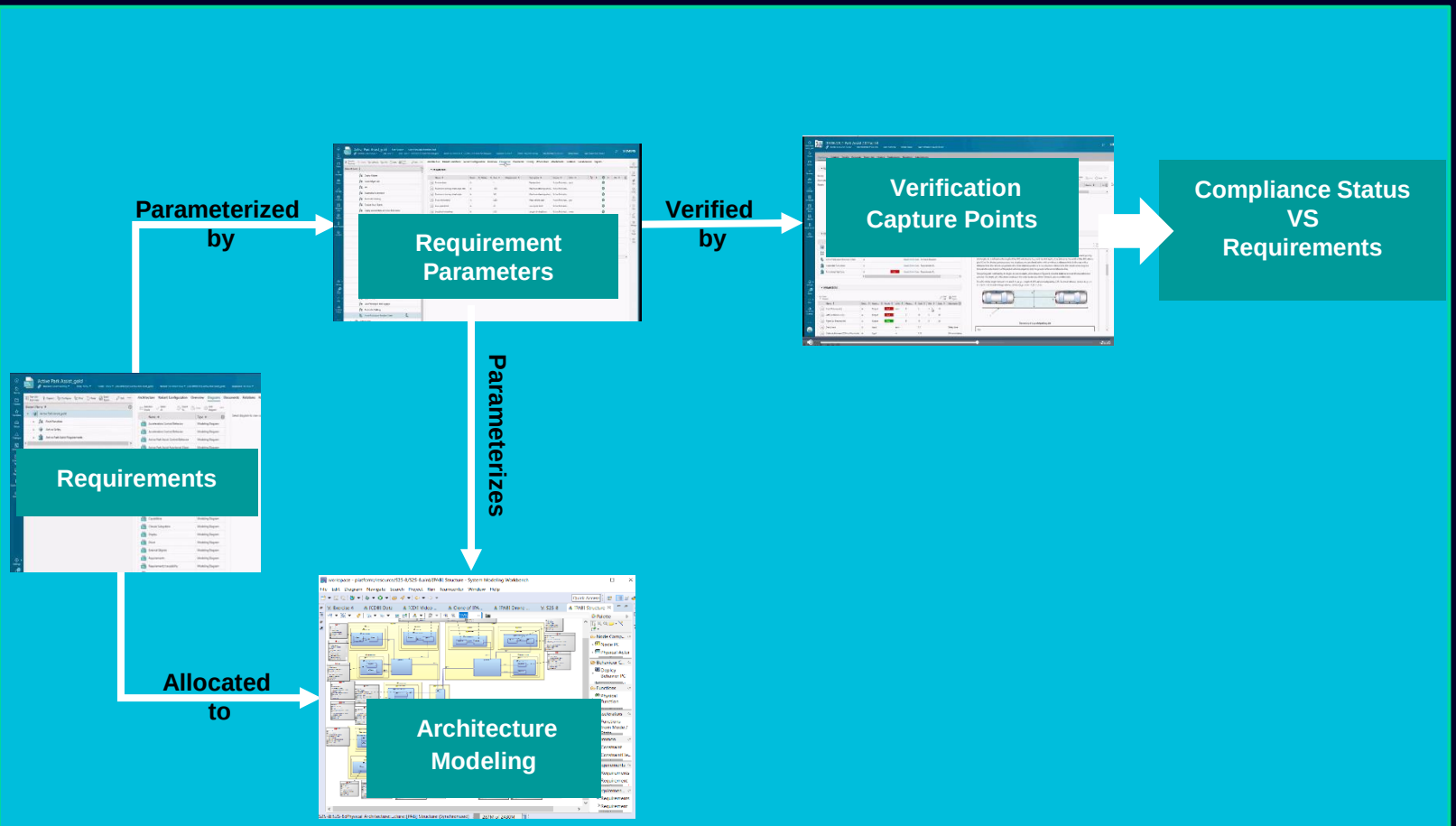
- A shall statement is not enough
- More progress is needed to parameterize and manage parameters
- The VCP math must be automatable
- Domain SMEs must own requirements decomposition



SIEMENS

Requirements Must Parameterize Architecture Models

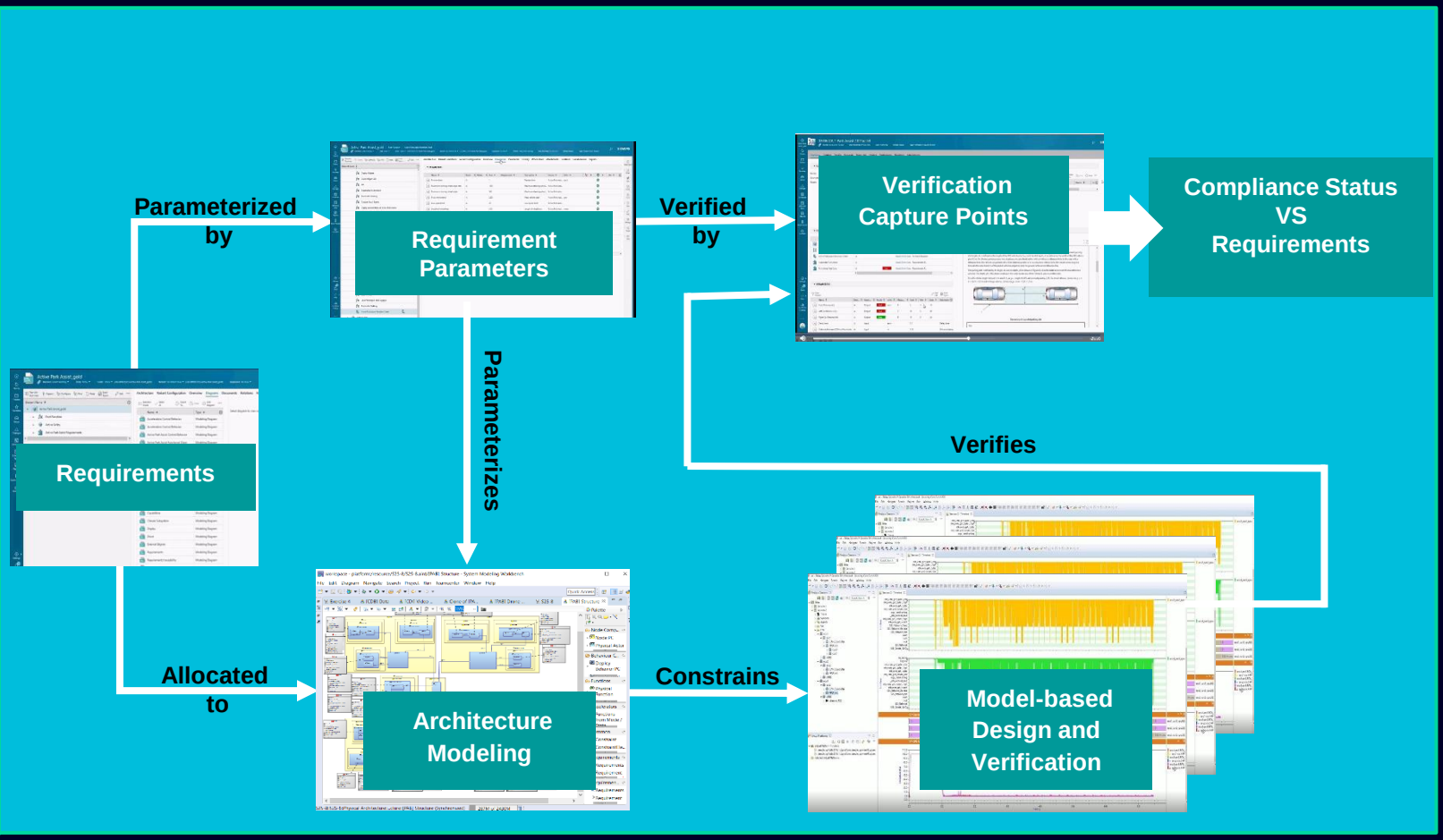
- Architecture must decompose from functions based on operational scenarios
- Requirement parameters must be allocated to architecture elements
- Enable the development and exploration of architecture options
- Domain SMEs must own architecture decomposition and refinement



SIEMENS

Closing the Info Gap

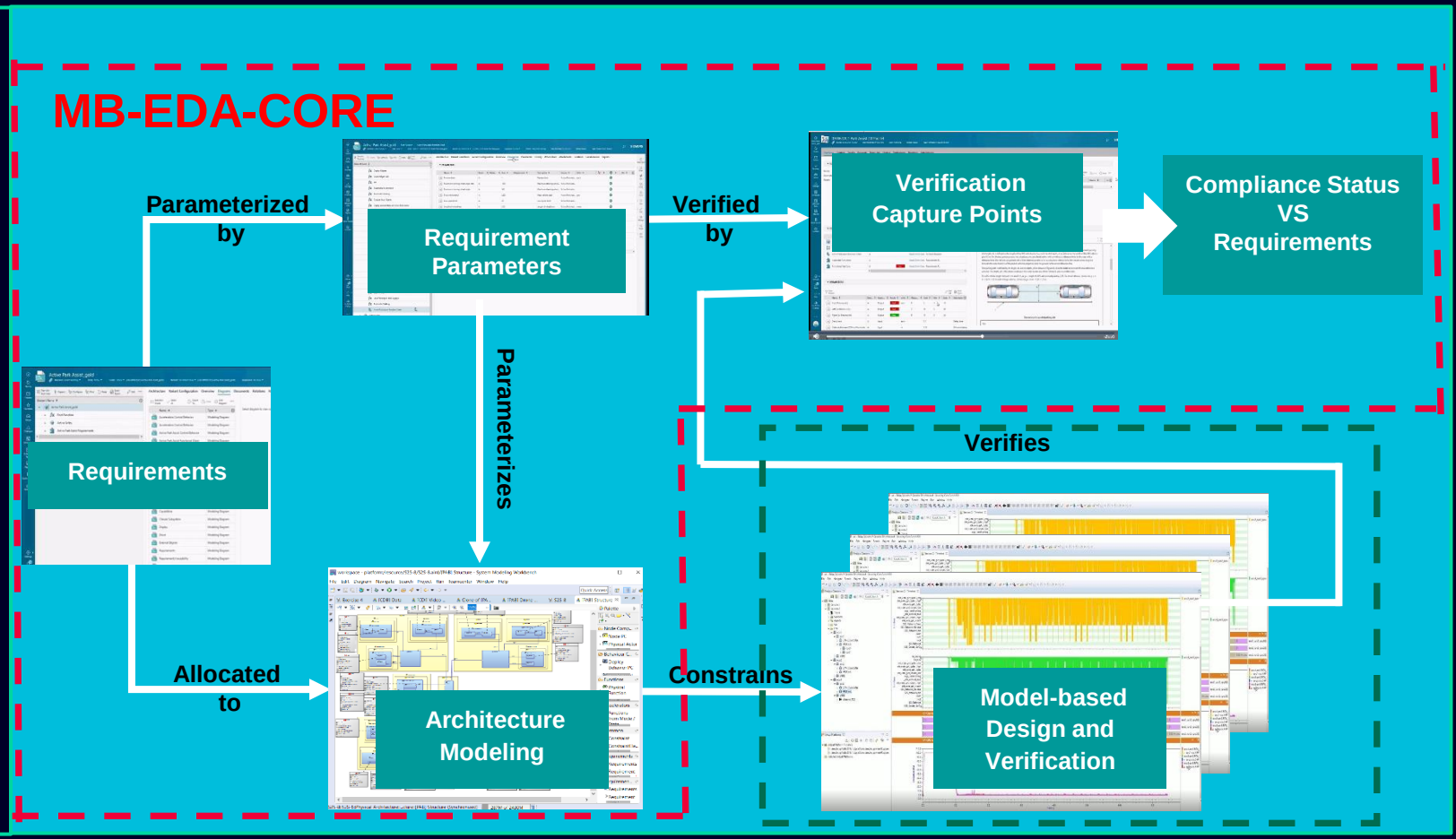
- One architecture can drive multiple sub-domains
- Enables simulation-based architecture optimization
- Architecture compliance to requirements is captured in the VCP
- Optimized architecture constrains and specifies design and implementation



SIEMENS

A Solution Pattern Implementation Consists of both Domain Independent (ASoT) and Domain/Sub-domain Dependent Workflow Components and Tools

- Enabling the ASoT can be domain independent and non-ECAD specific
- Domain specific tools can potentially be any design and verification toolset
- Domain specific tools will likely need automation to increase efficiency / reduce cycle time
- Bottom-up approach: Implement VCPs for what is simulated today



SIEMENS

Path to Standards Conformance:
ISO 24641 for Systems Engineering Methodology and Tools

Tooled Method to: Define, Analyze, Design & Verify System, SW, HW Architectures

Operational Analysis

System Analysis

Logical Architecture

Physical Architecture

Define Stakeholder Needs and Environment

Capture and consolidate operational needs from stakeholders
Define what the users of the system have to accomplish
Identify entities, actors, roles, activities, concepts

Formalize System Requirements

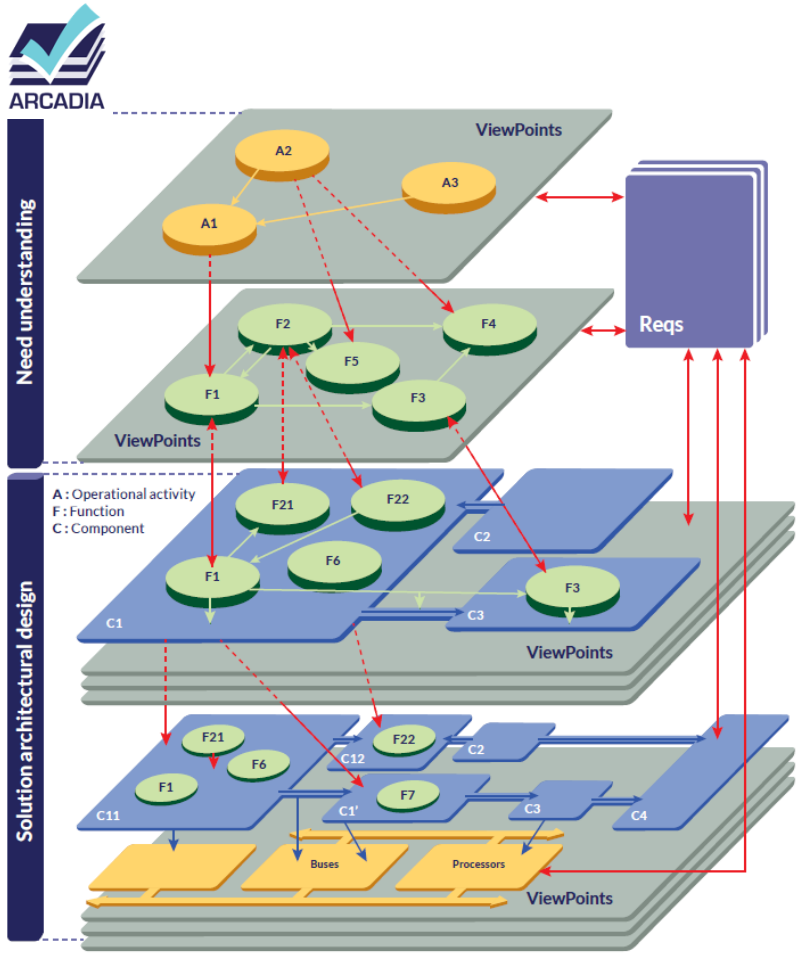
Identify the boundary of the system, consolidate requirements
Define what the system has to accomplish for the users
Model functional dataflows and dynamic behaviour

Develop System Logical Architecture

See the system as a white box: define how the system will work so as to fulfill expectations
Perform a first trade-off analysis

Develop System Physical Architecture

How the system will be developed and built
Software vs. hardware allocation, specification of interfaces, deployment configurations, trade-off analysis



Operational Analysis
What the users of the system need to accomplish

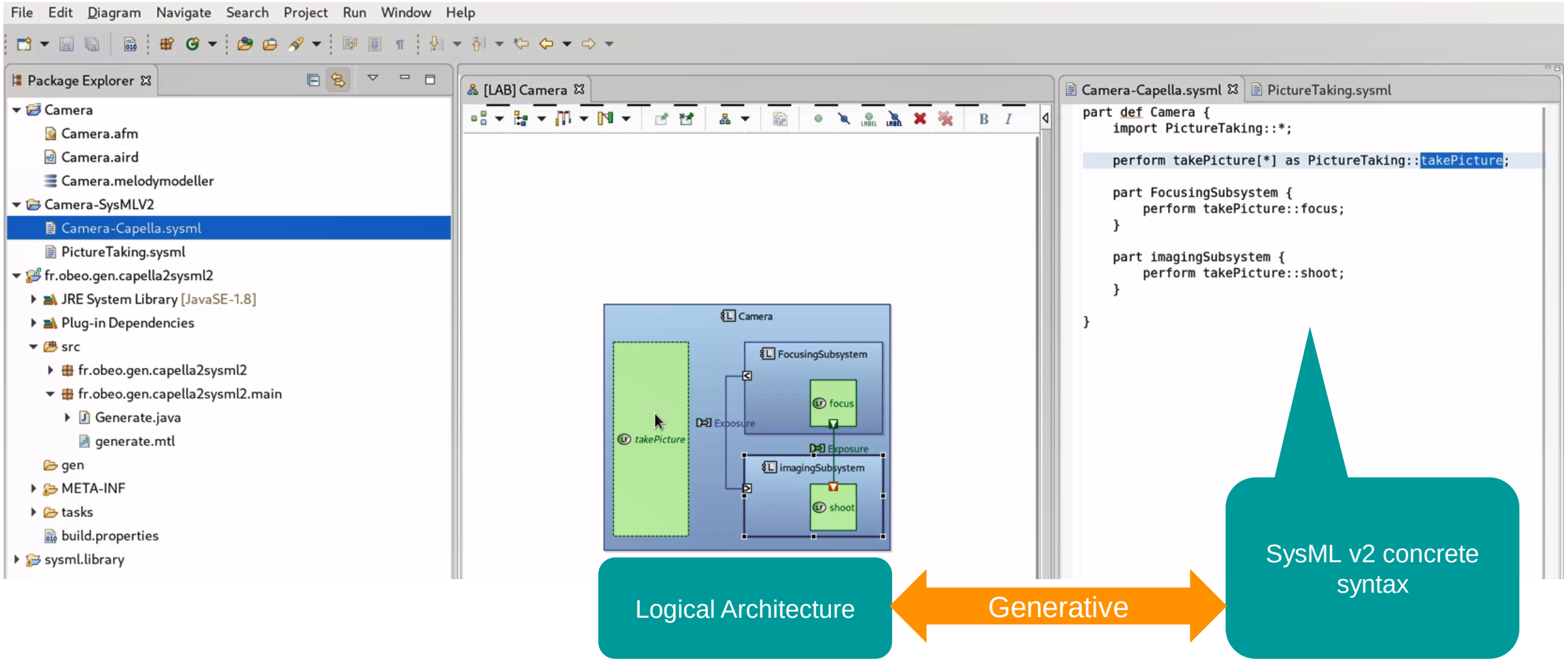
Functional & Non Functional Need
What the system has to accomplish for the users

Logical Architecture
How the system will work to fulfill expectations

Physical Architecture
How the system will be developed and built

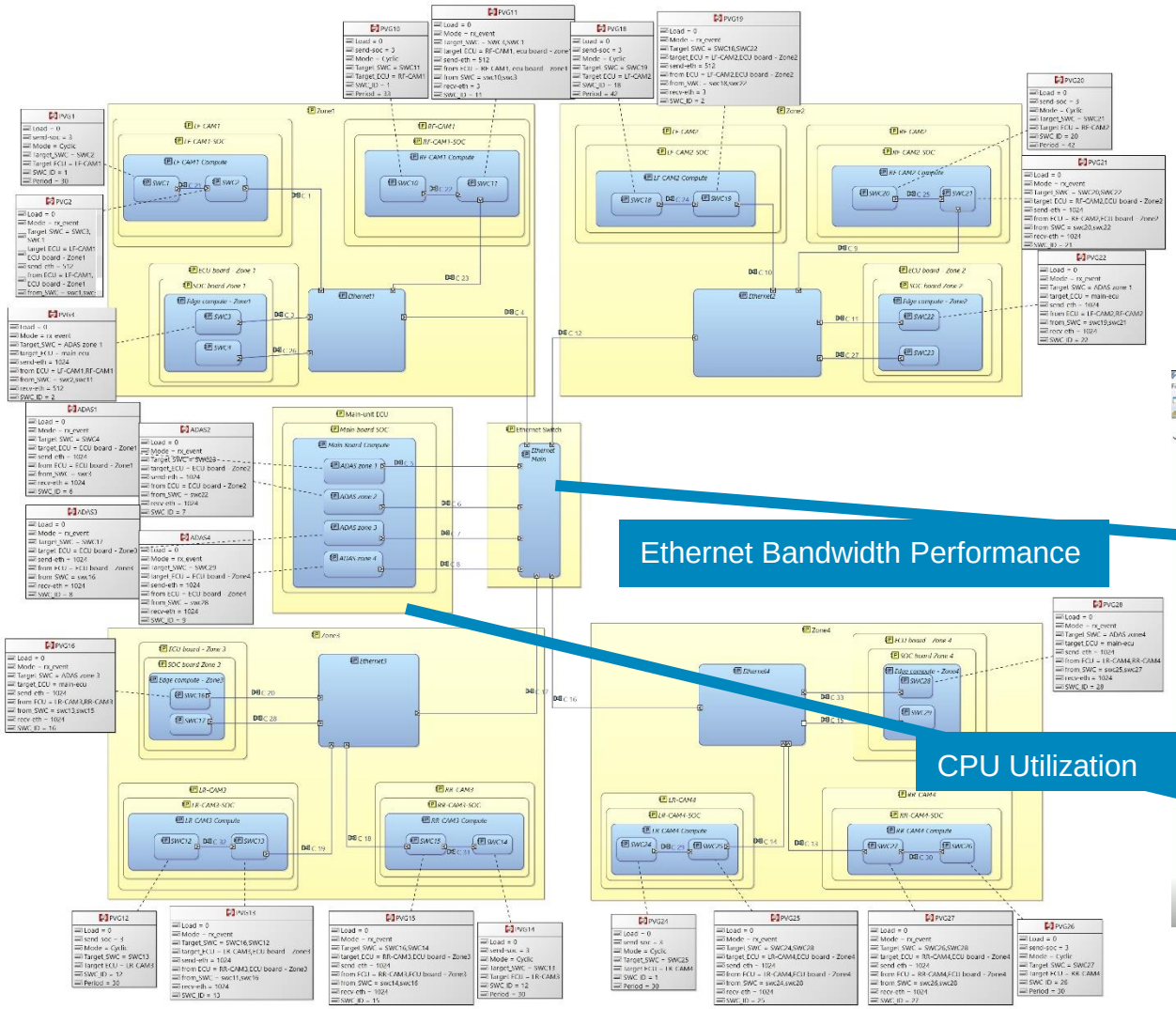
SIEMENS

Path to Standards Conformance:
Working toward Capella Generative SysML V2 Concrete Syntax



SIEMENS

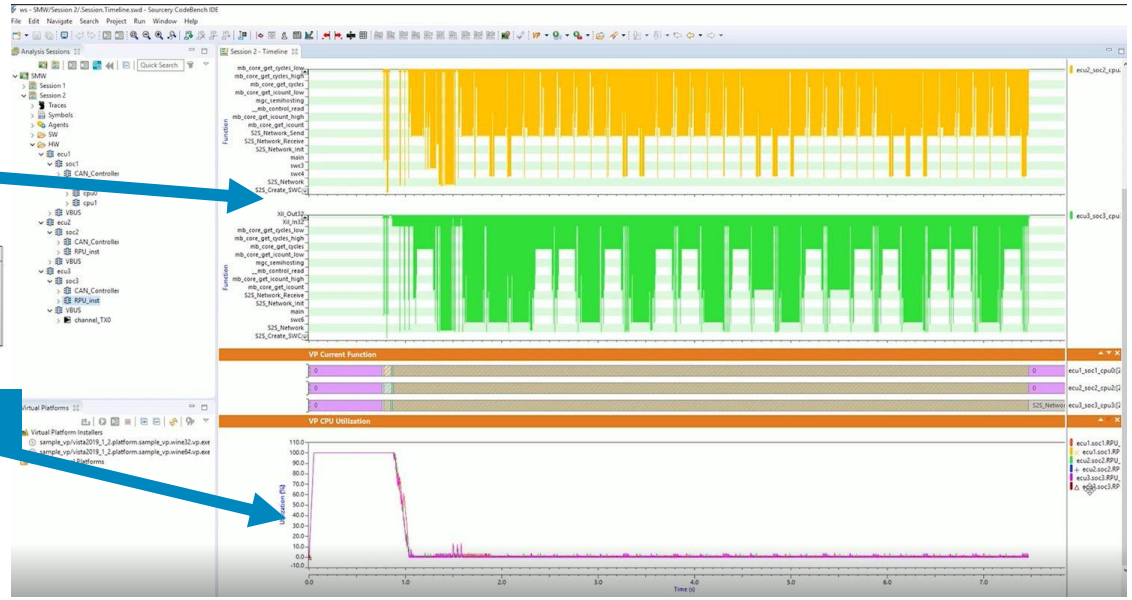
Architecture Exploration by Transaction Level Simulation: System-to-Silicon



Ethernet Bandwidth Performance

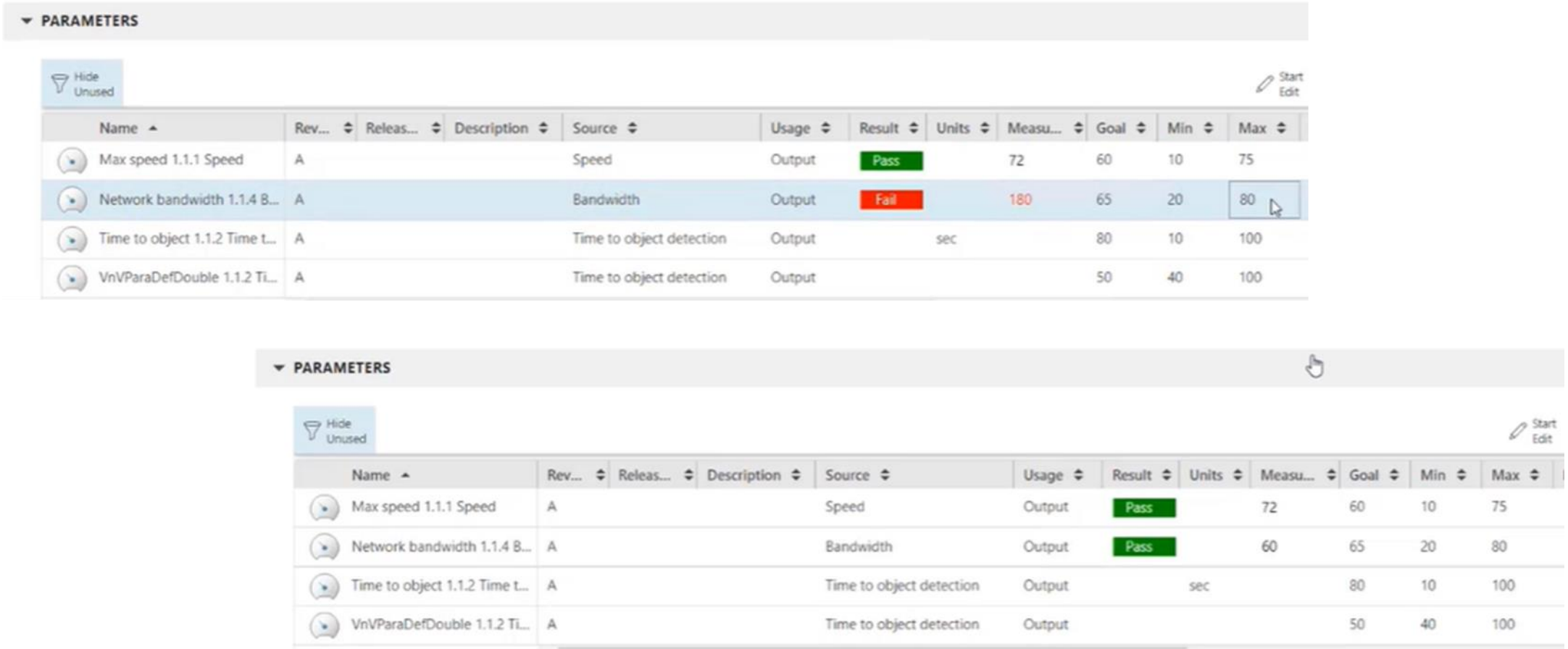
CPU Utilization

Dynamic Transaction Analysis



SIEMENS

Verification Capture Point Example



PARAMETERS

Hide Unused

Start Edit

Name	Rev...	Releas...	Description	Source	Usage	Result	Units	Measu...	Goal	Min	Max
Max speed 1.1.1 Speed	A			Speed	Output	Pass		72	60	10	75
Network bandwidth 1.1.4 B...	A			Bandwidth	Output	Fail		180	65	20	80
Time to object 1.1.2 Time t...	A			Time to object detection	Output		sec		80	10	100
VnVParaDefDouble 1.1.2 Ti...	A			Time to object detection	Output				50	40	100

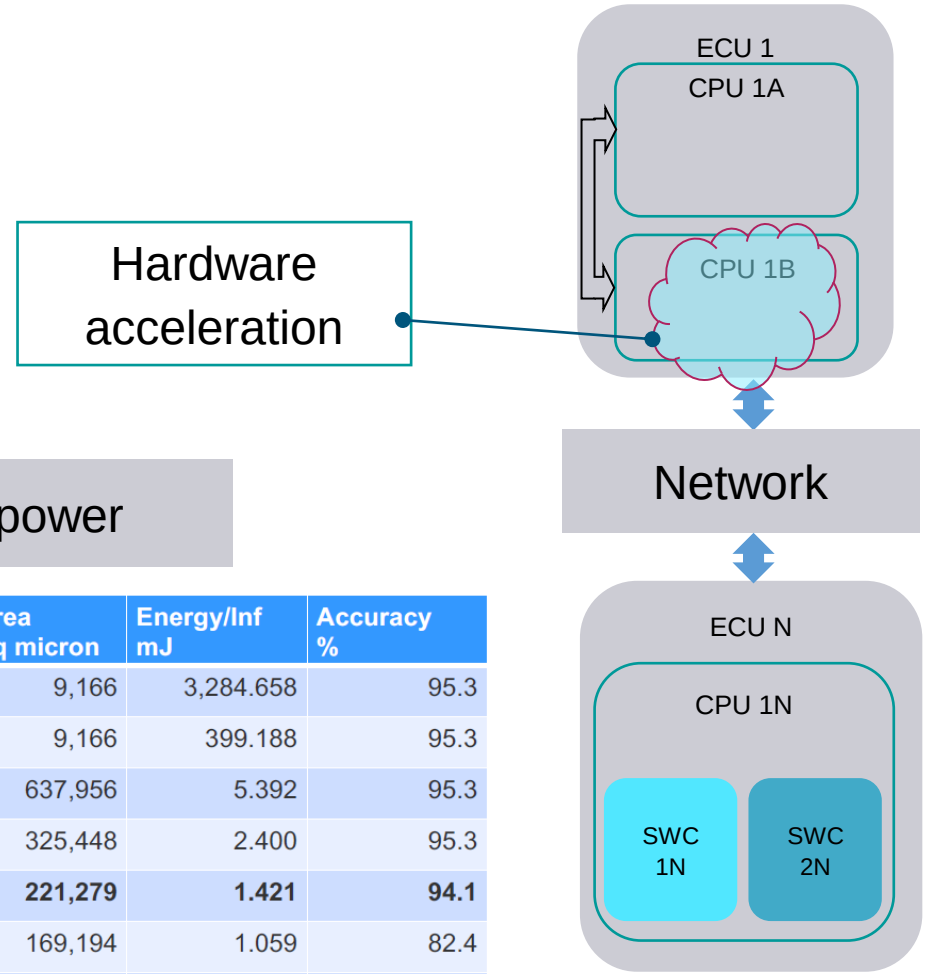
PARAMETERS

Hide Unused

Start Edit

Name	Rev...	Releas...	Description	Source	Usage	Result	Units	Measu...	Goal	Min	Max
Max speed 1.1.1 Speed	A			Speed	Output	Pass		72	60	10	75
Network bandwidth 1.1.4 B...	A			Bandwidth	Output	Pass		60	65	20	80
Time to object 1.1.2 Time t...	A			Time to object detection	Output		sec		80	10	100
VnVParaDefDouble 1.1.2 Ti...	A			Time to object detection	Output				50	40	100

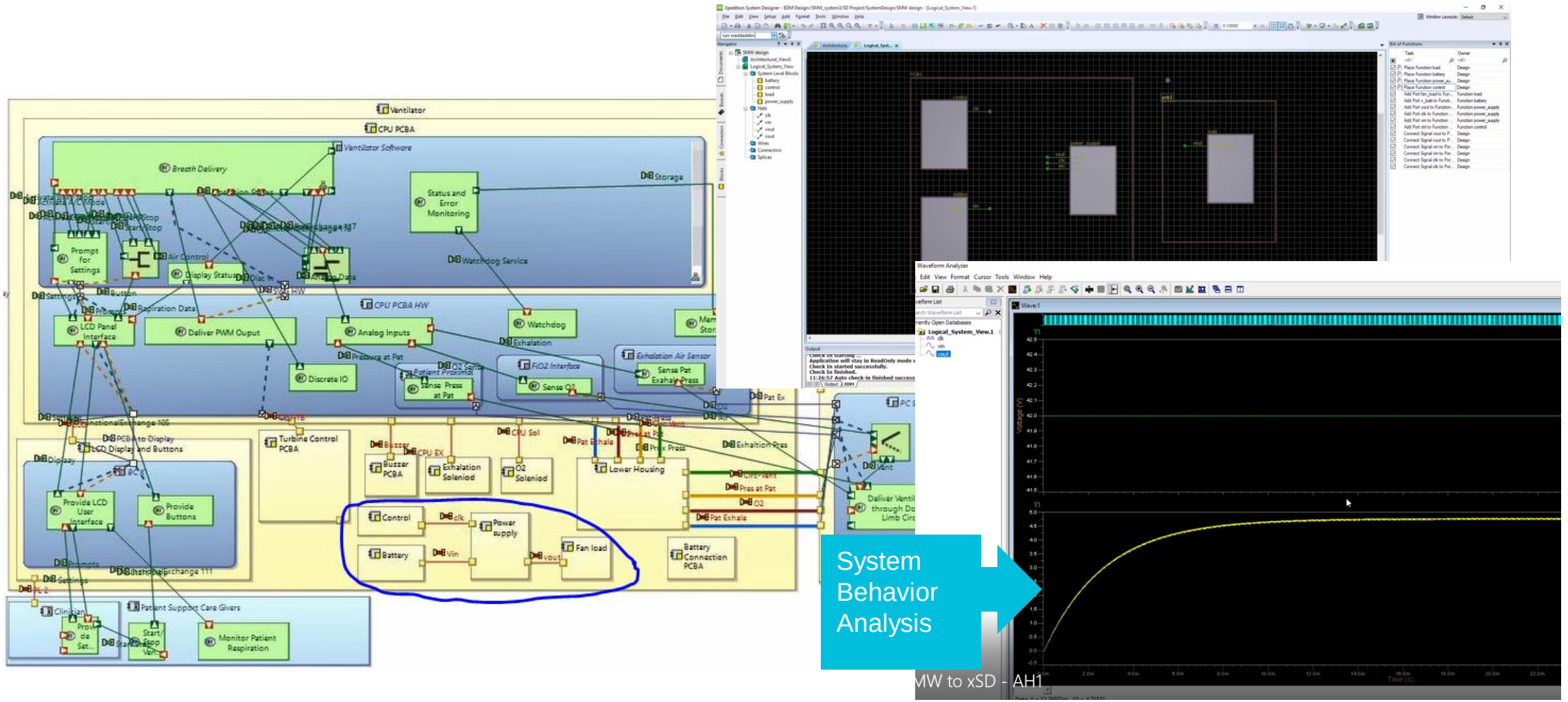
Architecture can be Refined using H/W Acceleration Synthesis



KPI analysis for speed/power

Configuration	Speed seconds	Power mW	Area Sq micron	Energy/Inf mJ	Accuracy %
Software Float	4,961.719	0.662	9,166	3,284.658	95.3
Software Fixed	616.031	0.648	9,166	399.188	95.3
Par1	2.003	2.692	637,956	5.392	95.3
Par2	1.001	2.398	325,448	2.400	95.3
Par3	**0.667**	**2.131**	**221,279**	**1.421**	**94.1**
Par4	0.536	1.975	169,194	1.059	82.4
Par5	0.416	1.776	137,994	0.739	44.8

Architecture Implementation: Interoperable PCB Flow

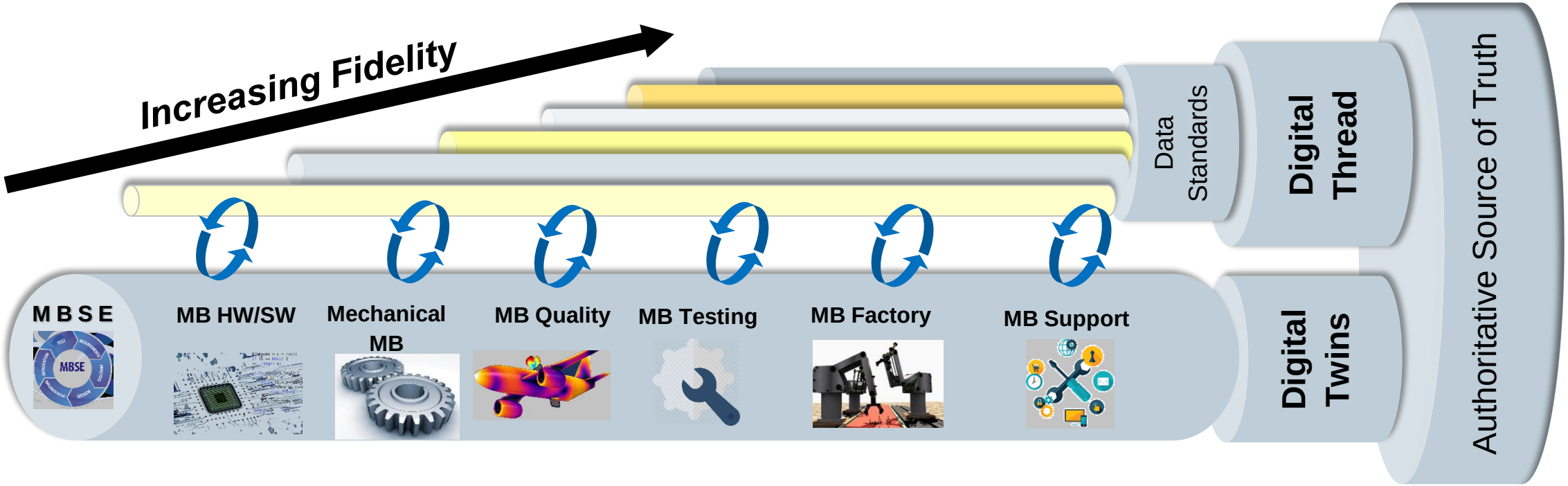


SIEMENS

Digital Transformation is Enabled by Digital Twinning and Threading

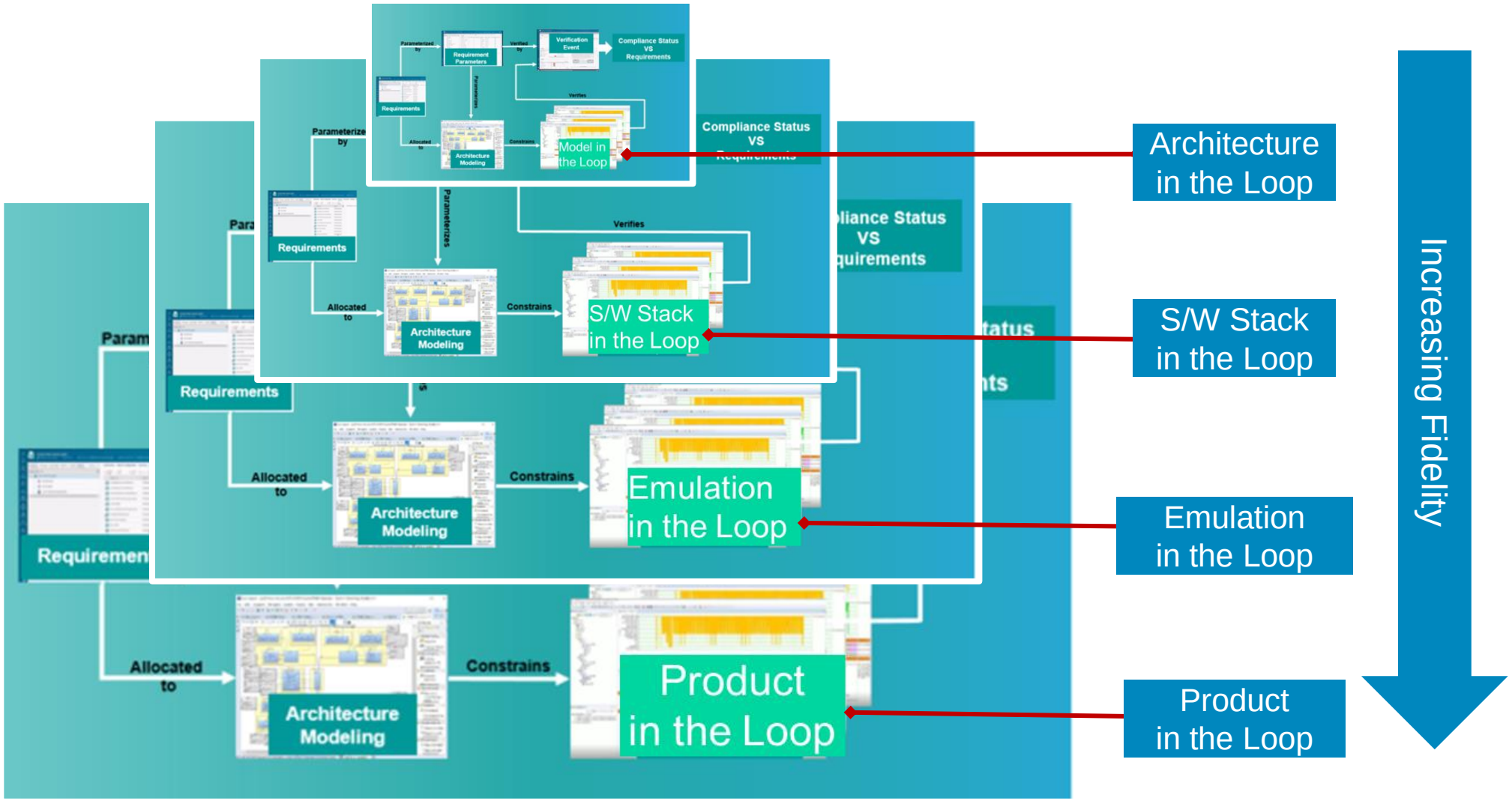
Digital Thread: The authoritative technical data providing decision makers the right data at the right time across the system life cycle

Digital Twin: An integrated digital simulation, enabled by digital threading



SIEMENS

Hybridizing the Digital Twin



SIEMENS

Closing the System to Silicon Gap for Trustworthy Electronics

Siemens is delivering MBSE-Enabled Digital Electronics Verification

We offer a solution pattern for electronics verification in an MBSE context

Initial pilot project results are encouraging; progress made in challenging areas

Additional projects being pursued to industrialize solution

SIEMENS

Contacts

Lisa Murphy
Technology Consultant
Siemens Digital Industries Software
Aerospace, Defense, Federal & Marine
Atlanta, Georgia
USA

Phone (770) 548-5225

E-mail lisa.murphy@siemens.com

Mark Malinoski
Technology Consultant
Siemens EDA
MBSE Solutions Director
Kirkland, Washington
USA

Phone (503) 685-1556

E-mail Malinoski@siemens.com

SIEMENS

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Engineering Design Patterns

The Johns Hopkins Applied Physics Laboratory

Brooke Guare
Cyber Systems Engineer
Brooke.Guare@jhuapl.edu

Introduction

Background: In order to aid engineers in designing sufficiently cyber resilient systems, the Office of the Under Secretary of Defense for Research and Engineering (OUSD (R&E)) / Resilient Systems (RS) tasked the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to curate and develop design patterns.

Challenge: The majority of systems have been designed to meet physical performance and functional requirements, as well as be resilient to a set of kinetic threats. However, there has not been as much attention paid to the resilience of the system to cyberspace threats.

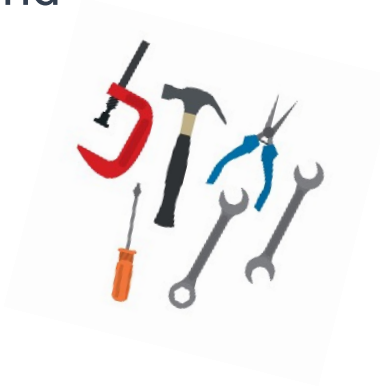
Approach

Solution: Development of design patterns

- A *design pattern* is a general, reusable solution to commonly occurring problems within a given context in system design

Impact: Compile design patterns proven successful or asserted to be useful, in order to:

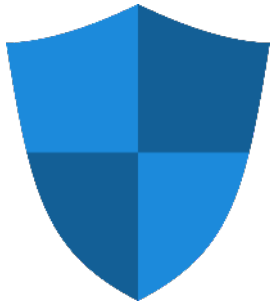
- Allow engineers to identify gaps and mitigate potential cyber related problems in their system
- Provide building blocks for cyber resilient system design
- Provide engineers the tools and knowledge they need to build resilient systems and meet cybersecurity requirements



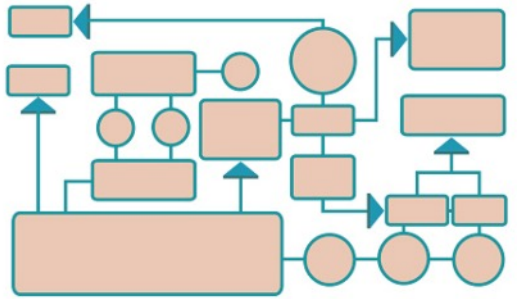
Cybersecurity-related Requirements

Design Patterns

+



Security Controls

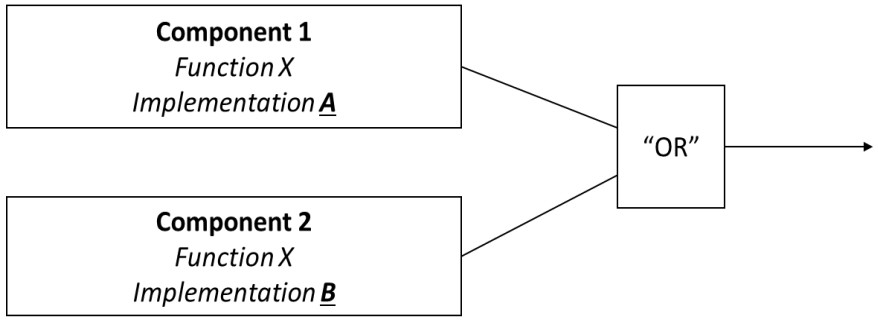


System Design

Resilient System

Case Study: Aircraft

Flight controls are electrically controlled

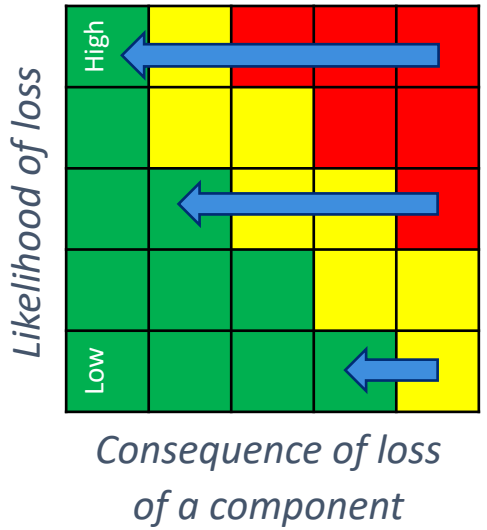


Threat:

- Loss of power to mission critical components

Application of Diverse Redundancy Design Pattern:

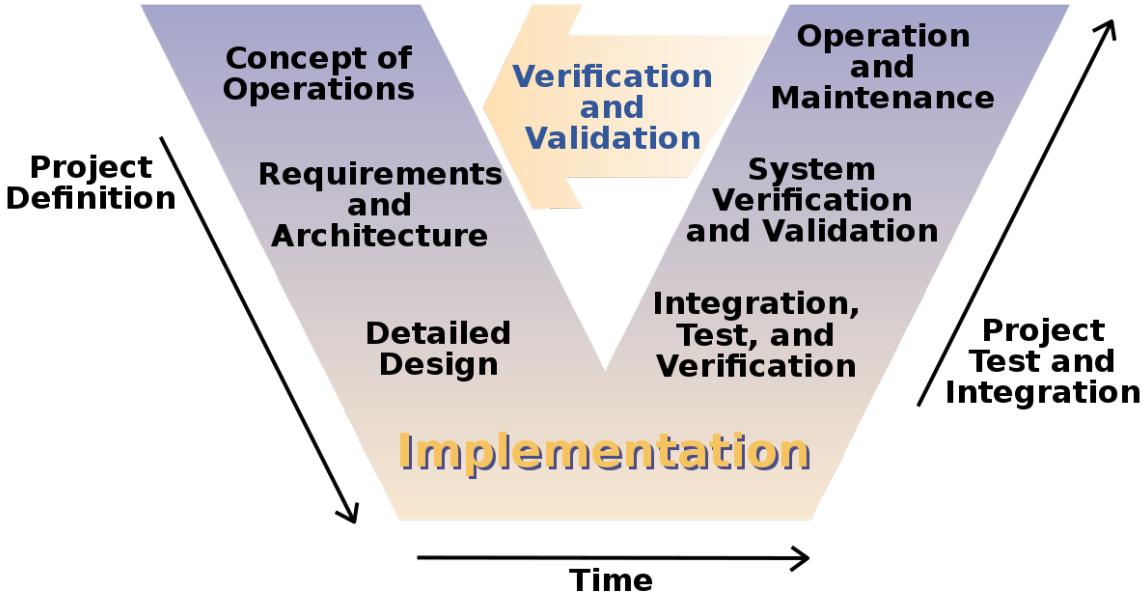
- Magnetic generator (primary source) allows power to be generated as long as engines are spinning
- 3 Electric Generators can power flight controls
- If electric backups fail, there is a battery backup



These mechanical examples can be translated to the cyber domain

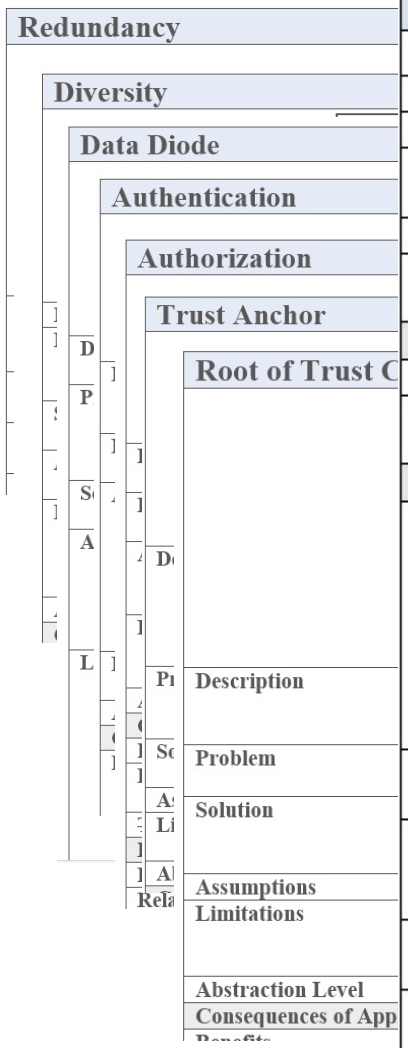
When Should Design Patterns Be Used?

- Integrating good design principles early in the systems engineering lifecycle helps ensure the system will be able to be resilient to the threat event, or set of threat events

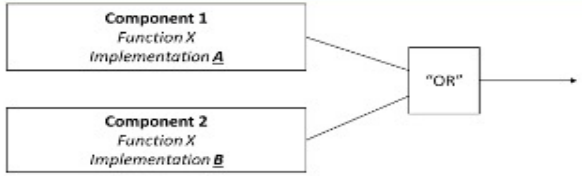


- However, design patterns can be applied throughout the systems engineering lifecycle in order to help secure existing systems

Design Pattern Template



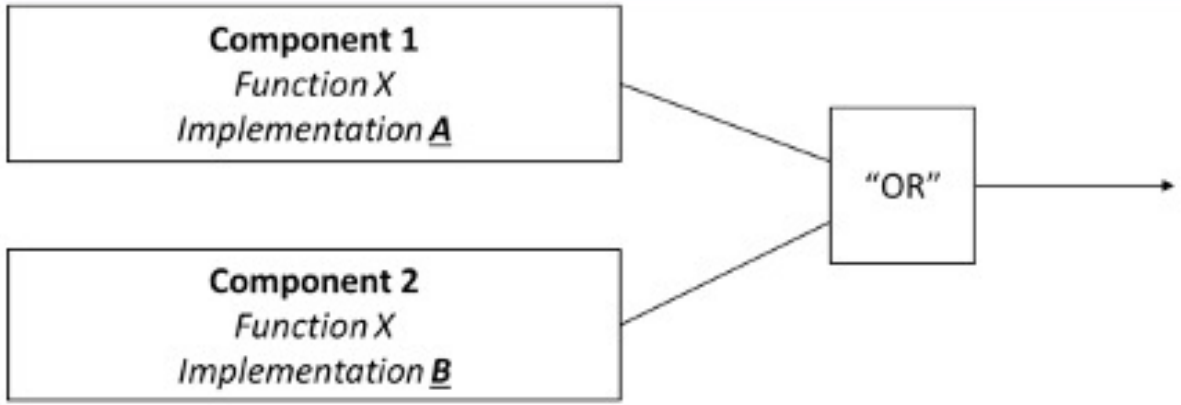
Design Pattern Title	**DRAFT**
Diagram illustrating pattern components in relation to one another	
Description	Summary of the main ideas about the illustrated design pattern.
Problem	An undesirable potential circumstance for which the pattern may provide a mitigating solution.
Assumptions	Conditions that must be true for proper application of the pattern. Assumptions provide context and dependences for the pattern's application.
Limitations	Cautions regarding the pattern's efficacy and applicable contexts.
Abstraction Level	An enumerated pattern category, one of either "base" or "compound." A *base* pattern is the lowest decomposition level. Combining base patterns results in *compound* patterns.
Consequences of Applying the Pattern	
Benefits	Desirable outcomes the pattern may enable; specifically, outcomes that address the stated problem.
Trade-Offs	Acknowledgment of possible consequences imposed by applying the pattern, possibly necessitating some compromises to otherwise beneficial system qualities elsewhere.
Related	
Loss Control Objective Addressed	An enumerated set of loss-related goals (from "Design Tenets Review," Draft, MITRE Corporation). The pattern can support one or more of these goals. The term "loss" may apply both to a component and to a mission capability, as specified in the completed template. The loss is usually in the context of mission capability or other end or outcome. The pattern may enable the system to: • Prevent the loss from occurring • Limit the extent of the loss • Fully or partially recover from the loss
Implementation Considerations	To help bridge the gap between abstract concept and specific implementation, this section provides considerations on how to implement the design pattern.
Related Design Patterns	Additional design patterns that, when used in conjunction with this pattern, contribute to solving this pattern's problem scope. Patterns listed here may complement this pattern to overcome limitations or combine to yield a more powerful capability.
Related Design Principles	This is a placeholder for tracing design patterns to draft MITRE Design Tenets document. Will be added once document is finalized.
Technical Standards and Examples	Texts, standards, applications, and/or examples that present the design pattern and/or describe its employed use cases. The references listed here may call the design pattern by a different name, but the application still meets the spirit and intent of the design pattern described in the template.
Potential Security Controls	The given pattern could be used to satisfy the listed security controls in NIST SP800-53. This is not meant to be a comprehensive list, only a subset of examples.

Diverse Redundancy	DRAFT					
						
Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.					
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.					
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.					
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.					
Abstraction Level	Base (Tier 1)		Compound (Tier 2)	X	(Combines redundancy and diversity)	
Consequences of Applying the Pattern						
Benefits	Despite losing a single component, the system can continue providing critical mission functionality by relying on the diverse redundant component. In other words, a *component* loss does not necessarily result in a *mission function* loss. The likelihood that an identical vulnerability is exploited across separate diverse components is lower than if all components have the same implementation. Apart from cyber, redundancy may allow for increased performance, help handle load balances, etc.					
Trade-Offs	• Potentially increases material cost, space, weight, power, and system complexity, likely beyond that of a homogenously redundant system. Applying this pattern throughout the entire system is probably impractical. Vetting diverse components adds cost and may increase implementation and compatibility complexity. Implementing diversity across all system aspects (e.g., power, CPU architecture) is challenging; thus, one may be forced to prioritize to which aspects to apply diversity. • Diverse redundancy requires adding multiple training and maintenance pipelines.					
Related						
Loss Control Objective Addressed	Loss Prevention	X	Loss Limitation	X	Loss Recovery	X
	Losing a single critical component does not necessarily result in loss of mission function.		Even if losing a component initially results in degraded mission functionality, switching to the redundant component thereafter can limit the duration of the degradation.		The "OR" box is where the logic for the recovery is held, determining whether one component goes down, to then seamlessly fall back to the diverse redundant second component.	
Implementation Considerations	• Are the redundant components operating all the time, or operating in a failover capacity • For failover capabilities, what are the detection and response actions necessary to failover to one to another • What are the time constraints for implementing redundant solutions					
Related Design Patterns	• Segmentation: To reduce likelihood that the same attack that degrades one component also degrades the other. • Redundancy: To have duplicate components in the system for failover purposes. • Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.					
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds					
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling					

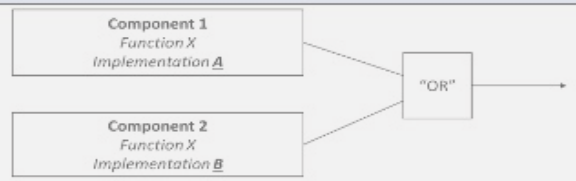
Subset of Design Patterns Developed:

- Redundancy
- Diverse Redundancy
- Data Diode
- Segmentation
- Authentication
- Authorization
- Trust Anchor
- Watch Dog
- Data Collection
- Analytics
- Alerts
- Response
- Load from Known State
- …. & More

Diverse Redundancy

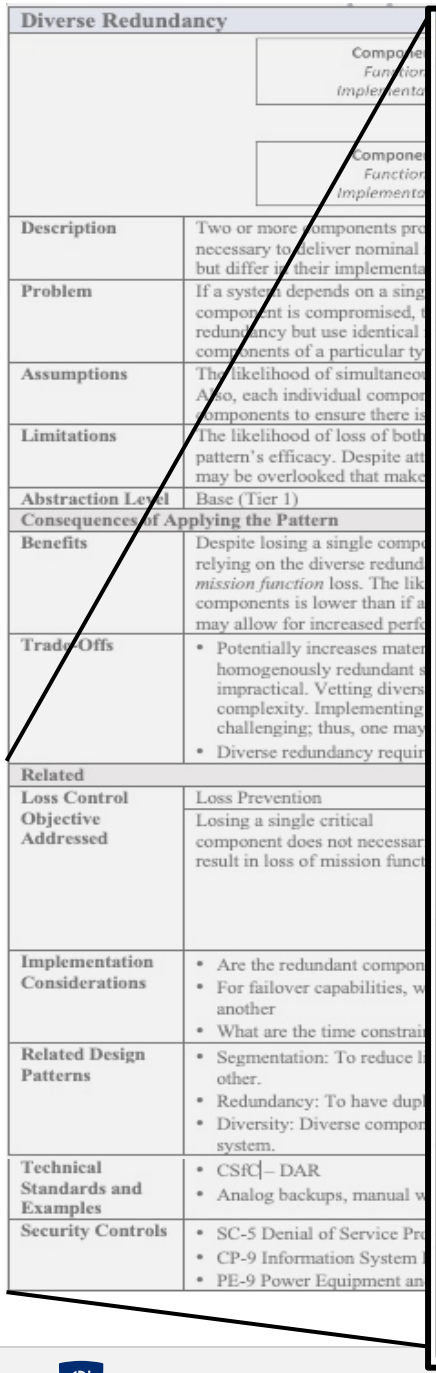


Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.				
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.				
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.				
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.				
Abstraction Level	Base (Tier 1)		Compound (Tier 2)	X	(Combines redundancy and diversity)

Diverse Redundancy	DRAFT
	
Description	Two or more components provide redundant functionality, where only one component is absolutely necessary to deliver nominal system capability. The redundant components provide equivalent functionality, but differ in their implementations.
Problem	If a system depends on a single component to perform a mission-critical function, and if that single component is compromised, the dependent mission-critical function is also lost. Further, if systems employ redundancy but use identical redundant components, common-mode failures (which possibly affect all components of a particular type) can thwart the intended benefits of redundancy.
Assumptions	The likelihood of simultaneous loss of both components to the same adverse occurrence is acceptably low. Also, each individual component's reliability is acceptable. Separate teams or vendors have developed these components to ensure there is a sufficient amount of diversity between them.
Limitations	The likelihood of loss of both components because of adverse conditions is inversely proportional to this pattern's efficacy. Despite attempts to introduce diversity between components, some form of commonality may be overlooked that makes them susceptible to the same exploit.
Abstraction L	
Consequences	
Benefits	
Trade-Offs	
Related	
Loss Control Objective Addressed	
Implementatio Consideration	
Related Desig Patterns	• Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling

Consequences of Applying the Pattern

Benefits	Despite losing a single component, the system can continue providing critical mission functionality by relying on the diverse redundant component. In other words, a *component* loss does not necessarily result in a *mission function* loss. The likelihood that an identical vulnerability is exploited across separate diverse components is lower than if all components have the same implementation. Apart from cyber, redundancy may allow for increased performance, help handle load balances, etc.
Trade-Offs	• Potentially increases material cost, space, weight, power, and system complexity, likely beyond that of a homogenously redundant system. Applying this pattern throughout the entire system is probably impractical. Vetting diverse components adds cost and may increase implementation and compatibility complexity. Implementing diversity across all system aspects (e.g., power, CPU architecture) is challenging; thus, one may be forced to prioritize to which aspects to apply diversity. • Diverse redundancy requires adding multiple training and maintenance pipelines.



Related					
Loss Control Objective Addressed	Loss Prevention	X	Loss Limitation	X	Loss Recovery	X
	Losing a single critical component does not necessarily result in loss of mission function.		Even if losing a component initially results in degraded mission functionality, switching to the redundant component thereafter can limit the duration of the degradation.		The "OR" box is where the logic for the recovery is held, determining whether one component goes down, to then seamlessly fall back to the diverse redundant second component.	
Implementation Considerations	• Redundant components should be implemented so that they aren't susceptible to the anticipated threats. For example, redundant hydraulic lines run right next to one another would both be susceptible to one kinetic impact. In cyberspace, redundant components should use segmentation or other resilience techniques to ensure they both don't fail due to the same cyberspace attack. • How quickly does one component need to perform the functions of a failed component? • Are all redundant components on all the time or are redundant components operating in a failover capacity? • If all component are on all the time and one component goes bad (via a failure or an integrity attack) how does the system determine which component is correct? • How will the system or the operator know when to switch from one redundant component to another? • Having multiple components with the same functionality comes with a funding tail. A training and maintenance pipeline must be established and maintained for each of the different components.					
Related Design Patterns	• Segmentation: To reduce likelihood that the same attack that degrades one component also degrades the other. • Redundancy: To have duplicate components in the system for failover purposes. • Diversity: Diverse components limit the ability for a single vulnerability to propagate throughout the entire system.					
Requirements	• The system shall maintain mission capability despite malicious data being written to the system. • The system shall maintain mission capability despite the execution of malicious code. • The system shall maintain mission capability despite the malicious execution of authorized instructions. • The system shall maintain mission capability despite the denial of authorized data. • The system shall remove adversary access to system data, without degrading mission capability, upon the detection of an adversary obtaining restricted (e.g., classified or sensitive) system data.					
Technical Standards and Examples	• CSfC – DAR • Analog backups, manual workarounds					
Security Controls	• SC-5 Denial of Service Protection • CP-9 Information System Backup • PE-9 Power Equipment and Cabling | Redundant cabling					

Next Steps

- Integrate design pattern into CRWS-BoK repository
- Demonstrate design pattern applicability and interoperability
- Continue development and refinement of existing patterns and template

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

The Most Important Trades Often Happen During Project Planning: Using Set-Based Practices to Optimize those Trade-Off Decisions

Brian M. Kennedy
CTO
Targeted Convergence Corporation

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the design of a UAV

Need to decide:

- Sensor Packages
- Wingspan
- Fuel Capacity
- Propulsion System
- Fuselage Length
- Weight
- Altitude

Analysis

To satisfy targets:

- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the design of a UAV

Need to decide:

- Sensor Packages
- Wingspan
- Fuel Capacity
- Propulsion System
- Fuselage Length
- Weight
- Altitude

To satisfy targets:

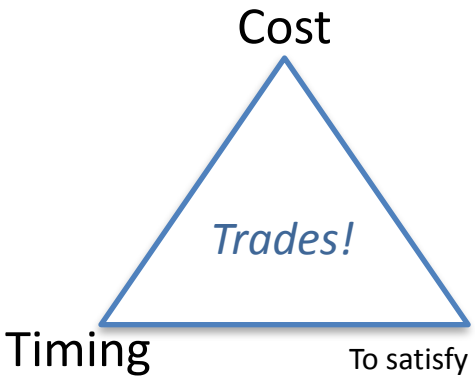
- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the project planning of the design of a UAV

Need to decide:

- Who does What
- What needs to be Learned
- What Options to Evaluate
- What Resources to Use
- What Testing to Do
- What Innovation
- What Risks



To satisfy Targets:

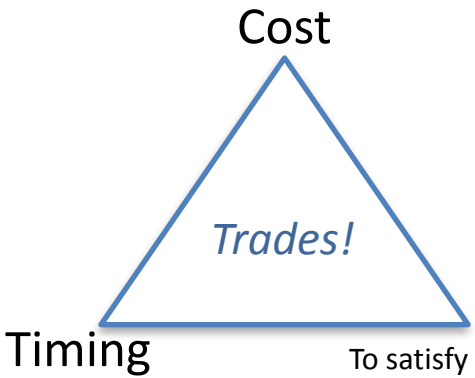
- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the project planning of the design of a UAV

Need to decide:

- Who does What
- What needs to be Learned
- What Options to Evaluate
- What Resources to Use
- What Testing to Do
- What Innovation
- What Risks



To satisfy Targets:

- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

?

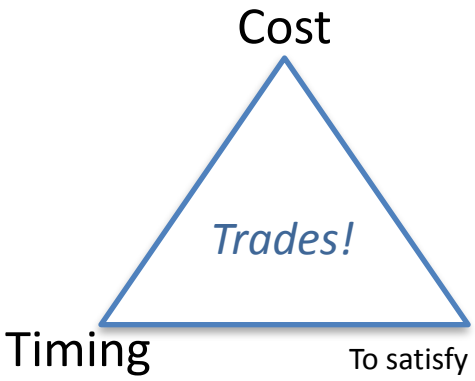
How?

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the project planning of the design of a UAV

Need to decide:

- Who does What
- What needs to be Learned
- What Options to Evaluate
- What Resources to Use
- What Testing to Do
- What Innovation
- What Risks



Traditional tools (Gantt, PERT, Project, etc.) show timing dependencies and perhaps support cost roll-ups, but they don't let you see all of these Trades!!

To satisfy Targets:

- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

?

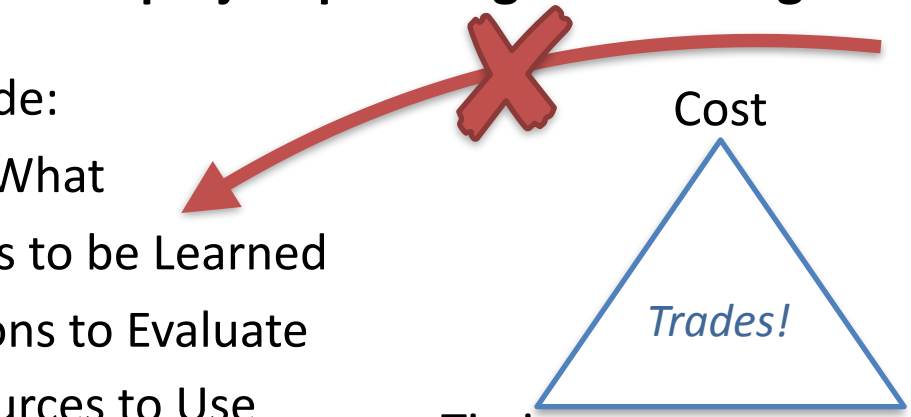
How?

Targeted Convergence Corporation
www.TargetedConvergence.com

Trade-Offs for the project planning of the design of a UAV

Need to decide:

- Who does What
- What needs to be Learned
- What Options to Evaluate
- What Resources to Use
- What Testing to Do
- What Innovation
- What Risks



Traditional tools (Gantt, PERT, Project, etc.) show timing dependencies and perhaps support cost roll-ups, but they don't let you see all of these Trades!!

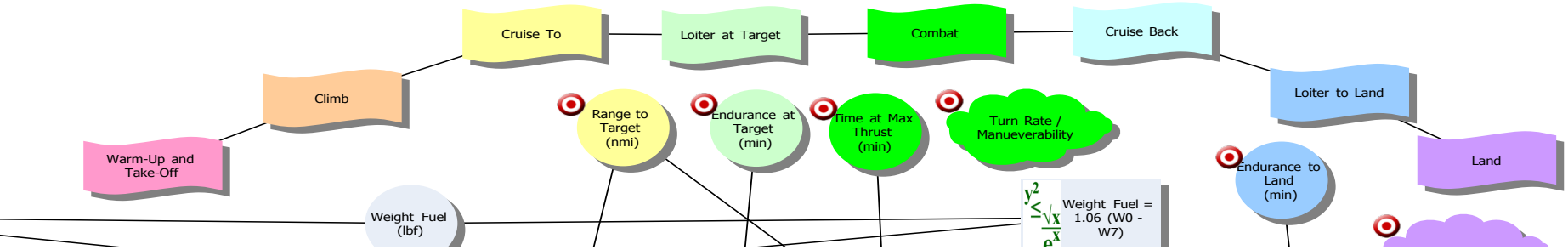
To satisfy Targets:

- Range to Target
- Time to Target
- Endurance at Target
- Area Scanned per Unit Time
- Size of Targets Detected
- Survivability
- Detectability
- Per Unit UAV Cost

How?

Targeted Convergence Corporation
www.TargetedConvergence.com

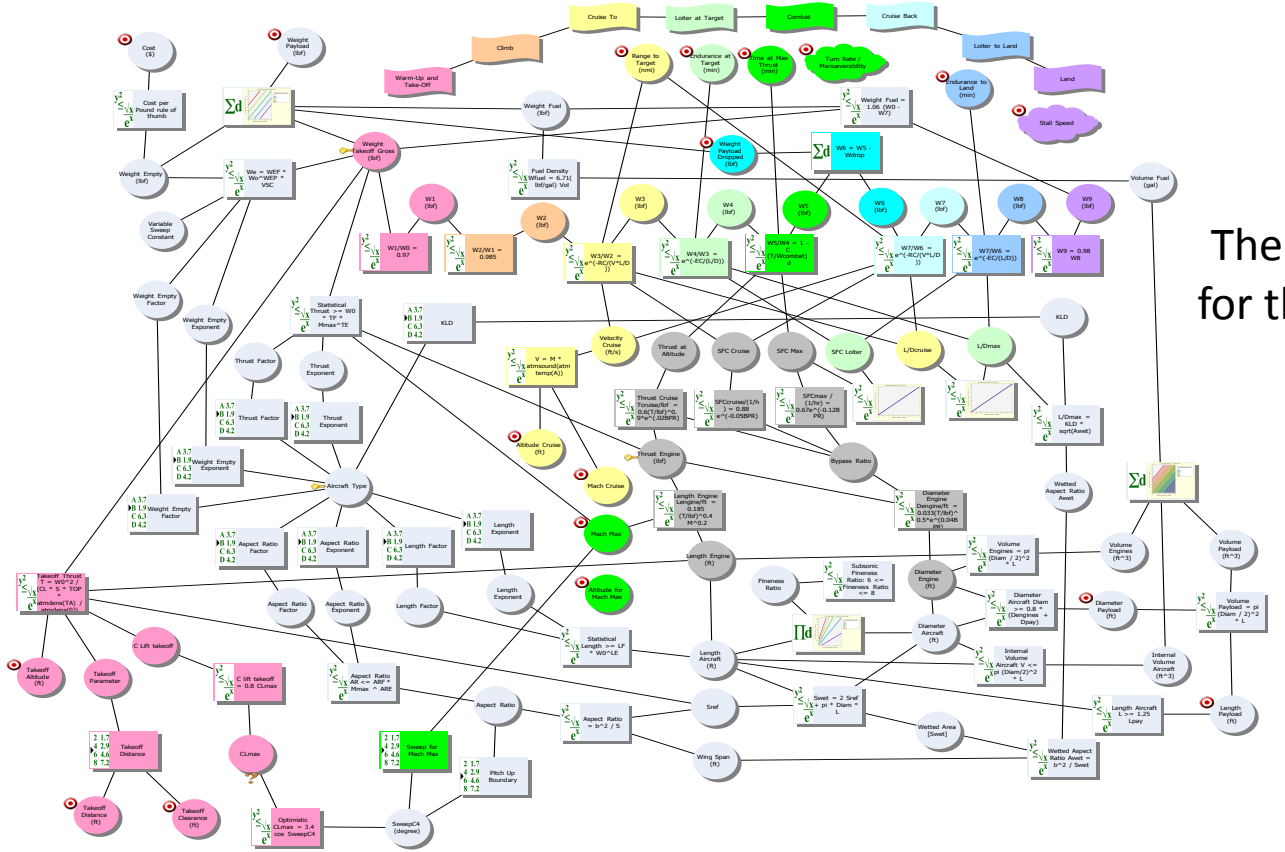
How? Use the same Set-Based Causal Map to do your Planning Trades!



In the same way that we laid out the steps of the UAV's target mission (to serve as a color coding for the rest of the Causal Map), you can lay out the development steps.

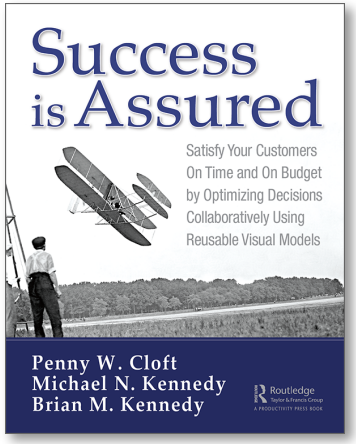
Targeted Convergence Corporation
www.TargetedConvergence.com

How? Use the same Set-Based Causal Map to do your Planning Trades!



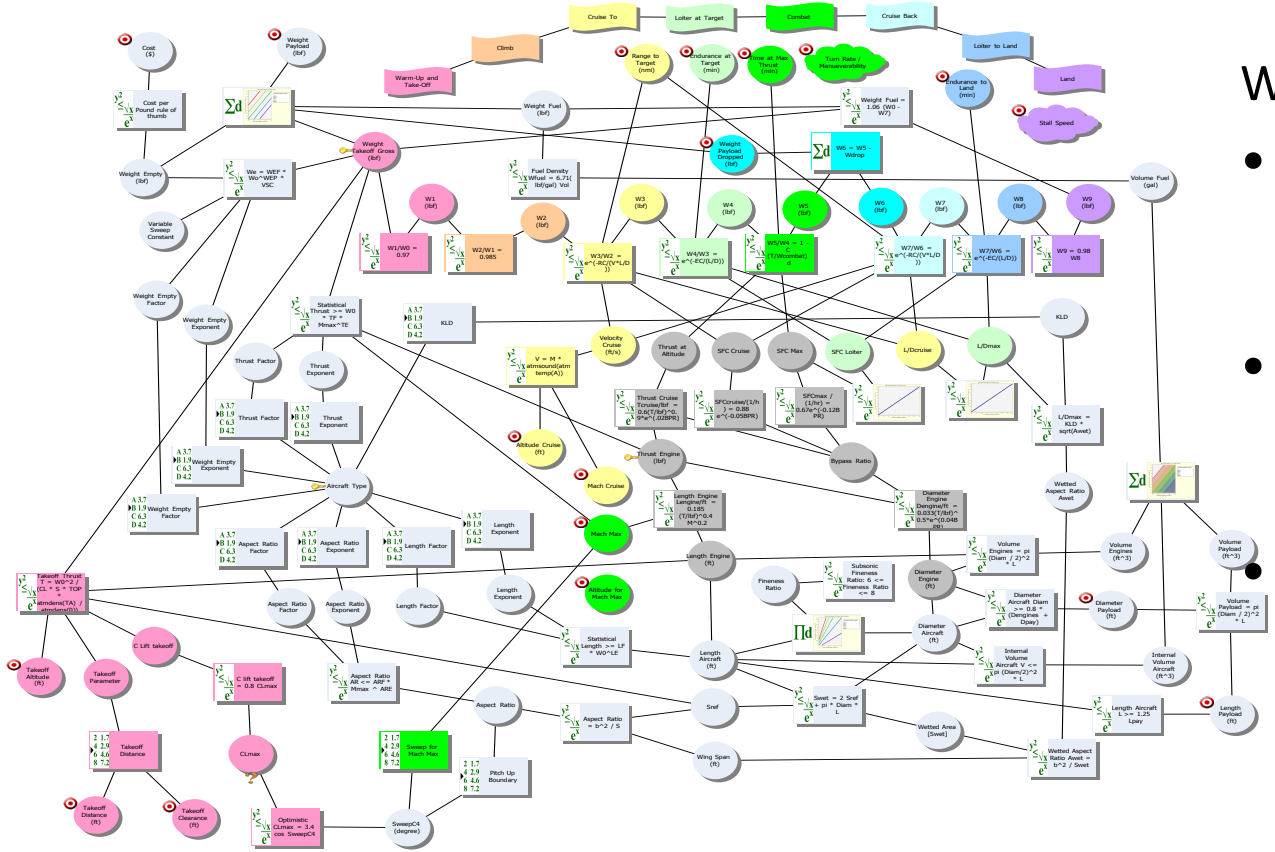
The full Causal Map for that UAV's Trades

details are in:



Targeted Convergence Corporation
www.TargetedConvergence.com

How? Use the same Set-Based Causal Map to do your Planning Trades!

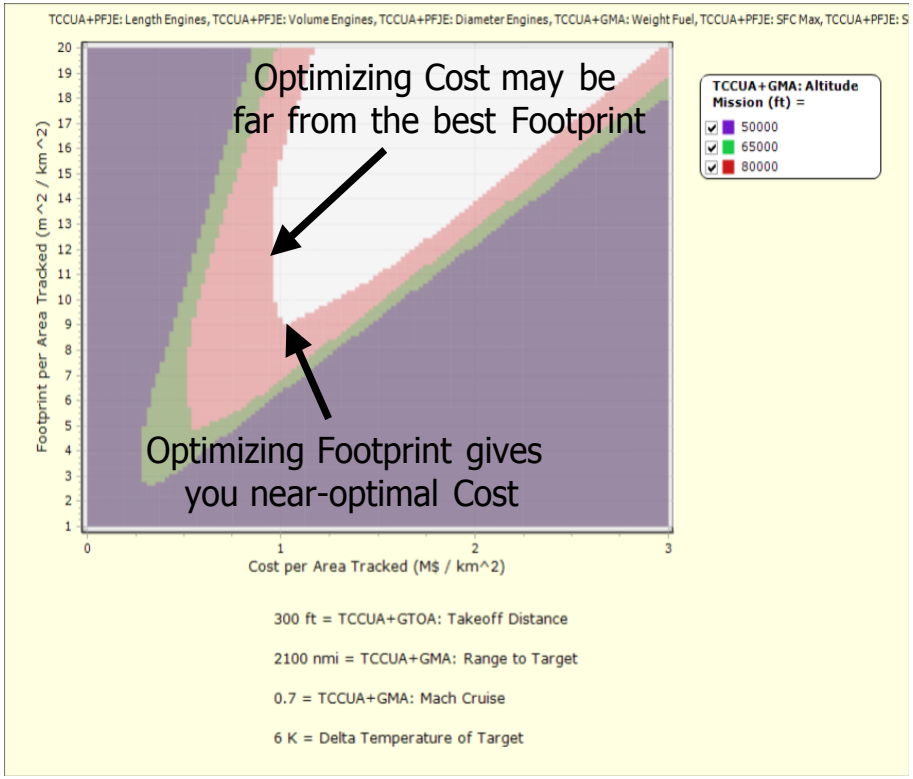


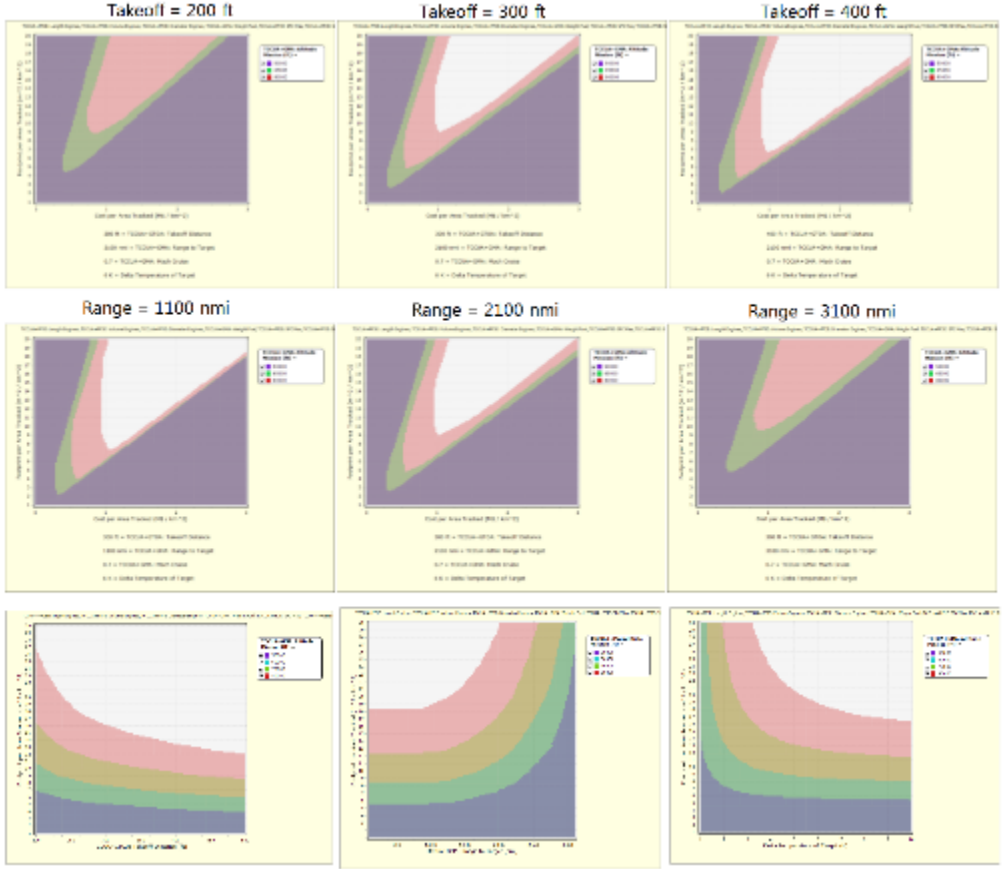
Which of these decisions:

- have alternatives that will require extra learning, testing, headcount, etc.?
- carry extra risks that need to be managed or eliminated via upfront learning efforts?
- limit performance such that innovations will be needed to overcome those limits?

Targeted Convergence Corporation
www.TargetedConvergence.com

Quick UAV Design example (Set-Based system design for a mission)





Targeted Convergence Corporation
www.TargetedConvergence.com

Benefits of Applying Set-Based System Design Techniques

- See how your Project Planning Decisions will impact your Timing, Cost, & Targets
- See the Causal Structure of the full Decision Space, as well as the Limits of it
- See the Sensitivities, and let those guide Human-in-the-Loop Optimization

- Accommodate Uncertainty – Make wise decisions even though things are Uncertain
- Accommodate Ongoing Learning – As you learn, just continue narrowing decisions
- Use the Limits and Structure to Focus Your Learning Efforts where most valuable

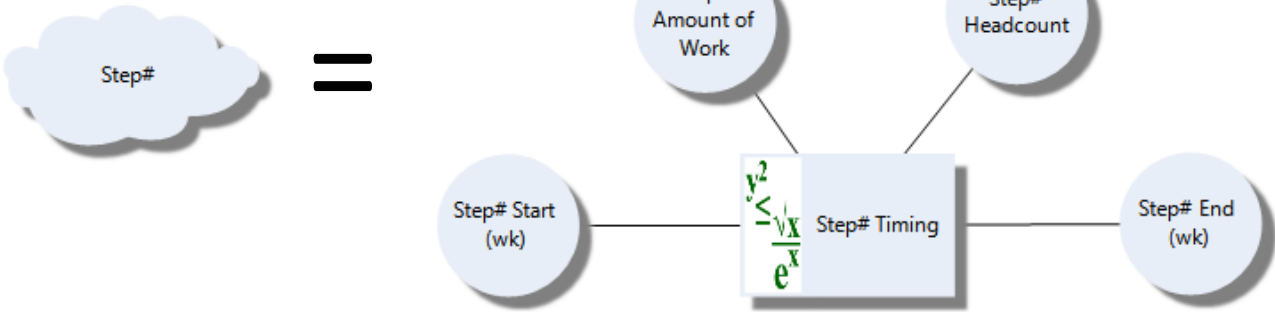
- The Visual Models enable effective Collaboration Across Different Areas of Expertise
- The “Eliminate the Weak” paradigm of converging to more optimal solutions enables Concurrency across different groups focused on different sub-systems (sub-missions)
- The Set-Based visual models are highly reusable and enable continuous improvement each time they are reused

Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a single Process Step

Need to decide:

- When to Start
- When to End
- Headcount
- Resources
- Amount of Work

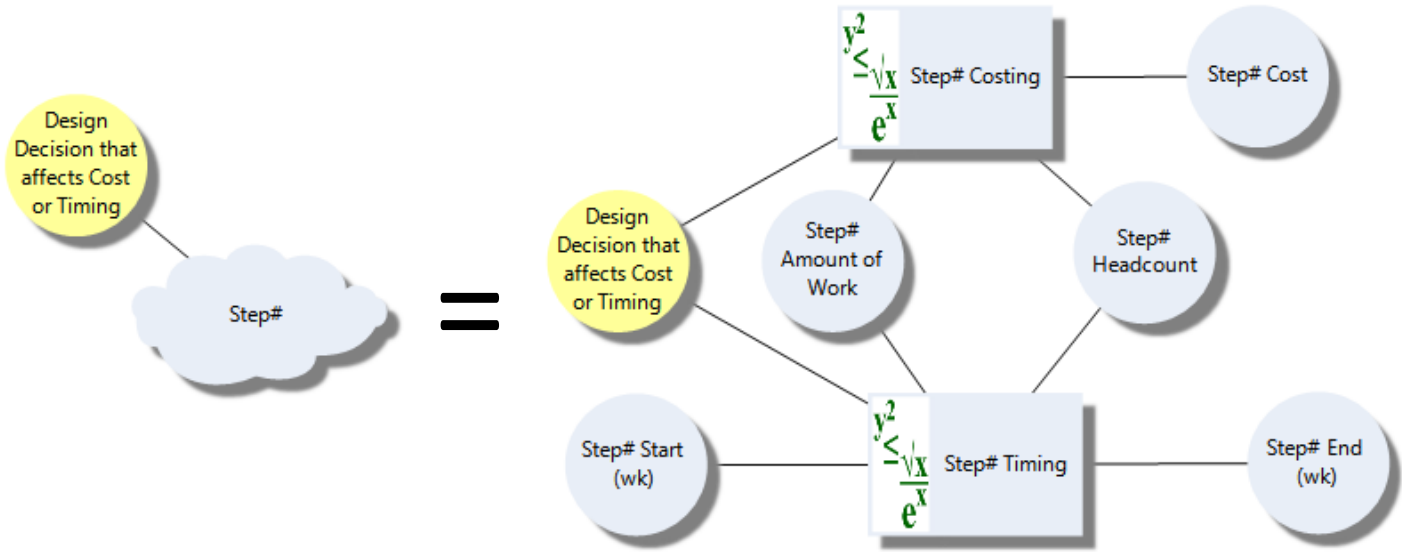


Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a single Process Step

Need to decide:

- When to Start
- When to End
- Headcount
- Resources
- Amount of Work
- Design Decisions to be Considered

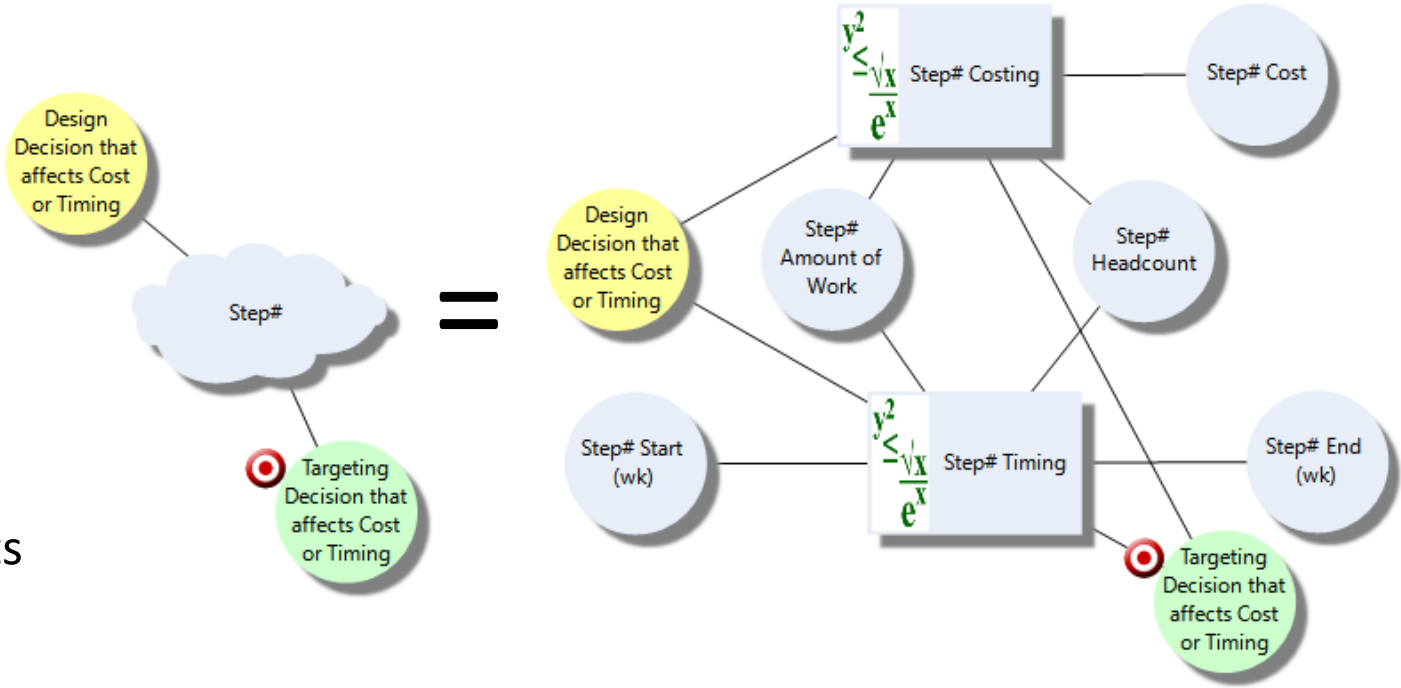


Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a single Process Step

Need to decide:

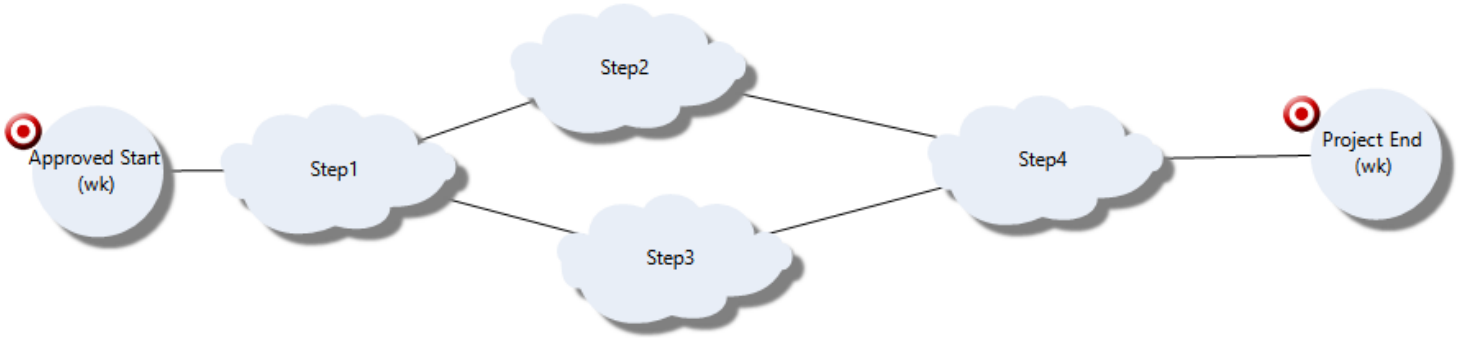
- When to Start
- When to End
- Headcount
- Resources
- Amount of Work
- Design Decisions to be Considered
- Targets for Results



Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a Project Plan

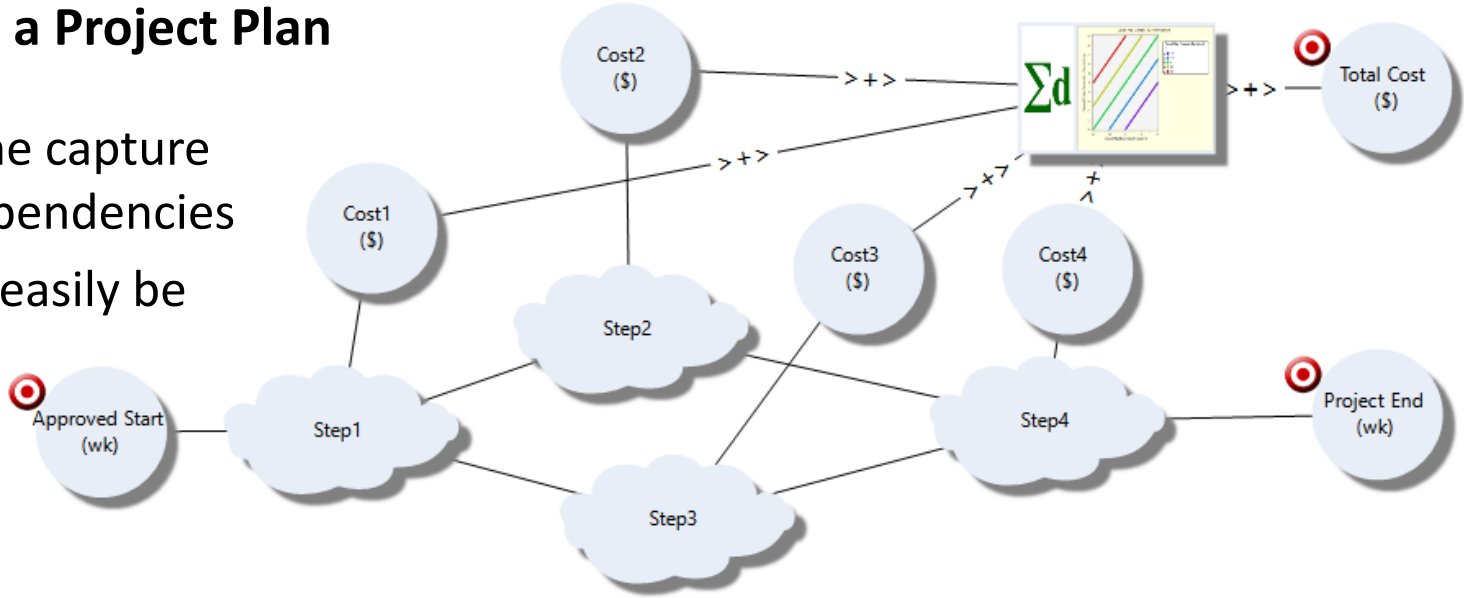
- The Steps alone capture the Timing dependencies



Targeted Convergence Corporation
www.TargetedConvergence.com

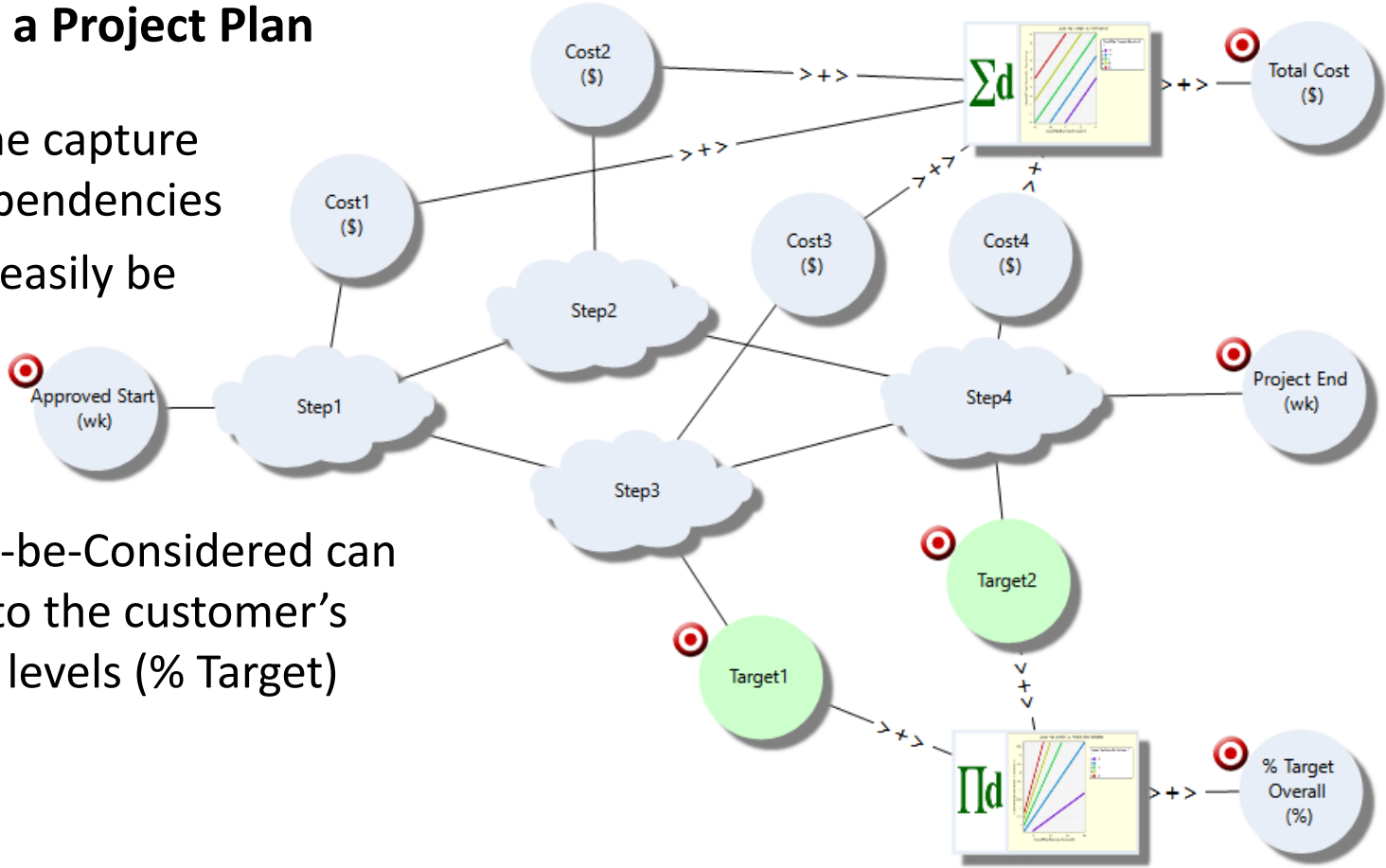
Causal Map for a Project Plan

- The Steps alone capture the Timing dependencies
- The Costs can easily be summed up



Causal Map for a Project Plan

- The Steps alone capture the Timing dependencies
- The Costs can easily be summed up

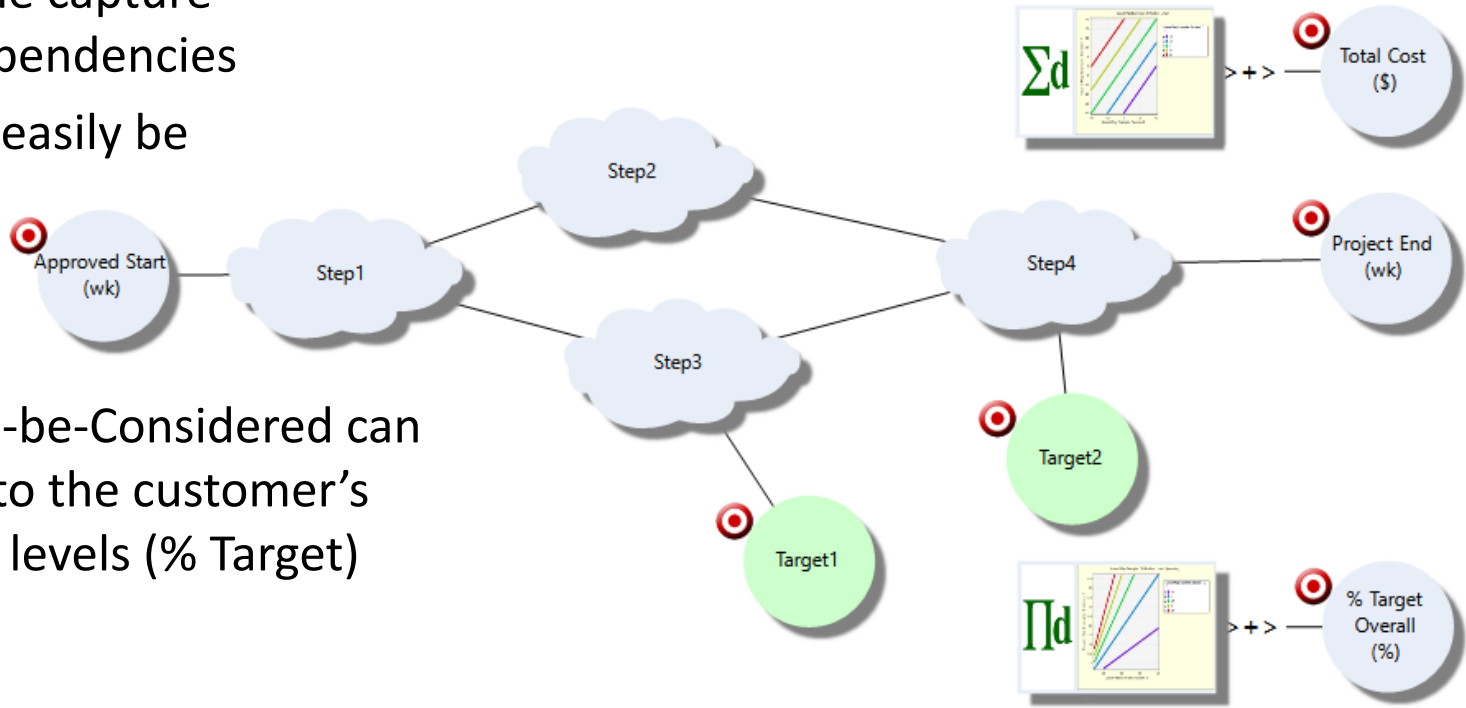


- The Targets-to-be-Considered can be compared to the customer's Goal and Veto levels (% Target)

Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a Project Plan — Visually Simplified

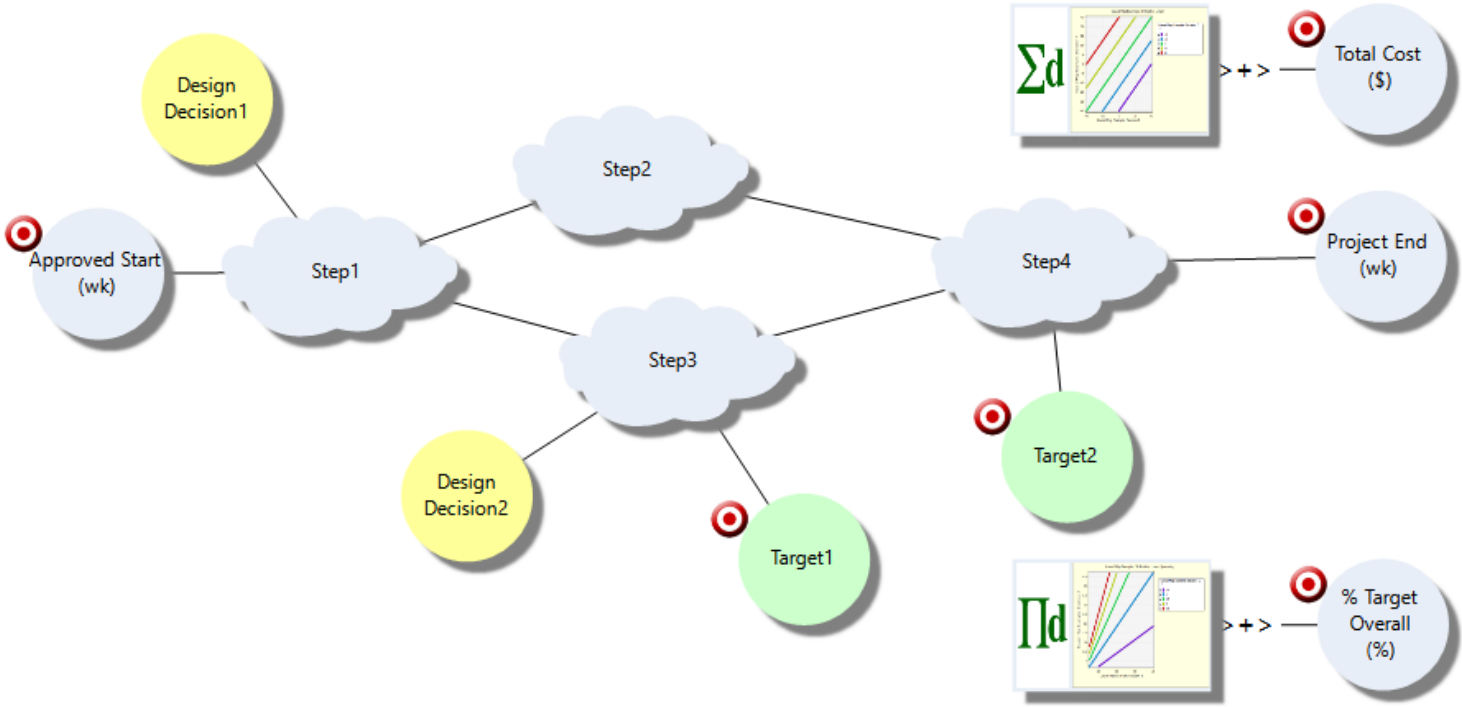
- The Steps alone capture the Timing dependencies
- The Costs can easily be summed up



- The Targets-to-be-Considered can be compared to the customer's Goal and Veto levels (% Target)

Targeted Convergence Corporation
www.TargetedConvergence.com

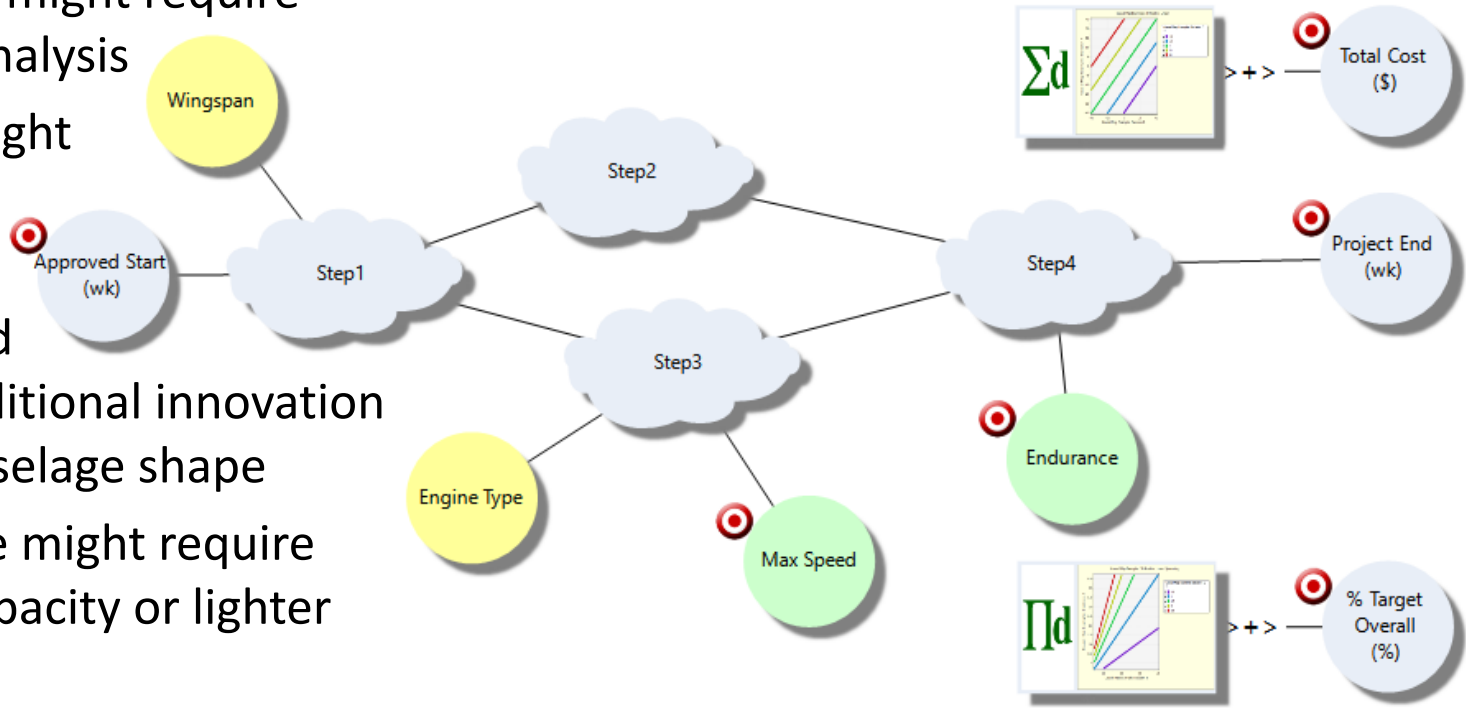
Causal Map for a Project Plan — “So, what Decisions might impact this?”



Targeted Convergence Corporation
www.TargetedConvergence.com

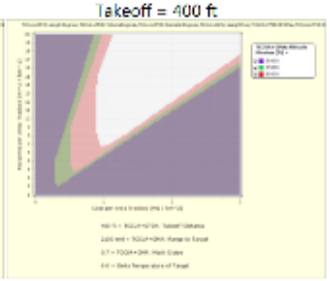
Causal Map for a Project Plan — Concrete Design Decisions and Targets

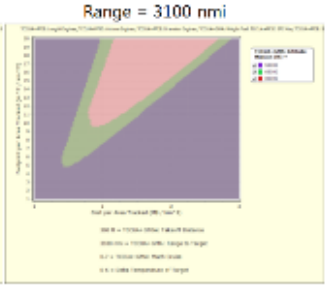
- Longer Wingspan might require extra structural analysis
- Electric Engine might require battery research
- Higher Max Speed might require additional innovation and analysis in fuselage shape
- Longer Endurance might require additional fuel capacity or lighter weight materials

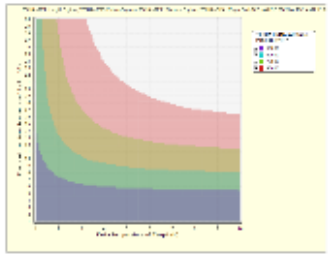


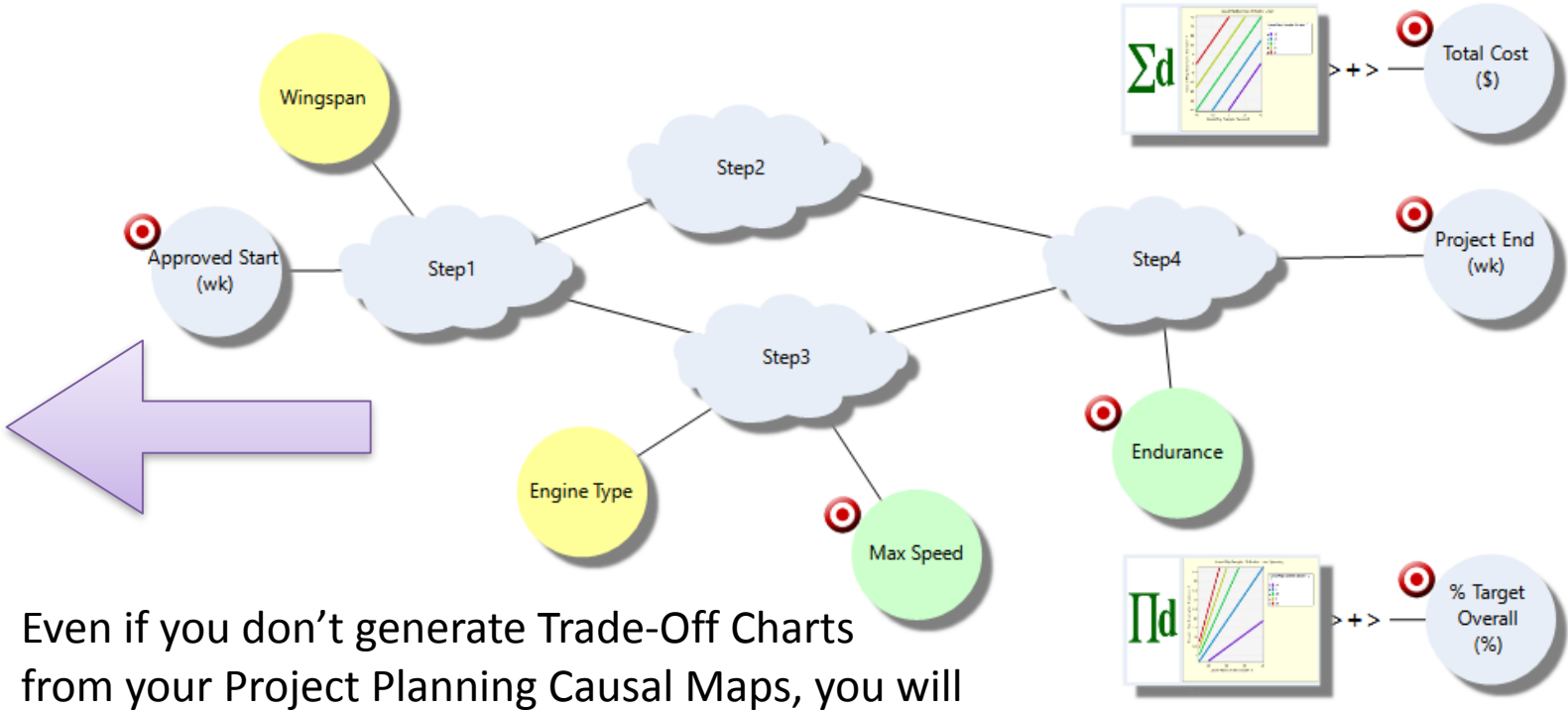
Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a Project Plan — Improved Collaboration





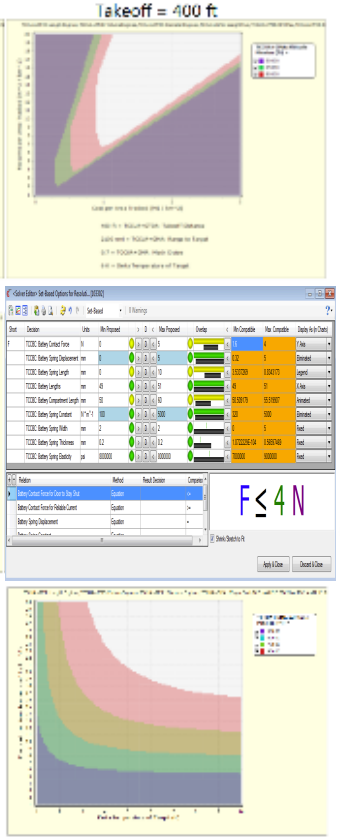


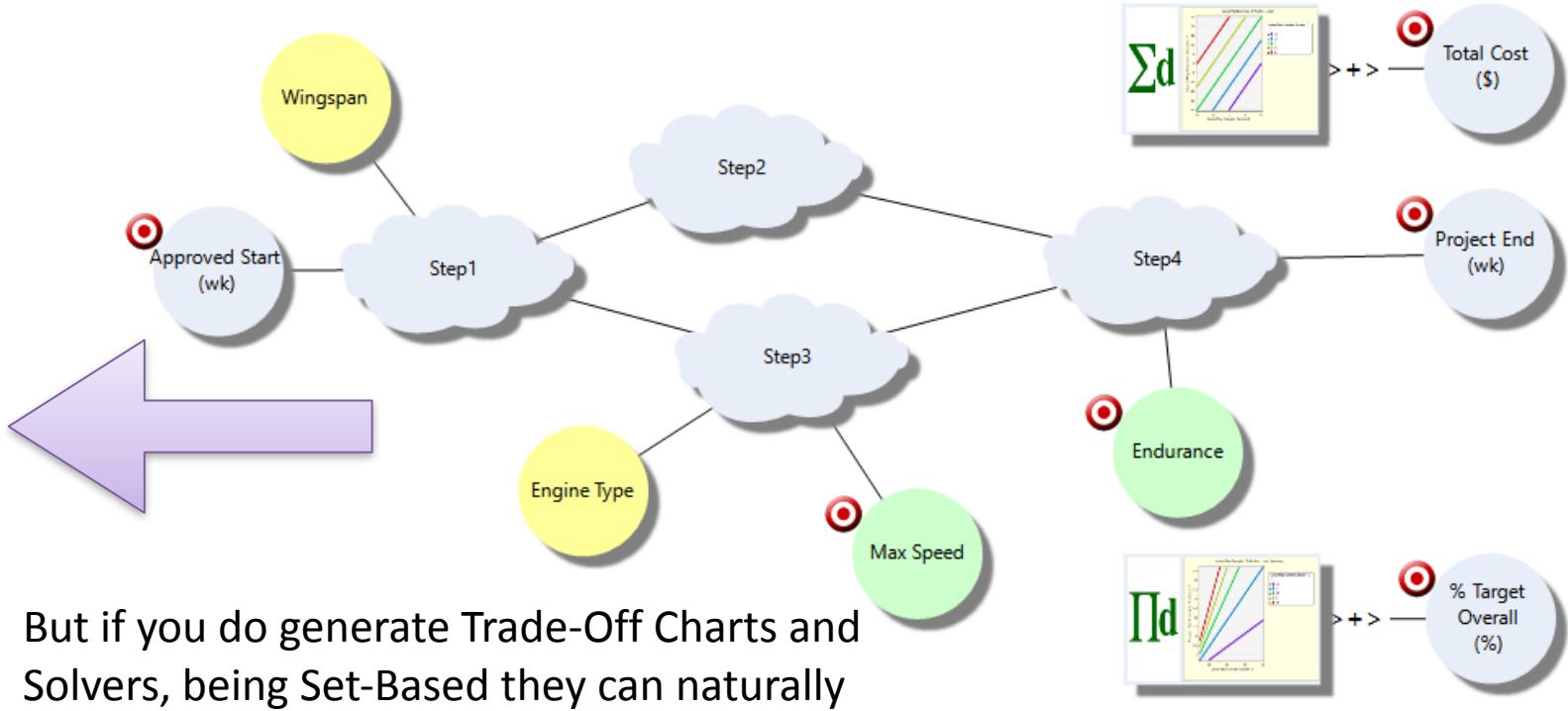


Even if you don't generate Trade-Off Charts from your Project Planning Causal Maps, you will still get huge benefits from the improved collaboration — the improved thinking.

Targeted Convergence Corporation
www.TargetedConvergence.com

Causal Map for a Project Plan — Improved Collaboration



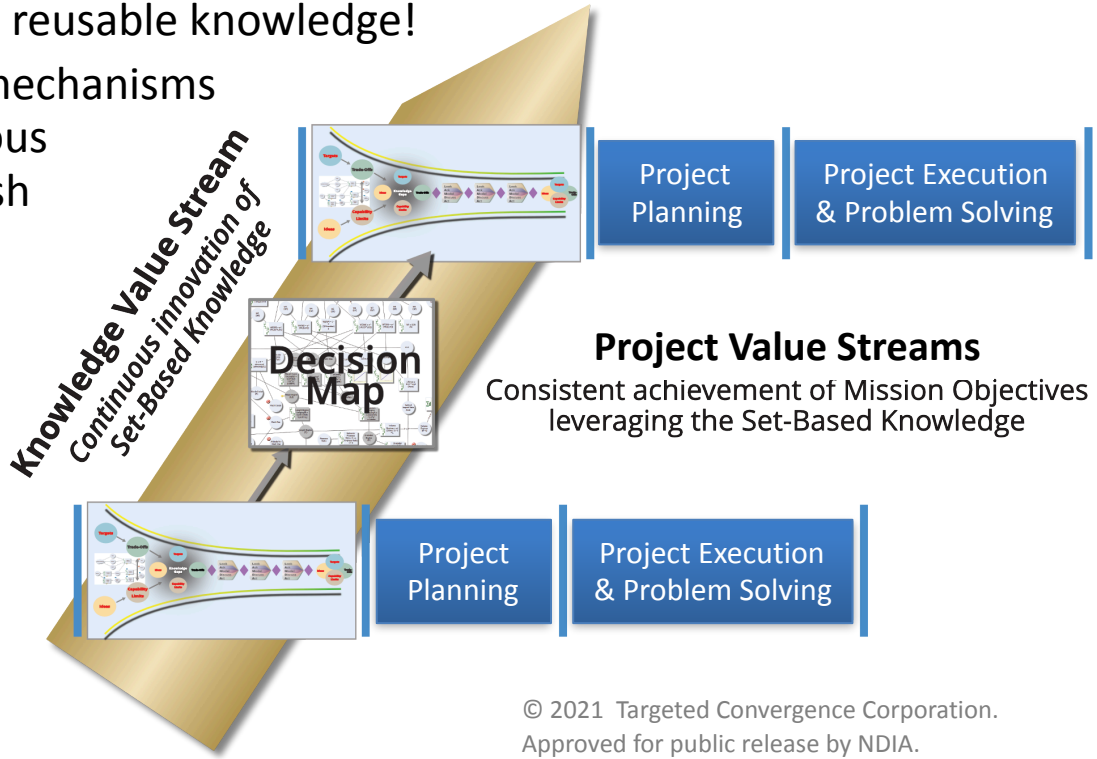


But if you do generate Trade-Off Charts and Solvers, being Set-Based they can naturally accommodate all the uncertainty that you will have early in the Project Planning effort.

Targeted Convergence Corporation
www.TargetedConvergence.com

That Set-Based Knowledge is Reusable and Continuously Improvable

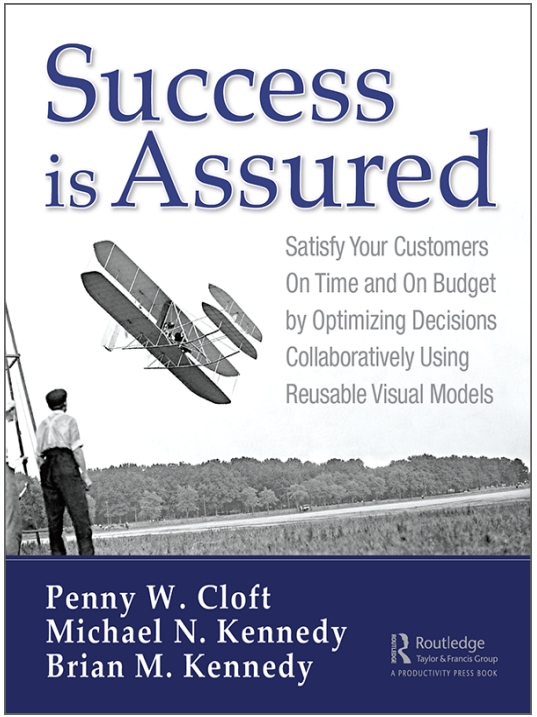
- The Visual Knowledge makes it easy to review, critique, and improve.
- And when easy-to-review, it becomes trustworthy.
- And only if trustworthy, is it truly reusable knowledge!
- By putting in place appropriate mechanisms for Knowledge Reuse & Continuous Improvement, teams can establish a Knowledge Value Stream that feeds their Project Planning & Execution Value Streams.
- The key Enablers for that are the Causal Decision Map and the Trade-Off Chart / Solver.



Targeted Convergence Corporation
www.TargetedConvergence.com

Any Questions??

- There's a short (2-minute) video trailer on our book at:
  http://SuccessIsAssured.com/



Targeted Convergence Corporation
www.TargetedConvergence.com

Systems Engineering Modernization

Co-Briefers:

Ms. Nadine Geier . Director, Systems Engineering

Dr Kelly Alexander, Chief Engineer, Systems Engineering Modernization

Office of the Deputy Director for Engineering

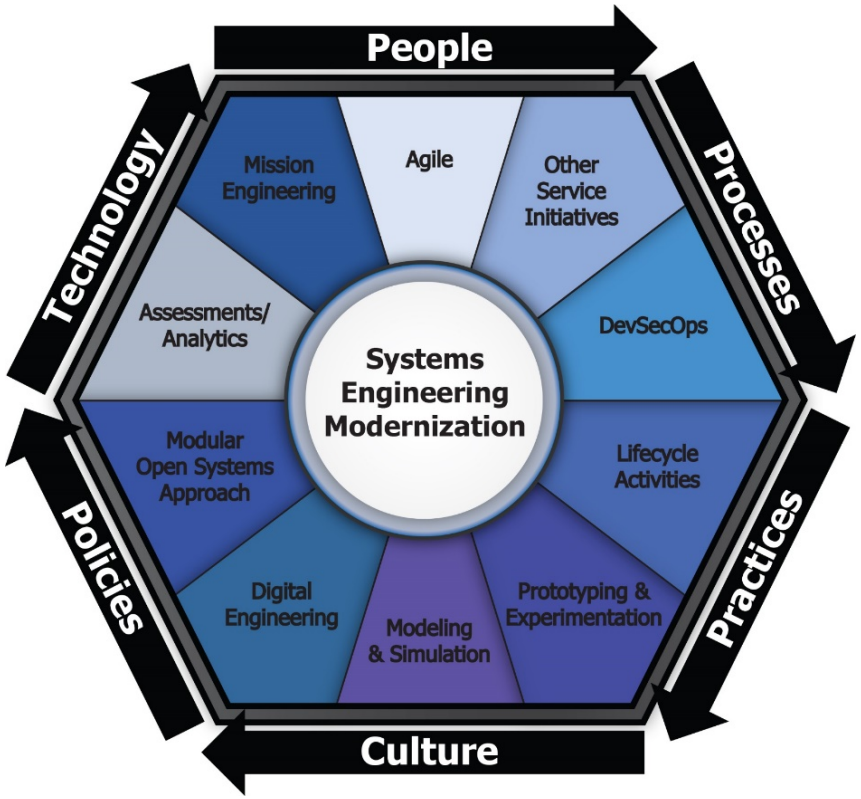
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems and Mission Engineering Conference

Virtual

December 2021

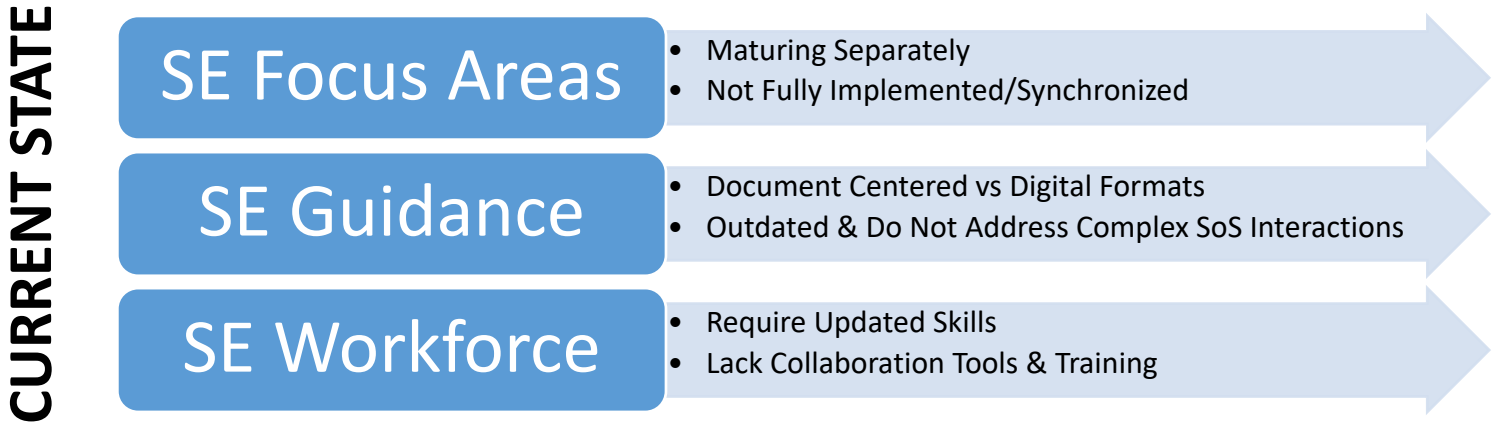
Systems Engineering (SE) Modernization Overview



- **VISION:** Integrate modernized SE practices that maintain the essential rigor and enable DoD to develop and field the newest technology with more confidence and relevance.
- **OBJECTIVE:** Modernize SE to support the delivery of capability to meet mission needs.
- **OUTCOMES:**
  - Strategy/Roadmaps to implement an integrated approach that coordinates the modern SE practices.
  - Updated SE practice, policy/guidance, and workforce development

Modernizing SE is a journey of evolving mind-sets and integrating initiatives

SE Modernization Problem Statement

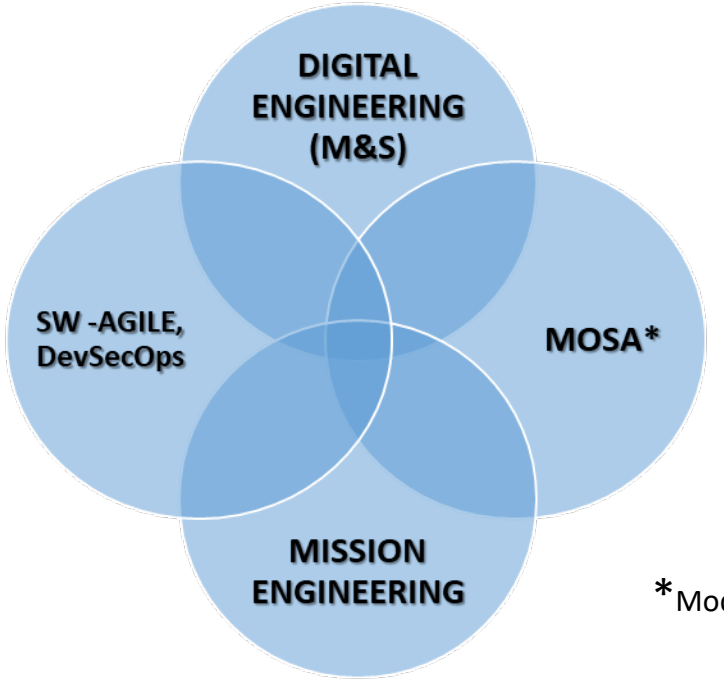


"There is a **lack of an integrated approach** to implementation of SE Focus Areas that is necessary to ensure the relevant guidance, skills, and training are available to deliver a robust, disciplined approach to weapon systems acquisition."

"The practice of systems engineering must further evolve to support the demands of ever-increasing system complexity and enterprise competitiveness"
- INCOSE Vision 2035 (Executive Draft)

SE Modernization Focus Areas and Key Enablers

SE Modernization Focus Areas (Initial Scope)

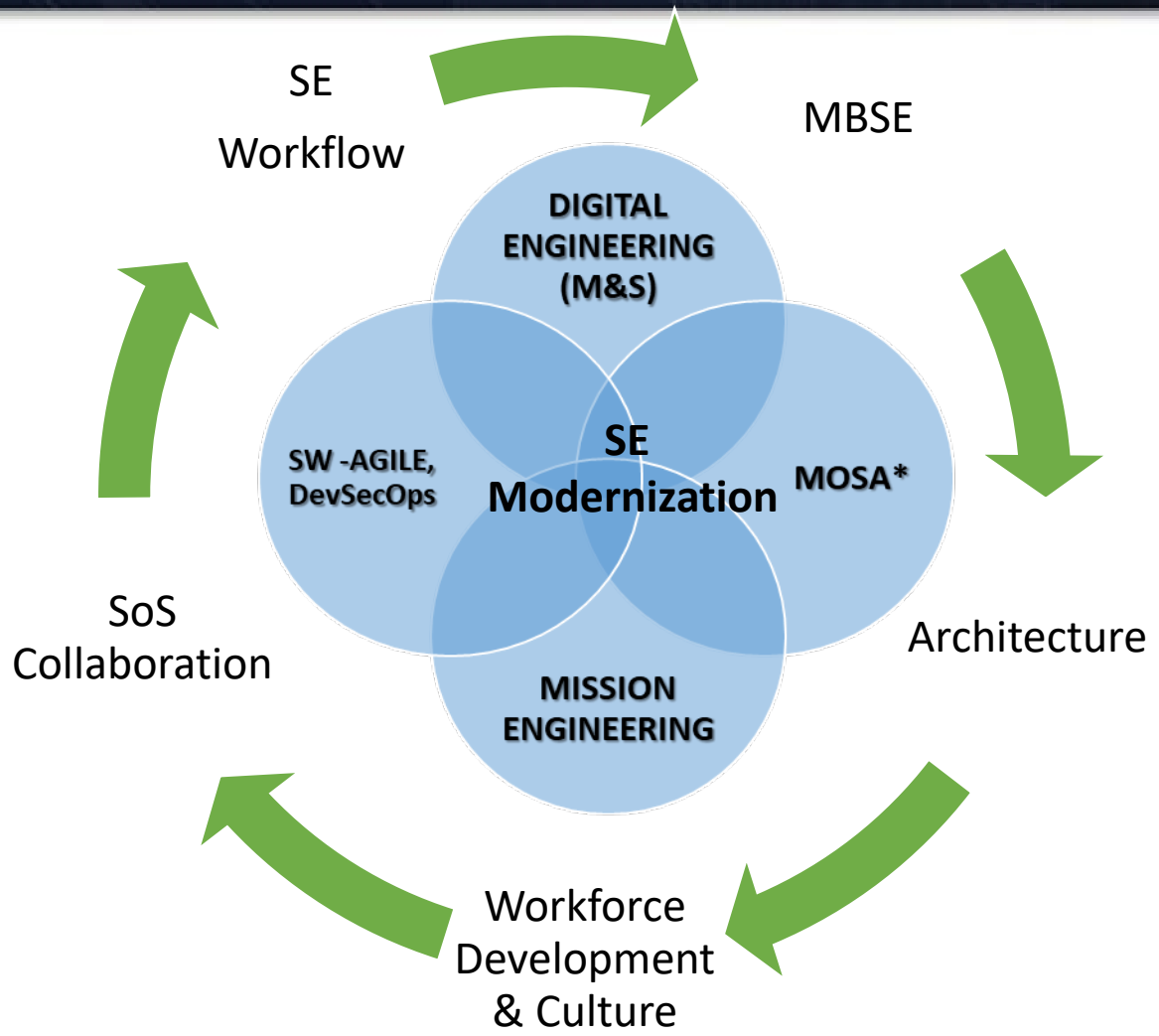


*Modular Open Systems Approaches

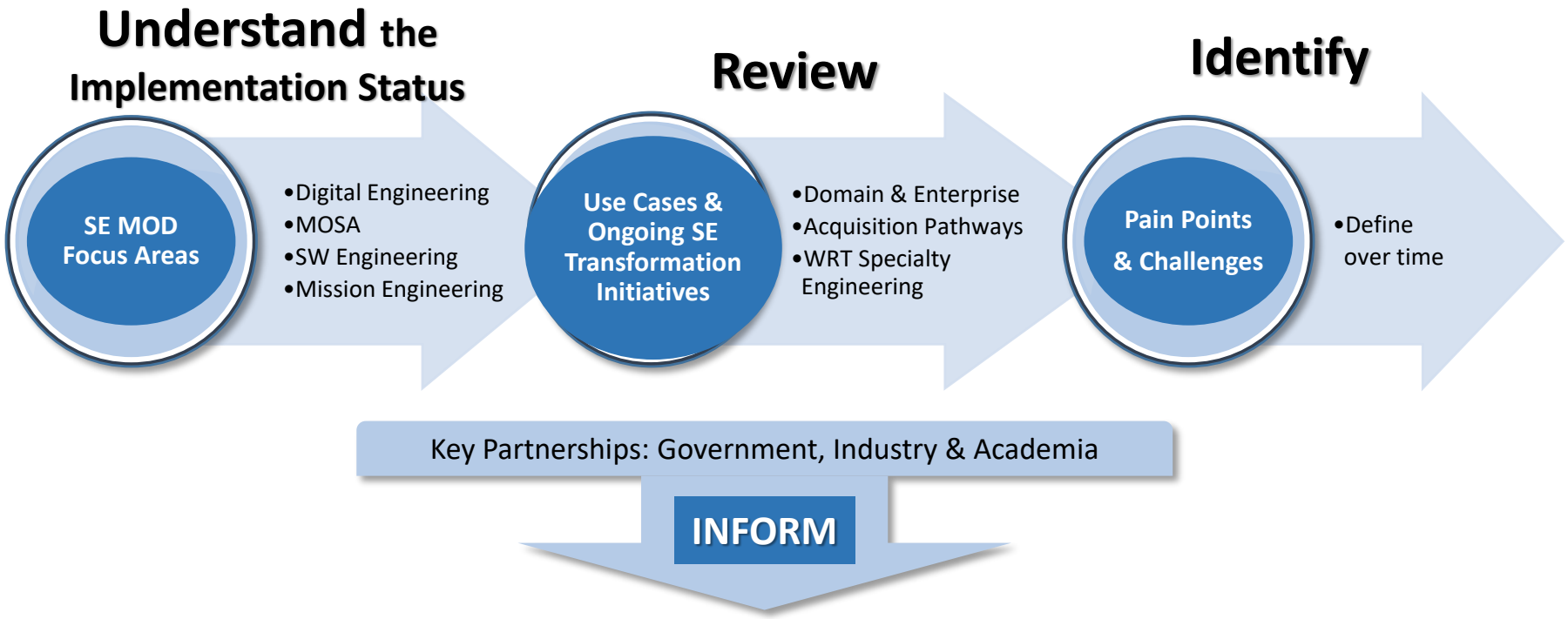
Cross Cutting Key Enablers

Architecture	Modeling Mission & Platform levels, embracing Reference Architectures
Model Based Systems Engineering (MBSE)	Enterprise-wide implementation; models as Source of Truth
SOS/Enterprise Collaboration	Understand/Assess cross-platform capabilities
Engineering Workflow	Evolving SE processes/ techniques, including V&V
Workforce Culture	A focused approach to workforce initiatives that enable culture change

SE Modernization Focus Areas and Key Enablers



SE Modernization Approach



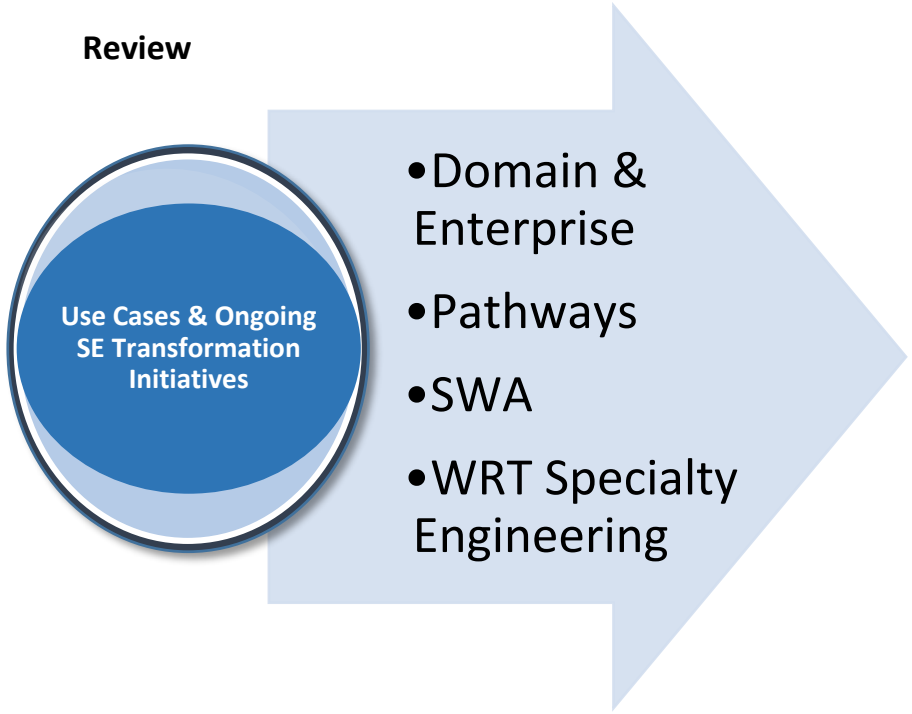
Action

- Best Practices/Lessons Learned/Use Cases
- SE Workforce Roles & Responsibilities
- SE Workforce Training
- Updated SE Guidance/Policy

SE Modernization Lines of Effort

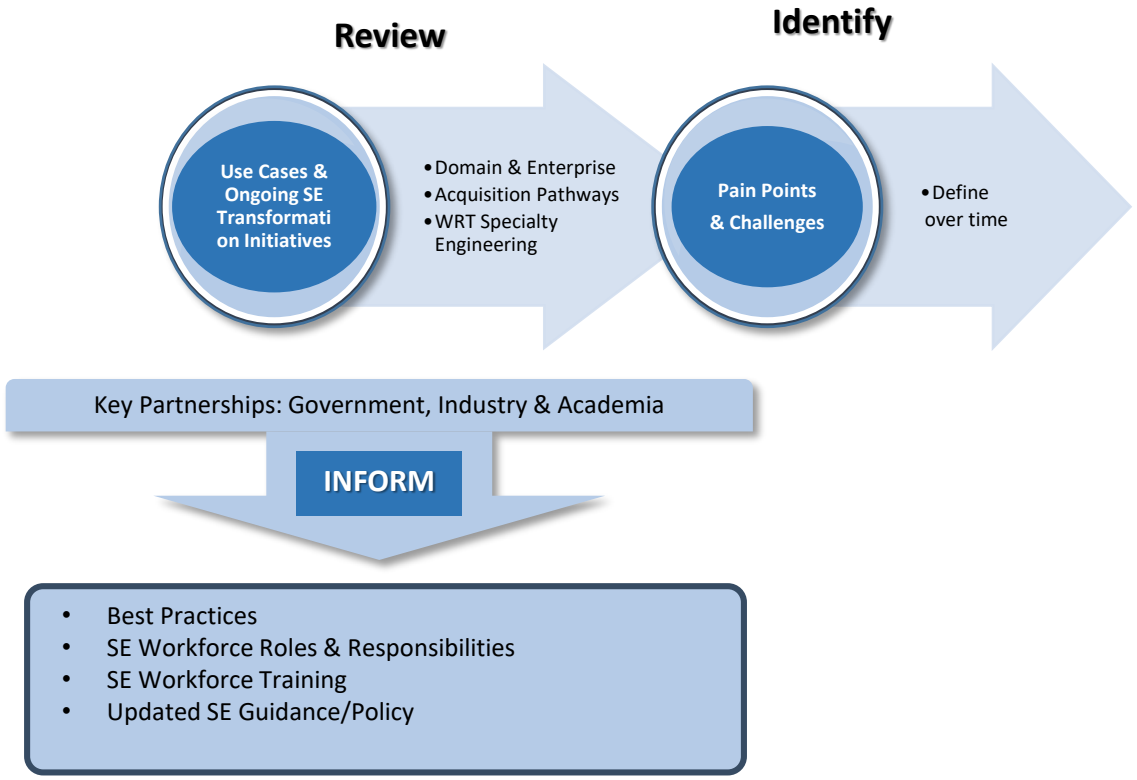
R&E Focus Areas (Synch)	Services/Industry/Academia (Collaborate)	SEMOD Team (Lead)
• BoK/WG • MOSA • Digital Engineering • SW Development (DevSecOps) • Mission Engineering • Workshops	• Information Exchanges • Service Transformation Efforts • NDIA • INCOSE • IEEE (Document Review) • Potential Use Cases	• SEMOD Bok • Emerging Pain Points • PM ToolKit/Workshops • SE Mod Framework • Implementation Roadmaps • Guidance/Policy Updates • Workforce Development Recommendations • SERC SE MOD Tasks

SERC PLANNING (Task 1)



- **Collect data and lessons learned** broadly across the DoD and SE communities
- **Conduct selected deep dives into DoD projects** that are emerging across these focus areas
- **Collect and integrate data** across perspectives
- **Develop initial framework** linking SE Mod areas by information flow

SERC Planning (Task 2)



- **Collect roadmaps and implementation strategies** to determine synergies and knowledge integration opportunities for executing and implementing SE modernization
- **Model best practices and use cases from the initial framework**
- Develop an **information graph** linking information from these sources using a widely available modeling tool
- **Align DoD's SE-related policies and practices** and integrate with specific acquisition pathways
- Iterate a prototype **body of knowledge** that supports selection of guidance from different DoD documents as well as lessons learned from our research and program interviews
- **Review and assess SE workforce roles and responsibilities** to determine workforce development strategies to fill skills gaps

SE Outreach/Information Sessions

- **NDIA SE Division (Industry Partners)**
  - Architecture Committee sensing session July 29
  - SE Division (SED)-facilitated discussion August 18
  - Key SED Industry Engagements in all SE Modernization Focus Areas
    - Modular Open Systems Approach (MOSA): Architecture Committee fully engaged in MOSWG activities
    - Digital Engineering (DE): Modeling & Simulation Committee leading Industry participation in the DE Working Group (DEWG)
    - Mission Engineering (ME): System of Systems (SoS) Committee engaged with Mr. Roman to define Industry's role in ME
    - SW Engineering: Software Committee leading Industry's engagement with R&E

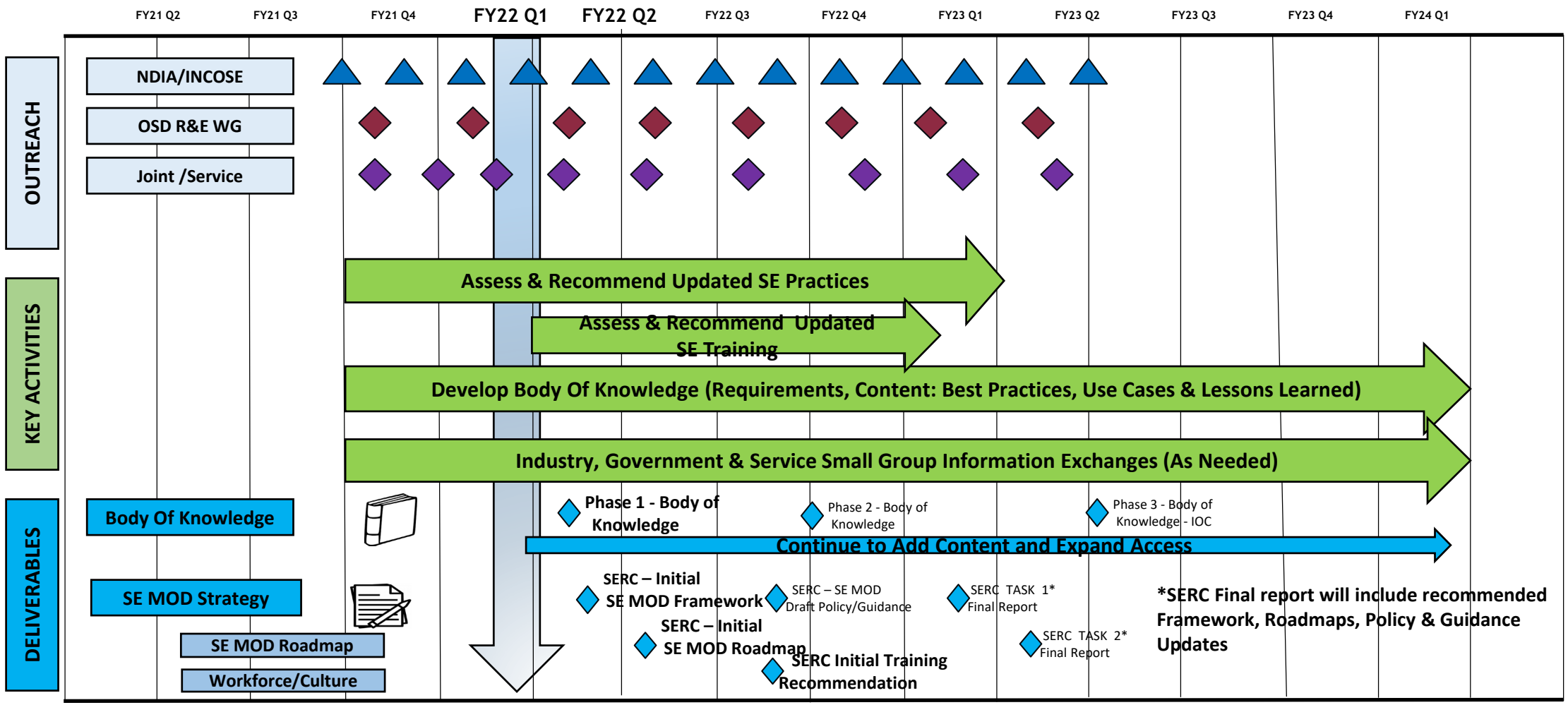
- **INCOSE (SE Practitioners)**
  - Half-day summit on SE Modernization with key INCOSE leaders August 23
  - Key INCOSE efforts reviewed:
    - SE Vision 2035
    - Future of SE (FuSE)
    - Updates to SE guidance documents (ISO/ IEC 15288, INCOSE Handbook)
    - Incremental and Product Line approaches to system development
    - Improvements to SE education

- **Government Joint/Interagency Community**
  - Collaboration/Synch Sessions (NASA, MDA, Interagency WG, Service Transformation Efforts)

SE Modernization Deliverables

- **Draft SE Modernization Strategy** to include recommended:
  - SE Modernization Framework to align SE focus areas
    - Addressing pain points
  - Roadmaps indicating paths to SE modernization
  - Policy and guidance updates
    - Align and integrate into the Acquisition Pathways
  - Workforce strategy
    - Key roles and responsibilities from an integrated perspective
    - Gaps in skills/training
- **SEMOD Body of Knowledge (SEMODBoK)**
    - Best practices integrating SE Modernization Focus Areas
    - Align with the Adaptive Acquisition Framework
    - Use cases
    - Lessons learned
    - Synergy with CRWS/DE BoK

SE MODERNIZATION
Program Objectives and Milestones (POAM)



SE Modernization Pain Points (Emerging)

- **Lack of Digital Processes and Products (Digital Acquisition/E-Program)**
  - "What does a Model Based Technical Assessment look like?"
- **Lack of an Enterprise Approach** to **Integrated** SE Focus Area Implementation
  - DE/MOSA/SW/ME maturing separately
  - Problems with data sharing and collaboration across DoD
  - Digital tools/methods is a critical enabler for SE Modernization
  - Role of Reference Architecture.
- Not enough **Use Cases and Examples of Artifacts** (processes/artifacts not yet mature)
  - "What does a Model Based Program SEP look like?"
- Not enough emphasis on **Ways and Means to Shift Culture**
- **Lack of Metrics** to measure impact of SE implementation success
- Lack of **common understanding between Government and Industry for collaboration and shared artifacts**
  - Maintain company competitive advantage while increasing transparency and collaboration through shared SE artifacts and processes (Related to Data Rights and Intellectual Property)
- **Lack of a Shared Ecosystem**

SE Modernization Next Steps (Through Dec 2021)

- **OUTREACH** - Continue Information Sharing Sessions
  - Review/Assess/Identify Status of SE Focus Areas
  - PM Focused Opportunities (F-35, OMFV, NGI, GBSD, FVL)
  - Refine Problem Statement (As Needed)
  - DoD Modernization Priorities
  - Additional Communities of Interest (AI, Cyber)
- **NDIA Systems and Mission Engineering Conference Briefing (Dec 7, 2021)**
- **Refine Emerging Themes (Pain Points and Key Enablers)**
  - What are the SE Mod Pain Points and Priorities?
  - What are Success Stories?
  - What's in the way of progress?
- **SERC Support Tasks**
  - Coordinate Industry/Government/Academia
  - Synch with ongoing SERC efforts
- **Define/Deploy Initial SEMODBoK Prototype**
  - Refine - Requirements/Content/Location
  - Assess/Leverage existing COPs and BoKs (DEWG, MOSWG, CRWSBoK, DeBoK, INCOSE, NDIA)
- **Support Workforce Development Efforts with DAU and Army Working Group**

SE Modernization Points of Contact

Government Lead

Ms Nadine Geier

Director, SE

nadine.m.Geier.civ@mail.mil

Contractor Support

Dr Kelly D Alexander

Chief Engineer, SE Modernization

kelly.d.alexander12.ctr@mail.mil

Mr Ed Moshinsky

SE Modernization

edward.a.moshinsky.ctr@mail.mil

Mr Thomas McDermott

SERC Team Lead

tmcdermo@stevens.edu

Contact

Office of the Deputy Director for Engineering

osd.r-e.comm@mail.mil

Attention: Systems Engineering Modernization

ac.cto.mil/engineering

Headquarters U.S. Air Force

Integrity - Service - Excellence

USAF Work on Weapon System Government Reference Architectures

Presented By: Robert Bond
AFMC/ENS
December 2021

U.S. AIR FORCE

U.S. AIR FORCE

Overview

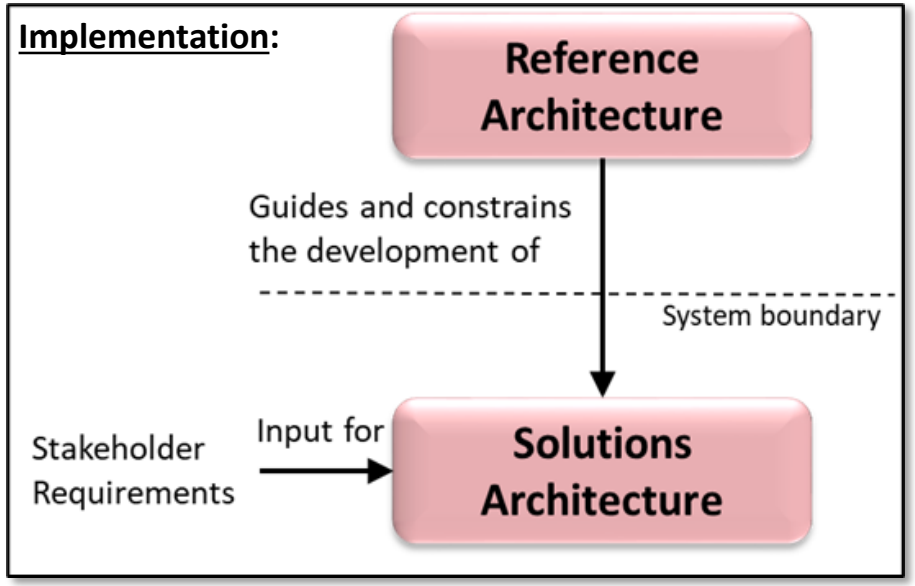
BLUF: The AF is working to develop a Weapon System Government Reference Architecture (GRA) Strategy to reduce waste from duplicative efforts

- **High Level Definitions - Difference Between Reference & Solution Architectures**
- **Example of Multiple Reference Architectures Working Together**
- **How Standards Relate to Reference Architectures**
- **USAF GRA & Standards Catalog**
- **How Models Relate to Architectures**
- **Future Work for Air Force GRA Governance**

U.S. AIR FORCE

GRA Term Clarity

- RA: An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions[1,2]
- GRA: Government-owned, authoritative source of information about a specific subject area that guides and constrains the instantiations of capability architectures and solutions[2]
- Per the Mission Eng Guide a GRA: integrates the data, information, boundary conditions and rules that describe the mission capability needed by the warfighter in sufficient detail to allow for transition of technology-based solutions



Reference Architecture Purpose[3]

[1]DoD Reference Architecture Description, June 2010

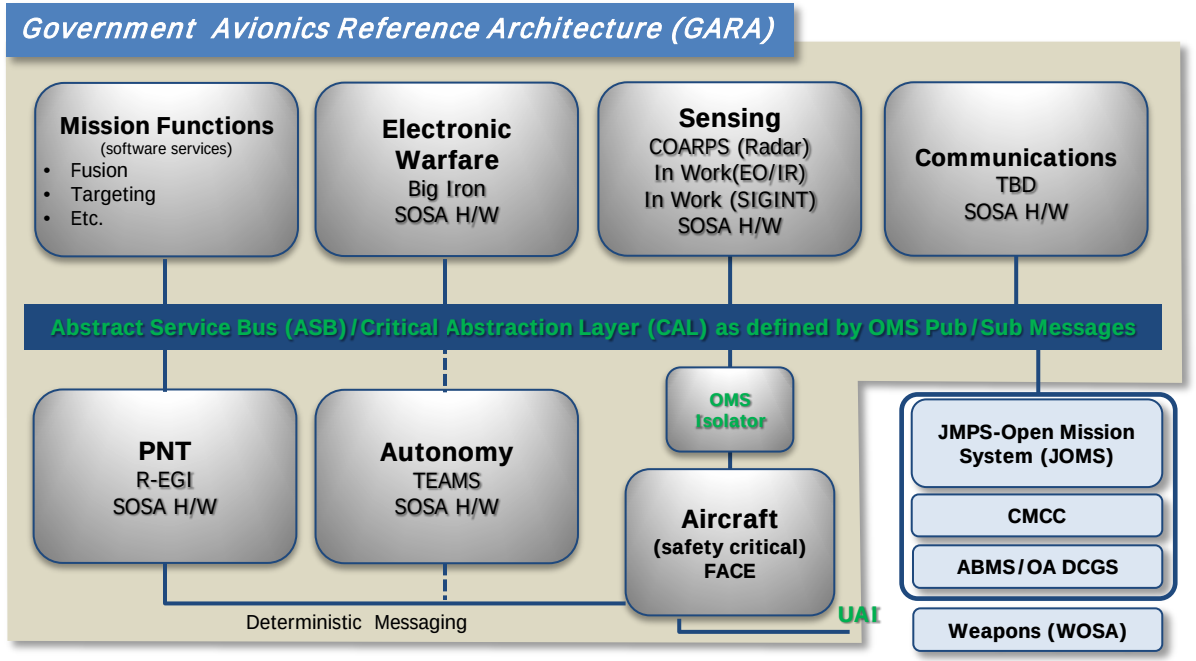
[2]Mission Engineering Guide, November 2020

[3]DoD Reference Architecture Purpose June 2010

Example Case of a GRA for USAF Avionics

U.S. AIR FORCE

Standards
OMS/UCI
Universal Armament Interface (UAI)
Sensor Open Systems Architecture (SOSA)
Common Open Architecture Radar Program Specification (COARPS)
Resilient – Embedded GPS/INS (R-EGI)
Big Iron
Teaming-Enabled Arch for Manned-Unmanned Systems (TEAMS)
Future Airborne Capabilities Environment (FACE)



- **GRAs are not full implementations; they help *guide and constrain* designs**
- **Multiple Standards are combined in this GRA to create a holistic Avionics Picture**
- **Program Offices can take advantage of parts or all of a GRA to suit their specific needs**
- **Models of the GRA enable clearer industry-government communications**

U.S. AIR FORCE

Standards & Architectures

Interface Management:
The functional and physical characteristics required to exist at a common boundary or connection between persons, between systems, or between persons and systems. A system external to the system being analyzed that provides a common boundary or service that is necessary for the other system to perform its mission in an undegraded mode, e.g., a system that supplies power, cooling, heating, air services, or input signals – DAU Glossary

Standards:

Standards documents can serve as Interface Management Reference Architecture elements

Open Architecture Standards:

Help provide common interface management techniques for certain architectural areas (usually targeted to specific domains and/or functional areas

Standards are elements included in Reference Architectures

U.S. AIR FORCE

USAF GRA & Standards Catalog

- **The Air Force has developed an initial Catalog of Standards and Reference Architectures on the "Digital Guide" website. https://wss.apan.org/af/aflcmc/default.aspx**

- **We track GRA's, Standards Containing Interface Management Elements, and Standards Containing Reference Architecture and Interface Management Elements**

- **This Body of Knowledge allows Programs to understand the various efforts available across the Department of the Air Force**

U.S. AIR FORCE

How Do GRA's and Models Relate

- **Models are defined as "A representation of an actual or conceptual system that involves mathematics, logical expressions, or computer simulations that can be used to predict how the system might perform or survive under various conditions or in a range of hostile environments" – DAU Glossary**

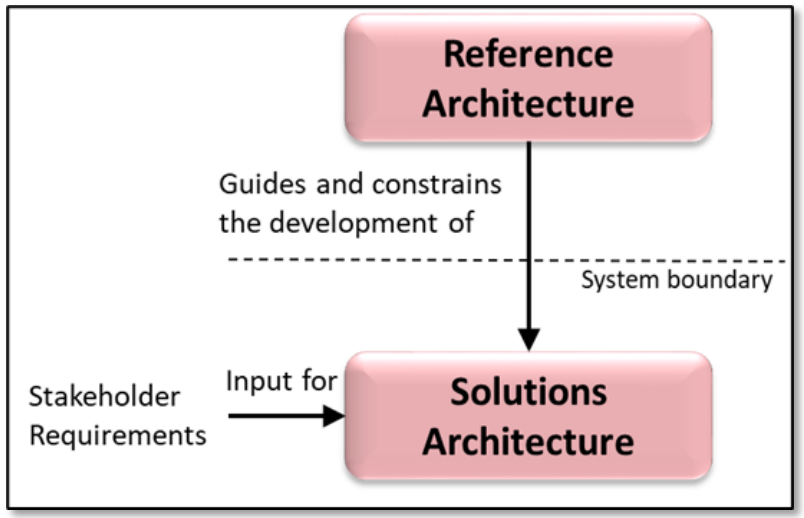
- **Architectures can be represented by models (and that is the desired end state as part of the USAF and USSF Digital Transformation)**

- **A Government Reference Model is a GRA provided as an output of a Modeling Tool. At this point the terms become synonymous**

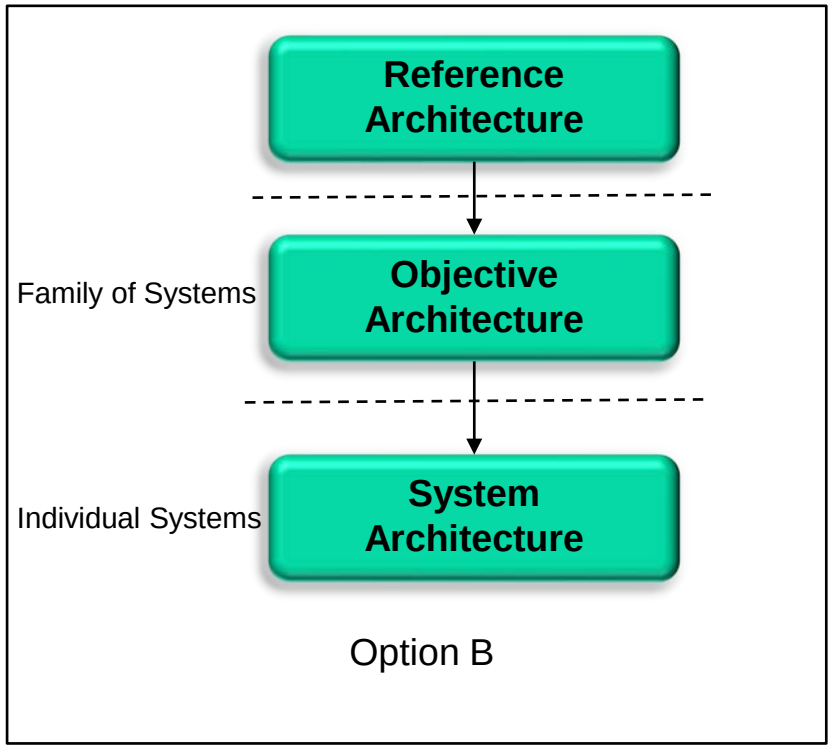
U.S. AIR FORCE

Side by Side Architecture Decomposition

- **The Digital Campaign has not settled on one architectural decomposition technique. Currently Program Offices are using the Terms, Program Architecture, or System Architecture in place of the term Solution Architecture**



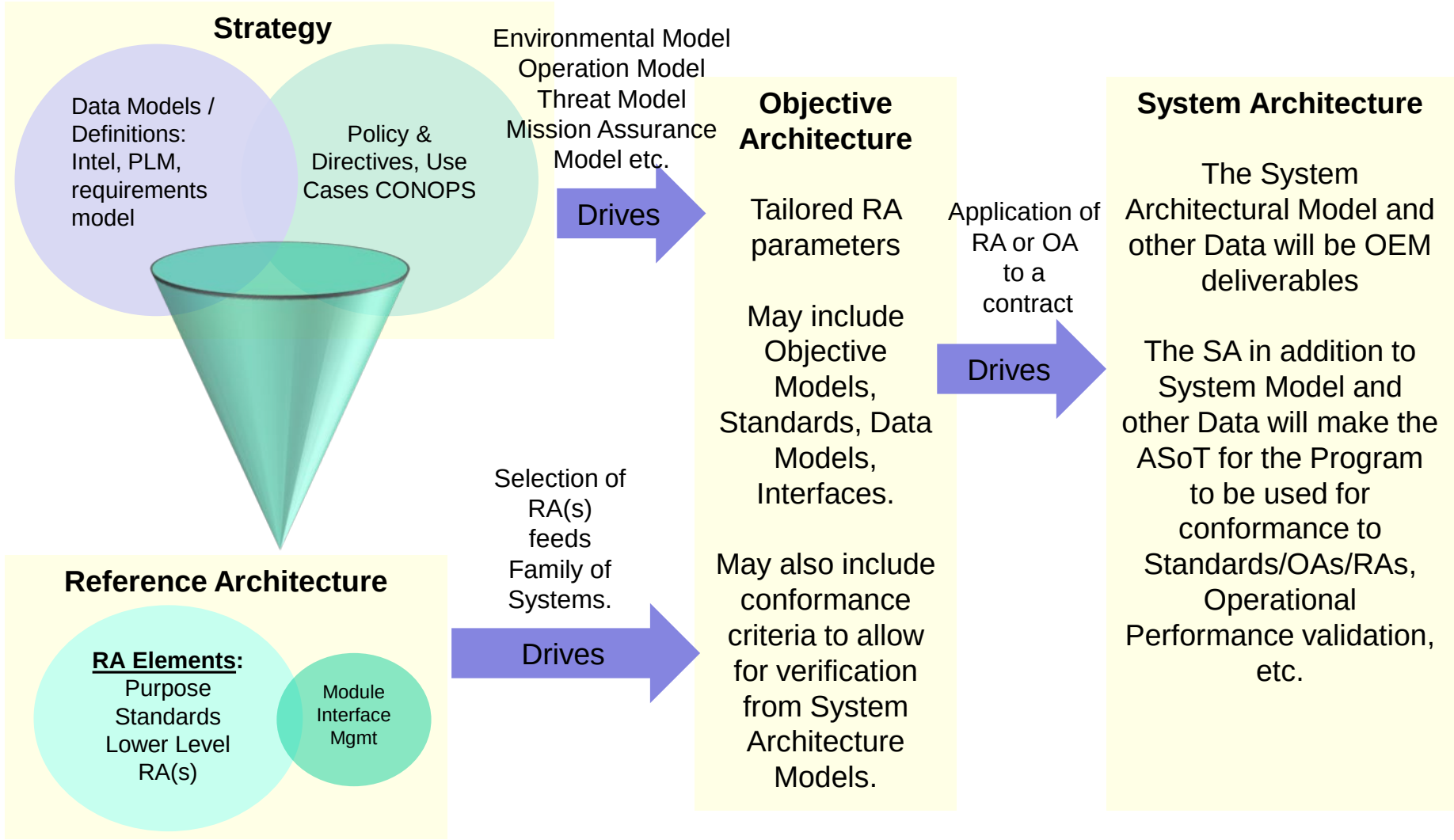
Option A



Option B

U.S. AIR FORCE

3 Layer View



U.S. AIR FORCE

Future Work for GRA Governance

- GRA development in the AF has been bottoms up, so governance structures are being explored
- Possible Courses of Action for improving GRA governance:
  - An Architecture Review Board Structure
  - Engineering Senior Leadership works in conjunction with the Directors of Engineering and execution organizations like the Open Architecture Management Office
  - Air Force Materiel Command Centers, and Space Program Executive Agents act as GRA Governance Board
  - Formal governance board established in conjunction with Digital Transformation Office

Questions?

Engineer Your Competitive Advantage

Feature-based Product Line Engineering in Aerospace and Defense

NDIA 2021 Virtual Systems & Mission Engineering Conference
December 6-8, 2021

Paul Clements, PhD, VP of Customer Success
Charles Krueger, PhD, CEO
BigLever

onePLE

ISO/IEC 26580

- On April 20, 2021, it became official:
  - ISO/IEC 26580, “Methods and Tools for the Feature-based Approach to Software and Systems Product Line Engineering”, was published as an international standard
  - https://www.iso.org/standard/43139.html
- For the aerospace and defense industry:
  - this powerful engineering approach, created to deliver unprecedented cost avoidance and quality, can now be readily and unambiguously mandated in RFPs and contracts,
  - which can then be unambiguously provided by contractors,
  - leveraging 26580 as the authoritative definition from the international engineering community

Business Context for PLE: Variation is the #1 driver of complexity

- *"The top driver of operational complexity in complex engineering organizations,* as identified by surveys of hundreds of business leaders, *is the number of product and system configurations engineered, manufactured, deployed, and sustained*."
  - Michelle Boucher, VP of Research for Engineering Practices at Tech-Clarity, an independent research and analyst firm. Michelle has spent over 20 years in various roles in engineering, marketing, management, and as an analyst. She has benchmarked over 7000 product development professionals and published over 90 reports on product development best practices. She focuses on helping companies manage the complexity of today's products, markets, design environments, and value chains to achieve higher profitability.
  - Source: "Why Should Business Leaders Care About PLE?," Momentum 2021 presentation, May 2021.
  - https://tech-clarity.com/about/michelle-boucher

Engineering Advancement from Early Generation Approaches

Independent Development
Systems are engineered independently, without taking advantage of commonality. No reuse or sharing.

Branch-and-Merge
Each new system created by branching from of a similar system. Maintenance attempts reuse by manual N² monitor for opportunities to merge across branches.

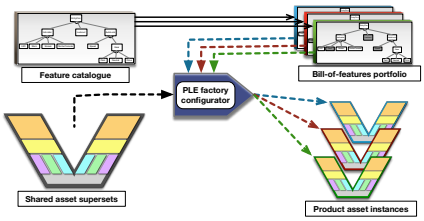
Discipline-centric Var Mgmt
Variation management techniques in a tool or discipline enable sharing and potential automation in one discipline, but results in silos and dissonance across other tools and disciplines.

Clone-and-Own
Each new system created by cloning a copy of a similar system, and then maintaining independently. 100% reuse on day one. 0% reuse and sharing every day thereafter.

Reuse Repository
Collection of assets are put into a repository for reuse by others. Engineers search repository in hopes of finding assets to clone-and-own. Opportunistic and ad hoc reuse, with no sharing.

1st Generation PLE
Collection of "core assets" in a repository for manual clone-and-own reuse within the product line. Strategic reuse, with no automation or sharing.

Early Generation Product Line Approaches



Feature-based Product Line Engineering

Product Line Engineering (PLE) Defined

ISO 26580 Methods and Tools for Feature-based PLE

Product Line:

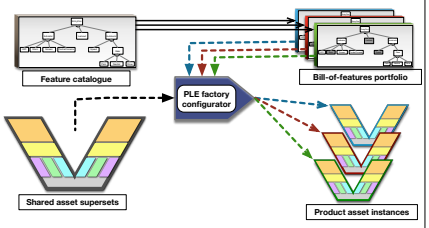
A family of similar products or systems with variations in features.

Product lines are ubiquitous — virtually all products and systems are built in the context of a family.

International Organization for Standardization

Product Line Engineering:

the engineering of a product line using
shared engineering assets,
a *managed catalog of features*, and
an *automated means of production*…



- taking advantage of the **commonality** shared across the family
- efficiently and systematically managing the **variation** among the products or systems

Feature-based Product Line Engineering

ISO 26580 Methods and Tools for Feature-based PLE

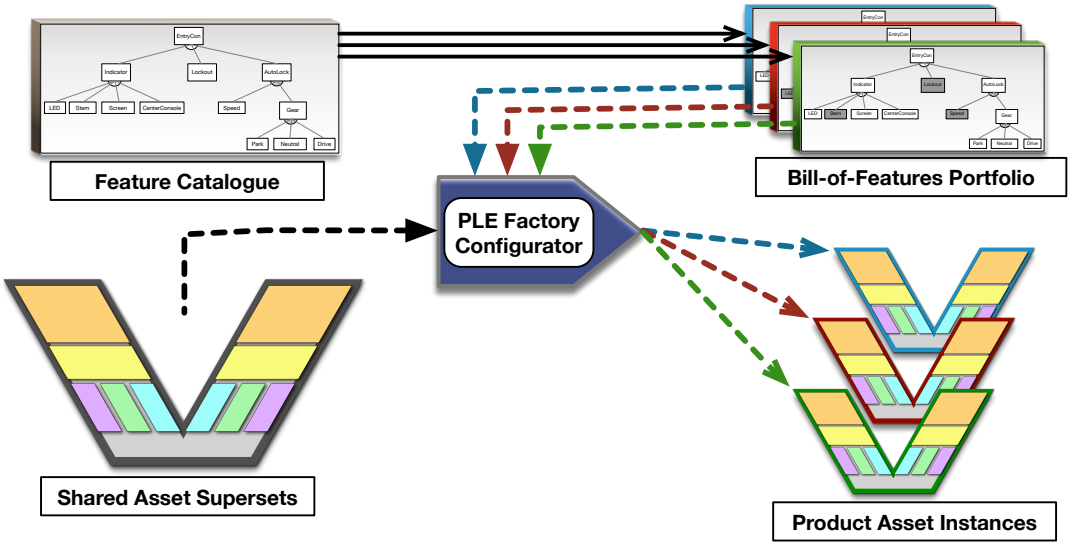


Figure from ISO/IEC 26580
Copyright © ISO/IEC 2021
https://www.iso.org/standard/43139.html

The ISO/IEC 26580 standard is new, but Feature-based PLE is not

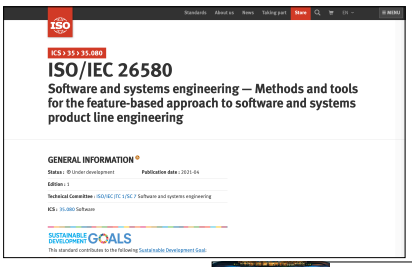
- Although the standard has just been finalized, Feature-based PLE has been in commercial practice in the A&D sector for nearly two decades
  - compiling hundreds of millions of dollars in cost avoidance each and every year
- The approach is being adopted or is already in widespread use by most of the top ten US defense contractors
- Feature-based PLE has earned its stripes by rising to the practicalities and hard challenges that are emblematic of the A&D sector

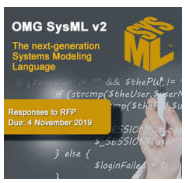
LOCKHEED MARTIN	GENERAL DYNAMICS	gm	Raytheon Technologies	GE Aviation
AEGIS Weapon System for US and International Navies	Live Training Transformation: US Army, Air Force, Marines. Plus enterprise initiative.	One of the largest and most complex product lines, comprising millions of instances per year	Rapidly growing and evolving portfolio of the world's most advanced missile systems	Helicopter engines for all configurations of the new US Army Future Vertical Lift (FVL) program
High cost of old approach threatened loss of entire contract	Innovative low-cost solution essential to win and retain major contracts	Significant challenges to provide suppliers with a family of complex specs for electronic controller unit families	Traditional methods of creating and testing prototypes are too slow, imprecise, expensive to meet mission demands	Demand to maximize sharing and reuse to prevent multiplicative costs for flight certification
Feature-based PLE Results with BigLever				
Turned an at-risk program into an enthusiastic long-term relationship by eliminating low-value redundant effort	**Grew a $2B+ business from scratch with the US DoD. Delivering 3x more capability within budget, to the delight of the customer**	**Digital transformation to a digital supply chain by applying PLE to MBSE**	**Using Feature-based PLE to proliferate best candidate simulations to find optimal solution within a trade space**	**Using a single Feature-based PLE Factory with a single collection of shared engineering assets for the full engineering lifecycle**

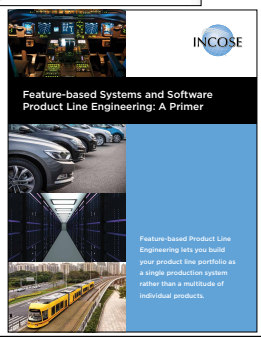
“Change is good. You go first.”

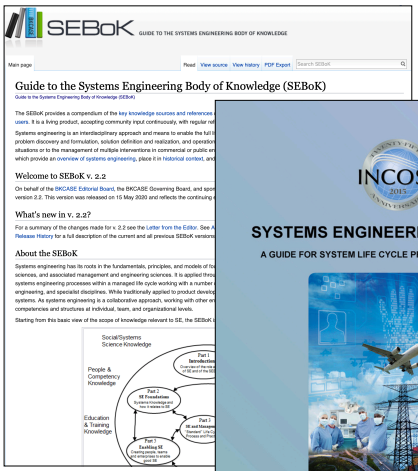
- When it comes to Organizational Change, technology is easy and people are hard
- “Feature-based PLE sounds great, but we’re different — it won’t work here…”
- Engineering organizations are justifiably risk-averse

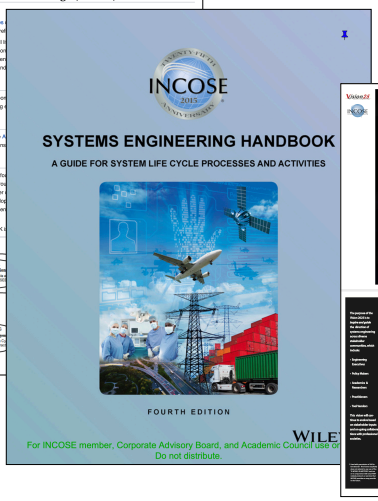
Lowering the risk of organizational change by elevating Product Line Engineering to a standard practice in the industry





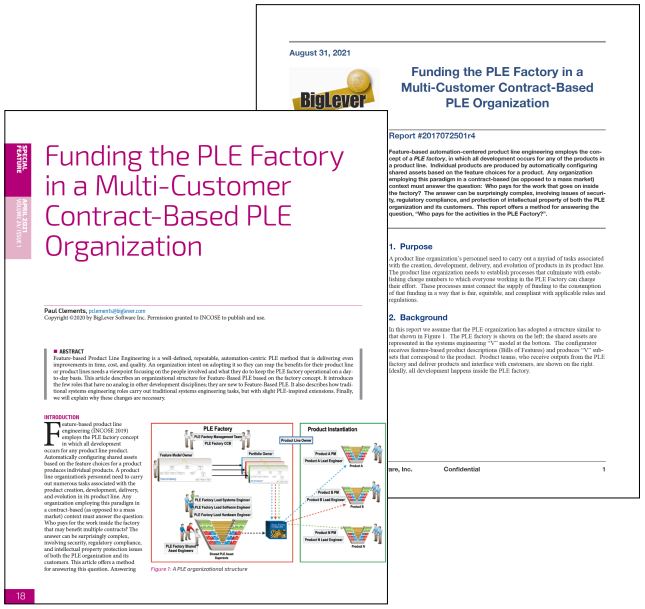






Feature-based PLE in a multi-contract funding context

- In A&D, sharing often needs to occur across programs, contracts, and customers.
- Can that happen? It can.
- Defense companies have worked out methods to pay for activities that benefit more than one program, using an approach that is compliant with acquisition regulations.



August 31, 2021

BigLever

Funding the PLE Factory in a Multi-Customer Contract-Based PLE Organization

Report #2017072501r4

Feature-based automation-centered product line engineering employs the concept of a *PLE factory*, in which all development occurs for any of the products in a product line. Individual products are produced by automatically configuring shared assets based on the feature choices for a product. Any organization employing this paradigm in a contract-based (as opposed to a mass market) context must answer the question: Who pays for the work that goes on inside the factory? The answer can be surprisingly complex, involving issues of security, regulatory compliance, and protection of intellectual property of both the PLE organization and its customers. This report offers a method for answering the question, "Who pays for the activities in the PLE Factory?".

1. Purpose

A product line organization's personnel need to carry out a myriad of tasks associated with the creation, development, delivery, and evolution of products in its product line. The product line organization needs to establish processes that culminate with establishing change numbers to which everyone working in the PLE Factory can charge their effort. These processes must connect the supply of funding to the consumption of that funding in a way that is fair, equitable, and compliant with applicable rules and regulations.

2. Background

In this report we assume that the PLE organization has adopted a structure similar to that shown in Figure 1. The PLE factory is shown on the left; the shared assets are represented in the systems engineering "V" model at the bottom. The configurator receives feature-based product descriptions (Bills of Features) and produces "V" subsets that correspond to the product. Product teams, who receive outputs from the PLE factory and deliver products and interface with customers, are shown on the right. Ideally, all development happens inside the PLE factory.

Confidential 1

SPECIAL FEATURE

Funding the PLE Factory in a Multi-Customer Contract-Based PLE Organization

Paul Clements, pclements@biglever.com

Copyright ©2020 by BigLever Software Inc. Permission granted to INCOSE to publish and use.

ABSTRACT

Feature-based Product Line Engineering is a well-defined, repeatable, automation-centric PLE method that is delivering even improvements in time, cost, and quality. An organization intent on adopting it so they can reap the benefits for their product line or product lines needs a viewpoint focusing on the people involved and what they do to keep the PLE factory operational on a day-to-day basis. This article describes an organizational structure for Feature-Based PLE based on the factory concept. It introduces the few roles that have no analog in other development disciplines; they are new to Feature-Based PLE. It also describes how traditional systems engineering roles carry out traditional systems engineering tasks, but with slight PLE-inspired extensions. Finally, we will explain why these changes are necessary.

INTRODUCTION

Feature-based product line engineering (INCOSE 2019) employs the PLE factory concept in which all development occurs for any product line product. Automatically configuring shared assets based on the feature choices for a product produces individual products. A product line organization's personnel need to carry out numerous tasks associated with the product creation, development, delivery, and evolution in its product line. Any organization employing this paradigm in a contract-based (as opposed to a mass market) context must answer the question: Who pays for the work inside the factory that may benefit multiple contracts? The answer can be surprisingly complex, involving issues of security, compliance, and intellectual property protection issues of both the PLE organization and its customers. This article offers a method for answering this question. Answering

PLE Factory

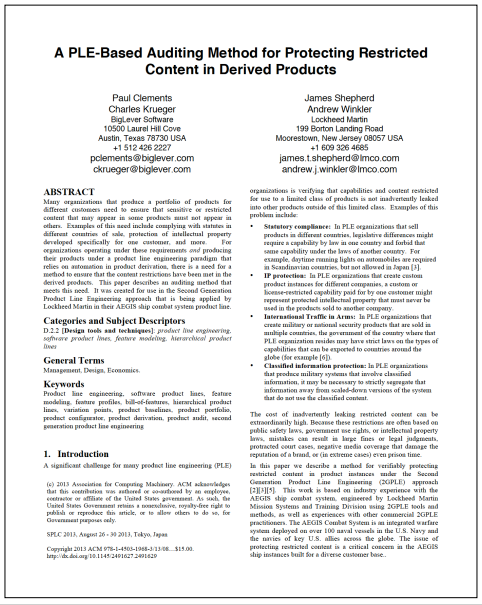
Product Instantiation

Figure 1: A PLE organizational structure

18

Feature-based PLE and export control compliance

- A product line may have members destined for sale in countries where ITAR or export control restrictions apply.
- Lockheed Martin pioneered a PLE method to ensure that no product contains any content that is not allowed to be exported.



A PLE-Based Auditing Method for Protecting Restricted Content in Derived Products

Paul Clements
Charles Krueger
BigLever Software
10500 Laurel Hill Cove
Austin, Texas 78730 USA
+1 512 426 2227
pclements@biglever.com
ckrueger@biglever.com

James Shepherd
Andrew Winkler
Lockheed Martin
199 Borton Landing Road
Moorestown, New Jersey 08057 USA
+1 609 326 4665
james.t.shepherd@lmco.com
andrew.j.winkler@lmco.com

ABSTRACT

Many organizations that produce a portfolio of products for different customers need to ensure that sensitive or restricted content that may appear in some products must not appear in others. Examples of this need include complying with statutes in different countries of sale, protection of intellectual property developed specifically for one customer, and more. For organizations operating under these requirements *and* producing their products under a product line engineering paradigm that relies on automation in product derivation, there is a need for a method to ensure that the content restrictions have been met in the derived products. This paper describes an auditing method that meets this need. It was created for use in the Second Generation Product Line Engineering approach that is being applied by Lockheed Martin in their AEGIS ship combat system product line.

Categories and Subject Descriptors

D.2.2 [**Design tools and techniques**]: *product line engineering, software product lines, feature modeling, hierarchical product lines*

General Terms

Management, Design, Economics.

Keywords

Product line engineering, software product lines, feature modeling, feature profiles, bill-of-features, hierarchical product lines, variation points, product baselines, product portfolio, product configurator, product derivation, product audit, second generation product line engineering

1. Introduction

A significant challenge for many product line engineering (PLE) organizations is verifying that capabilities and content restricted for use to a limited class of products is not inadvertently leaked into other products outside of this limited class. Examples of this problem include:

- **Statutory compliance:** In PLE organizations that sell products in different countries, legislative differences might require a capability by law in one country and forbid that same capability under the laws of another country. For example, daytime running lights on automobiles are required in Scandinavian countries, but not allowed in Japan [3].
- **IP protection:** In PLE organizations that create custom product instances for different companies, a custom or license-restricted capability paid for by one customer might represent protected intellectual property that must never be used in the products sold to another company.
- **International Traffic in Arms:** In PLE organizations that create military or national security products that are sold in multiple countries, the government of the country where that PLE organization resides may have strict laws on the types of capabilities that can be exported to countries around the globe (for example [6]).
- **Classified information protection:** In PLE organizations that produce military systems that involve classified information, it may be necessary to strictly segregate that information away from scaled-down versions of the system that do not use the classified content.

The cost of inadvertently leaking restricted content can be extraordinarily high. Because these restrictions are often based on public safety laws, government use rights, or intellectual property laws, mistakes can result in large fines or legal judgments, protracted court cases, negative media coverage that damage the reputation of a brand, or (in extreme cases) even prison time.

In this paper we describe a method for verifiably protecting restricted content in product instances under the Second Generation Product Line Engineering (2GPLE) approach [2][3][5]. This work is based on industry experience with the AEGIS ship combat system, engineered by Lockheed Martin Mission Systems and Training Division using 2GPLE tools and methods, as well as experiences with other commercial 2GPLE practitioners. The AEGIS Combat System is an integrated warfare system deployed on over 100 naval vessels in the U.S. Navy and the navies of key U.S. allies across the globe. The issue of protecting restricted content is a critical concern in the AEGIS ship instances built for a diverse customer base..

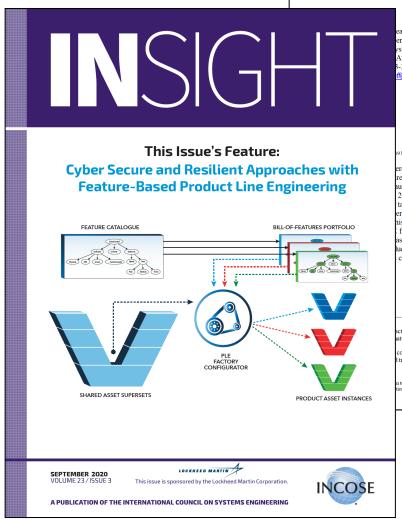
(c) 2013 Association for Computing Machinery. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the United States Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

SPLC 2013, August 26 - 30 2013, Tokyo, Japan

Copyright 2013 ACM 978-1-4503-1968-3/13/08...$15.00.
http://dx.doi.org/10.1145/2491627.2491629

Feature-based PLE in security-intensive settings

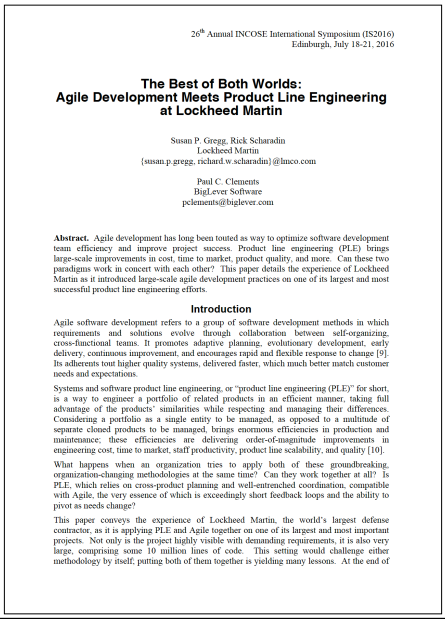
- Can PLE work in a case where some of the products' content is classified, or classified at higher levels, than other parts?
- Raytheon and General Dynamics have written about an effective approach to apply PLE in secure environments and in conjunction with System Security Engineering.




Applying Feature-Based Systems and Software Product Line Engineering in Unclassified and Classified Environments

Feature-based PLE and Agile

- As DoD follows industry trends in Agile development, can Feature-based PLE play effectively in these arenas?
- PLE is not applied in isolation.
- Raytheon, Lockheed Martin, General Dynamics, and (for good measure) General Motors have all shared their experience, which amounts to a resounding "yes."


26th Annual INCOSE International Symposium (IS2016)
Edinburgh, July 18-21, 2016

The Best of Both Worlds: Agile Development Meets Product Line Engineering at Lockheed Martin

Susan P. Gregg, Rick Scharadin
Lockheed Martin
{susan.p.gregg, richard.w.scharadin}@lmco.com

Paul C. Clements
BigLever Software
pclements@biglever.com

Abstract. Agile development has long been touted as way to optimize software development team efficiency and improve project success. Product line engineering (PLE) brings large-scale improvements in cost, time to market, product quality, and more. Can these two paradigms work in concert with each other? This paper details the experience of Lockheed Martin as it introduced large-scale agile development practices on one of its largest and most successful product line engineering efforts.

Introduction

Agile software development refers to a group of software development methods in which requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change [9]. Its adherents tout higher quality systems, delivered faster, which much better match customer needs and expectations.

Systems and software product line engineering, or "product line engineering (PLE)" for short, is a way to engineer a portfolio of related products in an efficient manner, taking full advantage of the products' similarities while respecting and managing their differences. Considering a portfolio as a single entity to be managed, as opposed to a multitude of separate cloned products to be managed, brings enormous efficiencies in production and maintenance; these efficiencies are delivering order-of-magnitude improvements in engineering cost, time to market, staff productivity, product line scalability, and quality [10].

What happens when an organization tries to apply both of these groundbreaking, organization-changing methodologies at the same time? Can they work together at all? Is PLE, which relies on cross-product planning and well-entrenched coordination, compatible with Agile, the very essence of which is exceedingly short feedback loops and the ability to pivot as needs change?

This paper conveys the experience of Lockheed Martin, the world's largest defense contractor, as it is applying PLE and Agile together on one of its largest and most important projects. Not only is the project highly visible with demanding requirements, it is also very large, comprising some 10 million lines of code. This setting would challenge either methodology by itself; putting both of them together is yielding many lessons. At the end of

Feature-based PLE and Digital Engineering / Model-Based Engineering

- As DoD leads industry trends by mandating advanced digital engineering and model-based approaches, Feature-based PLE becomes critical.
  - "Nobody builds just one"
  - Early generation product line engineering approaches are intractable for digital engineering
- Raytheon, Lockheed Martin, General Dynamics, and (for good measure) General Motors have all shared their experiences.

Product Line Engineering Meets Model Based Engineering in the Defense and Automotive Industries

How Missile Engineering is Taking Product Line Engineering to the Extreme at Raytheon

Model Based Engineering and Product Line Engineering: Combining Two Powerful Approaches at Raytheon

Feature-based PLE in a V&V-intensive environment

- Few sectors come close to A&D in terms of the cost required to validate systems.
- Aerospace companies have reported up to 8-fold improvements in the time to generate a certification package, cutting the time from weeks to days.
- Lockheed Martin reports that V&V can in many cases be shared among multiple members of a product line, saving significant time and money.

Product Line Engineering on the Right Side of the "V"

Summary

- The release of ISO/IEC 26580 is good news for the systems engineering community in general, and A&D in particular
  - Can be readily and unambiguously mandated in RFPs and contracts
  - Can be readily and unambiguously applied by contractors in their proposals and deliverables
- The better news is that Feature-based PLE does not need a break-in period for A&D to learn the ropes
  - It's been here all along, and continues to be ready to serve

Systems of Systems & Complexity
INCOSE SoS Working Group Initiative

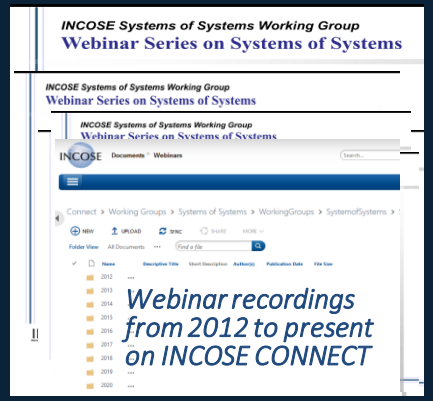
Dr. Judith Dahmann

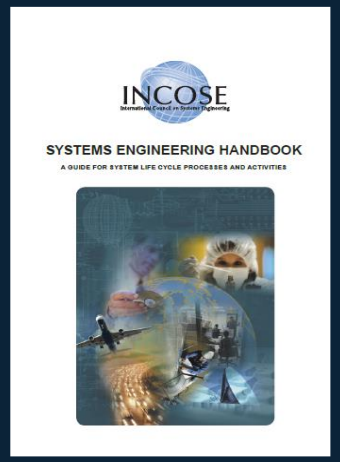
December 2021

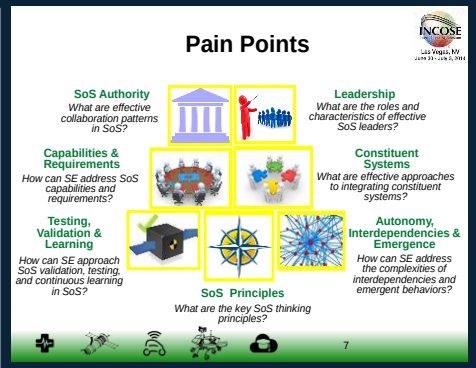
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

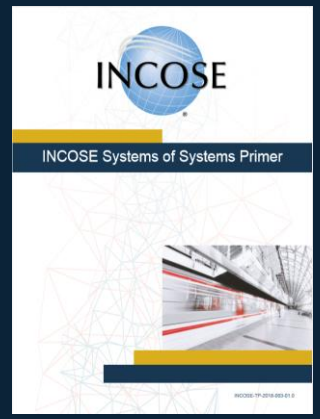
Approved for public release. Distribution unlimited 21-02348-3

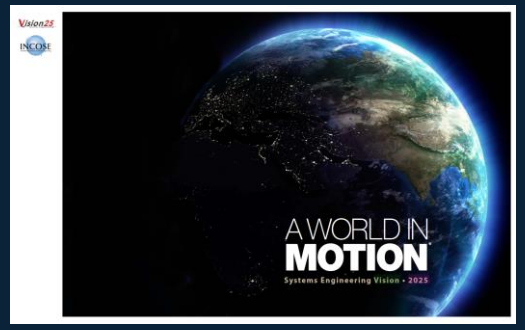
INCOSE Systems of Systems Working Group

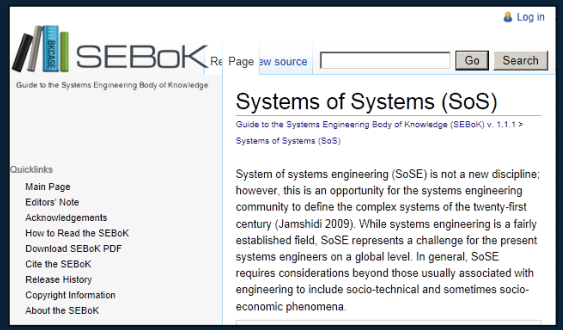








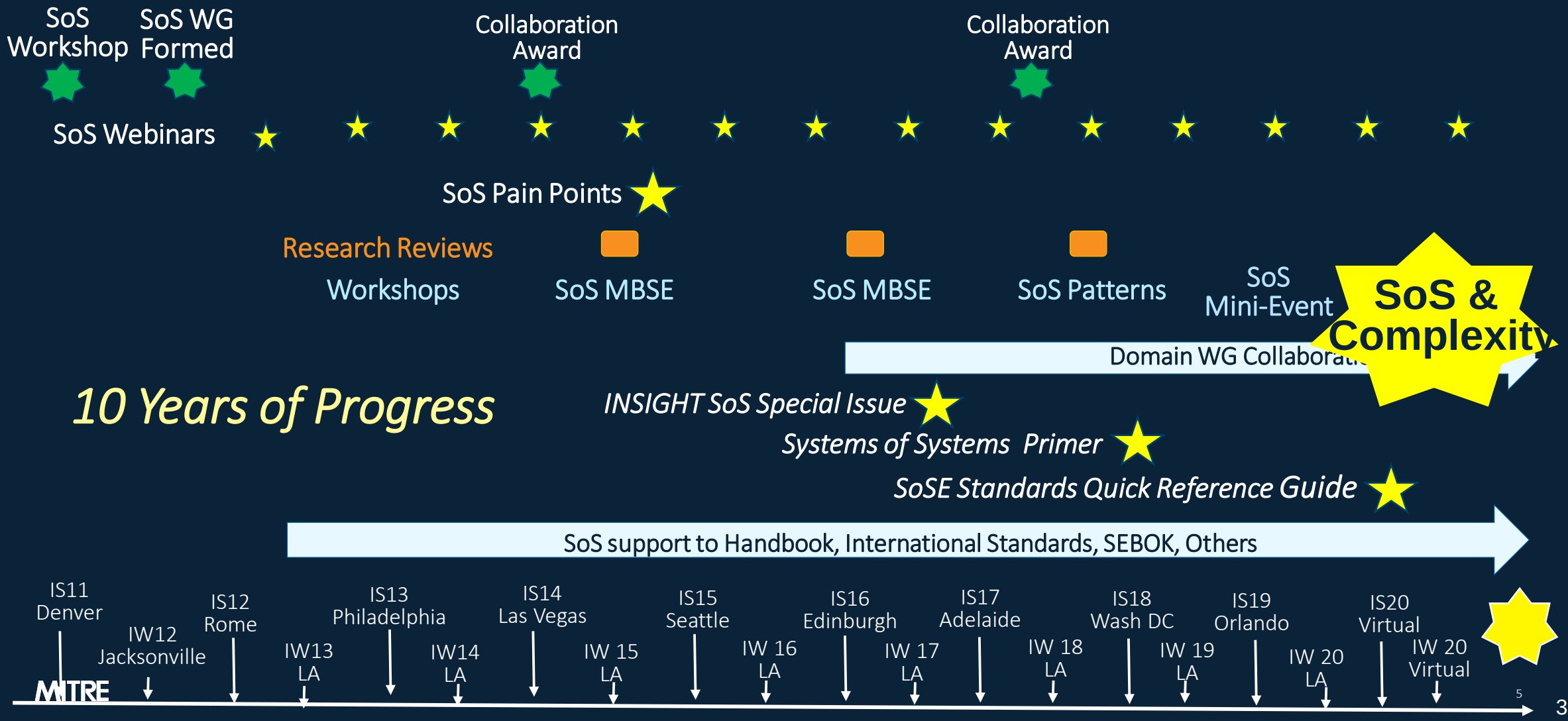




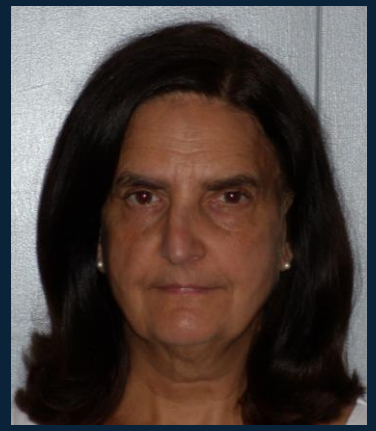
INCOSE

MITRE

SoS Working Group Activities in Review

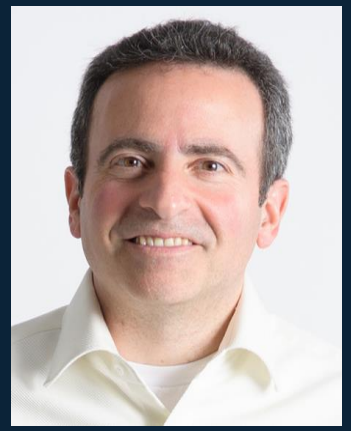


Systems of Systems & Complexity Project Core Team



Judith Dahmann

Eric Honour



Dan DeLaurentis

Ali Raz

Stephen Cook

INCOSE

MITRE

Systems of Systems and Complexity

"emergence is noted as a common characteristic of SoS particularly in SoS composed of multiple large existing systems, based on the challenge (in time and resources) of subjecting all possible logical threads across the myriad functions, capabilities, and data of the systems in an SoS.

…. there are risks associated with unexpected or unintended behavior resulting from combining systems that have individually complex behavior. These become serious in cases which safety, for example, is threatened through unintended interactions among the functions provided by multiple constituent systems in a SoS."

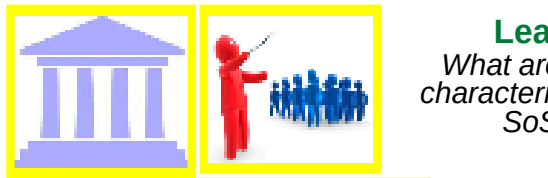
https://www.sebokwiki.org/wiki/Systems_of_Systems_(SoS)

INCOSE

MITRE

SoS Complexity

Pain Points



SoS Authority
What are effective collaboration patterns in SoS?

Leadership
What are the roles and characteristics of effective SoS leaders?

Capabilities & Requirements
How can SE address SoS capabilities and requirements?

Constituent Systems
What are effective approaches to integrating constituent systems?

Testing, Validation & Learning
How can SE approach SoS validation, testing, and continuous learning in SoS?

Autonom /, Interdepender cies & Emergen e
How can SE ac dress the complexiti s of interdependenci s and emergent beha iors?

SoS Pr nciples
What are the key SoS thinking principles?

7

Taming Complexity:
A System of Systems Challenge

Complex Adaptive Systems Conference

Baltimore, MD
November 2011

Sources of SoS Complexity

- Systems
- Users/stakeholders
- Development
- Operations

Technical Complexity Across Systems

Diversity in system concept, design, control structures, data syntax, semantics…..

User/Stakeholder Complexity

Independent system owners and stakeholders with their own goals, objectives, motivations……

SoS Development Complexity

Dynamics of asynchronous development

Taming Complexity:
A System of Systems Challenge

Complex Adaptive Systems Conference

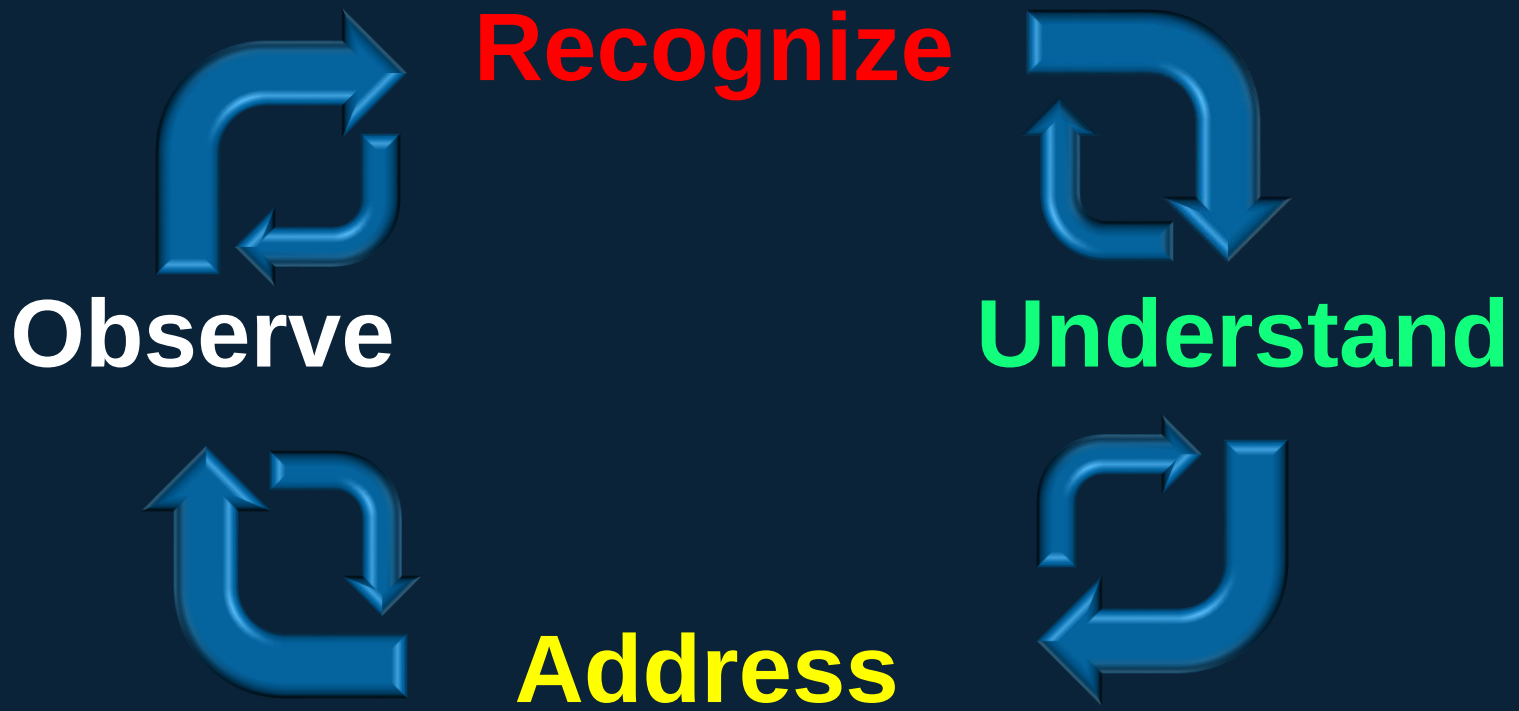
Baltimore, MD
November 2011

Complex Operational Dynamics

Dynamics of independent operations

MITRE

Addressing SoS Complexity



Where others see complexity, the person of action sees the thing that needs to be done.

Michael Lipsey

Taming Complexity:
A System of Systems Challenge

Complex Adaptive Systems Conference

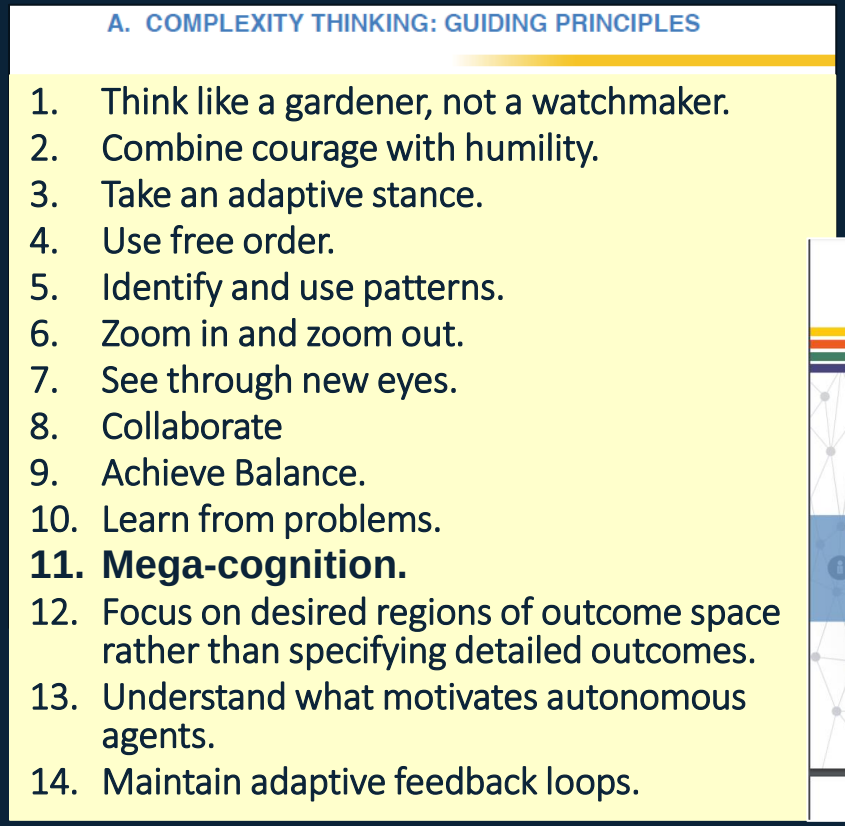
Baltimore, MD
November 2011

Time to go beyond "observe" -- admiring the problem

Partnership with Complexity Working Group

1. Diversity
2. Connectivity
3. Interactivity
4. Adaptability
5. Multiscale
6. Multi-perspective
7. Behavior
8. Dynamics
9. Representation
10. Evolution
11. Emergence
12. Disproportionate effects
13. Indeterminate boundaries
14. Contextual influences

Dimensions of Complexity



A. COMPLEXITY THINKING: GUIDING PRINCIPLES

1. Think like a gardener, not a watchmaker.
2. Combine courage with humility.
3. Take an adaptive stance.
4. Use free order.
5. Identify and use patterns.
6. Zoom in and zoom out.
7. See through new eyes.
8. Collaborate
9. Achieve Balance.
10. Learn from problems.
11. **Mega-cognition.**
12. Focus on desired regions of outcome space rather than specifying detailed outcomes.
13. Understand what motivates autonomous agents.
14. Maintain adaptive feedback loops.

Guiding Principles

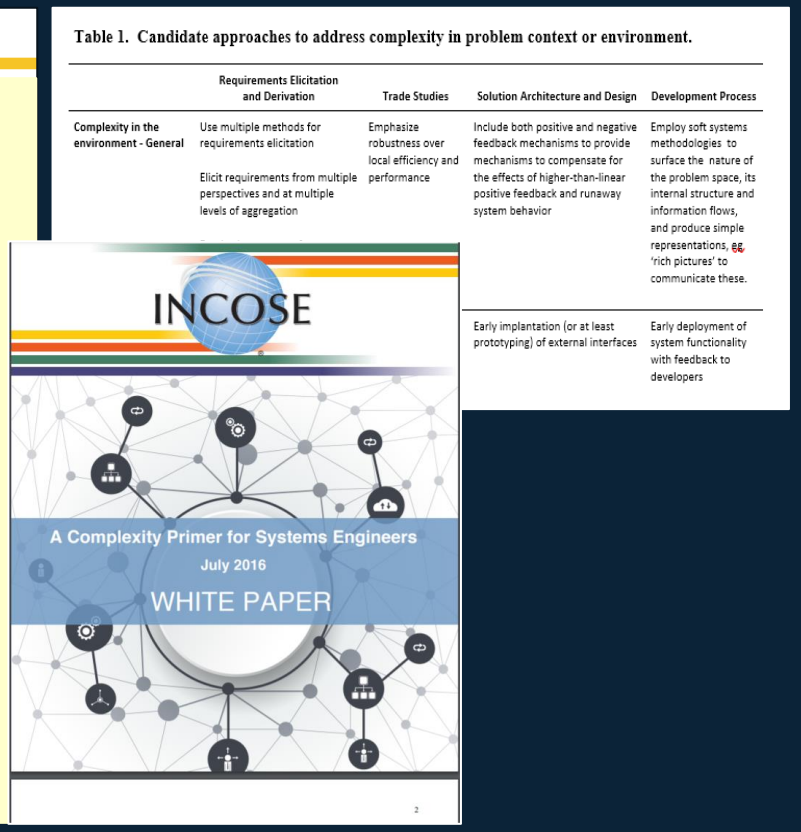


Table 1. Candidate approaches to address complexity in problem context or environment.

	Requirements Elicitation and Derivation	Trade Studies	Solution Architecture and Design	Development Process
Complexity in the environment - General	Use multiple methods for requirements elicitation Elicit requirements from multiple perspectives and at multiple levels of aggregation	Emphasize robustness over local efficiency and performance	Include both positive and negative feedback mechanisms to provide mechanisms to compensate for the effects of higher-than-linear positive feedback and runaway system behavior	Employ soft systems methodologies to surface the nature of the problem space, its internal structure and information flows, and produce simple representations, eg. 'rich pictures' to communicate these.
Early implantation (or at least prototyping) of external interfaces				Early deployment of system functionality with feedback to developers

Candidate Approaches

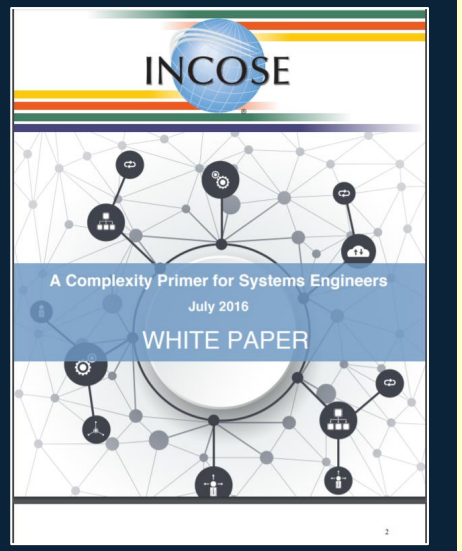
INCOSE

MITRE

Complexity WG offers foundational material to address SoS Complexity

INCOSE SoS & Complexity Project

Apply Complexity concepts to address Systems of Systems Complexity Challenges



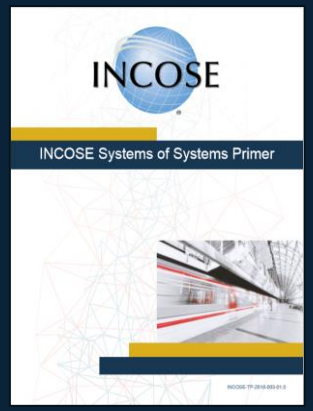
Practical application of

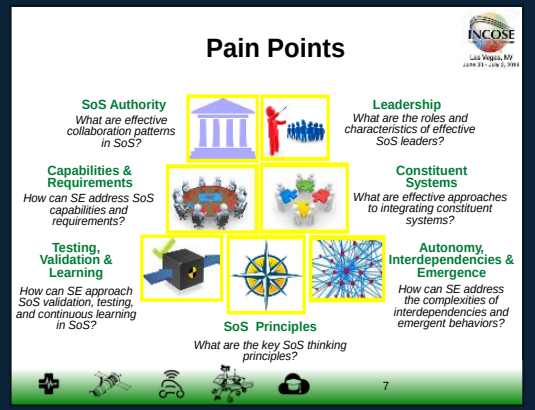
- Complexity dimensions
- *Guiding Principles for complexity thinking*
- *Candidate approaches to addressing complexity*

Practical approaches to

- identifying
- understanding
- addressing

Systems of systems complexity

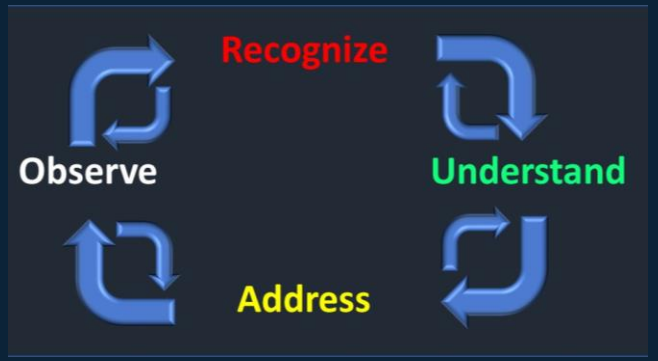




INCOSE

MITRE

‘Recognize’ and ‘Understand’



How and why are SoS characterized by different dimensions of complexity?

Dimension	Definition[1]	How SoS Exhibit…	Why?
Diversity	*The structural, behavior, and system state variables that characterize a system and/or its environments*	SoS can exhibit tremendous diversity across the various constituent systems which provide a range of different behaviors, functionality and technical approaches.	By definition, SoS are comprised of multiple independent systems with their own users, management structures, requirements etc. often developed prior to their membership in an SoS, increasing the likelihood that there will be differences among the constituents of an SoS.
Connectivity	*The connection of the system between its functions and the environment. This connectivity is characterized by the number of nodes, diversity of node types, number of links, and diversity in link characteristics. Complex systems have multiple layers of connections within the system structure.*	SoS include connectivity within each constituent system, among constituents in the SoS and between the SoS and its environment.	SoS are comprised of "connected" constituent systems, so in addition to the connectivity within each constituent, an SoS by its nature is characterized by additional connectivity among constituents. SoS typically have large numbers of nodes, a diversity of node types, a large number of links, and diversity in link characteristics, as well as multiple layers of connections within the system structure. Discontinuities (breaks in a pattern of connectivity at one or more layers) are often found in SoS.

First step was to recognize and understand how complexity dimensions and principles apply to SoS and why

Guiding Principles to Complexity Thinking Applied in Systems of Systems

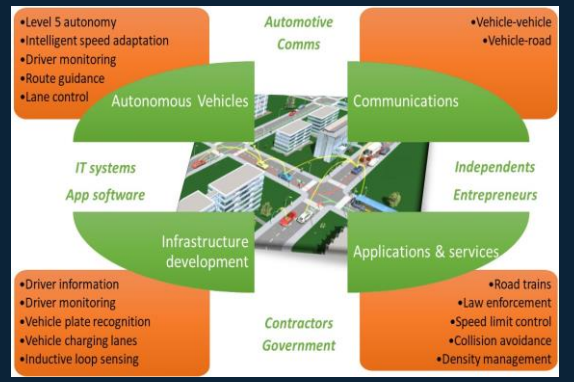
Name	Guiding Principles to Complexity Thinking	Relevance to SoS
Use free order	*In architecting and designing solutions, build in "order for free" using self-organization, presuming it has been modeled and can be limited to desired effects. This in particular applies when the system being designed must be resilient*	Particularly in collaborative or virtual SoS, where SoSE may be from within the SoS, understanding (and modeling) the behavior and interactions among constituents may be an effective way to anticipate effects of interest.
Identify and use patterns	*Patterns are exhibited by complex systems, can be observed and understood, and are a key mechanism in the engineering of complex systems. Patterns are the primary means of dealing specifically with emergence and side effects – that is, the means of inducing desired emergence and side effects, and the means of avoiding undesired emergence and side effects.*	Understanding systems, their behaviors and interactions is a core element of SoSE. By modeling these and treating them as opportunities, patterns can be an effective SoSE approach.
Zoom in and zoom out	*Because complex systems cannot be understood at a single scale of analysis, systems engineers must develop the habit of looking at their project at many different scales, by iteratively zooming in and zooming out. Can problems be solved more elegantly by addressing them at a higher or lower hierarchical level? The complex systems engineer must be especially open to solutions that arise from the bottom-up through self-organization, rather than only seeking to impose order from the top-down.*	Effective SoSE is often called a 'middle out' process, where there is a need to understand the top down drivers for the SoS, but also to respect the bottoms up needs and capabilities of the constituents. The dynamics between these two perspectives reflects this 'zoom in and zoom out' principle as reflected in SoSE thinking.

INCOSE

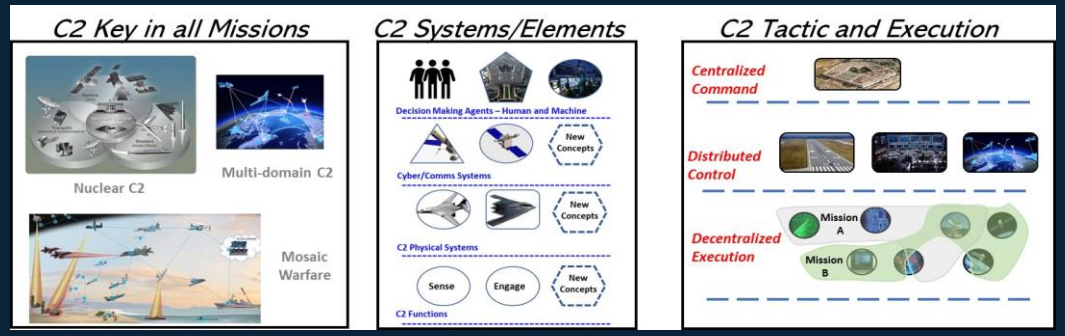
MITRE

How Do These Complexity Concepts Apply in Context of Selected SoS?

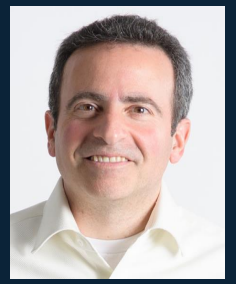
Dimension	Definition	Smart Highways	Defense Command & Control
Diversity	*The structural, behavior, and system state varieties that characterize a system and/or its environments*	• Managing entities live on different planets – different goals, different objectives. ▪ Humans will not agree. • System states and state variables highly different but interrelated. ▪ Vehicle: speed, position, destination ▪ Highway: flow rates, time of day • Diversity of interfaces ▪ Independence of the CS managers causes this as a default. • Some standardization through interoperability. • Diverse development methods/processes – infrastructure vs. vehicles vs software • life cycle of the CSs are diverse, ranging from ephemeral (updates in months) to decades • Diversity of regulation and laws • Diverse incentives	**Does this apply?** • Yes, by definition, diversity in SoS components/participants is present. • In fact, greater diversity could be an aspiration when putting together the SoS to enrich its capabilities and resilience. **Describe** • Diversity is present from an operational standpoint as well as a composition perspective. • Diversity brings different possibilities to combine different systems in various ways. **Example:** • Search and Rescue: Diversity is present in mission objectives (e.g., going from fire rescue to hurricane). • Training can be diverse as it is difficult to predict all the various mission the ISR will be applied to (e.g., rescue from land slide).



Smart Highways
Eric Honour



Topic of workshops at INCOSE IW 2020 and 2021 IEEE SoSE



Defense Command and Control

Dan DeLaurentis & Ali Raz

INCOSE

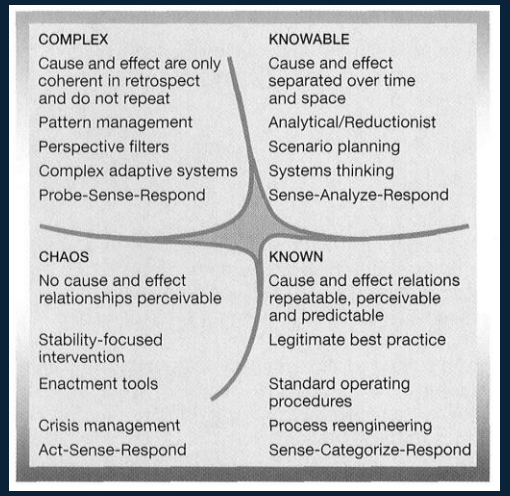
MITRE

Operationalising our Knowledge of Complexity

Use these ideas to classify the class of SoS challenge and use this knowledge to direct practice

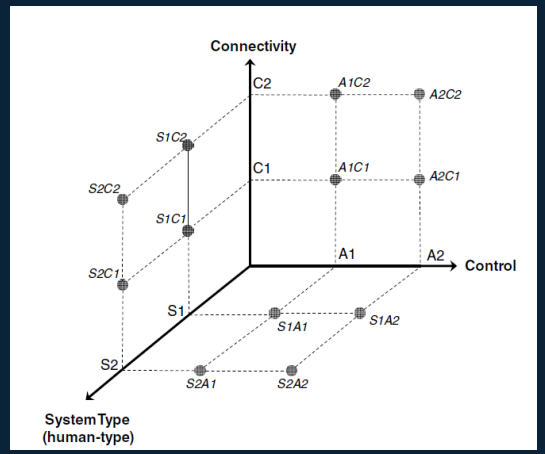
The latter is facilitated through the development of a discipline

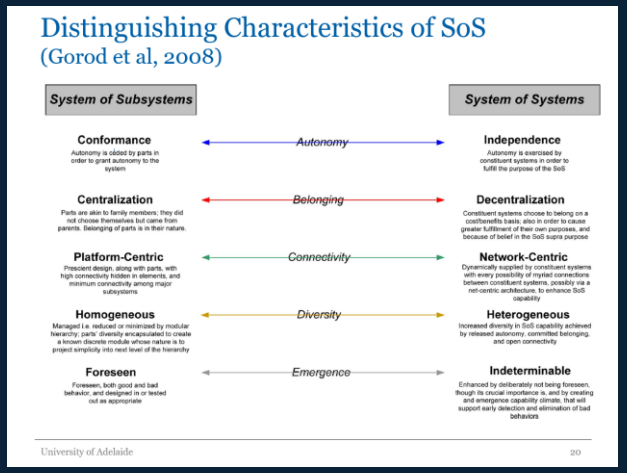
Stephen Cook



Kurtz and Snowden's Cynefin Domains (2003)

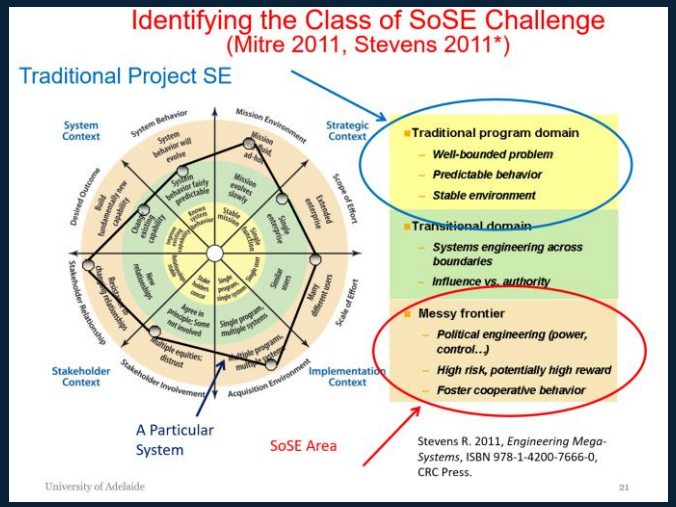
Taxonomy to Guide SoS Decision Making (DeLaurentis et al., 2011)





Flood and Jackson's Total Systems Intervention (1991)

	Unitary	Pluralist	Coercive
Simple	Operations research Systems analysis Systems engineering Systems dynamics	Social systems design Strategic assumption surfacing and testing	Critical systems heuristics
Complex	Viable system diagnosis General system theory Socio-technical systems thinking Contingency theory	Interactive planning Soft systems methodology	?



Classifying Dimensions (Cook & Pratt, 2016)

Dimension	Categories
Governance	Virtual, Collaborative, Acknowledged, Directed
Complexity	Based on technical, organizational and system performance complexity. Sets of these can be categorized or the SoS-of-interest can be benchmarked against known SoS, e.g. city transportation system, humanitarian aid deployment, international air traffic control, and the Internet
Degree of Stakeholder Agreement	Unitary, Pluralist, or Coercive
Dynamicity	Benchmark against well-known SoS that compare the dynamicity to constituent system lifetime. Using a change scale such as: slowly, moderately, rapidly
Domain	Key domain area. This need not be a small list e.g. transportation, defence, telecommunications
Level	Start with Hitchins' levels, could make domain specific e.g. business, industry, socioeconomic
Connectivity	Benchmark against well-known SoS, e.g. trucking fleet, global banking system, Internet, air traffic control
Sociotechnical Nature	Benchmark against well-known SoS, e.g. electricity distribution, transportation, international trade
SoS Lifetime	SoS lifetime as a proportion of average life of constituent systems. Scales such as: < 0.1, 0.1-2.0, and > 2.0

SoSE 2021 Panel

MITRE

Next Steps

Raytheon Technologies

Mission Engineering Approach for Influencing Warfighter Actions using Computational Social Sciences (IWACSS)

Paul Hershey, Ph.D.

December 7, 2021

Problem

- As the DoD strives to incorporate advanced technologies, such as Machine Learning (ML) and Artificial Intelligence (AI), into decision support products, computer science alone is not sufficient to account for the complexity of the systems and the biases of the scientists and engineers who create them.

- Additionally, warfighters need the ability to collect, analyze, and visualize social-based-behavior data to support timely and effective decision-making for complex battle environments, such as Multi-Domain Battle Management Command and Control (MD BMC2).
- One attempt to fill this gap involves Modeling and Simulation (M&S)-based DoD military wargaming. However, previous wargaming exercises have not effectively used technology, such as AI/ML, to assist with the prediction of Red and Blue Force reaction to dynamic changes (e.g., changes in the Rules of Engagement (ROE)).
- A new Mission Engineering Approach for Influencing Warfighter Actions using Computational Social Sciences (IWACSS) is required to address these issues.

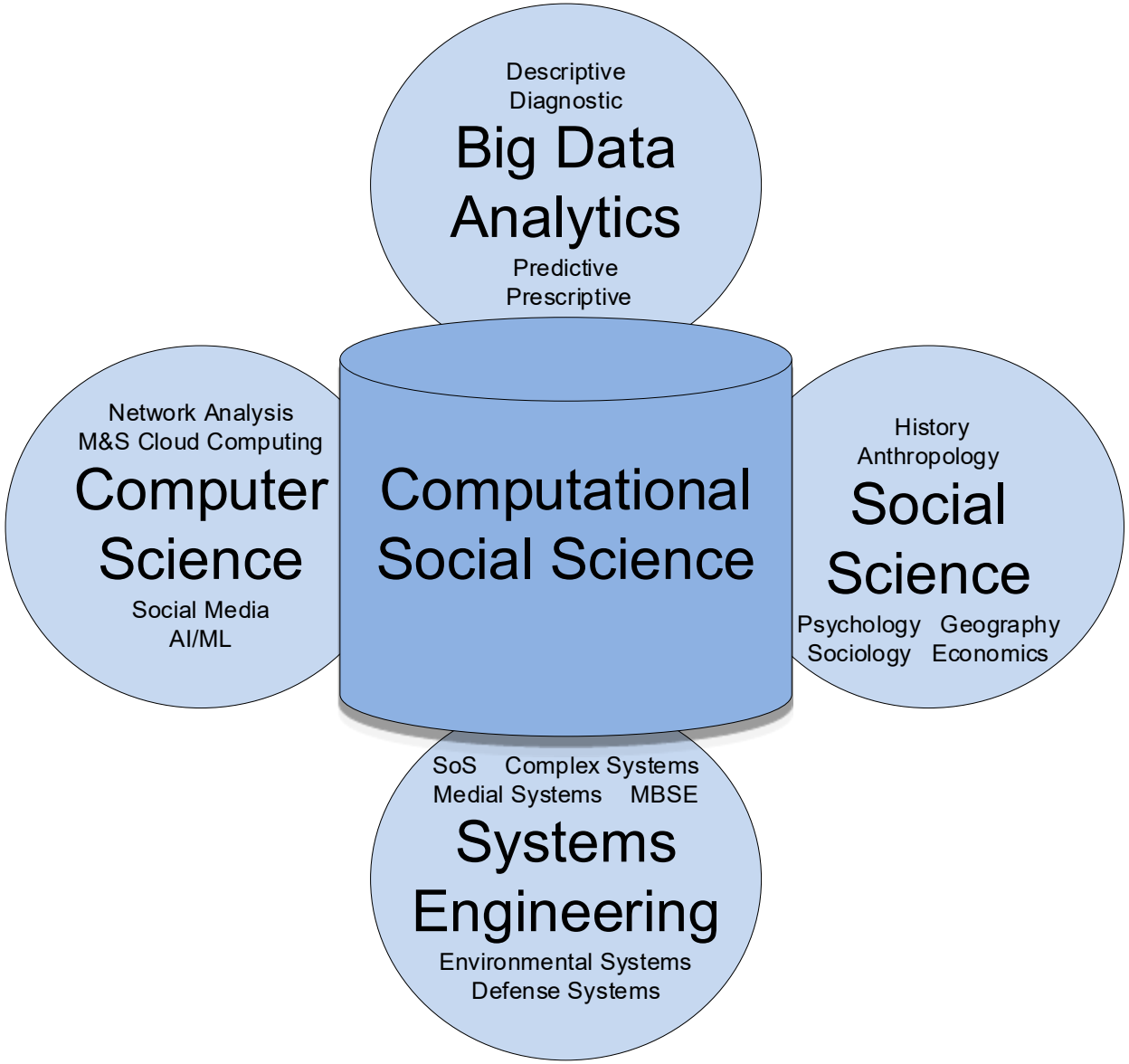
Prior Works

- Computational Social Science (CCS) has been defined as the “interdisciplinary science of complex social systems and their investigation through computational modeling and related techniques,” and may be depicted as a cross section of computer science and social science. [https://cos.gmu.edu/cds/computational-social-science/, accessed 1/30/2019].
- Other views of CSS incorporate philosophy, neuroscience, linguistics and cognitive psychology, along with Artificial Intelligence (AI) **[Cognitive Social Psychology: The Princeton Symposium on the Legacy and Future of Social Cognition 1st Edition, Kindle Edition, by Gordon B. Moskowitz (Editor) © 2001 Lawrence Erlbaum Associates, Inc.]**
- CSS investigates social complexity at all levels of analysis: cognitive, individual, group, societal, and global, through medium of computation. It is based on an information-processing paradigm of society that encompasses both pure science and policy analysis (applied science). **[https://cos.gmu.edu/cds/computational-social-science/, accessed 1/30/2019]**
- The goal of SocialSim is to develop innovative technologies for high-fidelity computational simulation of online social behavior. SocialSim will focus specifically on information spread and evolution. Current computational approaches to social and behavioral simulation are limited in this regard. **[Computational Simulation of Online Social Behavior (SocialSim) Proposers Day, DARPA-SN-17-19, January 17, 2017]**
- Causal Exploration seeks to develop a modeling platform to aid military planners in understanding and addressing underlying causal factors that drive complex conflict situations**. [Special Notice Causal Exploration of Complex Operational Environments (Causal Exploration) Proposers Day, DARPA-SN-17-11, December 02, 2016]**
- Center for Naval Analysis (CAN) designed and conducted a table-top exercise (TTX) at the U.S. Pacific Command (PACOM) Amphibious Leaders Symposium (PALS) in July 2016 that explored seabasing operations and interoperability during future contingency operations. Using a scenario that revolved around a massive natural disaster striking a fictitious country in the southern Indian Ocean, the TTX**. [Gaming Sea-based Multinational HA/DR Operations at PACOM Amphibious Leaders Symposium 2016, Catherine K. Lea, Edsel D. McGrady, Douglas J. Jackson, Daniel Powell, Elizabeth A. Collins, and Nilanthi R. Samaranayake, November 2016]**

IWACSS extends and fuses ideas in prior works by focusing CSS to influence decision making for war-fighters in the heat of battle.

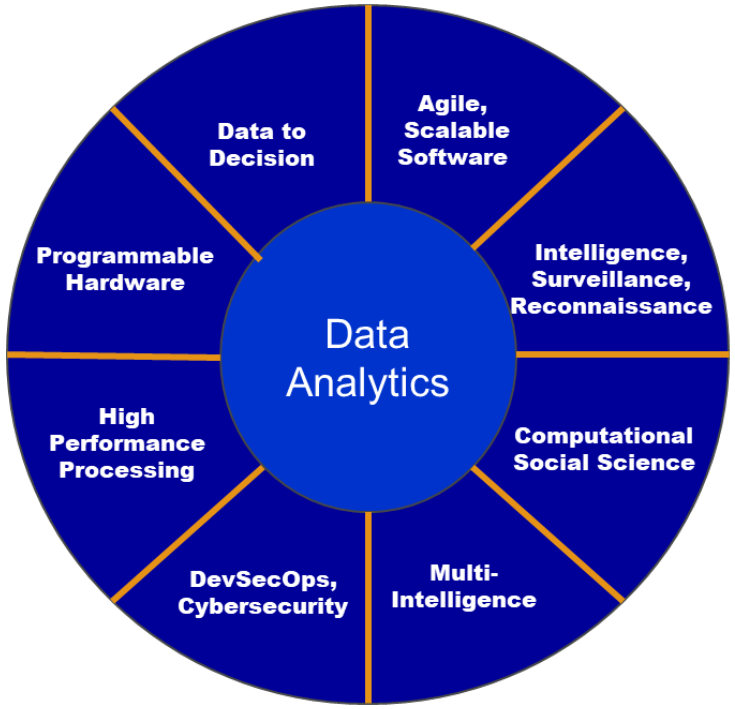
Background: CSS

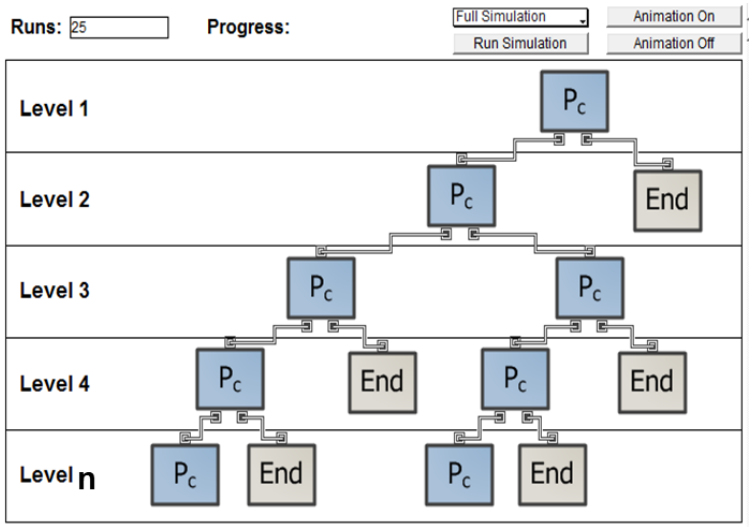
- CCS has been defined as the “interdisciplinary science of complex social systems and their investigation through computational modeling and related techniques.” [1]
- CSS may be depicted as a cross section of computer science, social science, big data analytics, and systems engineering. [2]



Background: Data Analytics

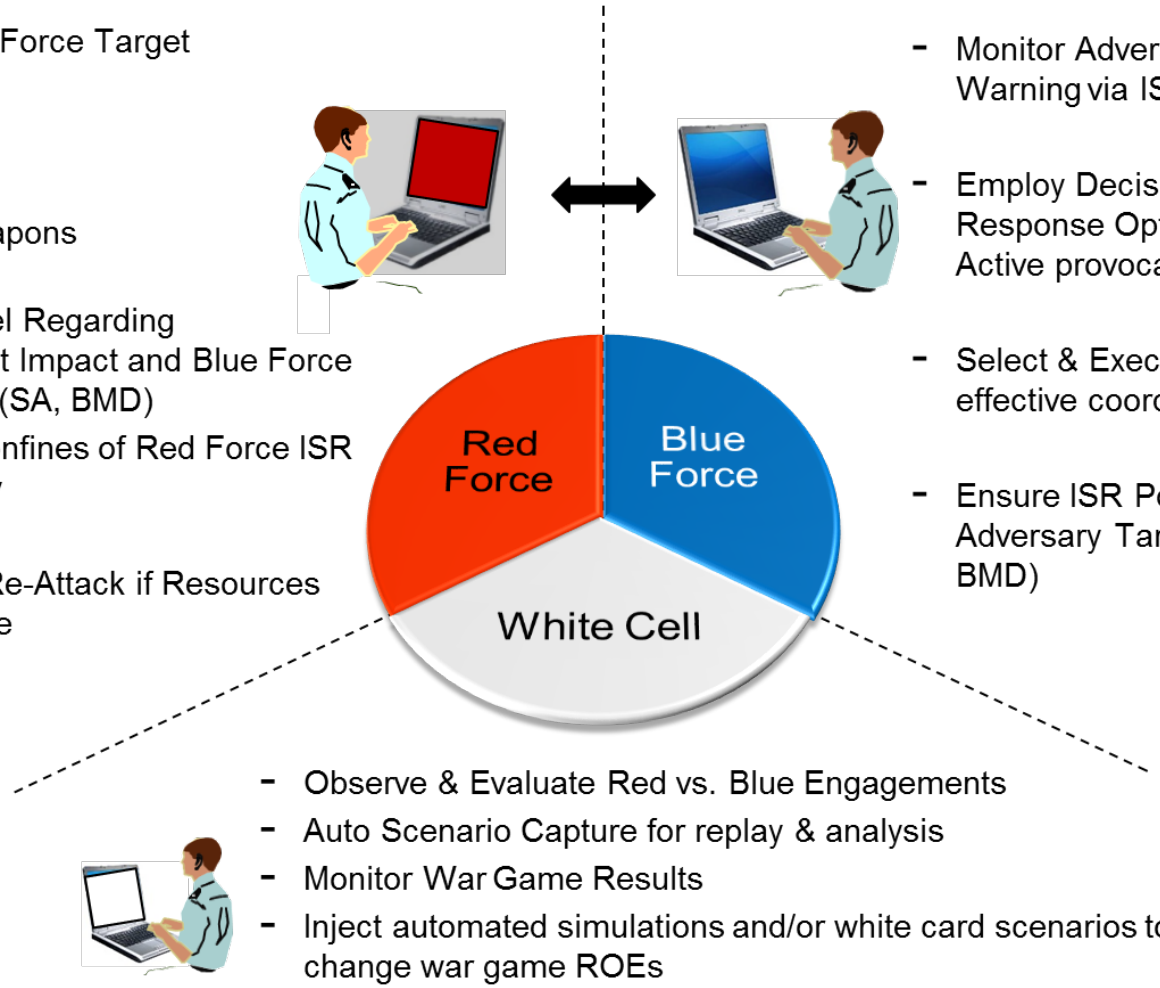
- Definition:
  - Data analytics is the science of collecting and processing raw data in order to improve human decision making
  - Data analytics encompasses many types of data and data analyses
  - Data analytics can be processed by many different hardware and software techniques
  - Data analytics supports cyber security and autonomous systems
  - Data analytics techniques can reveal trends and metrics that would otherwise be lost in the mass of raw data
- Data analytics is broken down into four basic types:
  1. Descriptive analytics describes what has happened over a given time period;
  2. Diagnostic analytics focuses on why something happened;
  3. **Predictive analytics describes what is likely going to happen in the near term;**
  4. **Prescriptive analytics suggests a course of action.**





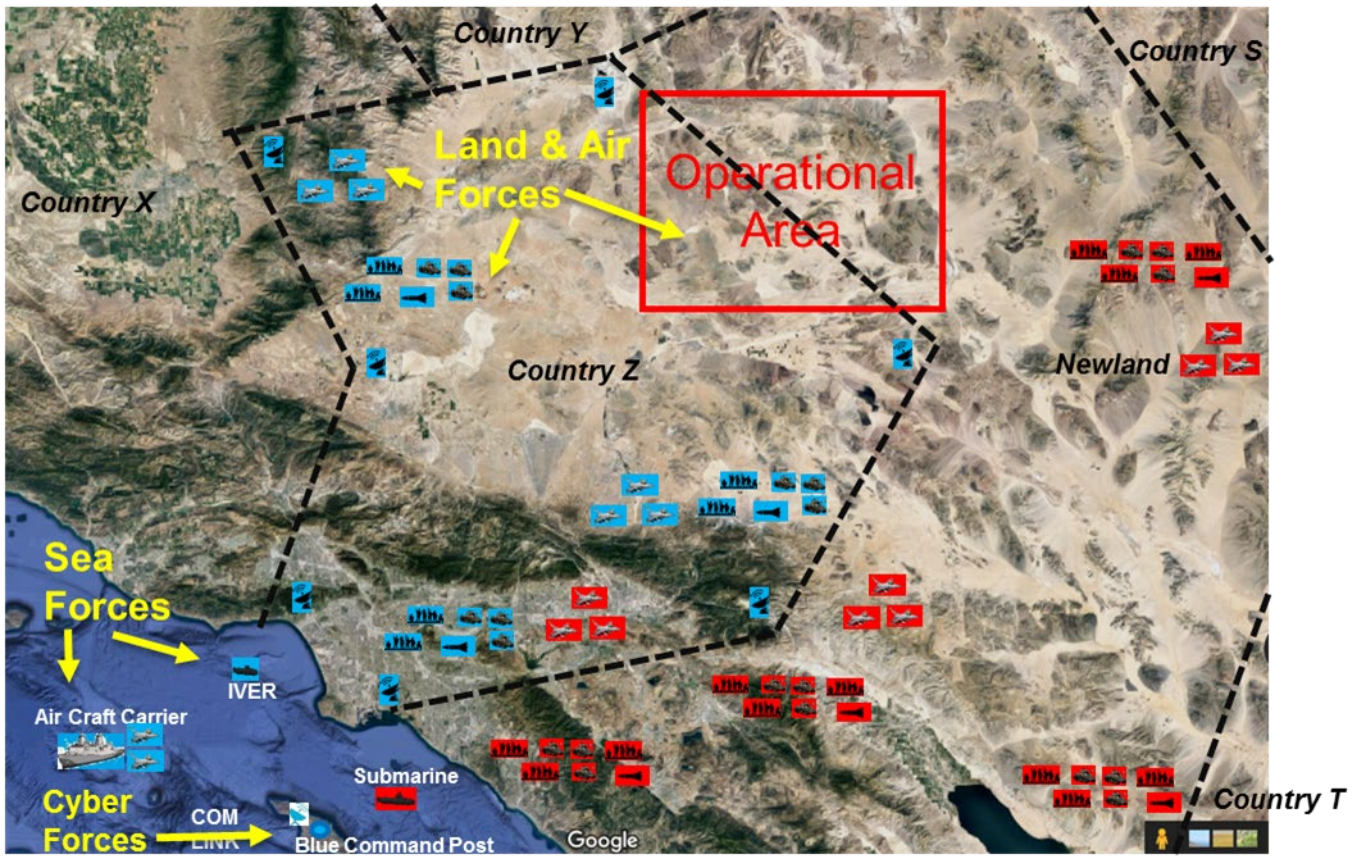
Background: Wargame

- Wargames are modeling and simulation capabilities in which theories of warfare can be explored in the absence actual warfare.
- These games assist DoD operators and analytics with tactical, operational, or strategic planning.
- There are 3 components to a wargame.
  - Blue Force (friendly)
  - Red Force (enemy)
  - White Cell (possible instructor who can observe and make changes, such as changes to the Red or Blue Force
- IWACSS includes these three elements as described in the figure.



Background: Scenario

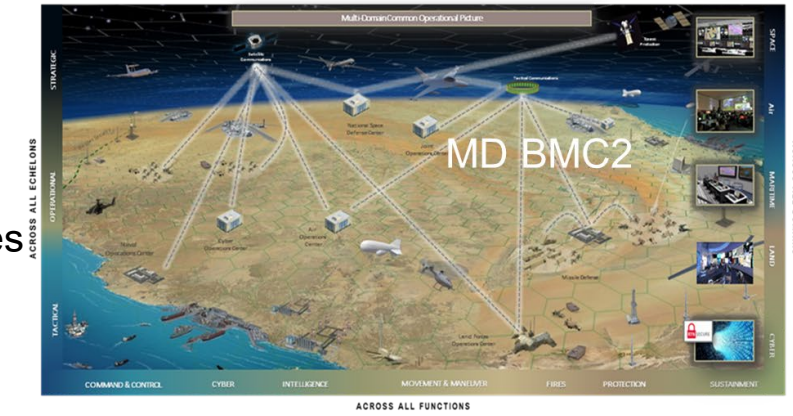
- For decades, Country Z has lived in peace with our neighbor, Newland, however, since the ascent to power 2 years ago of the son of the deceased dictator, tensions between the countries have escalated. Yesterday, during an announced military training exercise, forces from Newland the international border and are currently occupying territory within Country Z. Newland maritime forces have also been intercepted, via SIGINT, of planning coastal operations against undefended ports of entry. Additionally, Newland UAVs have been seen, via SIGINT, operating in the Northeastern sector.
- Blue forces from Country Z are tasked to repel the invaders from our territory, pushing them back at least 50 kilometers from our border in the area of conflict. In addition, our border defenses must be shored up over all domains, to prevent another incursion into our territory. Denying the enemy intel on our movement is key to our success so eliminating this ISR source and denying access to Red satellites is critical. Protecting our borders, our military C2 headquarters, and our capital city are essential. To prevent re-attack, we must soften the enemy border defenses, with a longer-term goal of taking out Newland defenses along the Country Z border. Make every effort to avoid civilian casualties, and provide protection to our citizens in the area of conflict. Evacuation has been ordered from the area of conflict, but some patriotic citizens remain in place to fight against the invaders. Reserve forces are located on an island outside of the area of operations.

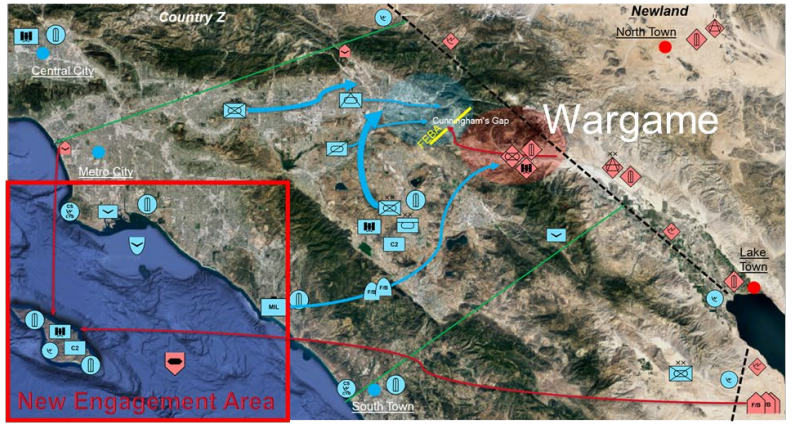


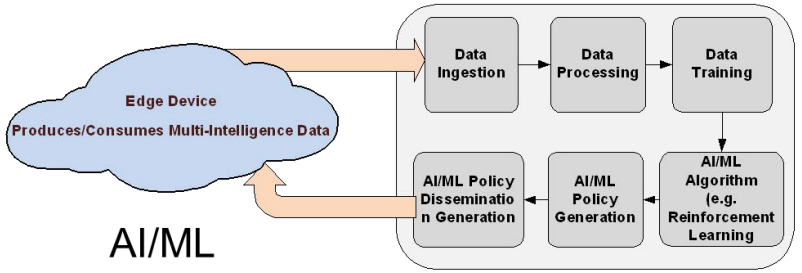
Approach

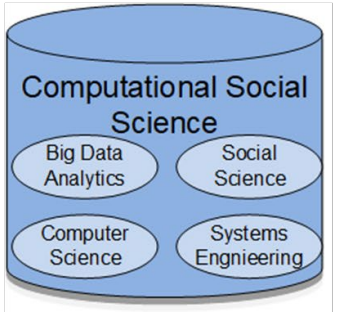
The IWCSS method enables the end-users to accomplish the following complex mission engineering functions:

1. Combine war-gaming techniques with CSS through a white cell dynamically changing rules of engagement for Red Force and Blue Force
2. Demonstrate ability of white cell to apply “Deception” to change the Rules of Engagement (ROE) and, thereby, influence multiple mission functions, including: Course of Action (COA) Generation, COA Analysis, Mission Feasibility Analysis
3. Demonstrate ability of red and blues forces to respond to ROE at speed of battle: Self-healing COA
4. Introduce gamification concepts to support intuitive and time-efficient use by end-users







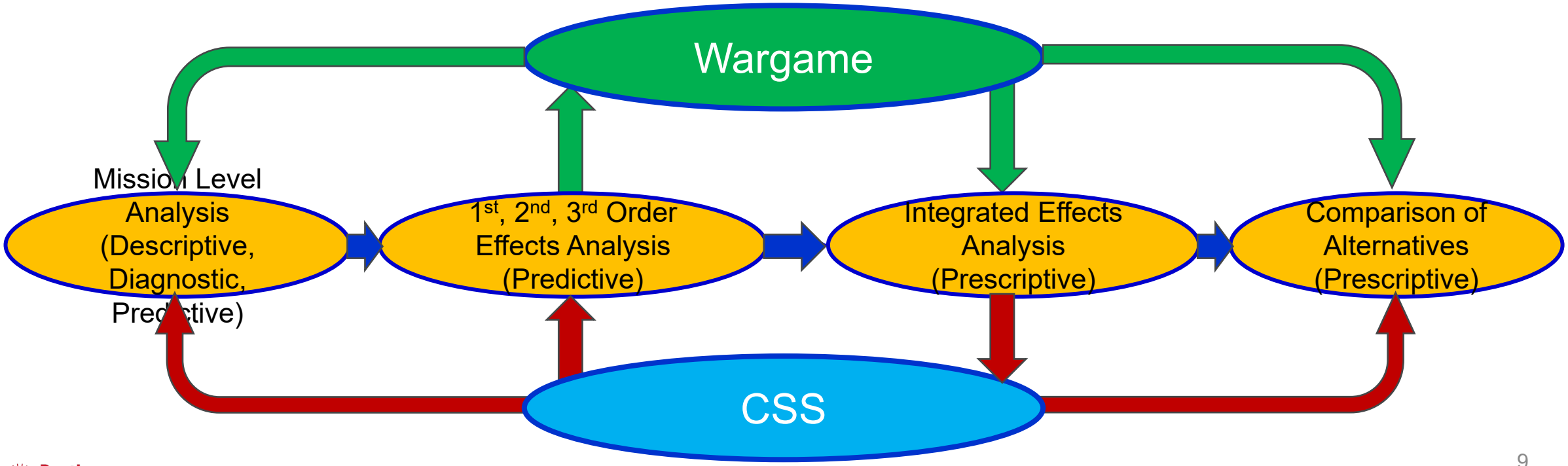


Computational Social Science (CSS)

5. Apply **Artificial Intelligence and Machine Learning** to actual and synthetic data training sets to enable white cell to determine expected behavior of red and blue forces in the face of mission events. Include use of predictive analytics
6. Demonstrate new **M&S, AI, and ML IWACSS method for multi-domain battle management command and control scenarios** of interest military supported and supporting commands. These scenarios would include both Unclassified and Classified cases, where classification is determined based on classification of training data
7. Analyze **integrated kinetic and non-kinetic fires** across all mission phases
8. Evolve to real-time decision support, and incorporate emerging, high speed effects such as hypersonic weapons
9. Extend to Asymmetrical Warfare analysis and assessment

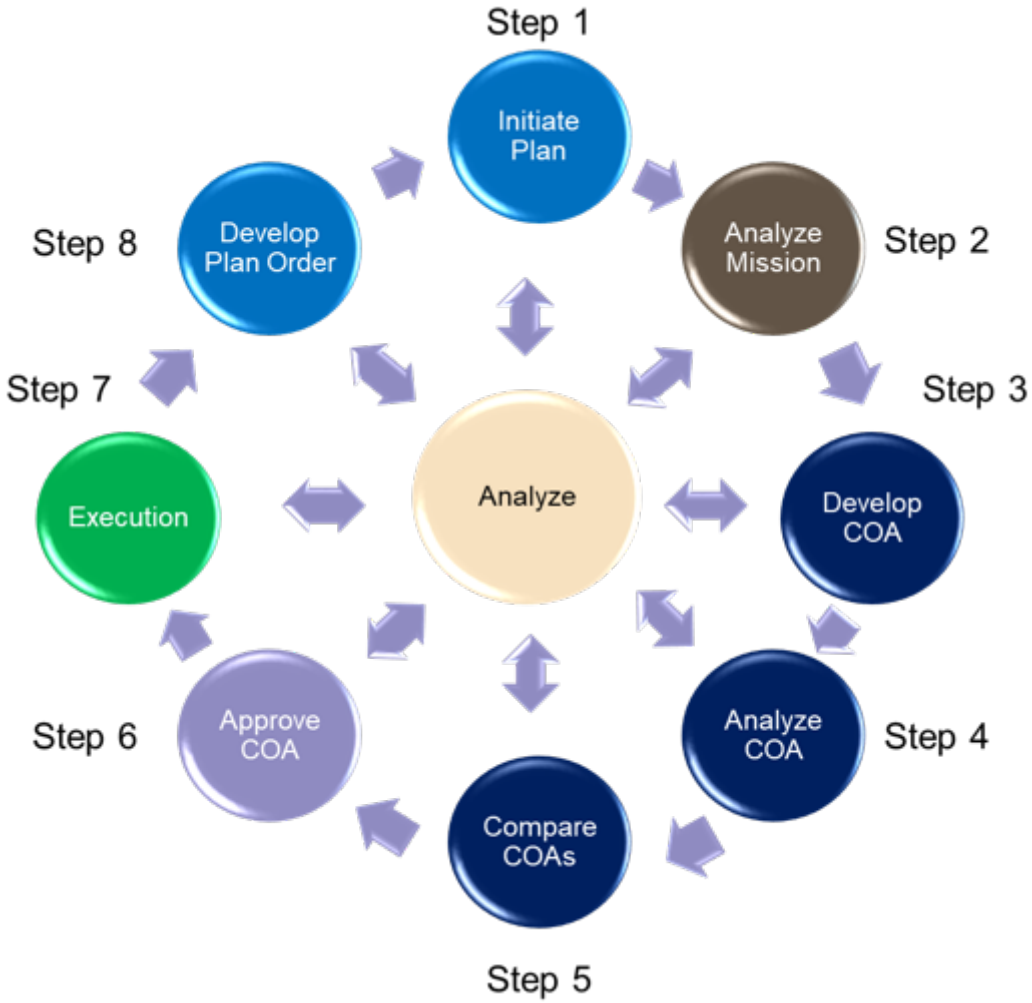
Approach: Relationship between CSS and Wargame

- Combine detailed COA development , analysis, and comparison, from wargame with CSS engine
  - Wargame produces results for initial performance measures through RL and predictive analytics
  - CSS engine checks for 1st, 2nd, and 3rd order effects and provides feedback to wargame to refine performance analysis (predictive analytics).
  - After sufficient iterations, the confidence level in performance analysis reaches the desired threshold and calculates effect and wargame outcome results for alternative COAs (prescriptive).
  - Alternative COA results are compared and best COA to meet commander's intend is selected



Approach: Dynamic COA Update - SCOAR

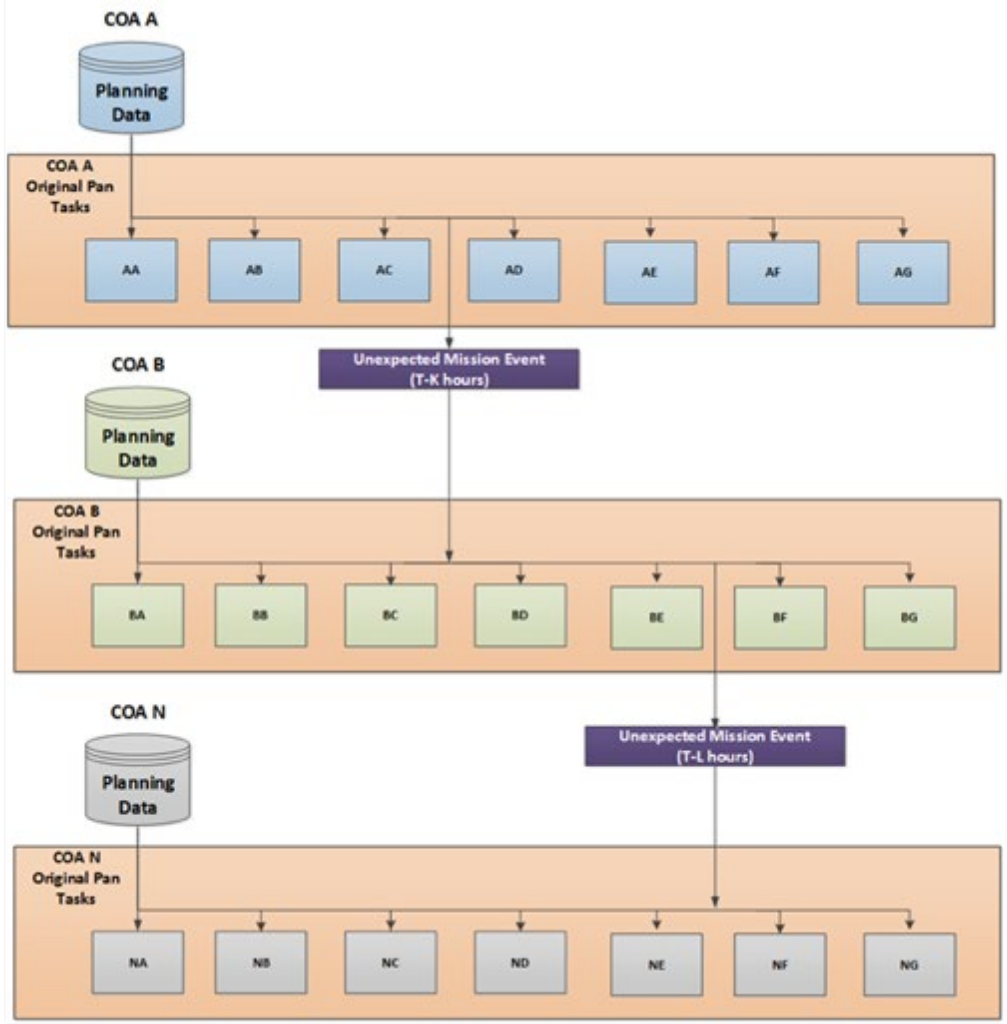
- The COA process requires 7 steps for COA revision:
  - Initiate plan, analyze mission, COA generation (including COA development, COA analysis, and COA comparison), COA approval, and develop COA plan order
- After the mission initiation, there is no opportunity for COA adjustment if events change unexpectedly
  - Changes in the Rules of Engagement (RoE)
- A new Self-Healing Course of Action Revision (SCOAR) technique based on Reinforcement Learning (RL) was applied to vented to enable dynamic adjustments in the COA
  - Continuously assesses mission events during mission execution
  - Applies machine learning to adjust the presently executing COA dynamically.
    - Asset positions, maintenance, and tasking - actively monitored
    - If the primary asset suffered attrition or was unable to complete its goals, then next best asset automatically tries to take its place
    - If no assets are available, swaps out the COA activity being performed for an activity in a different COA that achieves the same end state



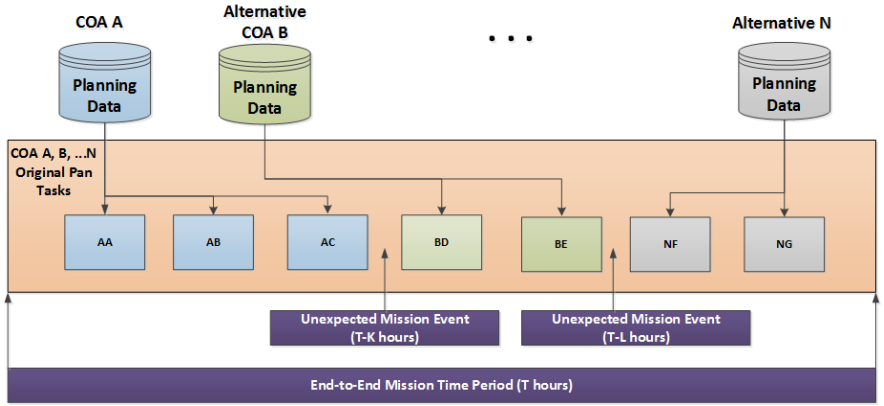
COA Revision Process

Approach: Example

- In this example, “N” different COAs are planned and generated for a defined mission in a **wargame**.
- During COA compare, COA A is selected as the COA to execute during the mission.
- However, after the mission is initiated and has begun executing, unexpected mission events occurred (**such as 1st , 2nd or 3rd order events injected by white cell**) at mission times T-K hours and T-L hours, where T hours is the total mission time and K hours and L hours are times less than T hours.
- SCOAR enables the overall mission COA to move from COA A activities to COA B activities and eventually to COA N activities as mission events change.
- This COA revision and assessment process is done without repeating the entire COA generation process.



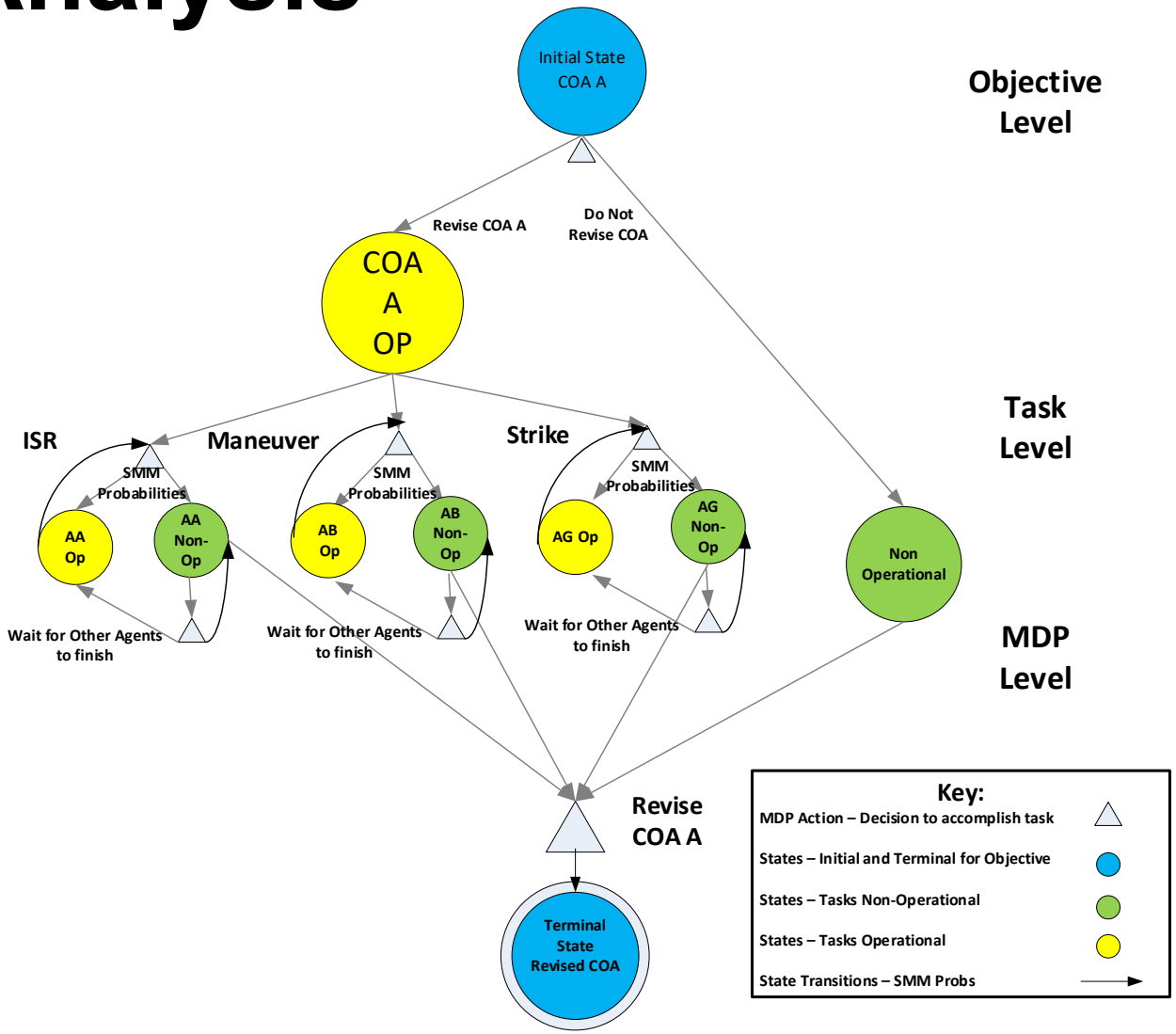
Individual COA Response to Unexpected Mission Events



Combined COA Response to Unexpected Mission Events

Approach: Predictive Analysis

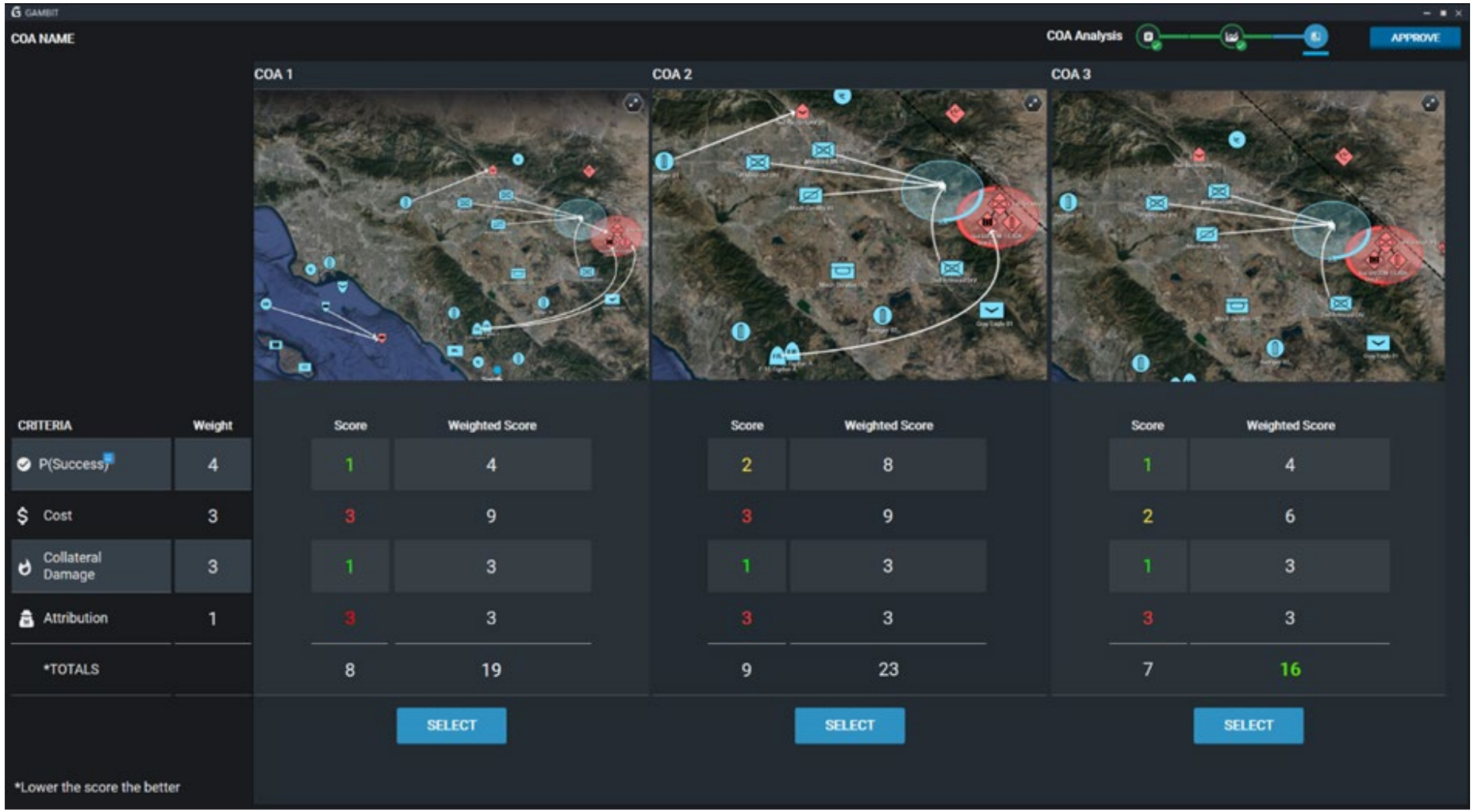
- Analysis approach applies Markov Decision Processes (MDP) and Stochastic Mathematical Model (SMM)
- Represents all COA activities for mission as a non-deterministic state machine in which each activity is a state
- Applies Markov Decision Processes (MDP) to determine all possible state transitions
- Computes transition probabilities (Psuccess) and associated confidence intervals (CI) between all COA activities using the SMM.
- Uses a new method to Propagate Transition Probabilities (Psuccess) and associated Confidence Intervals (CI) across COA Activities.



SCOAR Notional MDP Representation of a COA Task

Results: IWACSS Prototype –Prescriptive Analytics

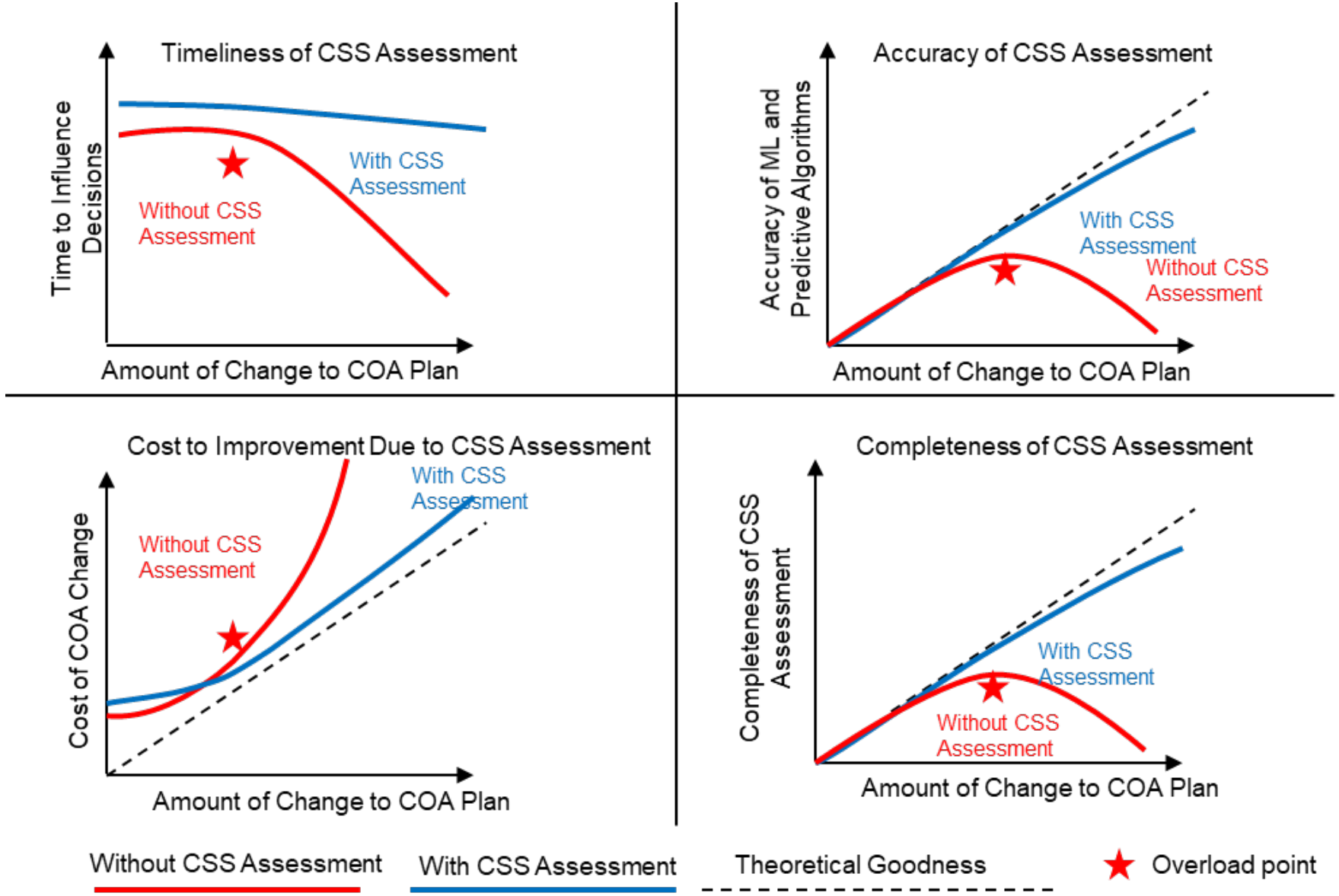
- Implemented a prototype that generated metrics relevant commander's criteria for three alternative COAs.
  - Compared each COA with respect those metrics
  - COAs 2 and 3 were revised as Rules of engagement (RoE) changed during the simulated battle.
  - Each COA was given a weighted score to help both the mission planner and the commander determine whether the revised COA resulted in a better plan.
    - In accordance with military doctrine, lower score wins
    - COA 3 provided lowest score for metrics considered



COA Results and Comparison

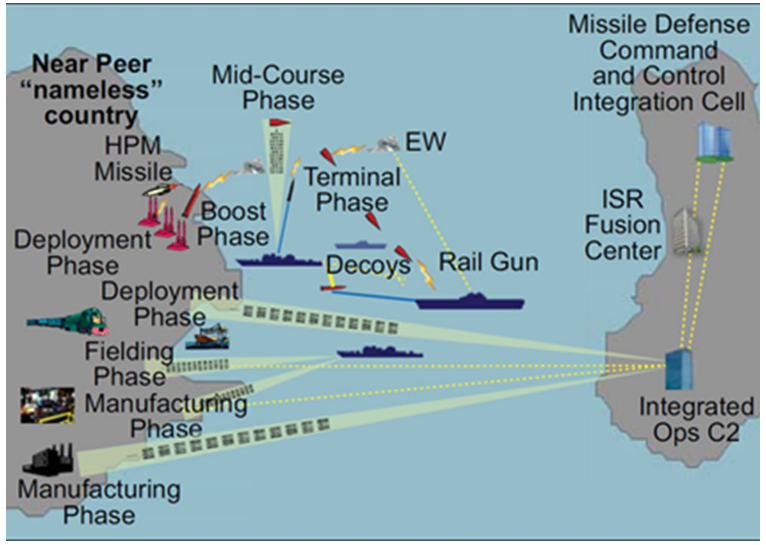
Raytheon Intelligence & Space

Notional Results – Improvement to Wargame Results with CSS

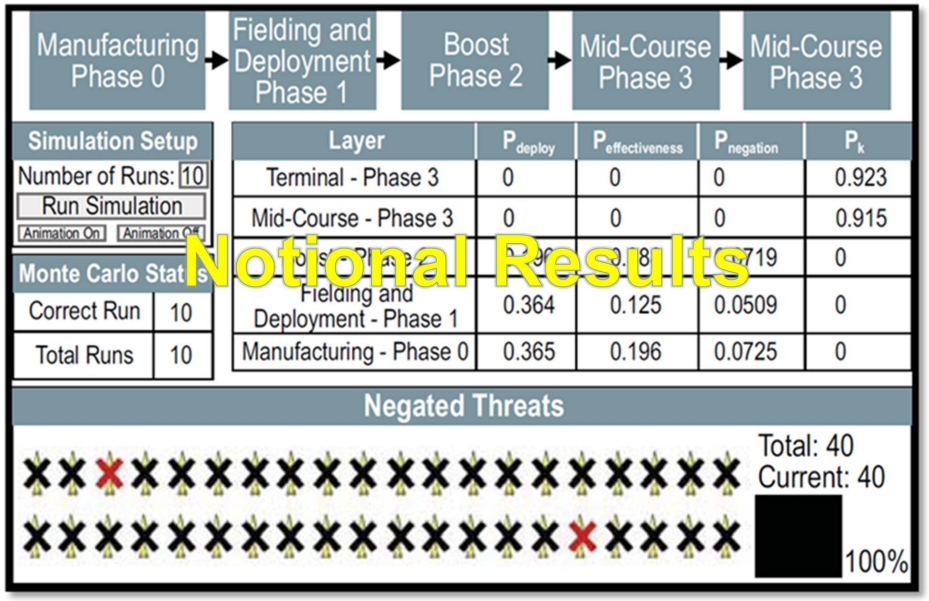


Notional Results for Integrated Kinetic/Non-kinetic Fires

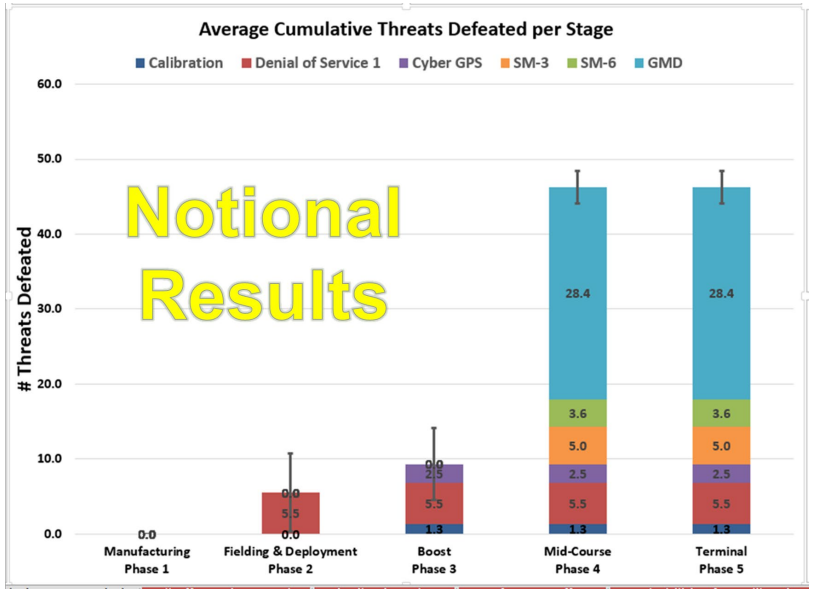
- IWACSS applied SMM and SCOAR to derive results for a notional multi-domain Integrated Air and Missile Defense (IAMD) Scenario.



- SCOAR used prescriptive analytics to permit consideration of alternative 1st, 2nd, and 3rd order effects per mission phase



- SMM derived predictive analytics results for Probability of Defeat for individual and integrated kinetic and non-kinetic threat/effect pairings per mission phase.



Conclusion

- Presented an approach that integrates wargaming and Computation Social Science such that red-force and blue force square off to fight, while a white cell player applies deception to manipulate red force blue force Courses of Action (CoAs).
- White Cell has the ability to inject unexpected events that can change the Rules of Engagement (ROE) between Red Force and Blue Force.
- Introduces a new Self-Healing Course of Action Revision (SCOAR) capability that enables dynamic adjustments in the COA
- Events are meant to elicit responses due to both subjective social interpretation and objective rules-based interpretation.
- CSS will also be used to assist red and blue force teams in predicting the next move of the other.

Backup

Abstract

As the DoD strives to incorporate advanced technologies, such as Machine Learning (ML) and Artificial Intelligence (AI), into decision support products, computer science alone is not sufficient to account for the complexity of the systems and the biases of the scientists and engineers who create them. Additionally, warfighters need the ability to collect, analyze, and visualize social-based-behavior data to support timely and effective decision-making for complex battle environments, such as Multi-Domain Battle Management Command and Control (MD BMC2). One attempt to fill this gap involves Modeling and Simulation (M&S)-based DoD military wargaming. However, wargaming exercises do not effectively use technology, such as AI/ML, to assist with the prediction of Red and Blue Force reaction to dynamic changes, such as changes in the Rules of Engagement (ROE). A new mission engineering approach is required to address these issues.

In this paper, we present such a mission engineering method and system for Influencing Warfighter Actions using Computational Social Sciences (IWACSS) to fill the gap in both in traditional DoD wargaming and in emerging Computational Social Science. IWACSS incorporates the social domain into battle management where real-time analysis is required to support timely decision-making. Our extensive research of prior literature and patents reveals that, although prior wargaming has incorporated aspects of social science, these attempts fail to provide calculated results derived from mathematically-based prediction that consider the effects (e.g., 1st, 2nd, and 3rd order effects) of social parameters on the outcome of the battle. In fact, for these approaches, the concept of applying predictive techniques is limited based on the perceived randomness of human social behavior. IWACSS overcomes this limitation by applying foundational stochastic mathematics and CSS techniques in combination with Reinforcement Learning (RL) to improve timely decision making and provide predictive results that include confidence levels.

The IWCSS method enables the end-users to accomplish the following complex mission engineering functions:

- Apply war-gaming techniques with white cell dynamically changing rules of engagement for Red Force and Blue Force
- Demonstrate ability of white cell to apply “Deception” to change the Rules of Engagement (ROE) and, thereby, influence multiple mission functions, including: Course of Action (COA) Generation, COA Analysis, Mission Feasibility Analysis
- Demonstrate ability of red and blues forces to respond to ROE at speed of battle: Self-healing COA
- Introduce gamification concepts to support intuitive and time-efficient use by end-users
- **Apply Artificial Intelligence and Machine Learning** to actual and synthetic data training sets to enable white cell to determine expected behavior of red and blue forces in the face of mission events. Include use of predictive analytics
- Demonstrate new **M&S, AI, and ML IWACSS** method for multi-domain battle management command and control scenarios of interest military supported and supporting commands. These scenarios would include both Unclassified and Classified cases, where classification is determined based on classification of training data
- Analyze **integrated kinetic and non-kinetic fires** across all mission phases
- Evolve to real-time decision support, and incorporate emerging, high speed effects such as **hypersonic weapons**
- Extend **to Asymmetrical Warfare** analysis and assessment

Preliminary results were generated using the IWACSS prototype for three alternative COAs. These results were compared with respect to how they met the Commander’s criteria for selected metrics including Probability of Mission Success (Psuccess) with associated Confidence interval, Cost, Collateral Damage, and Attribution. **RL was used to enable dynamic adjustment of COAs** in response to changes in the RoE during the simulated battle. The results were presented to the end-users in the form of a decision matrix in which each COA was given a weighted score to help the mission planner and the commander determine whether the revised COA resulted in a better plan.

Bio

Paul Hershey works for Raytheon Technologies Company, where he is a Principal Engineering Fellow focusing on data analytics, autonomous systems, modeling and simulation, and cyber security. He has been a member of IEEE since 1980 and was elevated to IEEE Fellow in 2021. He received his Ph.D. and M.S. degrees in electrical engineering from the University of Maryland, College Park, MD, USA, and the A.B. degree in mathematics from the College of William and Mary, Williamsburg, VA, USA. Dr. Hershey has published 39 patents (granted) and over 60 peer-reviewed technical articles. Previously, he was an adjunct professor at George Washington University where he also served on the Curriculum Advisory Board. He presently serves on technical program committees for the IEEE International Systems Conference and the IEEE International System of Systems Engineering Conference. Dr. Hershey is a Distinguished Lecturer on data analytics for the IEEE Systems Council.