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 2

EVENT INFORMATION 4

TRACK INFORMATION 5

AGENDA 7

LIVE SESSIONS 18

ON DEMAND 28

BIOGRAPHIES 32

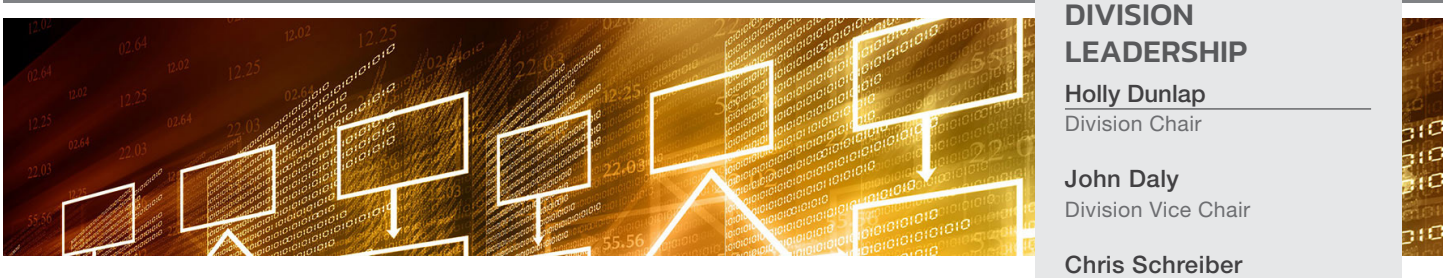
SPONSOR DESCRIPTIONS 34

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

NDIA | CAREER CENTER

Connecting Talent with Great Opportunities

This latest member benefit of the National Defense Industrial Association offers qualified defense and national security professionals and employers an intuitive platform to identify the next best opportunity or candidate. With single-sign-on, quick and advanced searches, job alerts, career resources, pre-screen questionnaires, success tracking, and more, the NDIA Career Center is the defense industry's premier resource for career growth and advancement.

Log in and complete your profile today at Jobs.NDIA.org



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.

NDIA
MEMBERSHIP

BECOME A MEMBER OF THE TRUSTED LEADER AMONG DEFENSE AND NATIONAL SECURITY ASSOCIATIONS TODAY

NDIA is a non-partisan 501(c)(3) nonprofit organization that educates its constituencies on all aspects of national security in support of the warfighter to ensure the safety and security of our nation. Alongside our 1,610 corporate and 65,000 individual members, we drive a strategic and collaborative dialogue in national security, identifying key issues and leveraging our collective knowledge and experience to address them.

Become a member today to enjoy NDIA's many networking and professional development benefits:
Event registration and exhibition **discounts** | **Network** with top decision-makers in government and industry | Assignment to a **local** NDIA Chapter | Join any of NDIA's 29 **Divisions** | **Attend** symposia, conferences, and exhibitions | **Collaborate** with the defense industrial base | *National Defense* Magazine and *Defense Watch* **subscriptions** | And more!

Join today at NDIA.org/Membership

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

EMERGING TECH HORIZONS

An ETI Podcast

Listen in as our nation's security experts share their personal takes on the latest defense technology.

Hosted by our resident expert Dr. Mark Lewis, Executive Director of NDIA's new Emerging Technologies Institute, our brand-new podcast takes a deep dive into how technology will shape the future of warfare.

EmergingTechnologiesInstitute.org/Podcast

ETI EMERGING TECHNOLOGIES INSTITUTE



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.

NDIA Connect

AN ONLINE COMMUNITY FOR DEFENSE PROFESSIONALS

NDIA Connect is a members-only benefit that’s bustling with information, conversation, and activity stimulated by defense professionals from industry, government, and academia. Log in today to explore the platform’s various functionalities and contribute to our collective mission in support of the warfighter. From anywhere and at any time, use NDIA Connect to network with colleagues, collaborate on projects, and stay connected.

Connect.NDIA.org



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

Office of Director for Developmental Test, Evaluation, and Assessments D(DTE&A)

Model Readiness Levels: A Mathematical Construct for Validation and Trust

December 6, 2021

Darryl Ahner, PhD, P.E. Former Director of STAT COE

AFIT.EDU/STAT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.
CLEARED on 9 Aug 2021. Case Number: 88ABW-2021-0721

What Are Scientific Test and Analysis Techniques (STAT)?

Scientific Test and Analysis Techniques (STAT) are the **scientific and statistical methods and processes** used to enable the development of efficient, rigorous test strategies that will yield mission assurance during development. STAT encompasses such techniques as design of experiments, observational studies, reliability growth, software testing, and survey design used within a larger decision support framework. The suitability of each method is determined by the specific objective(s) of the test to assist the program manager to understand and quantify technical risk.

DoDI 5000.89 requires STAT for both developmental and operational testing

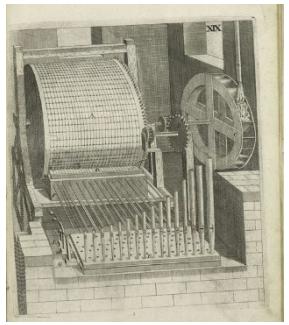
STAT: Innovation, Agility, Quality

AGILITY



Implements rapid & responsive solutions to program changes that occur during testing

Continually ensures alignment of desired mission capability with ***measurable*** objectives



INNOVATION

- Efficiently ***generates STAT-based information*** for technology development and testing
- ***Implementation costs are offset*** by test cost savings and post-production cost avoidance



QUALITY

- Test and evaluation ***enables the DoD & DHS to acquire systems that work*** while quantifying risk using STAT
- Produce the required data **to characterize system behavior and combat mission capability** in accordance with DoDI 5000.89 and other guidance
- STAT enables quantitative estimates of ***technical performance requirements*** and produces ***mission-oriented metrics***

We seek for Digital Engineering to enable Innovation, Agility, and Quality as well

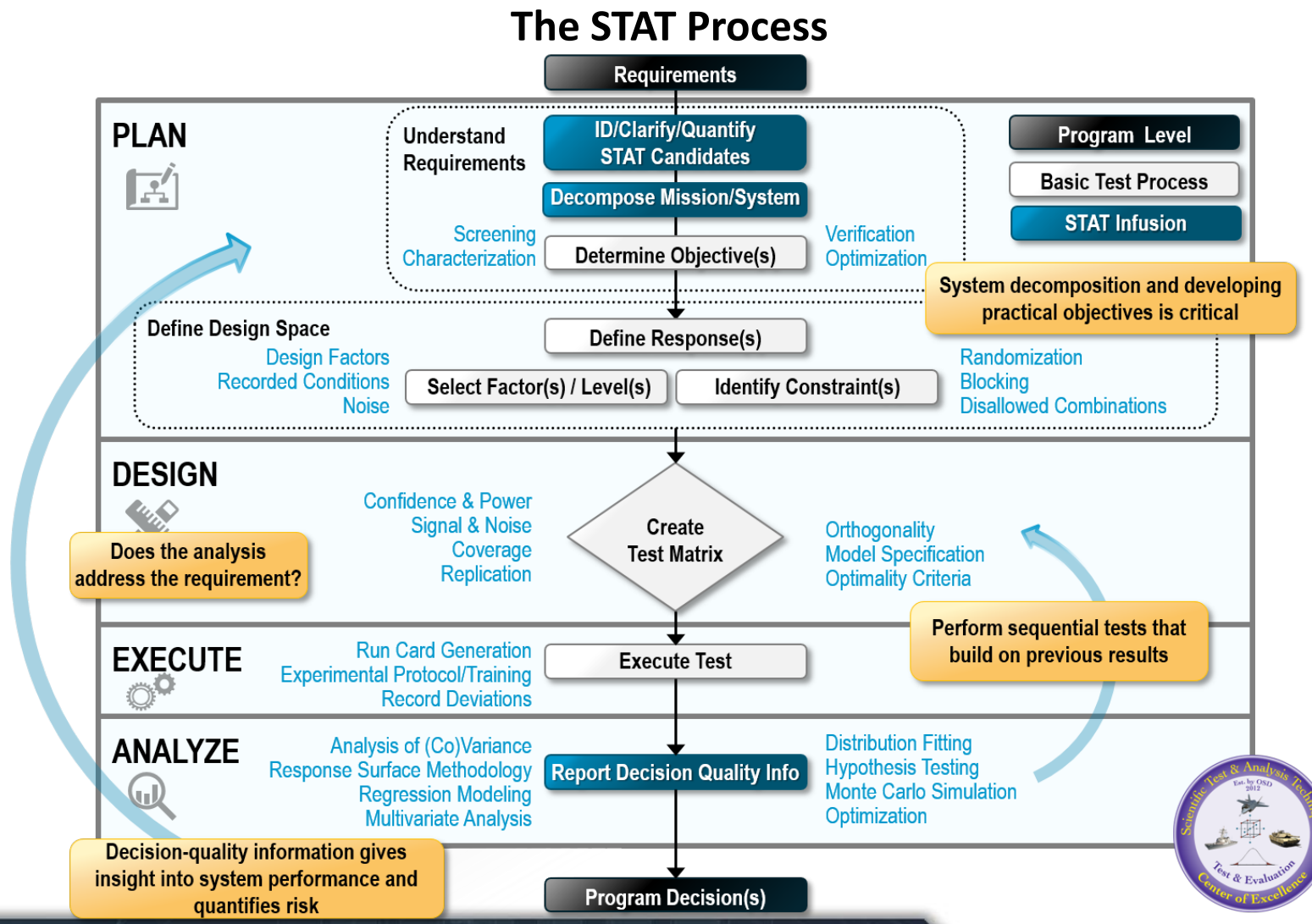
Digital Engineering and Testing in Virtual Environments

- Digital Engineering leverages models in a digital architecture to
  - **Accelerate** engineering design, test, evaluation, & analysis (TE&A)
  - **Virtualize** T&EA to reduce testing costs
  - **Continuously update** models & data to improve processes & procedures
  - **Reuse** models & data to prevent rework and carry forward lessons learned
- Digital Engineering builds on and augments other processes & technologies
  - MBSE, engineering design, Defense Acquisition
- Enterprise Digital Engineering feeds back into future engineering, requirements, logistics, and lifecycle management
- Model validity and readiness are critical to Digital Engineering and can be addressed via quantifiable, STAT-rigorous methods

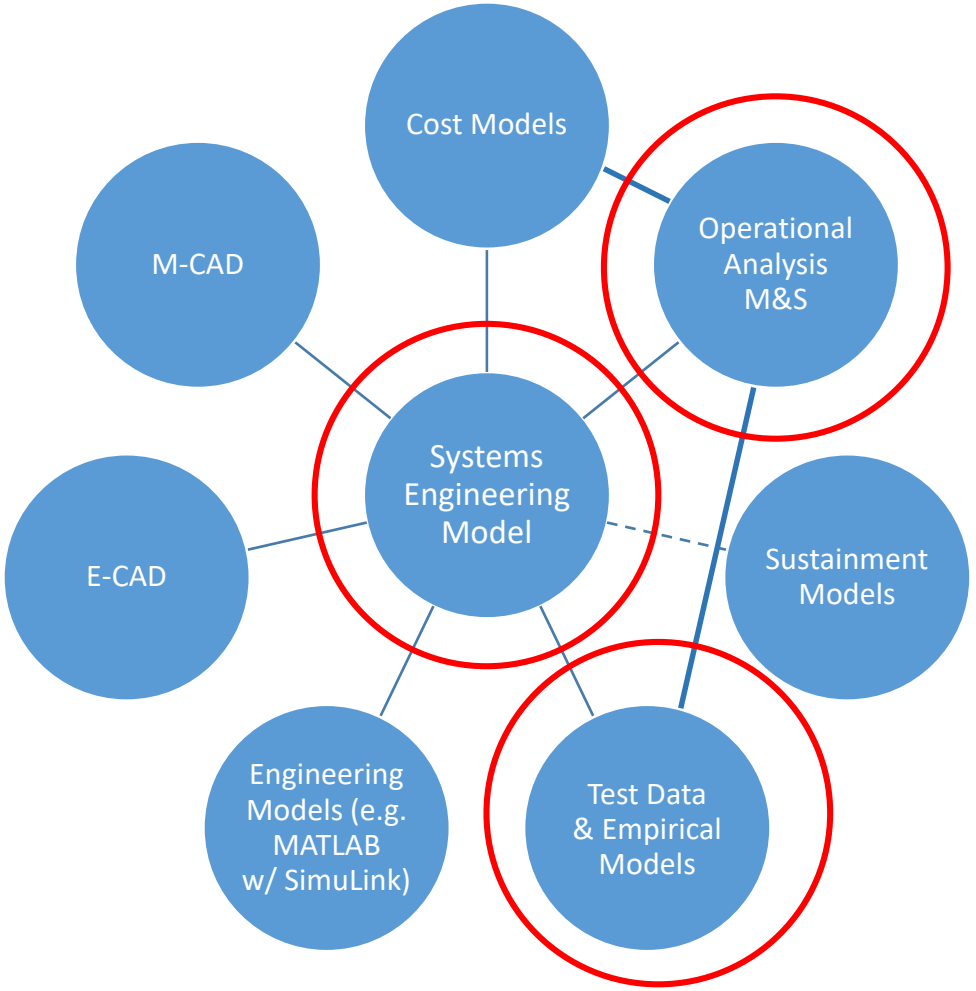
Digital Engineering and T&E support each other to accelerate development while reducing physical investment, STAT supports both

Test Planning in Digital Engineering

- Effective test planning is critical to successful testing and information for model Validation
- Test planning in Digital Engineering presents unique concerns:
  - Physical testing may not be feasible at all stages
  - M&S testing needs VV&A to be trustworthy
  - Difficult to know if models are ready for use when little physical reference data exists for VV&A



Digital Engineering Models

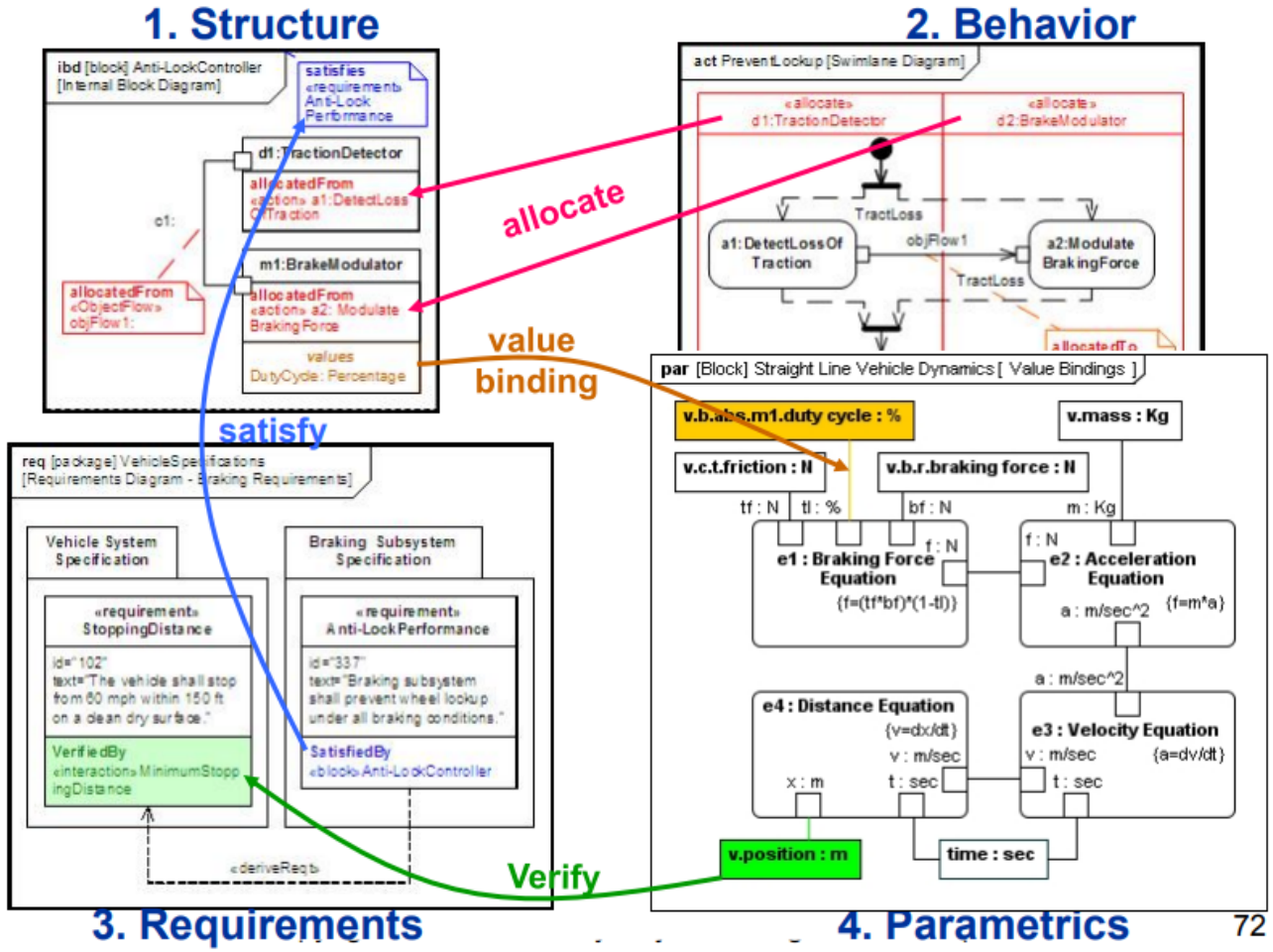


Focus of Today's Presentation

The MODELS are the authoritative source of truth

Model-Based Systems Engineering (MBSE)

- MBSE is a Systems Engineering Framework that tracks system attributes and requirements in a system architecture model
- Built on modeling languages like SysML
  - SysML uses Structure, Behavior, Requirements, and Parametric elements to capture and enforce relationships between system physical, functional, and required attributes
- MBSE provides numerous benefits
  - Provides Requirements traceability
  - Captures component relationships
  - Tracks and applies design constraints
  - Facilitates shared understanding and communication of design



Friendenthal, S, Moore, A., & Steiner, R. OMG Systems Modeling Language (OMG SysML™) Tutorial, 2009

All Digital Engineering models must be consistent

STAT in Physical and Simulated Test Environments for V&V Comparison

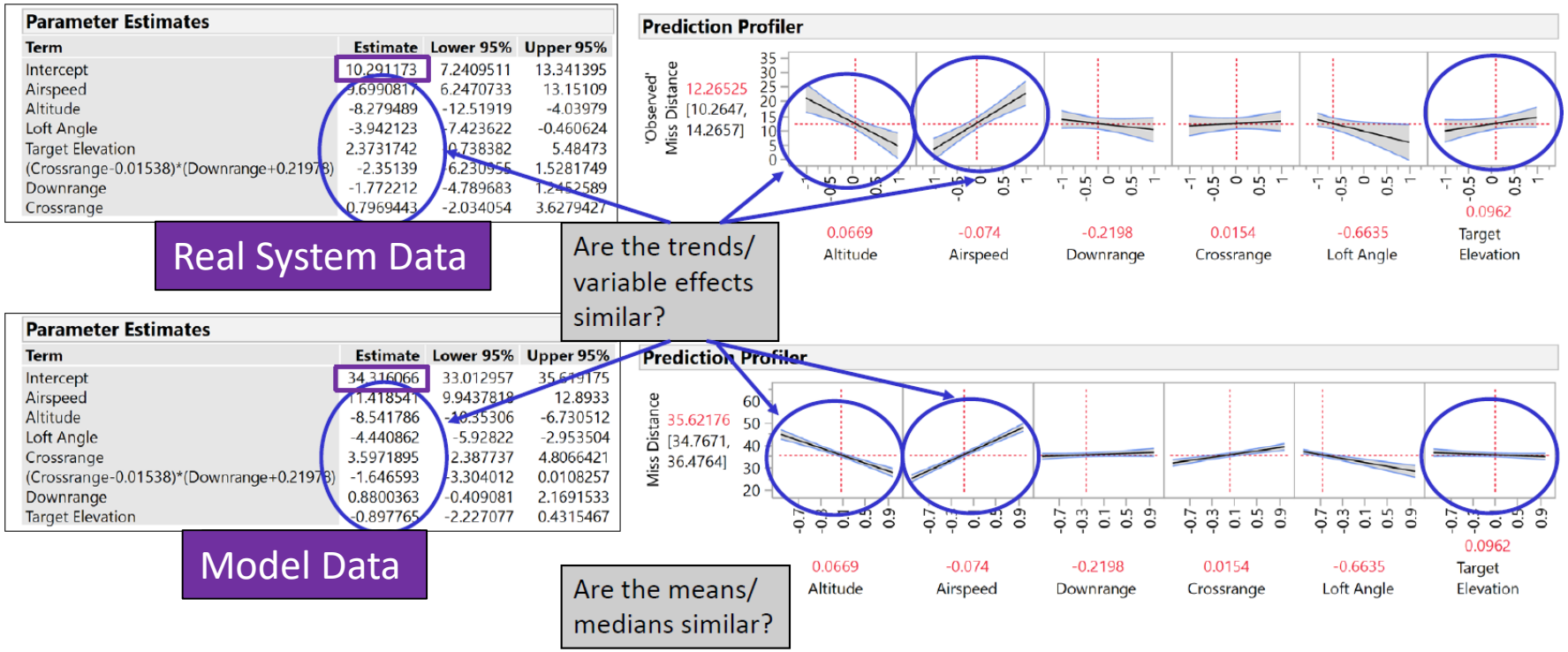
- STAT applies to both physical and simulated (M&S) environments
- STAT still strives for effective and efficient testing
- For successful physical and simulation testing, planning is critical

Physical Testing	Simulation Testing
Typically limited by schedule, test range, and test resources	May involve deterministic simulations with no variability
Typically limited by safety and manpower concerns	STAT methods seek to cover model space as fully as possible
STAT methods seek to understand system variability and coverage	Allow exploration of potentially dangerous operating regions
Meaningful results require rigorous test design	Larger numbers of test runs may be available
	Meaningful results require rigorous test design AND trusted models

Simulation testing seeks to understand the system being represented by a model, not the model itself

STAT for Validation of Models in Simulation

- STAT for validation differs from STAT for virtual testing because validation seeks to assess the quality of the model, not the properties of the modeled system



How does Digital Engineering Support T&E?

- Digital Engineering leverages models in a digital architecture to ensure program ownership of their technical baseline
- DE accomplishes this through:
  - **Reuse** models & data to prevent rework and carry forward lessons learned
    - Enabled by Digital Thread
  - **Virtualize** T&E to reduce testing costs
    - Enabled by Digital Twin and supported by Digital Thread
  - **Continuously update** models & data to improve processes, procedures, operations, & logistics
    - Enabled by Digital Telemetry and supported by Digital Thread
  - **Accelerate** engineering design, test, & evaluation
    - **Leverage the interplay of Digital Twin, Digital Telemetry, and Digital Thread**
- Use Cases (GBSD, T7, Space/ISR systems)

Digital Engineering leads to better systems engineering and acquisition decisions

Model Readiness Levels

- MRLs provide:
  - A measure for model developers to continuously improve their models
  - A means for decision makers to better understand the risk with making decisions based on models
- In order to accomplish this, MRLs need to:
  - Be usable
  - Be comprehensive
  - Have mathematical rigor and consistency
- Existing methods do not address all of these properties

An MRL needs to assess multiple aspects of the model

What Dimensions Matter in an MRL?

Fidelity

Image Credits: STAT COE



Model Referent

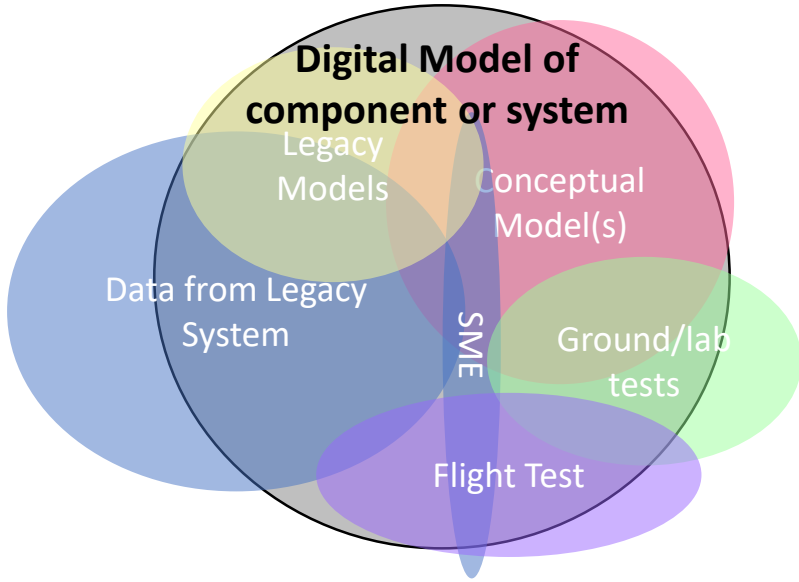
Fidelity quantifies model similarity to referent in 4 dimensions of **detail**

Authority

Authority Level	Relevant Referent
1	SME Judgement
2	First Principles/Physics Predictions
3	Subcomponent Lab Test Data
4	Component Lab Test Data
5	Lab-Scale System Test Data
6	Prototype Test Data
7	HWIL & SWIL Data
8	Live System Test Data
9	Operational Real-World Data

Referent Authority Ranking quantifies trust in **baseline** of comparison

Scope



Scope quantifies degree to which model and referent represent the **same system**

The MRL draws on the 3 Pillars of Validation to ensure the right things are compared, they behave the same way, and we trust the baseline

Dimensions of Fidelity

- **Fidelity**

  The level of detail in the model or simulation relative to the real world.

  - **Resolution**
    - Amount of uncertainty in observed value (M&S output) due to computational limitations
    - Rounding errors, precision of numerical calculations, precision of measurements
  - **Accuracy**
    - The difference between what the model should produce and what it actually produces
    - Are there tendencies to underestimate or overestimate results?
  - **Repeatability**
    - The variability in a *simulation* across runs with the same input conditions
    - Synonymous with statistical definition of precision
  - **Consistency**
    - Limiting behavior of M&S as resolution increases and/or repetitions increase trends towards expected result

Accuracy and Consistency require a valid referent.
Resolution and Repeatability do not (internal checks).

Fidelity



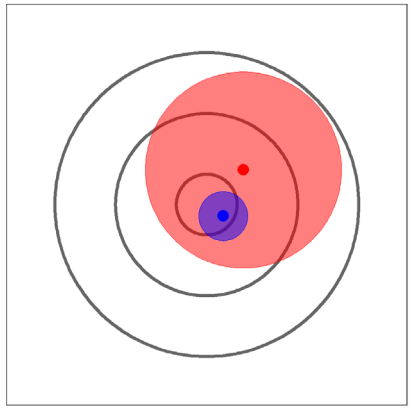
Model



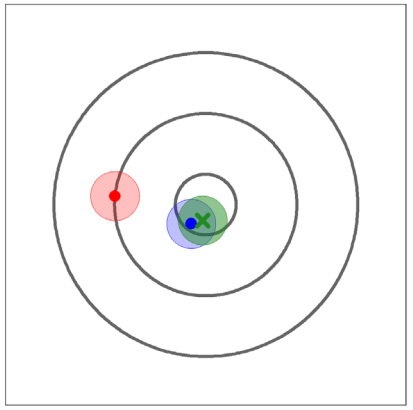
Referent

- Fidelity quantifies the level of detail in a model by its behavior in four dimensions
  - Accuracy:
  - Repeatability
  - Consistency
  - Resolution

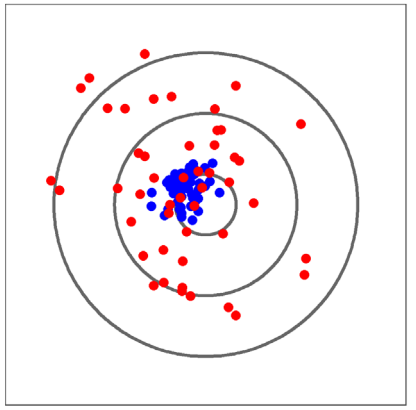
Resolution



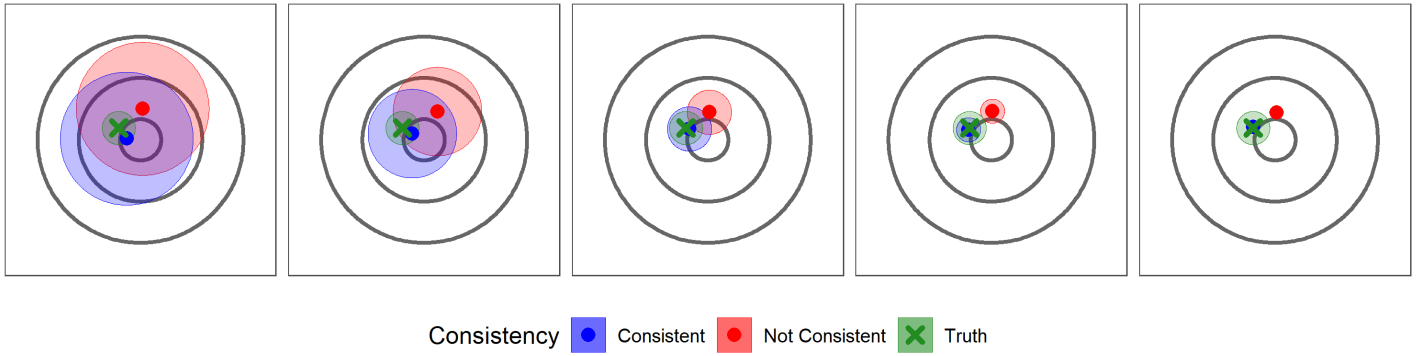
Accuracy



Repeatability



Consistency



Fidelity quantifies model similarity to referent in 4 dimensions of detail

Image credits: STAT COE

Referent Authority

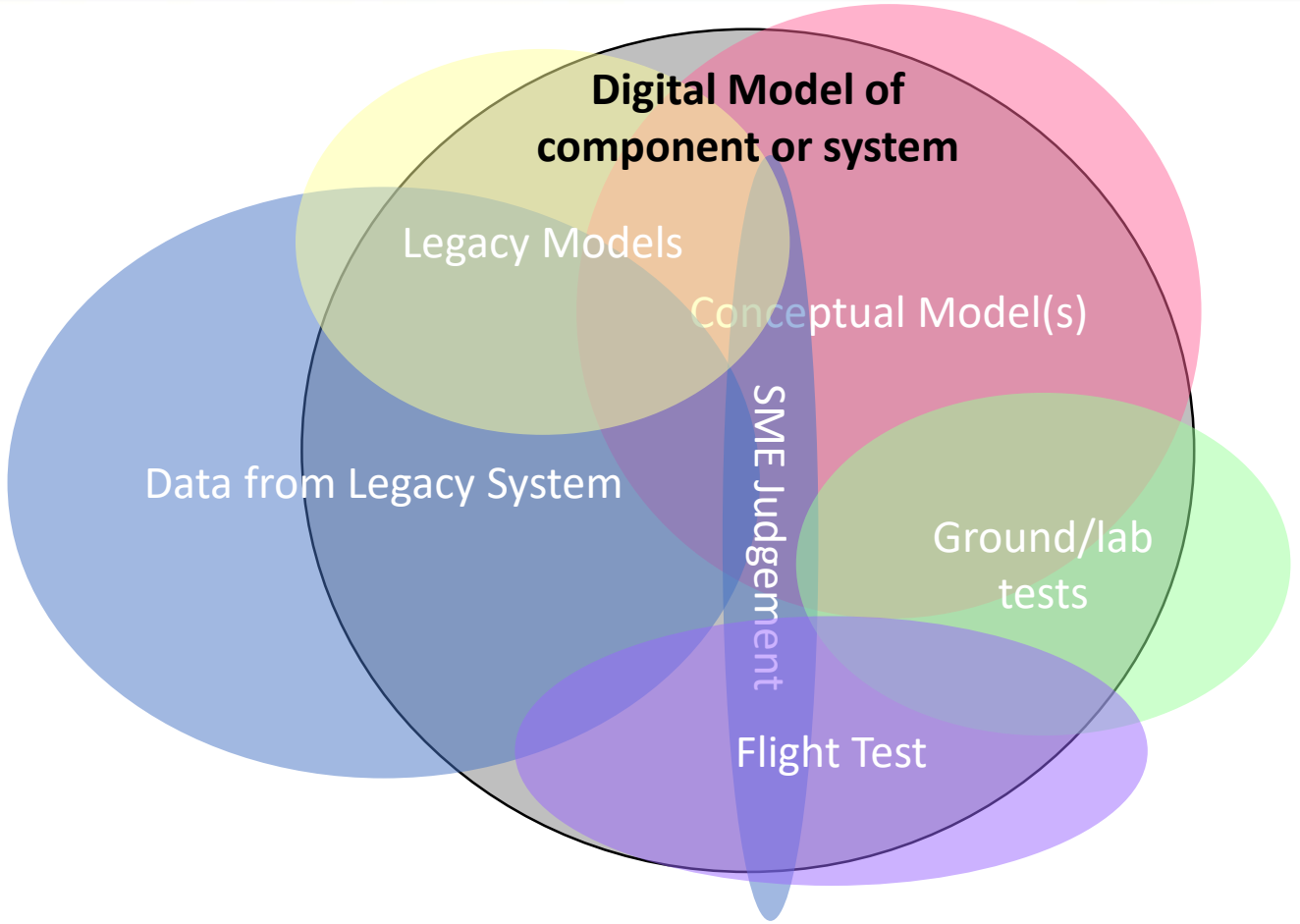
- Referent authority level is similar to TRLs:
  - To declare a technology at a TRL, some evidence must exist to show that the technology has been demonstrated at that TRL
  - That evidence is a referent trusted to that Readiness Level
  - A referent can transfer trust to a model up to its own level of authority
- Multiple referents of the same or different authority levels may be used
  - Referents can be weighted appropriately using a Rank Order Centroid (ROC) method applied at each authority level

Authority Level	Relevant Referent
1	SME Judgement
2	First Principles/Physics Predictions
3	Subcomponent Lab Test Data
4	Component Lab Test Data
5	Lab-Scale System Test Data
6	Prototype Test Data
7	HWIL & SWIL Data
8	Live System Test Data
9	Operational Real-World Data

Referent Authority quantifies trust in baseline of comparison

Scope

- Scope quantifies degree to which model and referent represent the same system
  - Scope compares the modeled variables, effects, and constraints to those present in the referent data
  - Referents which cover more of the model scope can validate more of the model and contribute more to model readiness
  - Several referents may be used to cover the full scope of a model
  - Coverage is multidimensional

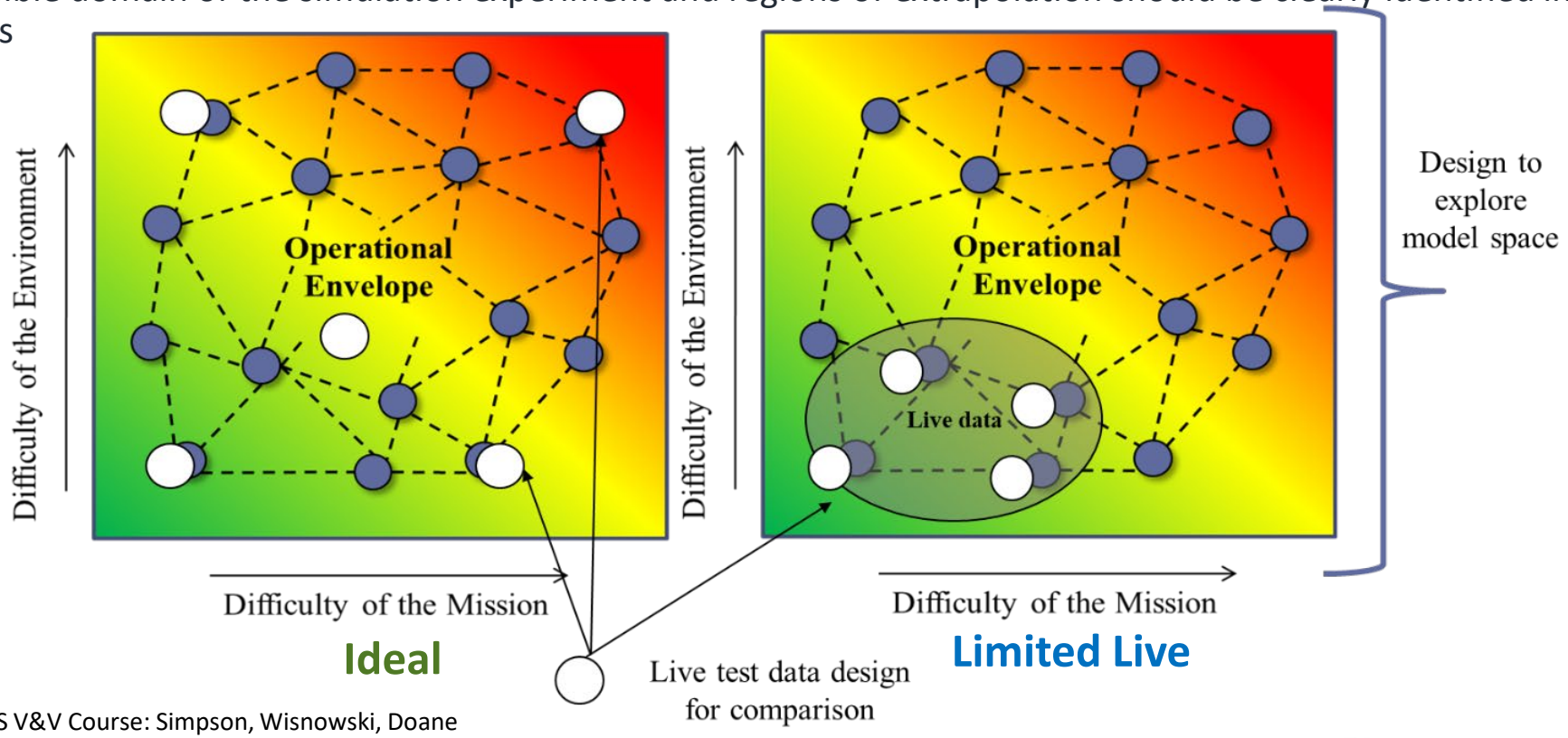


Scope quantifies degree to which model and referent represent the same system

Scope: Test Design Simulation vs. Live

Strategies for selecting the design space and points for live and simulation-based testing

- **Ideal**: the live design encompasses the simulation design space so comparisons between them are interpolations, not extrapolations
- **Limitation in Live Space**: often due to practical constraints that exist in live testing. Here the domain of the live testing should span the maximum possible domain of the simulation experiment and regions of extrapolation should be clearly identified in the validation limitations



Slides from STAT in M&S V&V Course: Simpson, Wisnowski, Doane

Fidelity: A Potential Measure

Fidelity Metric: Exponential Accuracy & Variability



Model

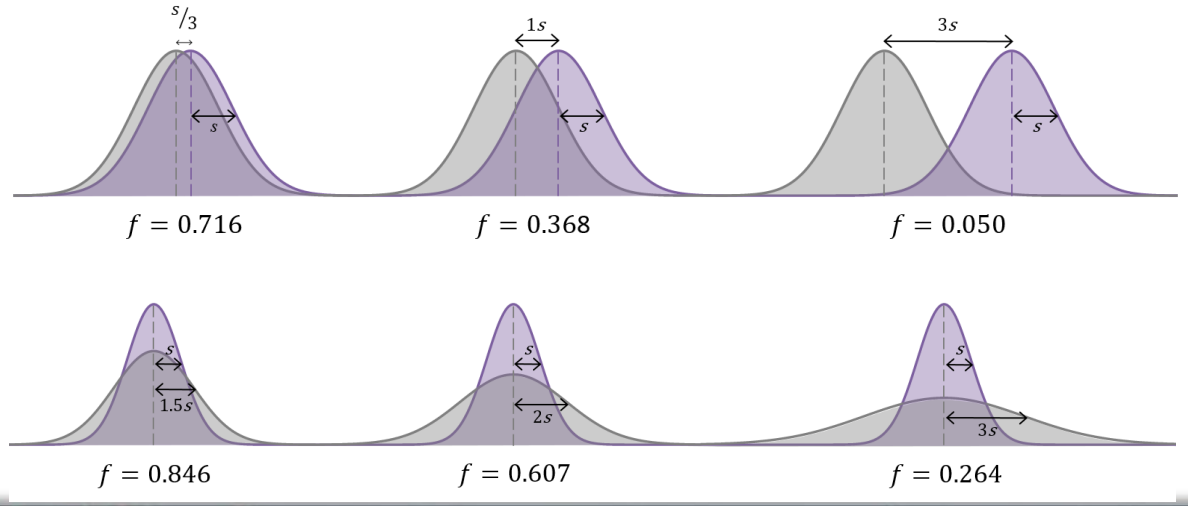


Referent

- Metric assesses both accuracy, repeatability, and resolution
  - Define $s^* = s + \delta$ as variability, where
    - s is the standard deviation, used for representing repeatability
    - δ is the resolution

$$f = f_a f_v = e^{-\left|\frac{\bar{x}_m - \bar{x}_r}{s_r^*}\right|} e^{-\frac{(s_m^* - s_r^*)^2}{s_m^* s_r^*}}$$

  - Requires that all models (stochastic or not) have a measured resolution



- Difference of means equal to one standard deviation:

$$f_a = e^{-\frac{|\bar{x}_m - \bar{x}_r|}{s_r}} = e^{-1} = 0.368$$

- Difference of means equal to three standard deviations:

$$f_a = e^{-3} = 0.050$$

Takeaways

- Digital Engineering provides the potential for increased innovation, agility, and quality
- STAT complements Digital Engineering in two ways:
  - Rigorous and defensible model validation
  - Efficient and effective test design
- MRLs must be useable & comprehensive with mathematical rigor and consistency
- MRLs facilitate continuous model improvement and informed decisions from models
- Test and evaluation is about determining the test events required, ensuring rigorous test planning that feeds effective evaluation

Questions?











More information at www.afit.edu/STAT as it becomes releaseable

Improving Digital Engineering and Modeling and Simulation Integration to Support Technology Adoption in Department of Defense (DoD) Systems

Philomena Zimmerman
Director, Engineering Tools and Environments

John Daly
Engineering Tools and Environments Mission Support

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

Approved for public release. DOPSR Case #22-S-0258.

Abstract

Integrating technology advances into Department of Defense (DoD)systems requires a change in environment from research and development to acquisition. Adoption of digital systems engineering early in technology development may assist in improving the application of modeling and simulation capabilities for describing system physics, design, performance, and linking system requirements directly to mission performance outcomes. There are challenges in blending a largely physics-based modeling and simulation research and development environment into systems-based DoD capability development and mission-based warfighting utility environments. Each has differing levels of detail, types of analysis, data and availability, and the required level of validity and trust of results. All are part of the overall systems engineering process and digital engineering practice can improve their integration. Continuous feedback on performance in all phases of acquisition is needed, and this is possible practically when a digital engineering construct is used from technology development to fielding and sustainment.

Approved for public release. DOPSR Case #22-S-0258.

Authors

Philomena Zimmerman
OUSD(Research & Engineering)
Director, Engineering Tools and Environments (OUSD(R&E)/ETE)

John Daly
Mission Support (OUSD(R&E)/ETE)

Valerie Schalk
Mission Support (OUSD(R&E)/ETE)

Scott Schutzmeister
Mission Support (OUSD(R&E)/ETE)

Michael Guba
Mission Support (OUSD(R&E)/ETE)

Approved for public release. DOPSR Case #22-S-0258.

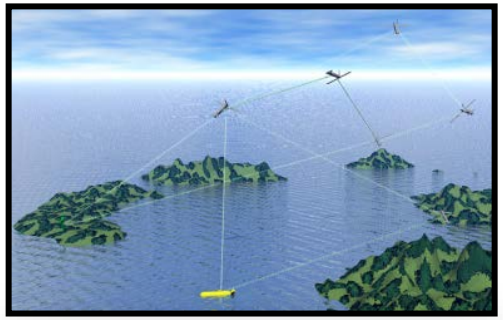
Outline

- **Digital Engineering**
- **Modeling and Simulation**
- **Modeling and Simulation Across Acquisition Today**
- **Engineering Activities Enabled by Modeling & Simulation and Digital Engineering**
- **Technology R&D Modeling and Simulation:**
  - Example: *Availability of Models, Simulations, Data, Results*
  - Example: *Challenge in scaling Models and Simulations*
  - Example: *Interoperability of Models, Simulations, Data, Results*
  - Example: *Validity and Trust of Models and Simulations*
- **A Digital Engineering Continuum**
- **Benefits & Expectations**

Approved for public release. DOPSR Case #22-S-0258.

USD(R&E) Mission

- **Ensure Technological Superiority for the U.S. Military**
  - Set the technical direction for the Department of Defense
  - Champion and pursue new capabilities, concepts, and prototyping activities throughout the DoD research and development enterprise
- **Bolster Modernization**
  - Pilot new acquisition pathways and concepts of operation
  - Accelerate capabilities to the warfighter





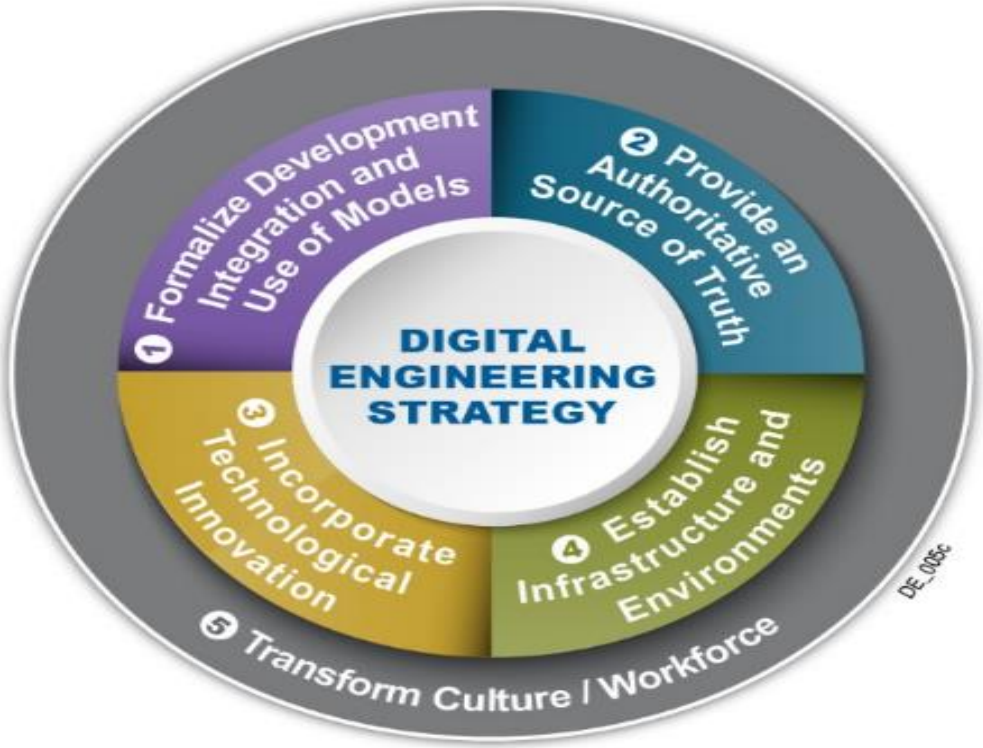


Approved for public release. DOPSR Case #22-S-0258.

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

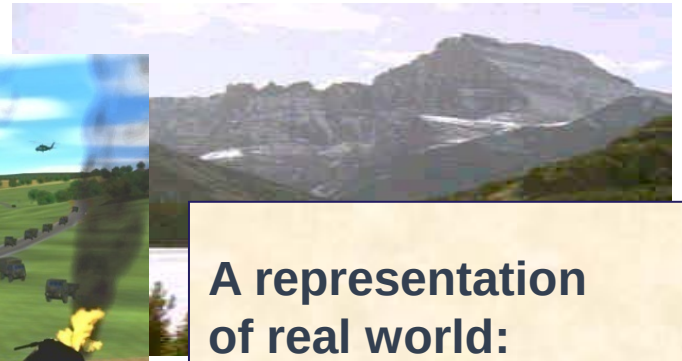
1. Formalize the **development, integration and use of models** to inform enterprise and program decision making
2. Provide an enduring **authoritative source of truth**
3. Incorporate **technological innovation** to link digital models of the actual system with the physical system in the real world
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



Approved for public release. DOPSR Case #22-S-0258.

What Is Modeling and Simulation?



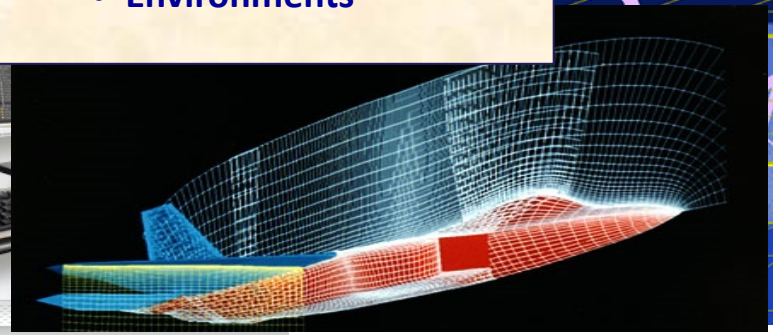


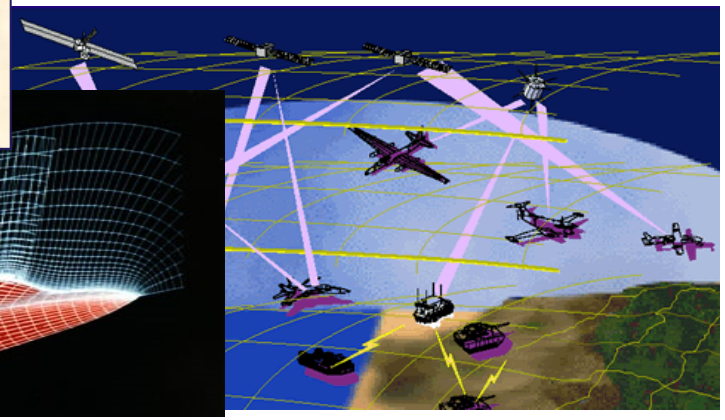


A representation of real world:

- **Equipment**
- **People**
- **Activities**
- **Processes**
- **Environments**







In the systems engineering of DoD capabilities, models and simulations are tools used to describe that capability in the level of detail required in engineering, development, acquisition and mission environments

Approved for public release. DOPSR Case #22-S-0258.

Key Modeling and Simulation Terms

There are a number of definitions of models, simulations, and modeling and simulation. Below are definitions published by the Department of Defense (DoD):

Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.

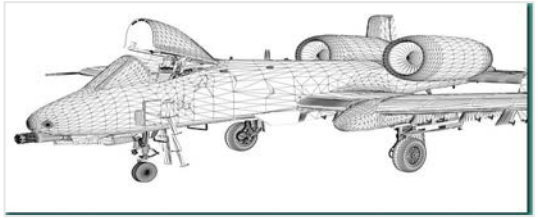
Simulation: A method for implementing a model over time.

Mathematical Model

$$\frac{dv}{dt} = a\left[1 - \left(\frac{v}{v_o}\right)^{\delta} - \left(\frac{s^*}{s}\right)^2\right]$$

$$s^* = s_o + \left(v'1' + \frac{v\Delta v}{2\sqrt{ab}}\right)$$

Wire Frame Model



- ***Engineers like to use "Modeling" to describe how they use these techniques in R&D and engineering analysis- "modeling" physics-based complex phenomena dynamically***
- ***Operations/Mission analysts like to use "Simulation" as they are approximating an operational environment in a realistic manner – executing models of all aspects in time***

Ref: Department of Defense Modeling and Simulation (M&S) Glossary, July 1, 2013. Available at http://www.msco.mil/MSGlossary.html

Approved for public release. DOPSR Case #22-S-0258.

Engineering Activities

Enabled by Modeling & Simulation and Digital Engineering

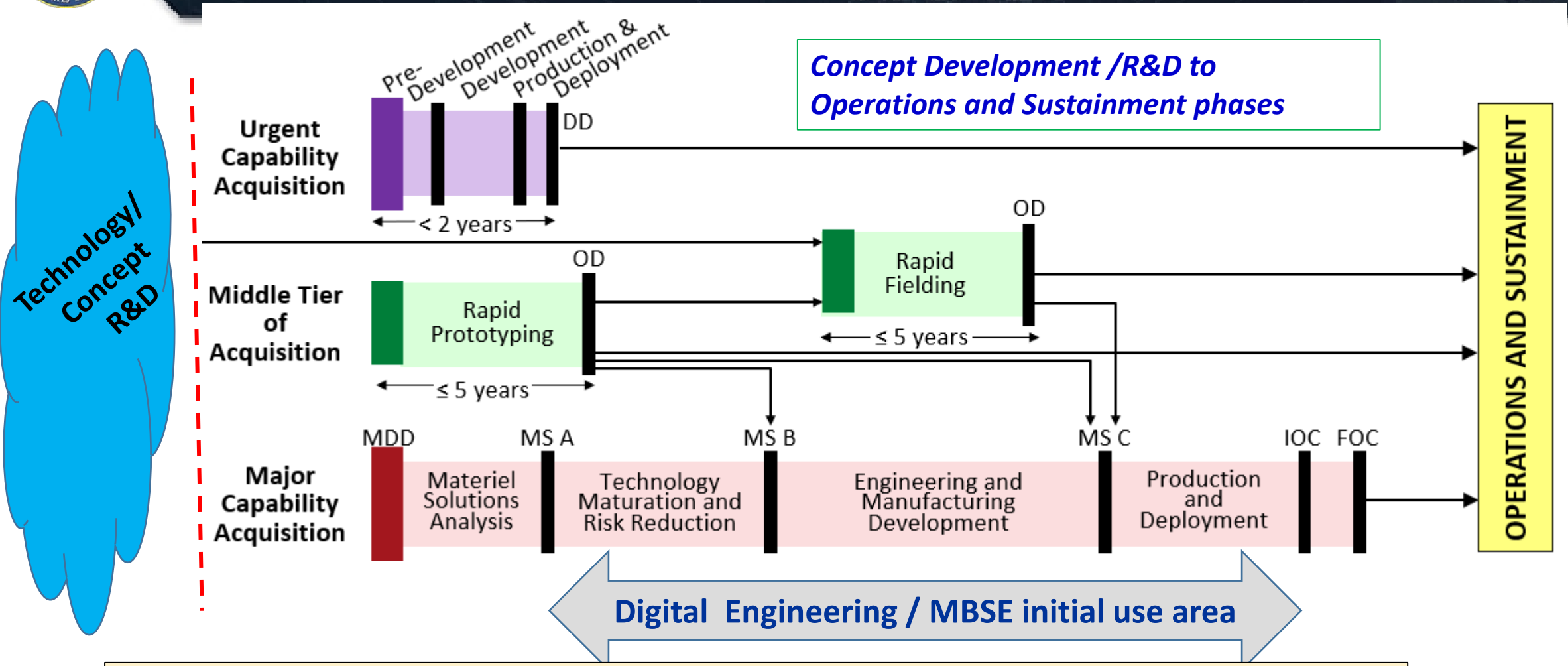
- Conduct analysis of mission scenarios and capabilities
- Explore new concepts and processes
- Investigate futuristic scenarios without risking harm to humans and/or infrastructure and integrate experiments into training and/or operational tests
- Prototyping capabilities in realistic conditions
- Enable virtual testing of complex and non-physical systems
- Determine actual mission performance of technology advances
- Organize modeling along a process with appropriate data/context digitally



Modeling and Simulation is typically used to address specific problem sets, more depth and not breadth; and Digital Engineering looks to integrate breadth and depth to ensure consistency

Approved for public release. DOPSR Case #22-S-0258.

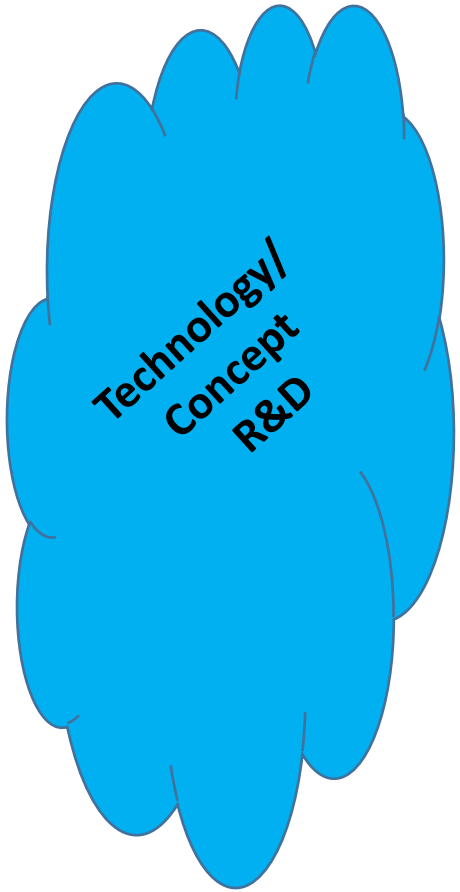
Modeling and Simulation Across Acquisition Today



Acquisition use of modeling and simulation is in nodes/stages enabled by digital engineering.... but little integration from Technology/Concept R&D and Acquisition

Approved for public release. DOPSR Case #22-S-0258.

Technology R&D Modeling and Simulation



Key Problem Areas:

- ***Availability of Models, Simulations, Data, Results***
- ***Challenge in scaling Models and Simulations Across Acquisition Phases, Needs and Purposes***
- ***Interoperability in R&D phase and beyond***
- ***Validity and Trust of Models and Simulations***

Some other Representative Problem areas:

- Valid physics representations using mod/sim based on available tools (not understanding limitations/assumptions)
- Expansion of physics-based R&D modeling tools to more accurately inform mission and decision - level capability analysis in the SE domain
- Prototyping - how much (detail) digital representation is required during development and during transition to Programs of Record?
- Challenges in blending/scaling data, models, and results from a largely physics-based modeling and simulation research and development environment into a systems-based DoD acquisition environment

Approved for public release. DOPSR Case #22-S-0258.

Example: Availability of Models, Simulations, Data, Results

- Exchange of models, data, and results more effectively between industry and Government entities. A more open (but secure) exchange of data, results of modeling and even models themselves would increase DoD's ability to overmatch adversaries (NDIA??)
- Models, simulations, data, and results are often "silo'ed" by organizations inadvertently. A digital discovery/exchange mechanism to allow potential users to find the tools and data as well as supporting "pedigree" and user information is a common need
- A virtual environment where modeling and simulation tools, licenses, and their data can be available (cloud hosted) on an "as needed" virtual basis (in various level of classification) to desktop users anywhere. This can be a key enabler of more widespread use and effectiveness of these tools and data

A Digital Engineering ecosystem could provide the tools, data and applications in one place for a user

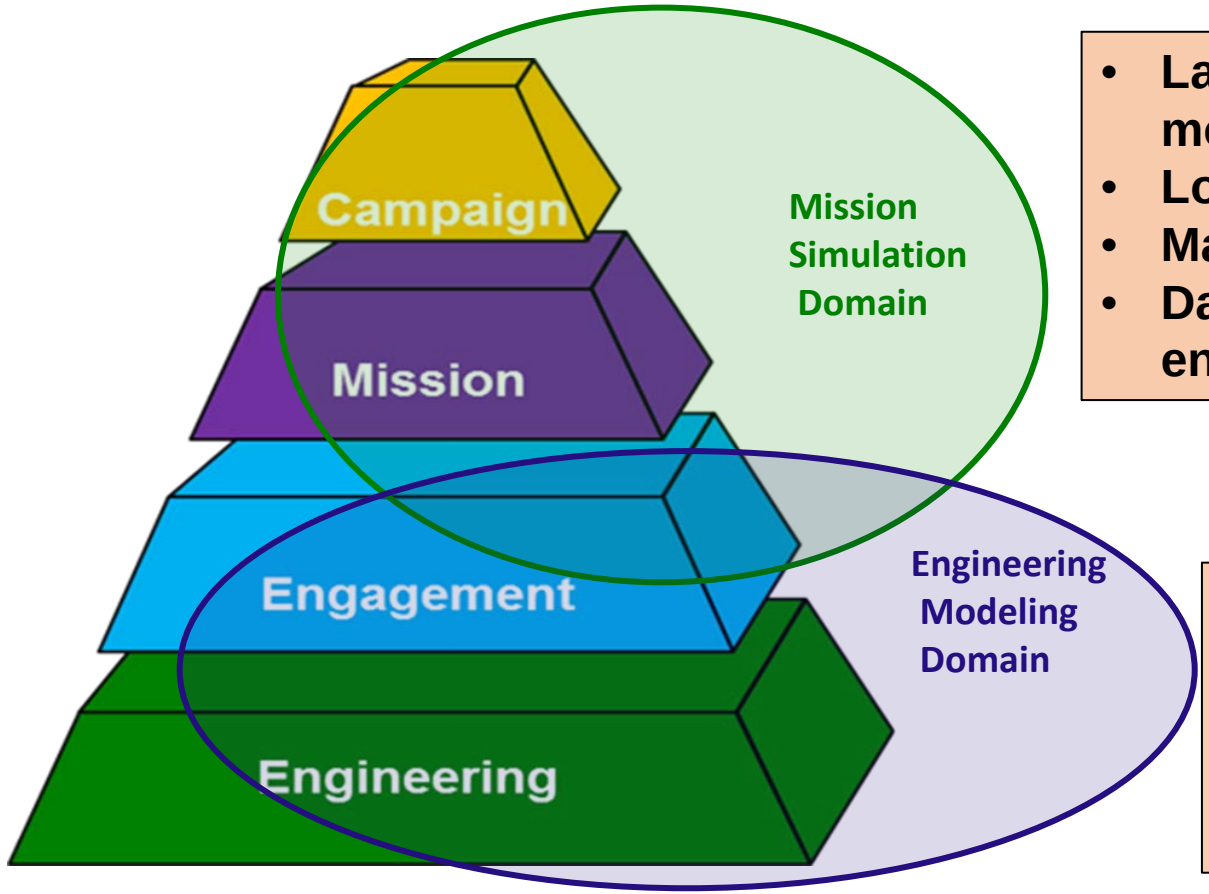
Approved for public release. DOPSR Case #22-S-0258.

Example: Challenge in Scaling Models and Simulations Across Acquisition Phases, Needs, and Purposes

System of Systems
Mission Performance

SE Process

System Development
Technology R&D



- Larger-scale: Multiple models/sims
- Lower resolution – broader range
- Macro insights – Mission +
- Data resolution lower- but more entities = Huge amounts of data

- Smaller-scale: System/component focus
- Focused insights
- Detailed data needs for high resolution analysis

Digital engineering tools could provide digital continuity up/down the Pyramid from Technology development to Mission use - <u>following the fundamental SE process</u>

Approved for public release. DOPSR Case #22-S-0258.

Example: Interoperability in R&D Phase and Beyond

- The classic "unintended use" problem in applying a model to uses that are unanticipated by the developer. The developer tendency is to restrict availability to prevent invalid use, but this also impedes valid use outside of the originating organization, and into capability development and mission-based warfighting utility environments
- There is no fundamental digital commonality in data or software among many of the models and simulations used in all phases of R&D and acquisition – especially those used in "deep dive" analysis on an aspect. Thus, they are not informed or interoperable with the models describing the overall characteristics of the system
- A baseline of overall system behavior is key towards moving insight from R&D into and across the various stages of acquisition- possibly a composable digital twin concept in a DE environment?

Digital engineering tools could provide digital continuity across all phases from Technology development to Mission use and provide continuity of modeling and simulation tools and data across organizations, functional uses, and scale of use to support system development – in a systems engineering construct

Approved for public release. DOPSR Case #22-S-0258.

Example: Validity and Trust of Models and Simulations

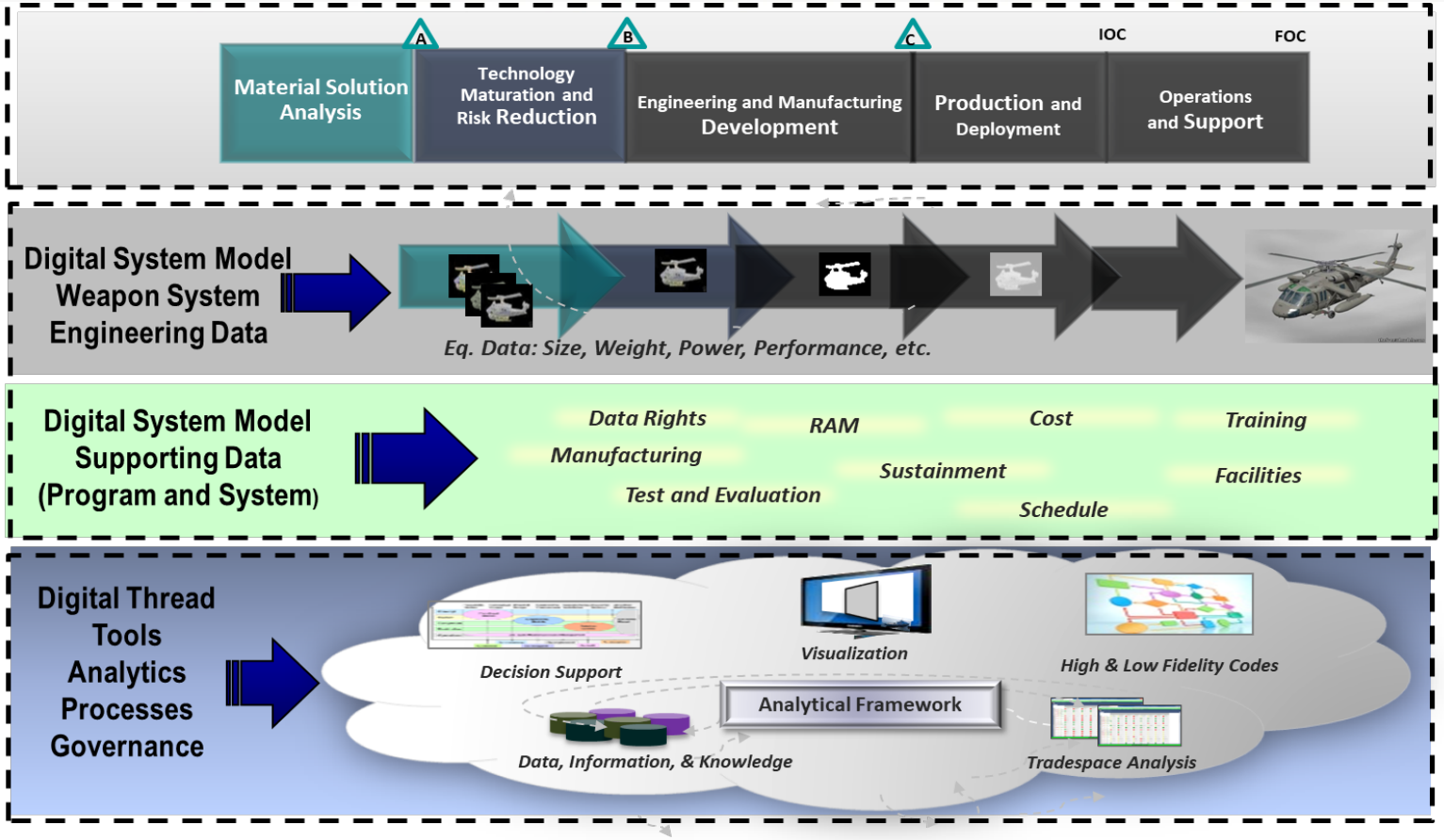
- Validity and Trust are key attributes of models, simulations and their data that are required for any use. But outside the developer, that critical information is not often known or available. A digital "pedigree" in a DE framework might enable more widespread use of DoD R&D models/simulations and their results
- Commonality of Validation and Verification (V&V) techniques, practice and description are issues in the use of models and simulations in the R&D environment and between acquisition phases
- A digital engineering framework/continuum could embed the V&V/Trust attributes directly into digital representations of models, simulations and their data

Digital engineering tools could host a "pedigree" of a model, simulation, or data set containing key attributes: validity, testing information, and specific capability and limitations – in a digital continuum across all phases from Technology development to Mission use – establishing trust in use based on that digital "pedigree"

Approved for public release. DOPSR Case #22-S-0258.

A Digital Engineering Continuum

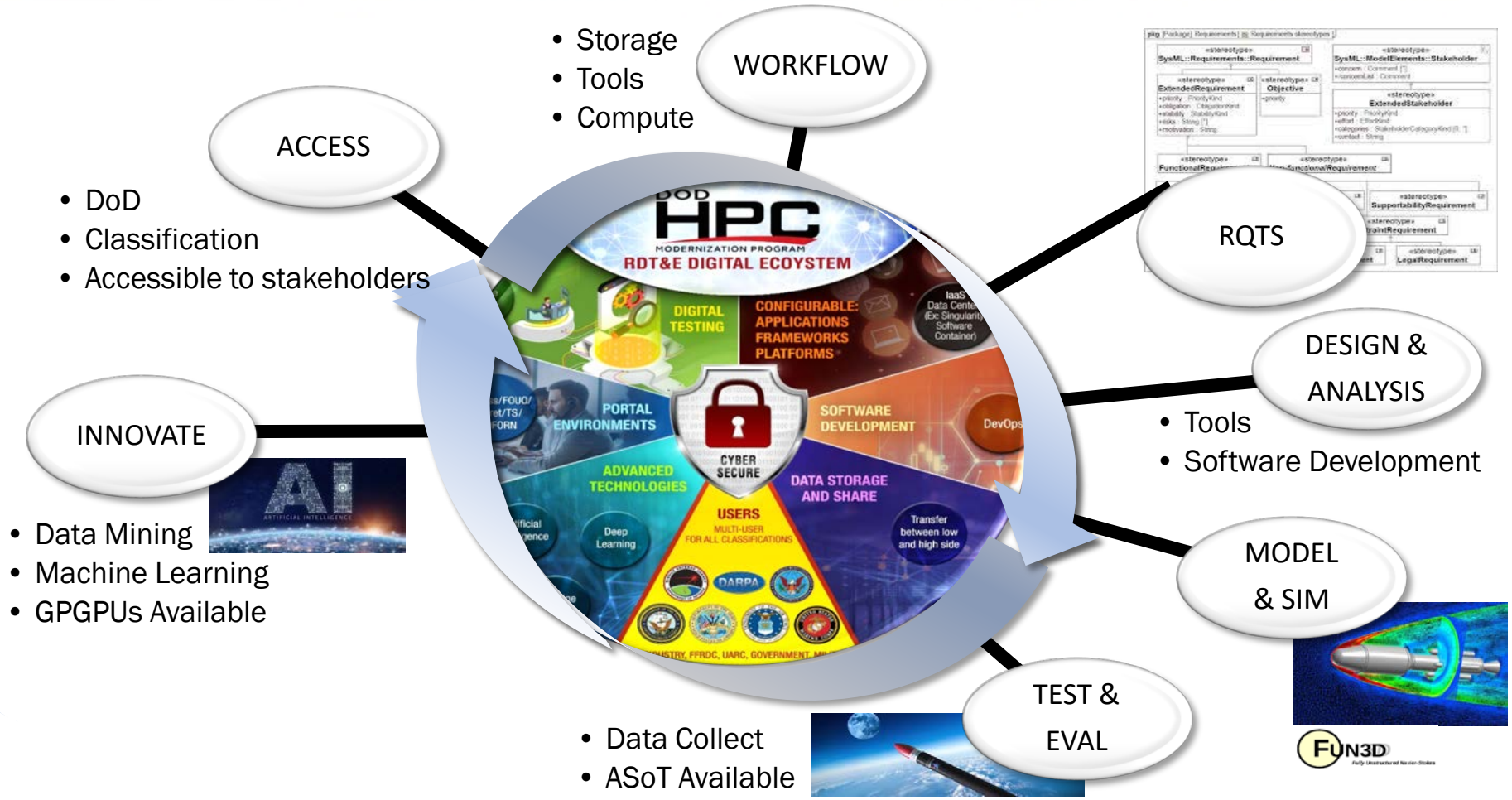
- Digital Engineering Model-Based Systems Engineering (MBSE) type tools are designed to enable a process: the development, testing and fielding of capabilities based on the SE process and lifecycle **– why not expand their use to promising technologies of interest?**
- They can provide a continuum of digital information and models/simulations in the context of what we are trying to accomplish: a systems engineering process – A **Framework for Communication**



A Digital Engineering - systems engineering approach from R&D to deployment in a digital computational continuum can support accelerated adoption of promising technology development (e.g. DoD Technology Modernization priorities) with systems engineering rigor

Approved for public release. DOPSR Case #22-S-0258.

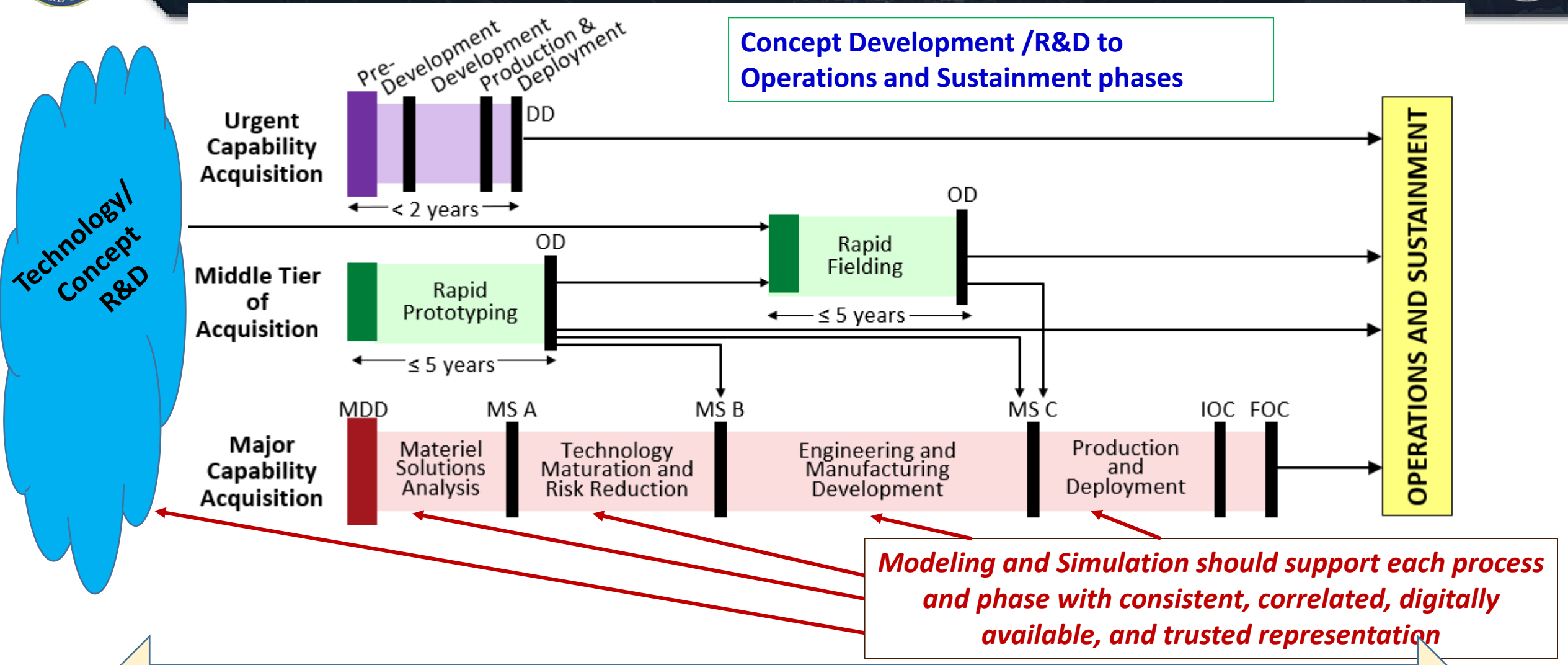
Digital Ecosystem



A Digital R&D ecosystem would benefit all partners and jump-start the Prototype to System process

Approved for public release. DOPSR Case #22-S-0258.

Modeling and Simulation Across Acquisition – A Continuum



Approved for public release. DOPSR Case #22-S-0258.

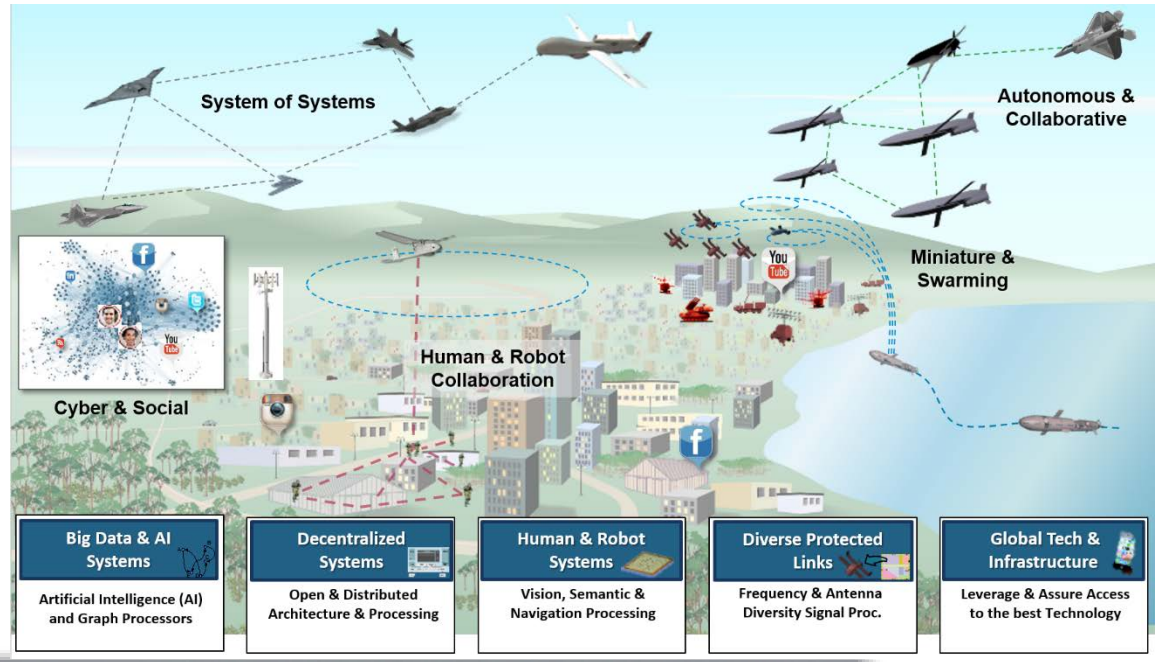
Benefits & Expectations

Digital engineering is structured to support engineering users.
Modeling and Simulation is a core capability to this mission through the use of formalized models.

- Digital Engineering integrates disparate models, simulations, data, analytics, design, visualization and collaboration tools that enterprises require
- Models and simulations are critical components of Digital Engineering that provide deep insight
- Digital Engineering depends on the practice of developing, accurately characterizing, using, reusing and curating models and simulations, and related items, such as interoperation of simulations, standards, etc.

Expectations:

- Traceability established between models and the requirements for verification and validation
- Traceability established between models and the simulations that use them
- Traceability established between models and the solution components that those models represent



Approved for public release. DOPSR Case #22-S-0258.

For Additional Information

Philomena Zimmerman
OUSD(Research & Engineering)
Engineering Tools and Environments (OUSD(R&E)/ETE)
Philomena.M.Zimmerman.civ@mail.mil

John Daly
Mission Support (OUSD(R&E)/ETE)
John.j.daly26.ctr@mail.mil

Valerie Schalk
Mission Support (OUSD(R&E)/ETE)
<valerie.l.schalk.ctr@mail.mil>

Scott Schutzmeister
Mission Support (OUSD(R&E)/ETE)
scott.schutzmeister.ctr@mail.mil

Michael Guba
Mission Support (OUSD(R&E)/ETE)
<paul.m.guba.ctr@mail.mil>

Approved for public release. DOPSR Case #22-S-0258.

Contact

Office of the Deputy Director for Engineering

osd.r-e.comm@mail.mil

Attention: Digital Engineering

ac.cto.mil/engineering

Approved for public release. DOPSR Case #22-S-0258.

Correlated Digital Representation Across System Lifecycle

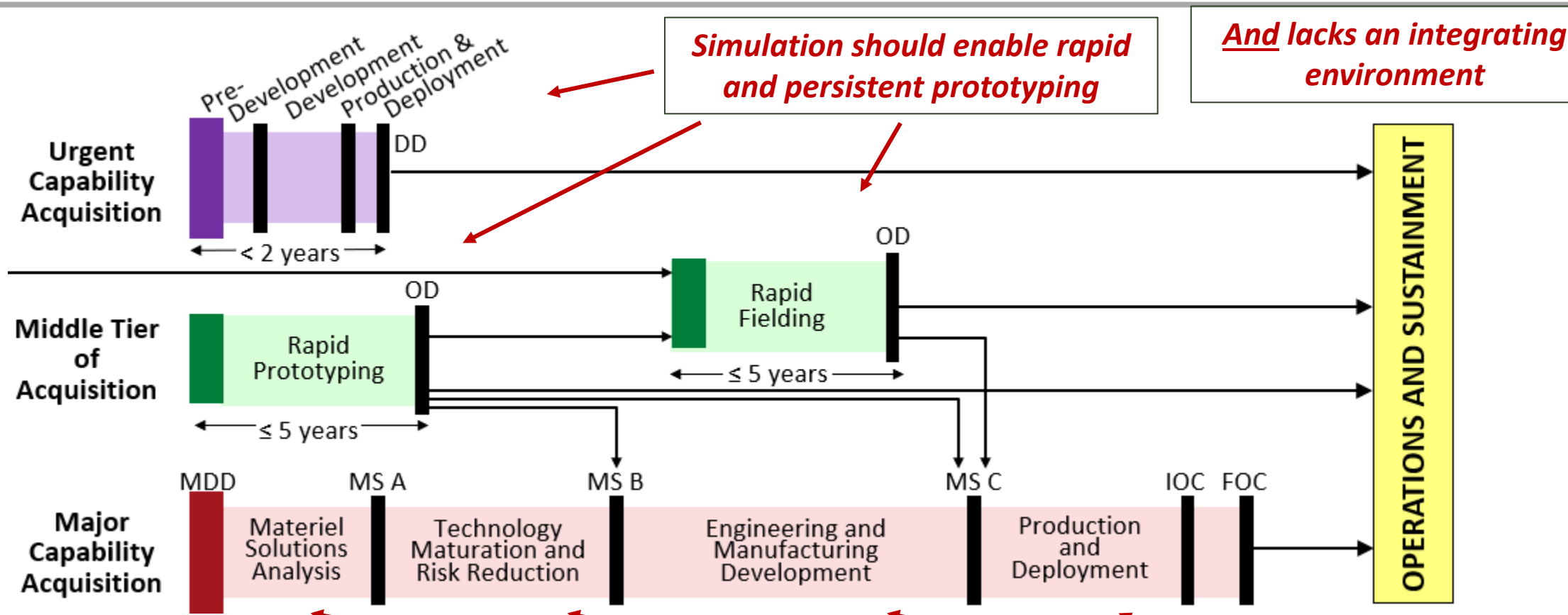
Dr. Chuck Sanders
~ Army Modeling and Simulation Office ~

Purpose

- To facilitate the collection, curation, and sharing of digital representation created across a system lifecycle.
- Desired outcome: Integrated simulations and systems engineering technical capabilities
- Build once, use often

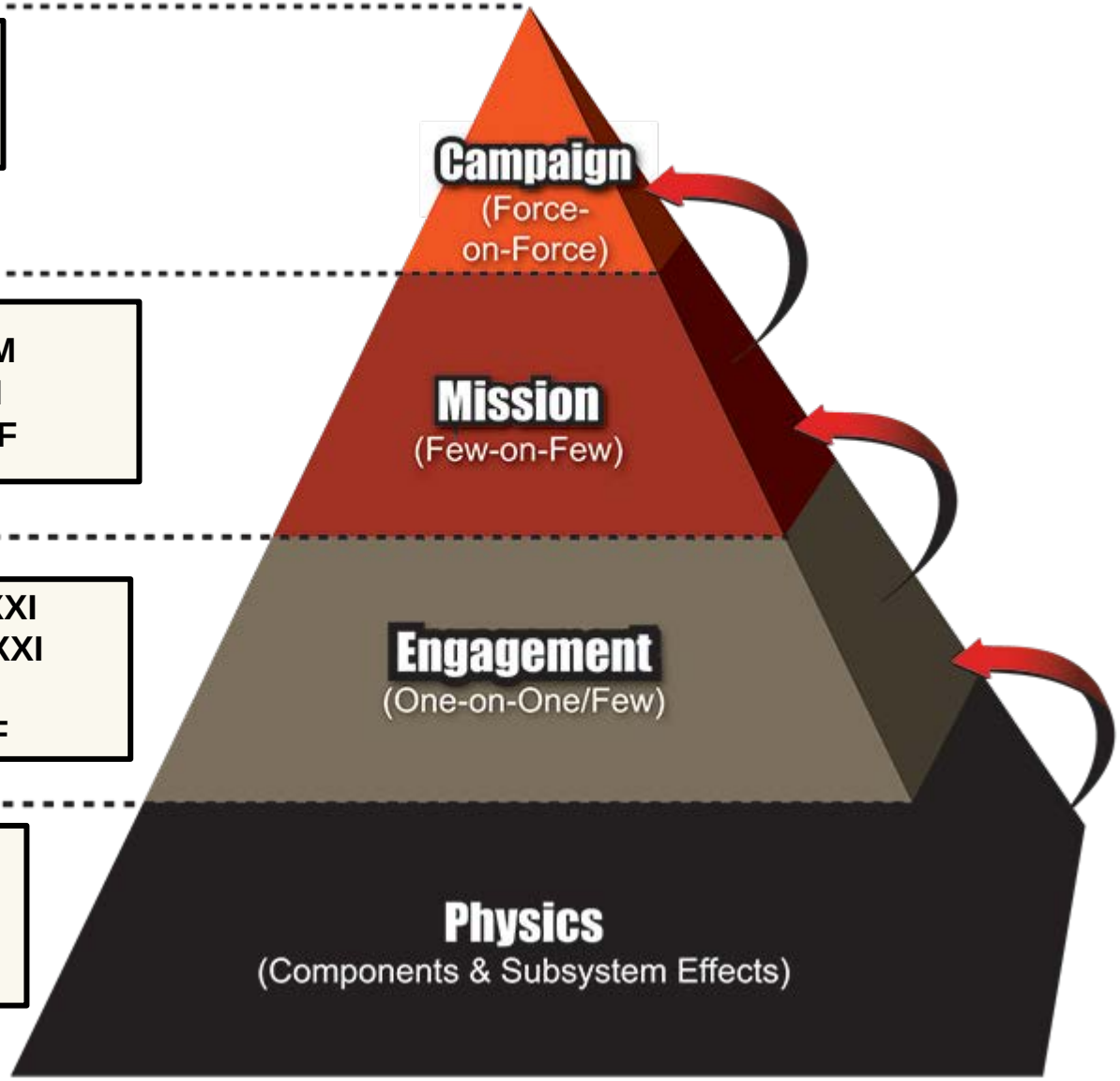
Approved for public release

Use of Simulations Across Acquisition Framework



Approved for public release

DOD MODELING PYRAMID



Examples
STORM JICM
EADSIM AFSIM OneSAF
FireSim XXI COMBATXXI AFSIM OneSAF
STRIDE AVCE

Forces

Multi-Platform

Platform

Subsystems & Components

Modeling Fidelity Correlation Maintained

Model Types

Attrition

Engagement

Performance

Behavior

Cost

Trade Space

Logistics

Supply Chain

Engineering

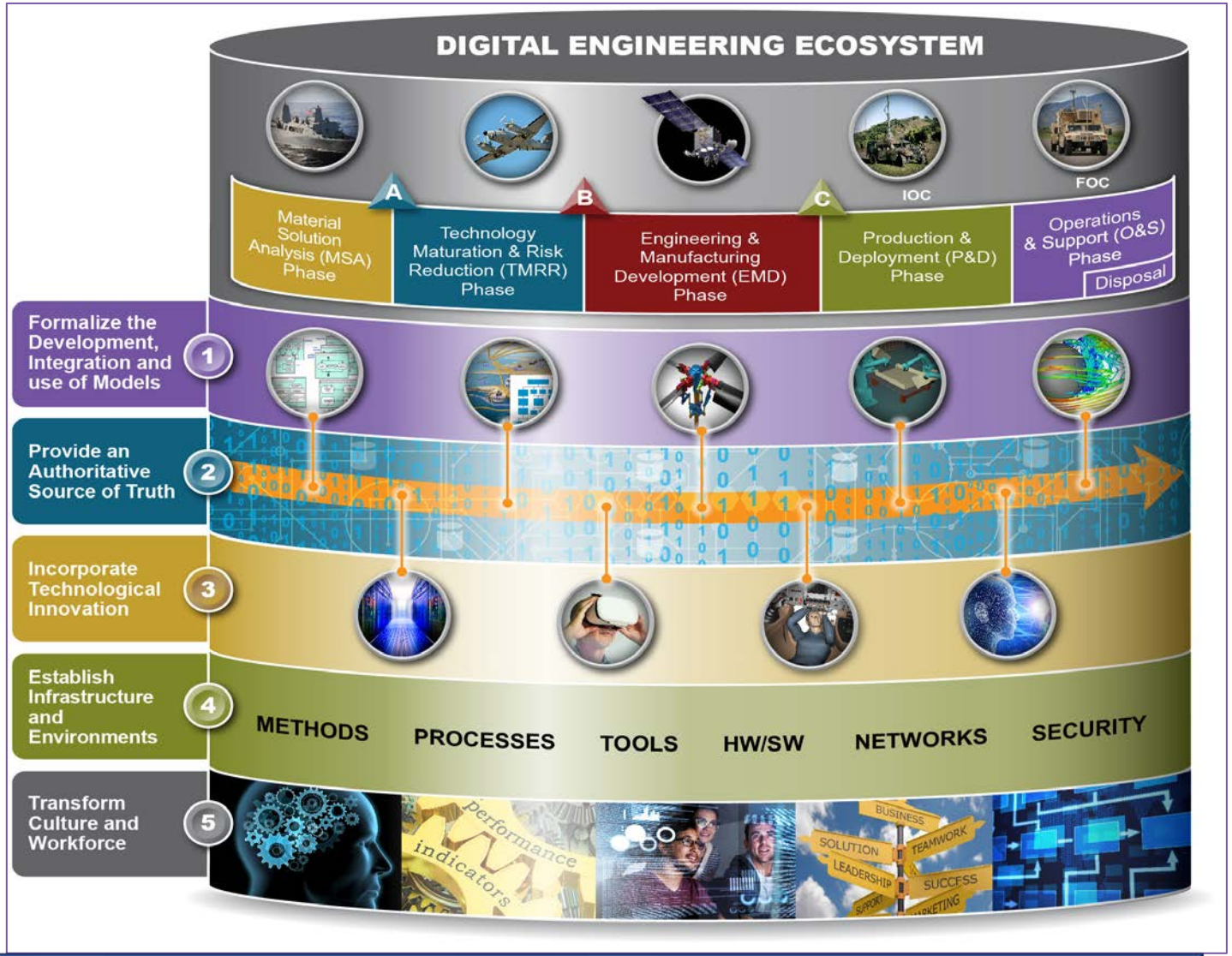
Simulation Community Challenges

- Technology and threat change is outpacing Defense Acquisition and simulation development processes
- Some Specifics:
  - Current simulations do not support agility
  - Current simulations do not adequately represent the emerging multi-domain operating environment and are difficult and costly to modify
  - Continue to struggle with interoperability
  - Inconsistent representation of systems, threats and operating environment across communities
  - Stovepipes inhibit data and model sharing and reuse

Approved for public release

DoD Digital Engineering Overview

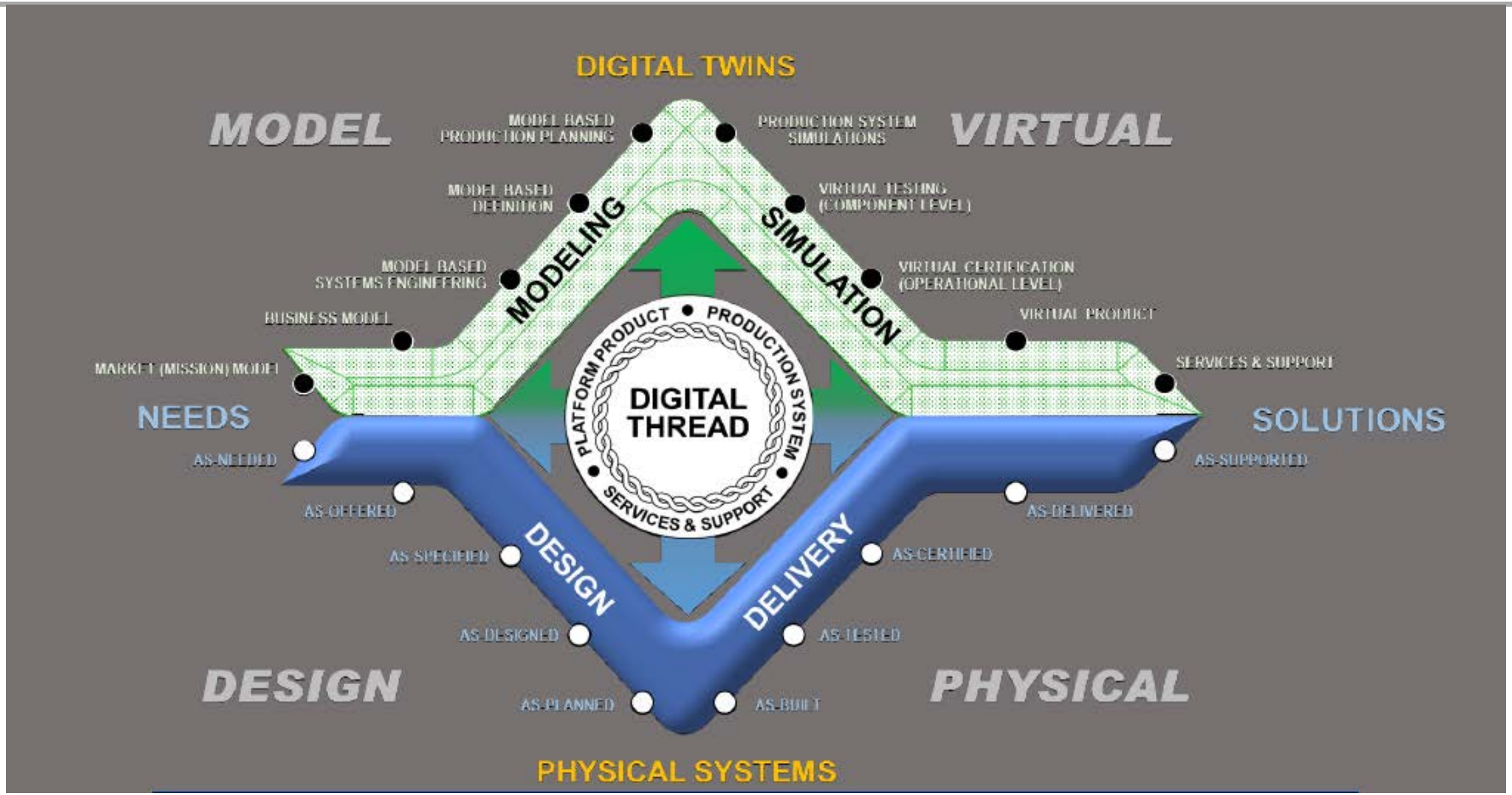
- **What is Digital Engineering?**
  - Combines model-based techniques, digital practices, and computing infrastructure
  - Enables delivery of high pay off solutions to the warfighter at the speed of relevance
- **Reforms Business Practices**
  - Digital enterprise connects people, processes, data, and capabilities
  - Improves technical, contract, and business practices through an authoritative source of truth and digital artifacts



Modernizes how we design, operate, and sustain capabilities to outpace our adversaries

Approved for public release

Boeing MBE Diamond



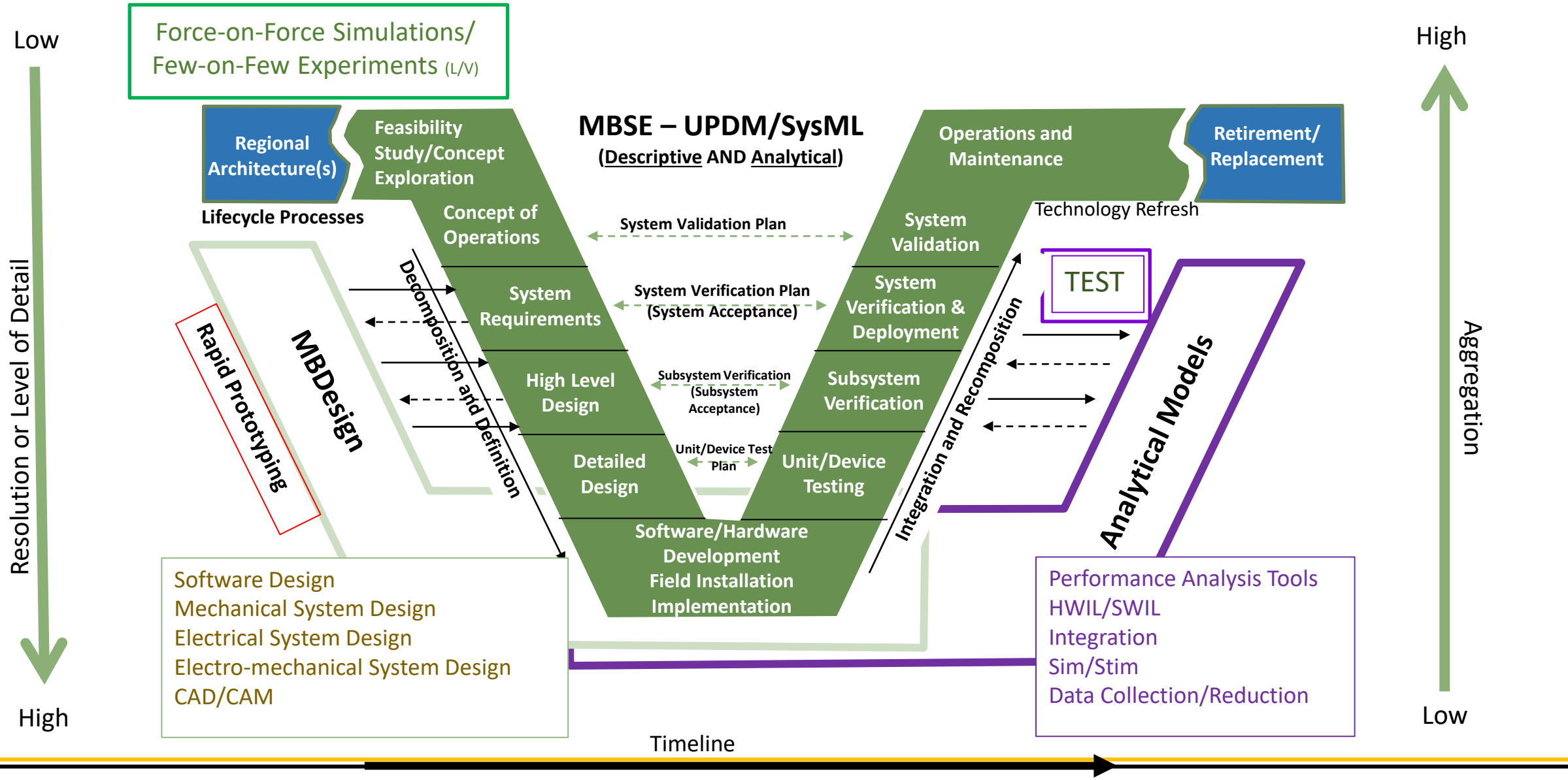
Source: Robert P. Scheurer 11/15/2018, DE ME MBSE and the Like –The One Underlying Essential Attribute

Some Army Implementations of MBSE/DE

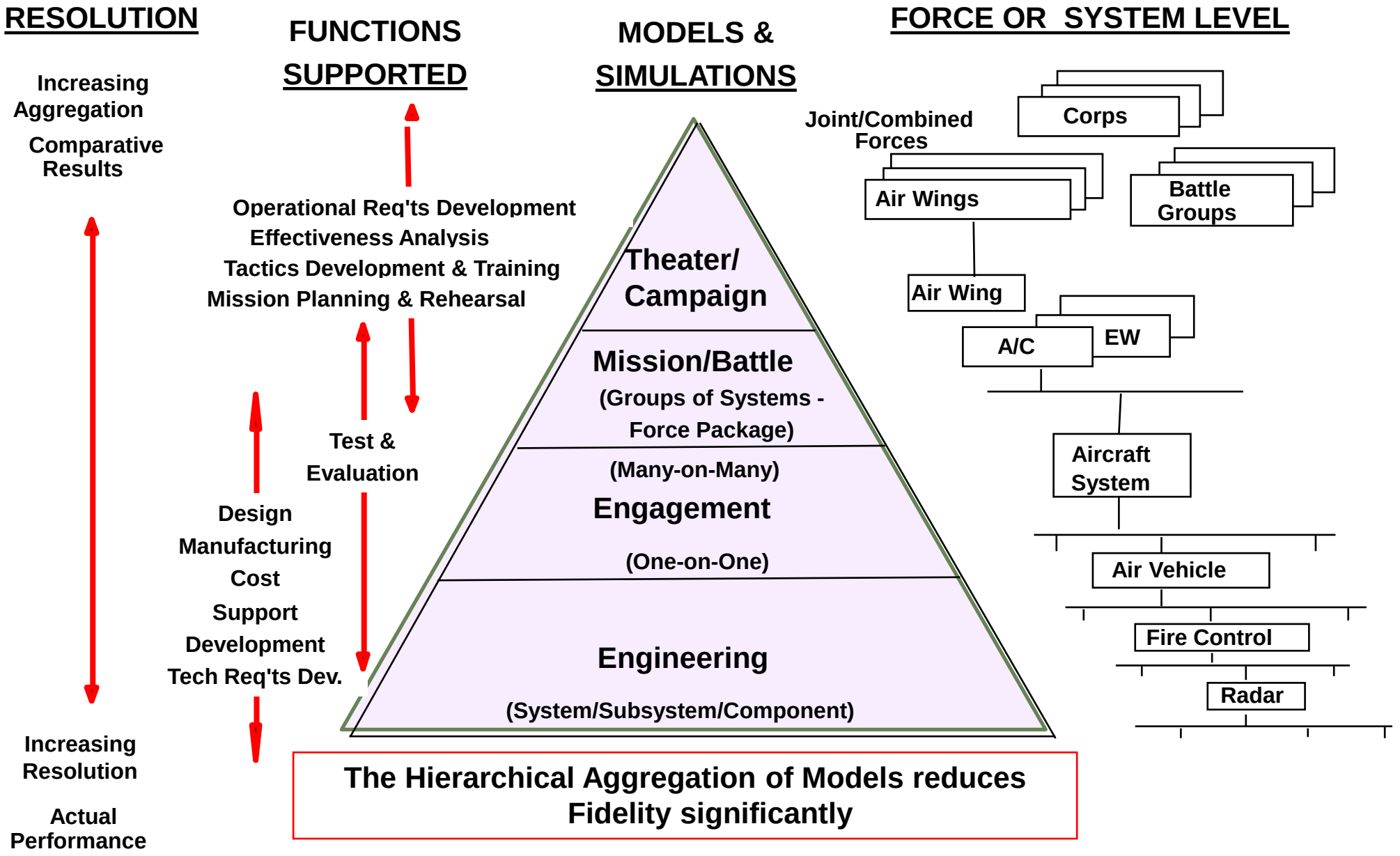
- CCDC/AvMC – Building behavioral simulations in tandem with MBSE process
- CCDC/AC - Armament Virtual Collaboratory Environment (AVCE)
- CCDC/GVSC - Virtual Prototyping with soldier assessments
- PEO Aviation – Requirements modeling and need to link MBSE models with simulations
- PEO Missiles and Space – developing an integrated approach

Approved for public release

“Model Based” Acquisition Toolbox



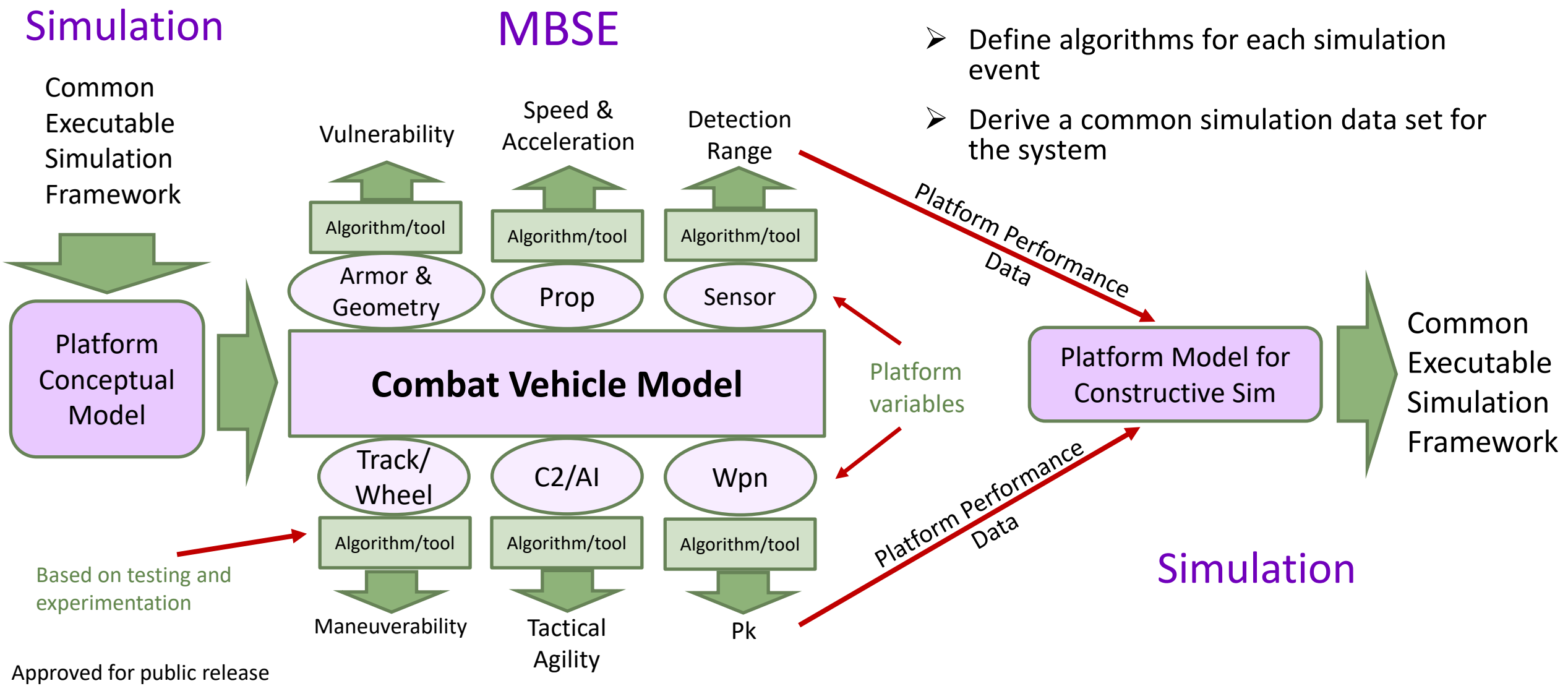
A Hierarchy of M&S Tools for Various Uses



Integrating MBSE System Data into Simulation

Example

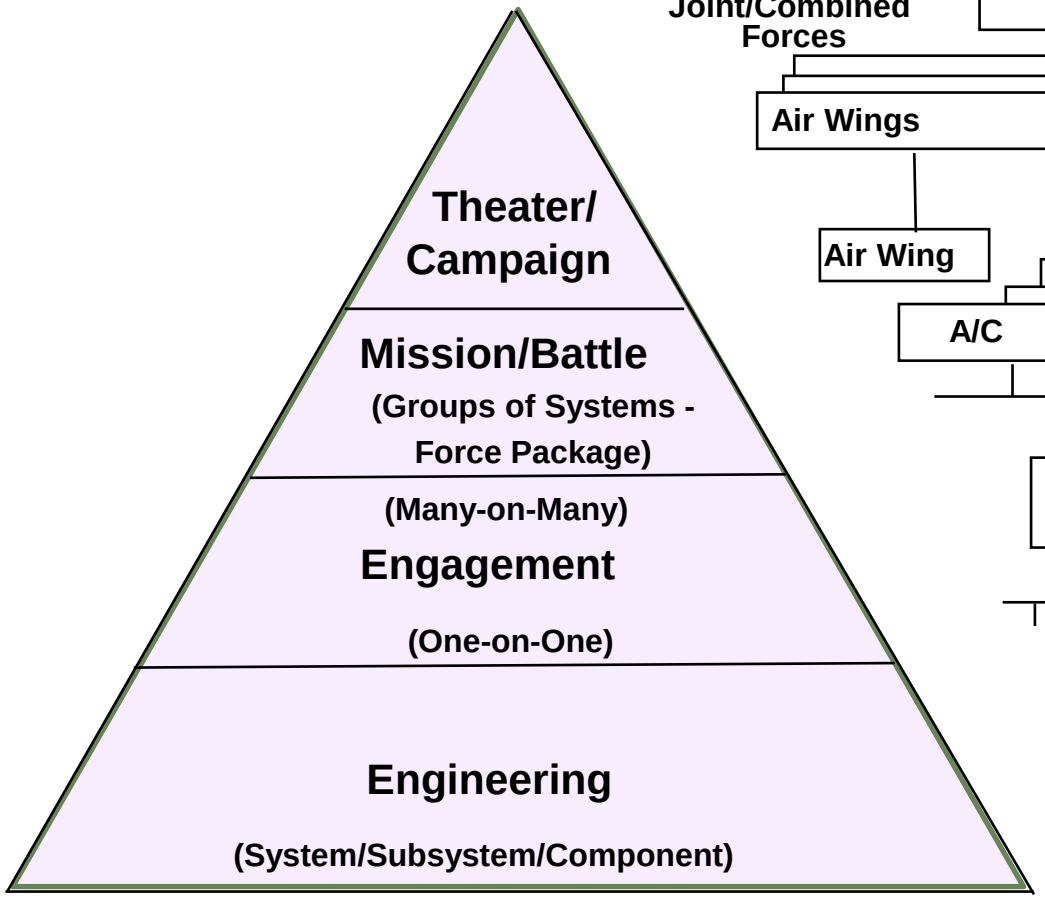
- Map MBSE system definition into an executable simulation structure
- Define algorithms for each simulation event
- Derive a common simulation data set for the system



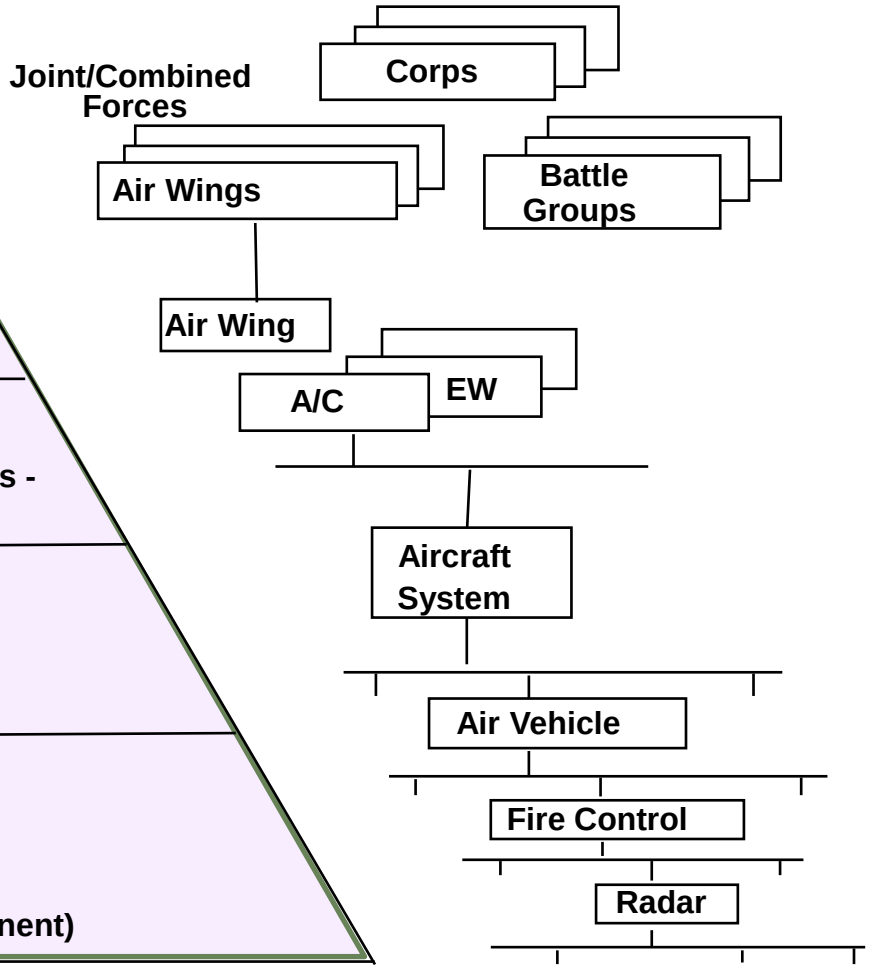
Approved for public release

Need Consistent System Representation Across Levels

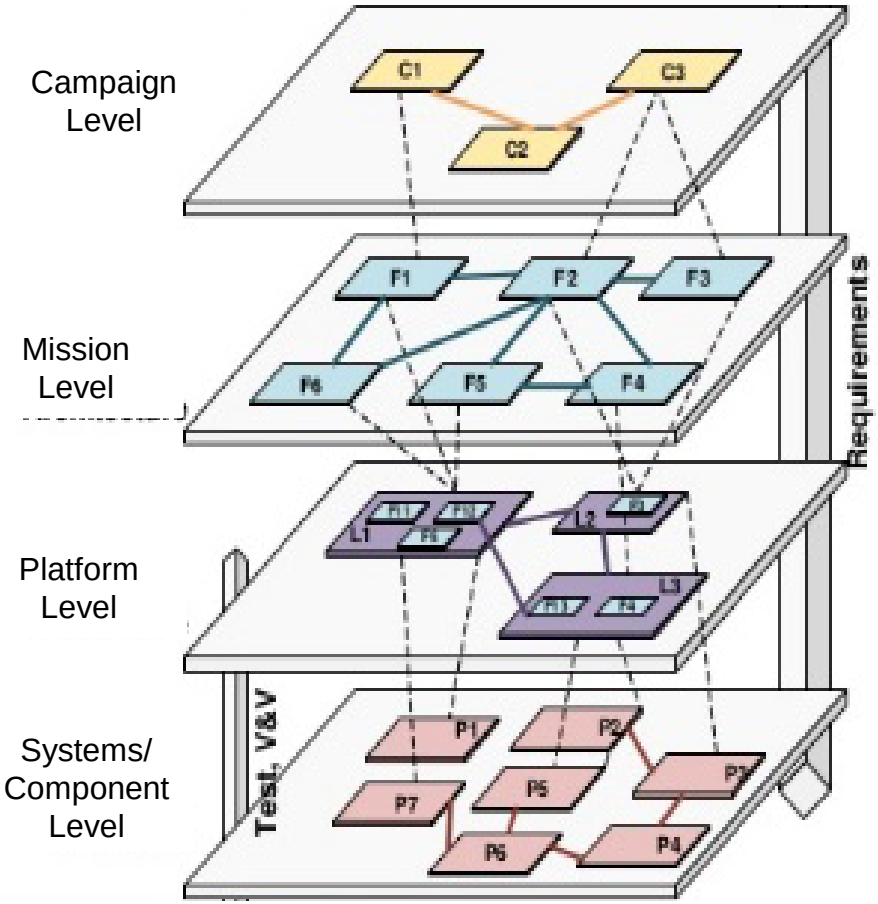
MODELS & SIMULATIONS



FORCE OR SYSTEM LEVEL

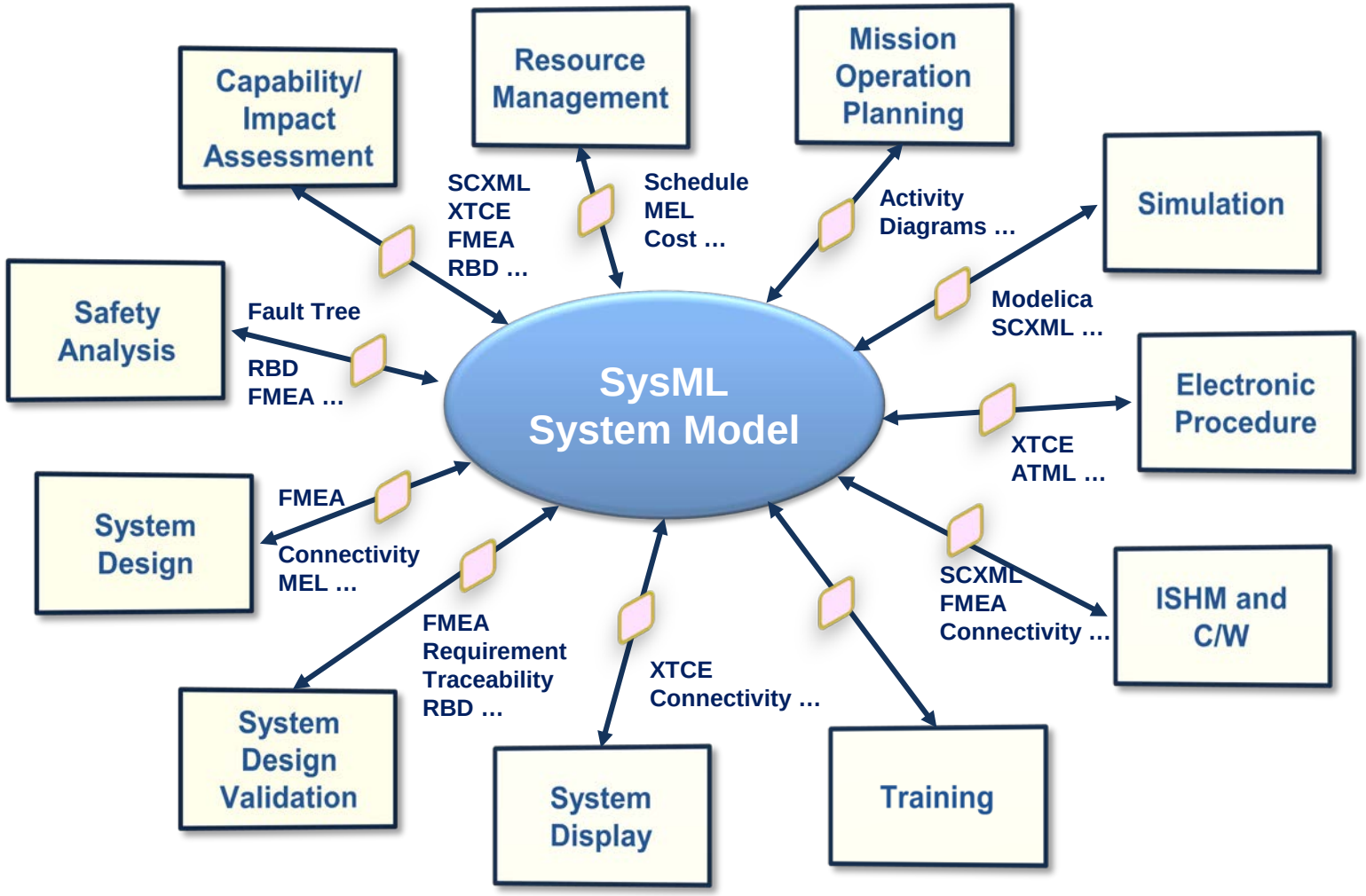


CORRELATED SYSTEMS DATA/MODELS



SysML Models Provide Reusable, Single Source, System Knowledge Capture

The vision is to build a system representation that allows multiple system stakeholders to extract their artifacts for their own intended use



Model Once and Use Many Times

Common Digital Representation Environment

- Designed on system of systems concept

➢ Facilitate capture and reuse of data and models generated during system design and development

➢ Facilitate continuous interoperability

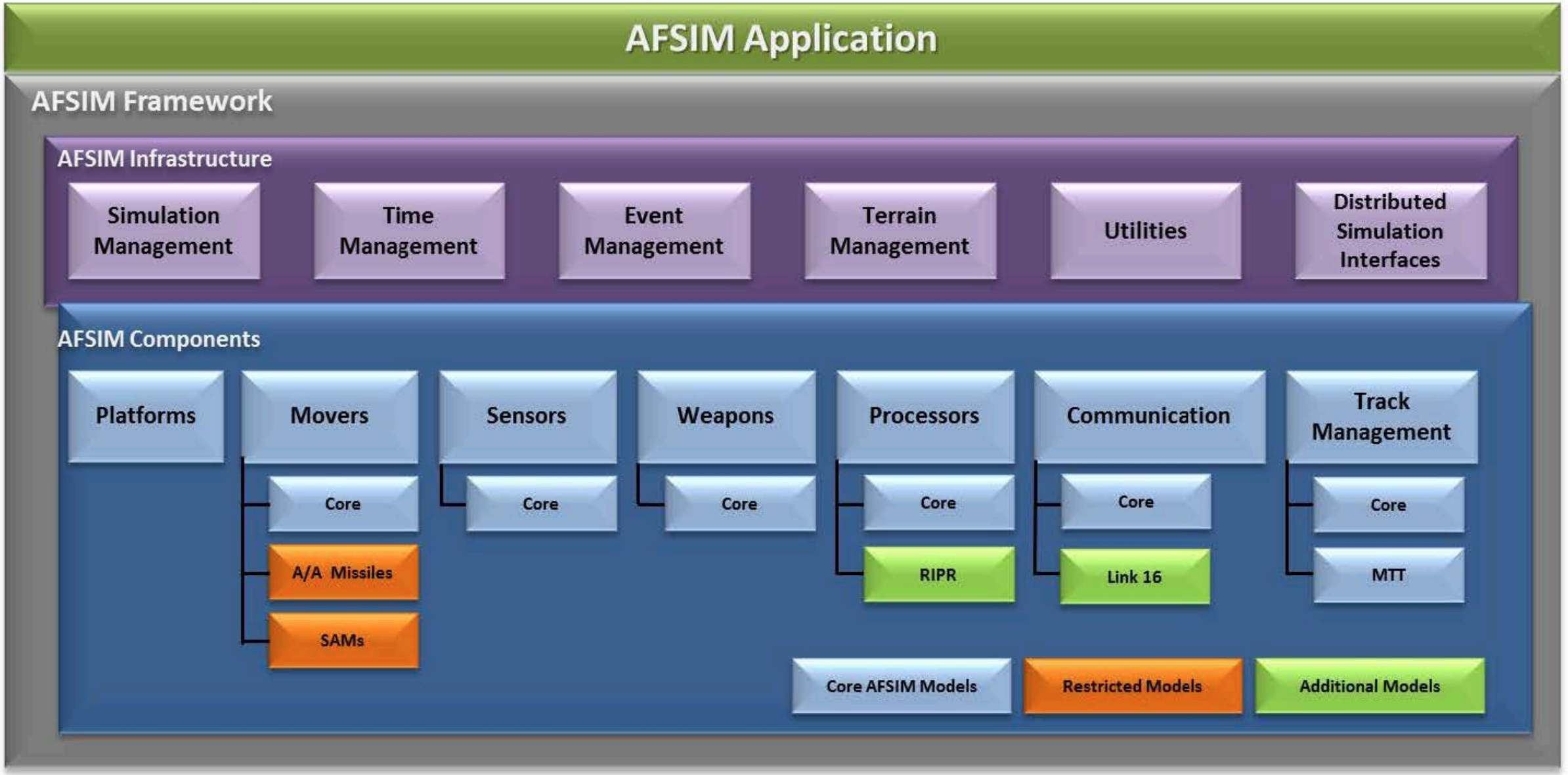
➢ Enable persistent prototyping

➢ Enable more effective warfighter involvement

- Built on a common modeling framework
- Shared with industry partners

Approved for public release

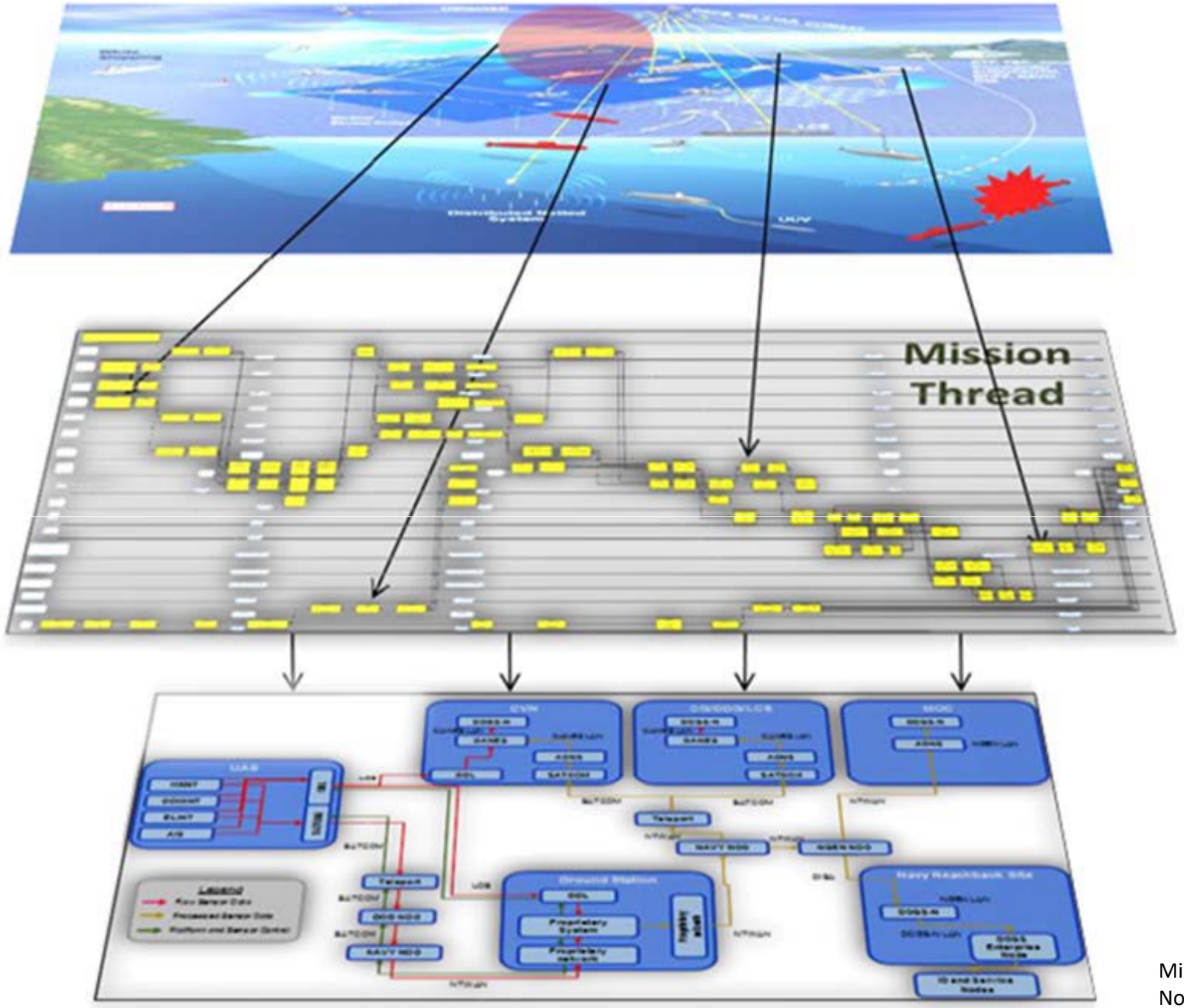
Advanced Framework for Simulation, Integration, and Modelling (AFSIM)



Approved for public release

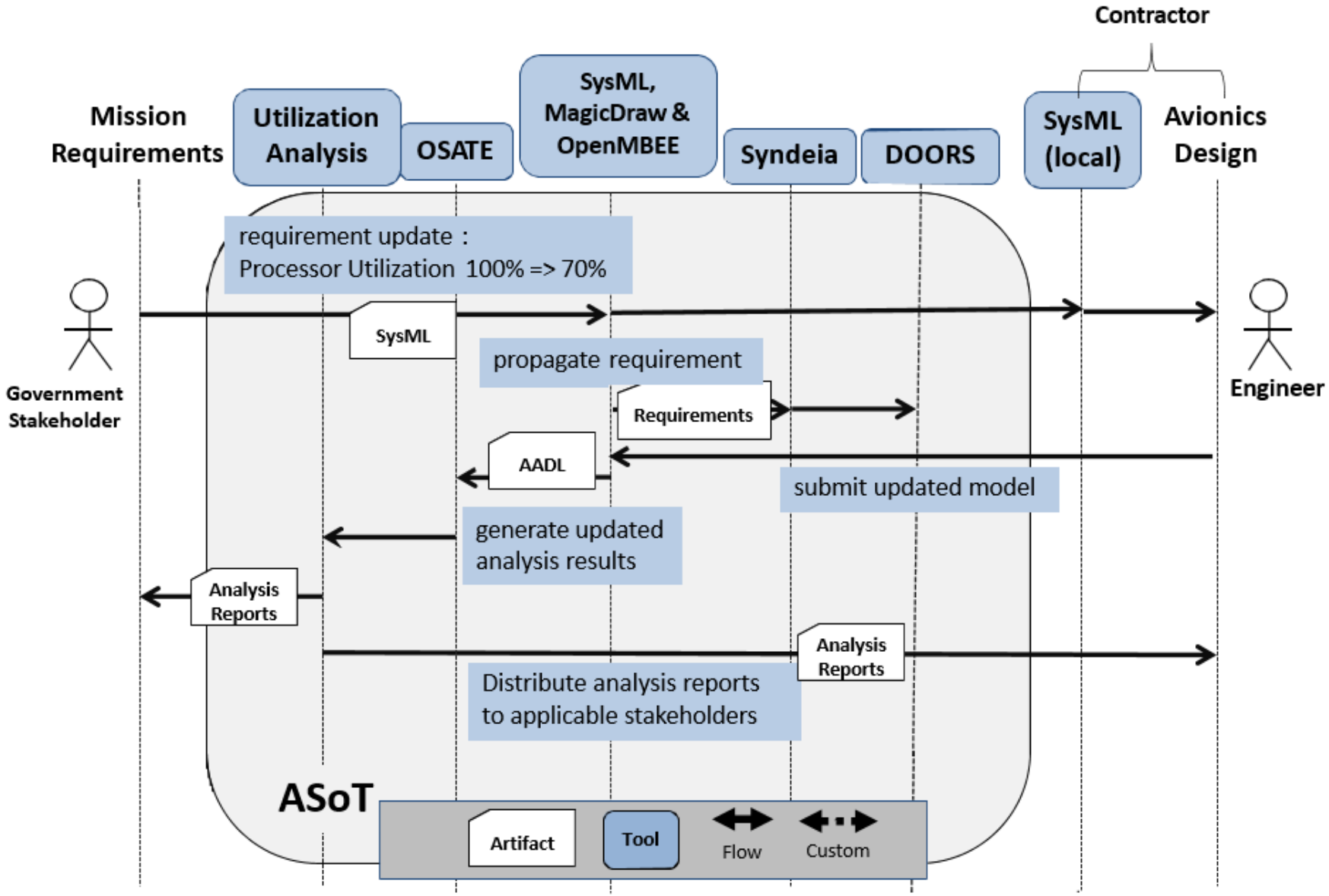
Mission Architecture

Conceptual modeling of concepts, approaches, and systems of systems that enables details of the process flow, timing, interactions, data, capabilities, and performance to be examined in relation to the other processes, entities, and systems that contribute to achieving the mission objective



Mission Engineering Guide
Nov 2020

Example of Govt-Industry Collaboration Approach



Potential Benefits

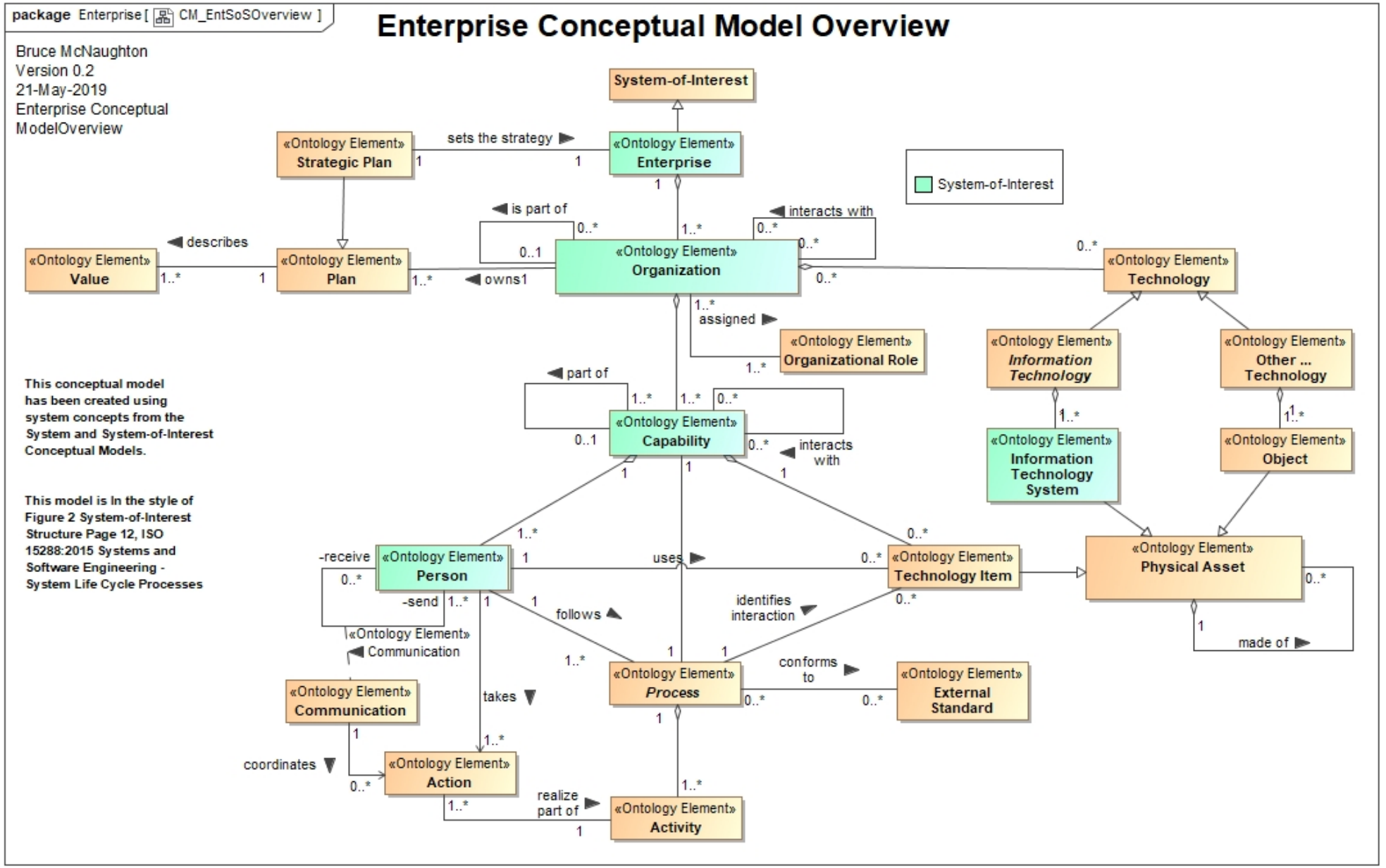
- Govt can share mission level modeling of desired system requirements
- Enable efficient sharing of industry design test results
- Industry control of IP for Govt access to system modeling

Approved for public release



Dr. Chuck Sanders
757-810-3708
charles.g.sanders.ctr@mail.mil

System Conceptual Model



Approved for publ

Approved for public release

Some Recommended Simulation Framework Characteristics

- Modular
- Enables Composable Simulations for a variety of uses
- Varied time management
- Works with models built in other frameworks (through APIs)
- Facilitates rapid introduction of new models/data
- Correlated data repository-management service
- Can be run from the cloud

Approved for public release

Questions to Answer

- What systems data is required for each level of representation?
- Who should collect, curate, and share systems data?
- Should the systems data/modeling be organized in a standard way?
- Who should pay for and/or build the infrastructure?
- How should the infrastructure be set up? Centralized or distributed?
- What is the role of industry? How use the infrastructure to better enable rapid development/delivery of capabilities?
- What should be the process for V&V of systems data/modeling?

Approved for public release

SYSTEMS ENGINEERING
Research Center

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Ontologies for Engineering: A Pragmatic Perspective

Presented by: Mark Blackburn, Ph.D. – Senior Research Scientist
Systems Engineering Research Center (SERC)
Stevens Institute of Technology
Co-Authors: Dr. Tom Hagedorn, Daniel Dunbar, Dr. Annie Yu, Dr. Benjamin Kruise

We would like to acknowledge and thank our research sponsors at NAVAIR, CCDC-AC and OUSD (R&E)

Approved for Public Release

Copyright and Disclaimer

Certain commercial software products are identified in this material. These products were used only for demonstration purposes. This use does not imply approval or endorsement by Stevens, SERC, or CCDC-AC/DEVCOM, NAVAIR, nor does it imply these products are necessarily the best available for the purpose. Other product names, company names, images, or names of platforms referenced herein may be trademarks or registered trademarks of their respective companies, and they are used for identification purposes only.

SYSTEMS ENGINEERING
Research Center

Research Tasks and Collaborator Network

RT-48 (2013)
- Mark Blackburn (PI), Stevens
- Rob Cloutier (Co-PI) - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-118 (2104)
- Mark Blackburn (PI), Stevens
- Rob Cloutier - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-141 (2015)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Gary Witus – Wayne State

RT-157 (2016)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Roger Blake - Stevens
- Mark Austin – Univ. Maryland
- Leonard Petnga – Univ. of Maryland

RT-170 (2016)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Deva Henry - Stevens
- Paul Grogan - Stevens
- Steven Hoffenson - Stevens
- Mark Austin – Univ. of Maryland
- Leonard Petnga – Univ. of Maryland
- Maria Coelho (Grad) – Univ. of Maryland
- Russell Peak – Georgia Tech.
- Stephen Edwards – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.

RT-168 – Phase I & II (2016)
- Mark Blackburn (PI), Stevens
- Dinesh Verma (Co-PI) – Stevens
- Ralph Giffin
- Roger Blake - Stevens
- Mary Bone – Stevens
- Andrew Dawson – Stevens (Phase I)
- Rick Dove
- John Dzielski, Stevens
- Paul Grogan - Stevens
- Deva Henry – Stevens (Phase I)
- Bob Hathaway - Stevens
- Steven Hoffenson - Stevens
- Eirik Hole - Stevens
- Roger Jones – Stevens
- Benjamine Kruse - Stevens
- Jeff McDonald – Stevens (Phase I)
- Kishore Pochiraju – Stevens
- Chris Snyder - Stevens
- Gregg Vesonder – Stevens (Phase I)
- Lu Xiao – Stevens (Phase I)
- Brian Chell (Grad) – Stevens
- Luigi Ballarinni (Grad) – Stevens
- Harsh Kevadia (Grad) – Stevens
- Kunal Batra (Grad) – Stevens
- Khushali Dave (Grad) – Stevens
- Rob Cloutier – Visiting Professor
- Robin Dillon-Merrill – Georgetown Univ.
- Ian Grosse – Univ. of Massachucetts
- Tom Hagedorn – Univ. of Massachusetts
- Todd Richmond – Univ. of Southern California
- Edgar Evangelista – Univ. of Southern California

RT-195 (2018)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Ralph Giffin - Stevens
- Benjamin Kruse - Stevens
- Russell Peak – Georgia Tech.
- Stephen Edwards – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.
- Donna Rhodes - MIT
- Mark Austin – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

WRT-1008 (2019)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- John Dzielski- Stevens
- Benjamin Kruse - Stevens
- Bill Rouse – Stevens/Georgetown
- Russell Peak – Georgia Tech.
- Selcuk Cimtalay – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.
- Alanna Carnevale (Grad) – Georgia Tech.
- William Stock (Grad) – Georgia Tech.
- Michael Szostak (Grad) – Georgia Tech.
- Donna Rhodes - MIT
- Mark Austin – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

WRT-1025 (2020)
- Mark Blackburn (PI), Stevens
- Mark Austin (Co-PI) – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

ART-002 (2018) – ART-022 (2021)
- Mark Blackburn (PI), Stevens
- Dinesh Verma (Co-PI) – Stevens
- Kunal Batra – Stevens
- Mary Bone - Stevens
- John Dzielski, Stevens
- Steven Hoffenson - Stevens
- Steve Hespelt - Stevens
- Roger Jones - Stevens
- Benjamin Kruse - Stevens
- Annie Yu- Stevens
- Chris Snyder - Stevens
- Brian Chell – Stevens
- Daniel Dunbar (PhD) - Stevens
- Jessica Driscoll (PhD) – Stevens
- Andrew Underwood (Ungrad) Stevens
- Benjamin Steinwurtzel (Ungrad)
- Cory Phillipe (Grad) - Stevens
- Ian Grosse – Univ. of Massachucetts
- Tom Hagedorn – Univ. of Mass
- Joe Gabbard – Virginia Tech
- Jared Van Dam (PhD) – Virginia Tech
- Kelsey Quinn (PhD) – Virginia Tech

WRT-1036 (2020)
- Mark Blackburn (PI), Stevens
- John Dzielski- Stevens
- Russell Peak – Georgia Tech.
- Selcuk Cimtalay – Georgia Tech.
- Taylor Fields – Georgia Tech.
- William Stock (Grad) – Georgia Tech.
- Sahil Panchal – Georgia Tech
- Jake Sisavath – Georgia Tech
- Gabriel Rizzo – Georgia Tech

Abstract

- The talks discusses fundamental aspects 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.

- Accordingly, Ontologies for digital engineering need to be interoperable to allow design reasoning across multiple domains (e.g., cyber security, aeronautics, communications) and to support model “integration” through “interoperability” across domains and disciplines. The core elements of ontologies for engineering are often hidden as part of the Digital Engineering infrastructure, allowing SWT to automate reasoning to help engineers understand consistency and completeness of their models in the context of other related models across the domains using their modeling tool of choice.

- The talk closes with an example of a Cyber Ontology Pilot demonstration that uses SWT to associate potential cyber vulnerabilities with a simple computer network modeled in System Modeling Language (SysML).

Outline

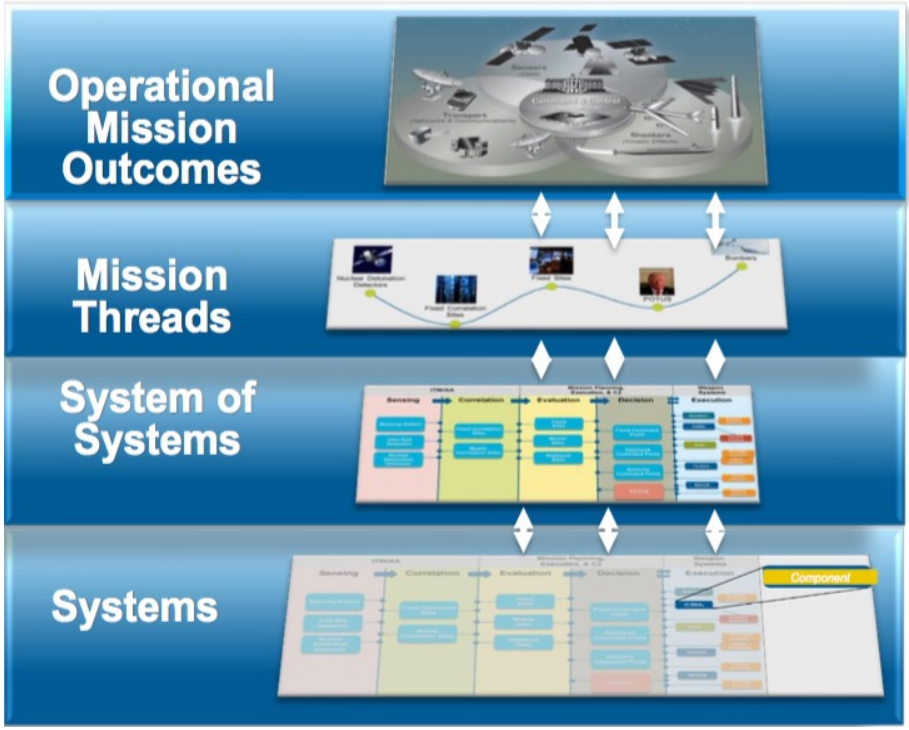
- **What:** Ontologies for Engineering
- **Why:** Ontologies and Semantic Web Technologies are enablers for DoD Digital Engineering Strategic Goals
- **How:** Semantic Web Technologies
  - —Engineering Ontologies are defined using Semantic Web Technologies
  - —Both are formalized for engineering using software methods and tools
- Case Study for Cyber Ontology Pilot for Vulnerability Detection

Ontologies for Engineering Concepts and Terms

- What – an ontology is somewhat similar to a database schema
  - —Ontologies focused on concepts & relationships (knowledge representation) formalized using OWL (Web Ontology Language)
  - —Database schema focused on structure of data for storage and querying
  - —Ontology uses a repository called a triple store
  - —Data stored as triples, subject-predicate-object in a triple store resulting in a graph of linked data formalized using RDF (Resource Description Framework)
  - —SPARQL is a standard query language that is notionally similar to SQL
  - —Databases and ontologies can be thought about as part of infrastructure
- Why – provides a means to semantically "integrate" models across different domains using **Interoperability**
  - —Tool-to-tool integration is brittle
  - —Ontologies most often evolve over time
- How - map different types of modeling artifacts to data stored in a triple store repository

DoD DE Strategy – Discussion Framework

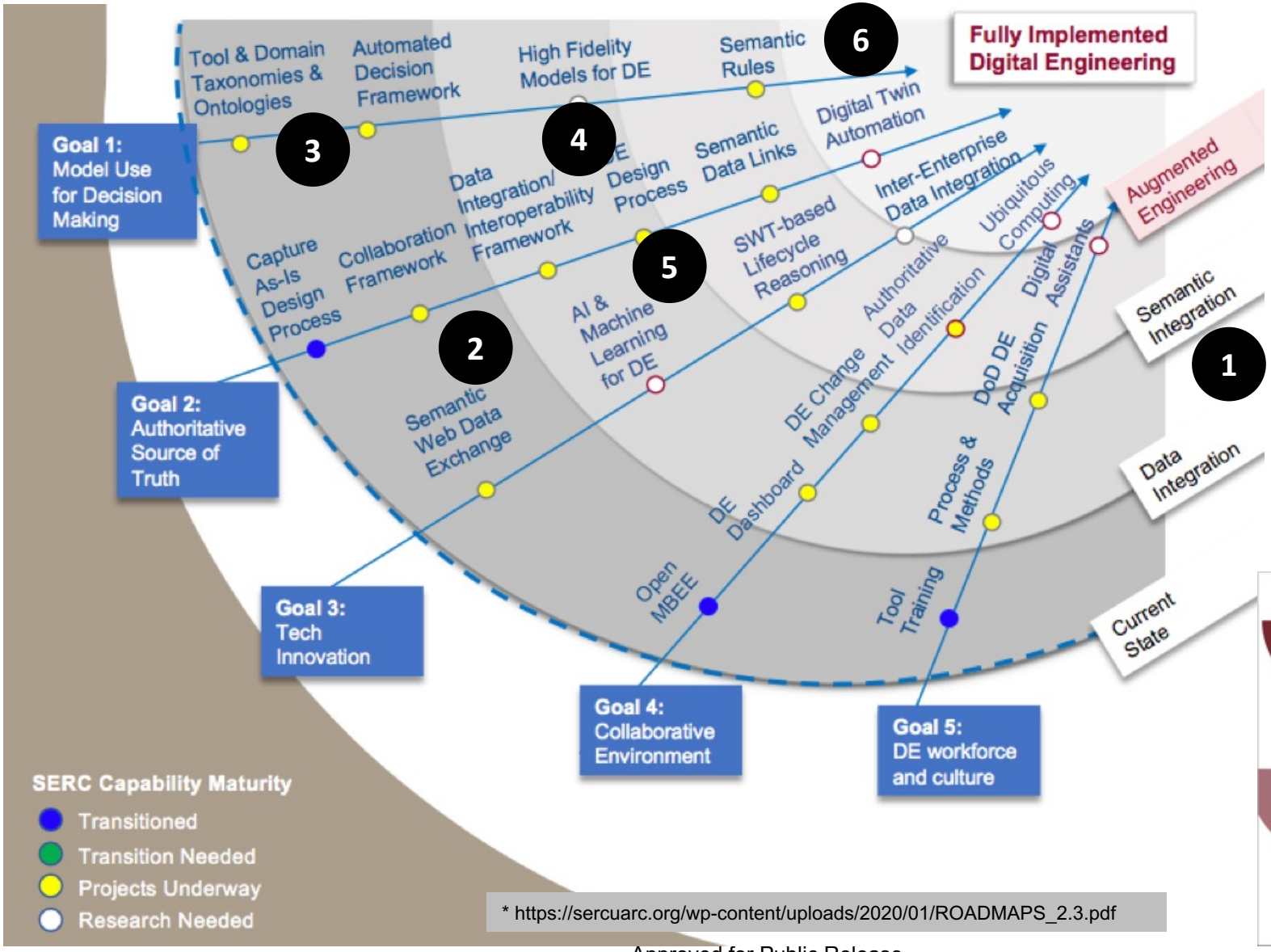
- DE/MBSE helps refactor and strengthen implementation of Systems Engineering principles (Goal 3)
  - Represent Structure, Behavior, Interfaces, Requirements and related interactions
  - Can characterize different levels of abstraction – Mission, System, Subsystem where different types of methods are needed
- DE requires a formalized system/design representation that links information in an Authoritative Source of Truth (Goal 2)
- Semantically linked system/design information to enable tradespace analyses and decision making (Goal 1)
- Need computation and methodological infrastructure to access and visualize on need-to-know basis (Goal 4)



Extending the DoD Digital Engineering Strategy to Missions, Systems of Systems, and Portfolios
P. Zimmerman, T. Gilbert, J. Dahmann
22nd Annual NDIA Systems and Mission Engineering Conference
Tampa, FL| 23 October 2019

SYSTEMS ENGINEERING
Research Center

Digital Engineering for Systems Engineering Roadmap: Goals are Mutually Supportive not Orthogonal







* https://sercuarc.org/wp-content/uploads/2020/01/ROADMAPS_2.3.pdf

Conceptual Examples

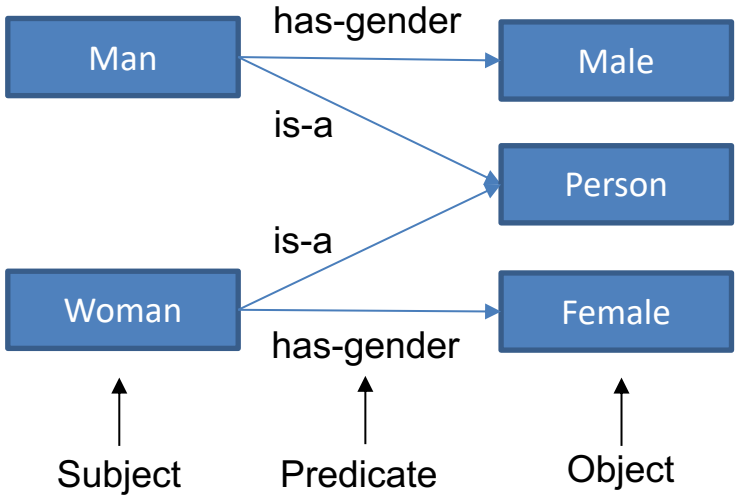
- Person ontology and RDF (data)
  - —Example of data: Subject – Predicate - Object
- Navy mission use case
  - —Mission objective: continuous surveillance
  - —System capabilities: UAV and Refueler
  - —System focus: refueling subsystem



- Cyber ontology pilot use case
  - —Computer network
  - —Vulnerability analysis using ontology and semantic

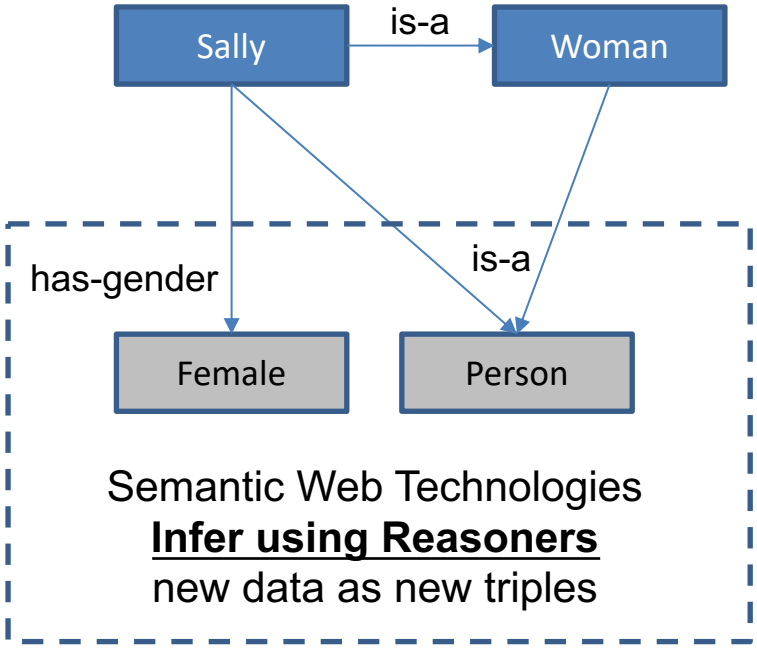
Basic Concepts of Ontologies and Semantic Technologies

Ontology
(Classes and Properties)



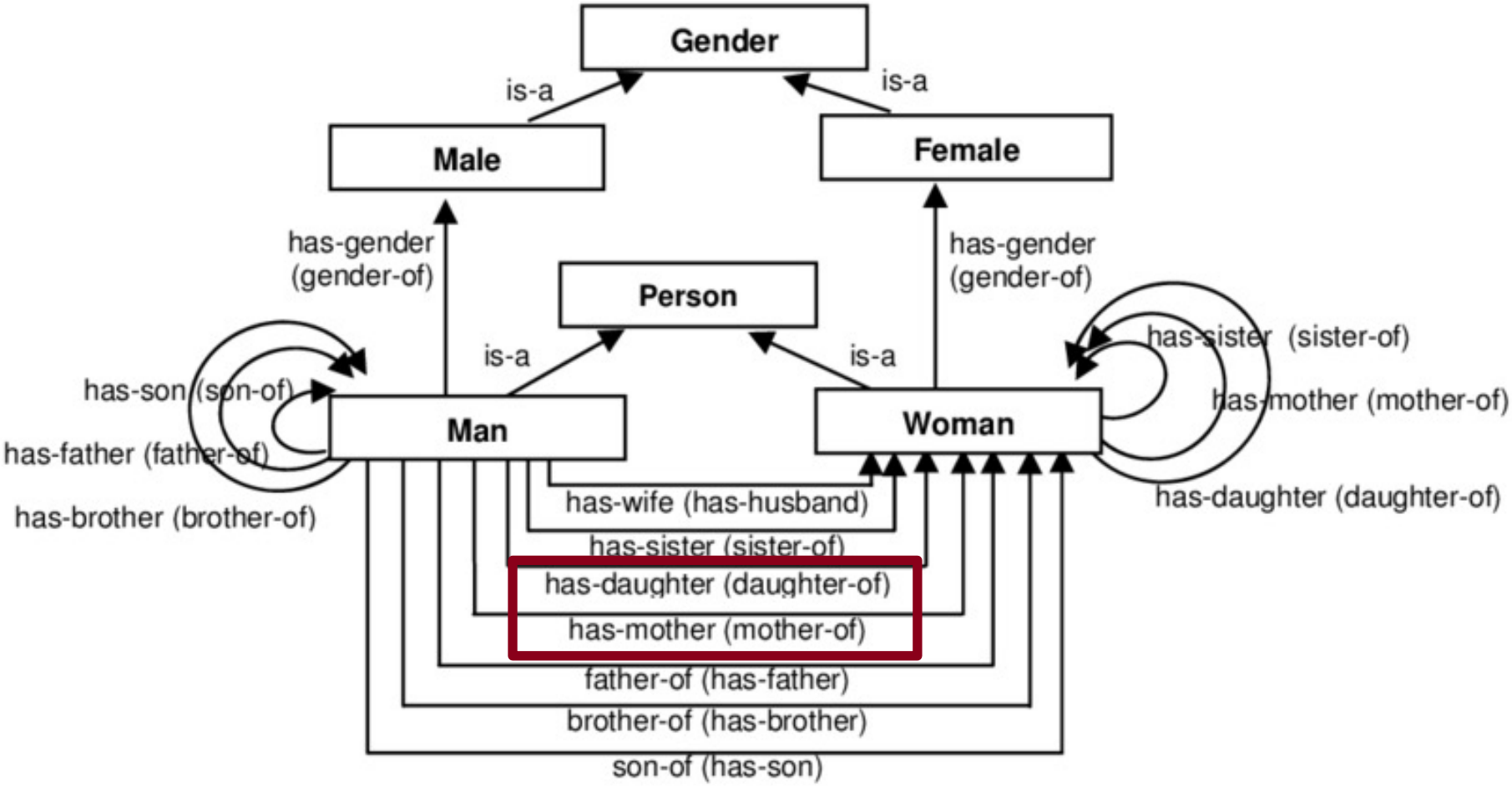
Data (RDF)
(Referred to as Instances)

If we assert



Everything is Represented as Linked Data as: Subject - Predicate - Object

Ontology: Classes and Properties



https://www.researchgate.net/figure/A-graphically-reproduced-segment-of-the-example-Family-ontology_fig13_234059795

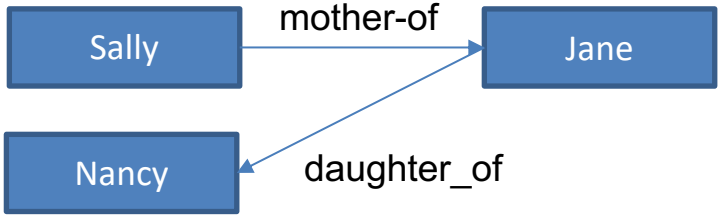
Automated Reasoning from Property Constraints Identifies Data Issues

Ontology
(Property Constraints)

- Mother has 1 or more children
- Daughter has only 1 mother

Data (RDF)
(Referred to as Instances)

If we assert



Semantic Web Technologies
Reasoners
will identify this as not possible
because Jane cannot have two mothers

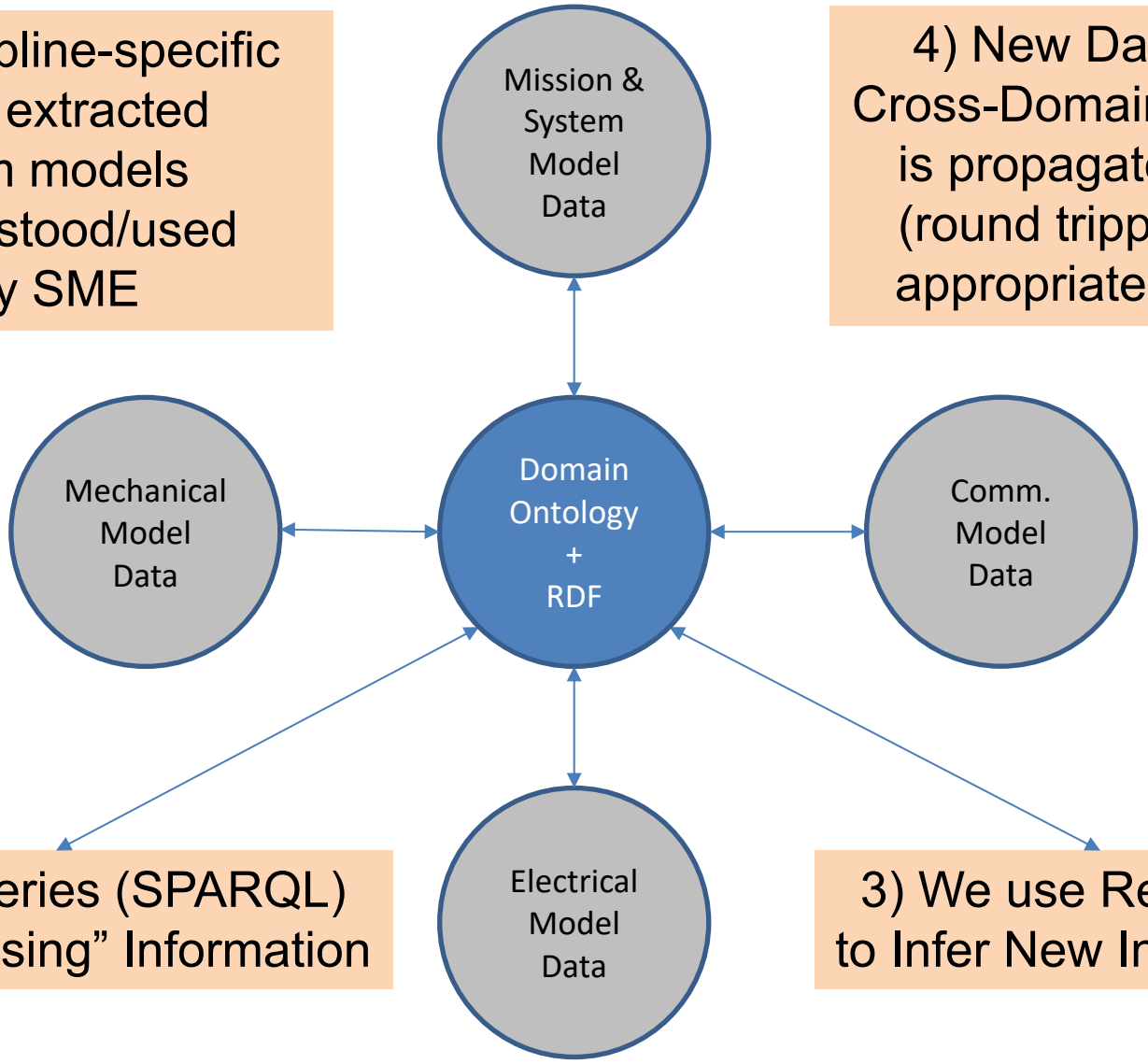
Example: Cross Domain Relationships Needed for System Trades, Analysis and Design

- Mission objective: continuous surveillance
- Capability Refueling UAV
- Systems: UAV and Refueler
- **Valve** – Cross-domain Object
- Mechanical Domain
  - Valve connects to Pipe
- Electrical Domain
  - Switch opens/closes Value
  - Maybe software
- Operator Domain
  - Pilot remotely sends message to control value
- Communication Domain
  - Message sent through network
- Fire control Domain
  - Independent detection to shut off valve
- Safety Domain



Bring Data Across Disciplines into Linked Data that Complies with Domain Ontology

1) Discipline-specific data extracted from models understood/used by SME



4) New Data from Cross-Domain analysis is propagated back (round tripped) into appropriate models

2) Use Queries (SPARQL) to Find "Missing" Information

3) We use Reasoners to Infer New Information

SYSTEMS ENGINEERING
Research Center

How to Develop and Interoperable Ontology

- Recognize that ontology development relies on software development skills, conceptual/information modeling
- Develop in OWL (now OWL2)
  - —Use Ontology Editor such as Protege
- Use an established foundational set of classes
  - —Like “programming libraries”
  - —E.g., Basic Formal Ontology (BFO) – referred to as an upper ontology
  - —May also use extensions of BFO such as the Common Core
- Start from established:
  - —Data dictionaries and lexicon formalizing “terms” that are “programmed” as classes
  - —Taxonomies to understand relationships
  - —Often aligned with Reference Architectures

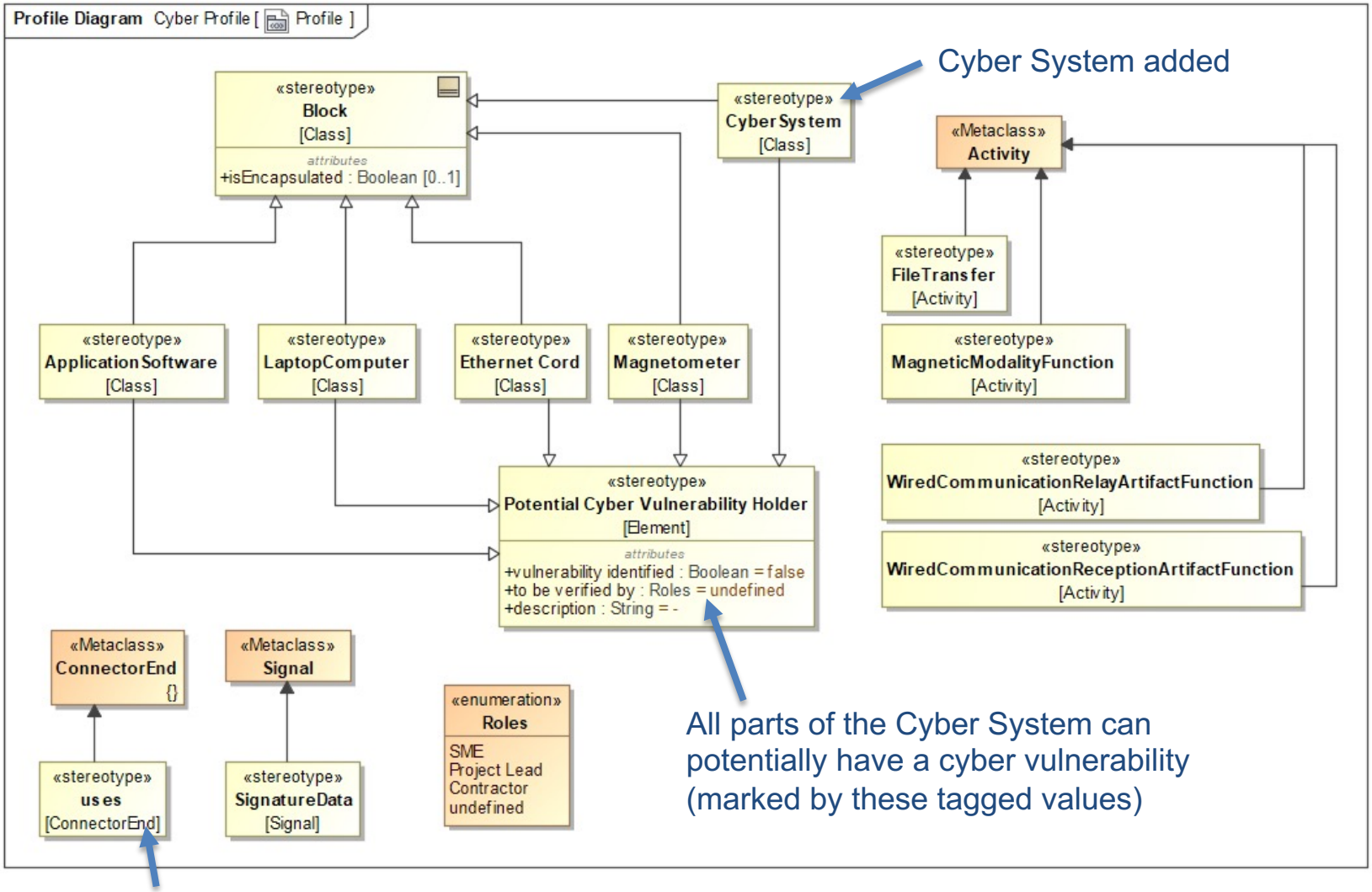
Approved for Public Release

Cyber Ontology Pilot Case Study

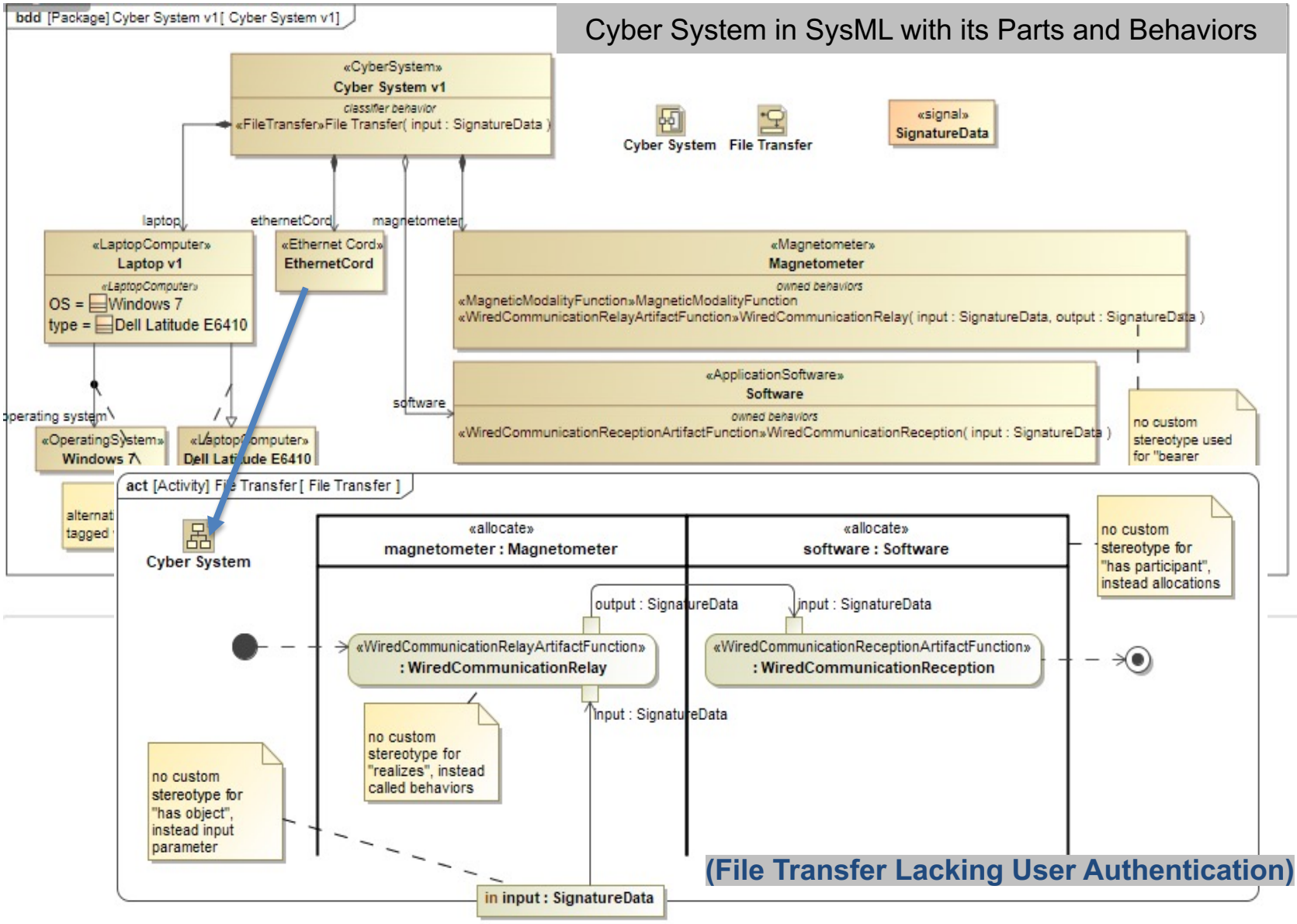
Use Case: transform system model of computer networks represented in SysML into ontology "data" that integrates with NAVSEA ontology (CVAST) to reason about potential vulnerabilities

Approved for Public Release

IoIF Cybersecurity Demo: SysML Profile



Cyber Demo SysML Model with Seeded Vulnerability



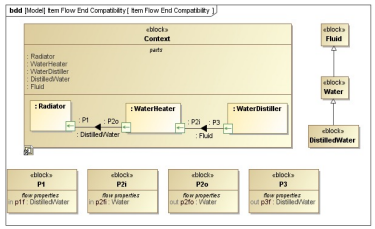
Workflow

1. Cameo / MagicDraw Model(s) synchronized into Model Management System (MMS) (repository for SysML Models)
2. IoIF* requests the model from MMS (also works with Teamwork Cloud)
3. IoIF parses the model into RDF, maps into its semantic model
4. IoIF looks for the vulnerability with a rule
5. IoIF writes documentation back into MMS
6. Synchronize from MMS into Cameo / Magicdraw

*Interoperability and Integration Framework (IoIF) is Semantic Web Technologies developed under SERC Research

IoIF Cyber Ontology-Based Use Case used in Course and Exercise (animated)

Cyber System Model of Computer Network in SysML

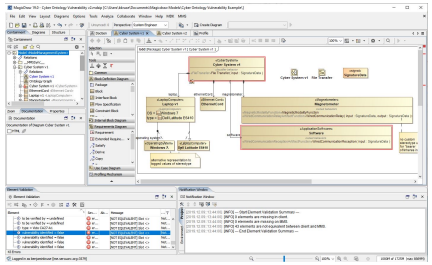


Transform SysML into Ontology "data"

python™

Interoperability and Integration Framework (IoIF) supports Loading, Parsing, Mapping and Querying of Linked Data across ontologies (domains)

Round Trip and Visualization of Reasoning Results



Compute Vulnerability Score

MATLAB

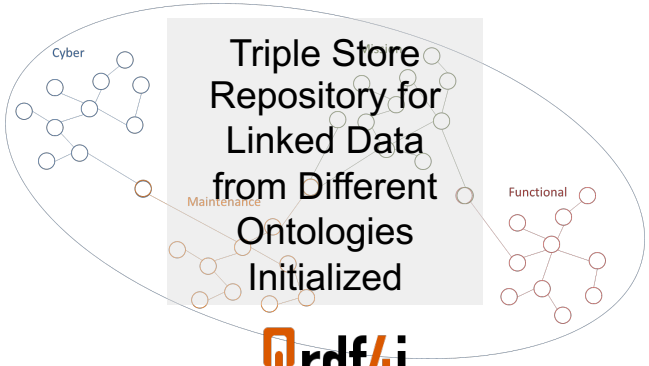
Uses Tool Proxy & IoIF Service

Analysis associates Vulnerabilities with Model

Visualize Score in Dashboard

python™

Uses Tool Proxy & IoIF Service



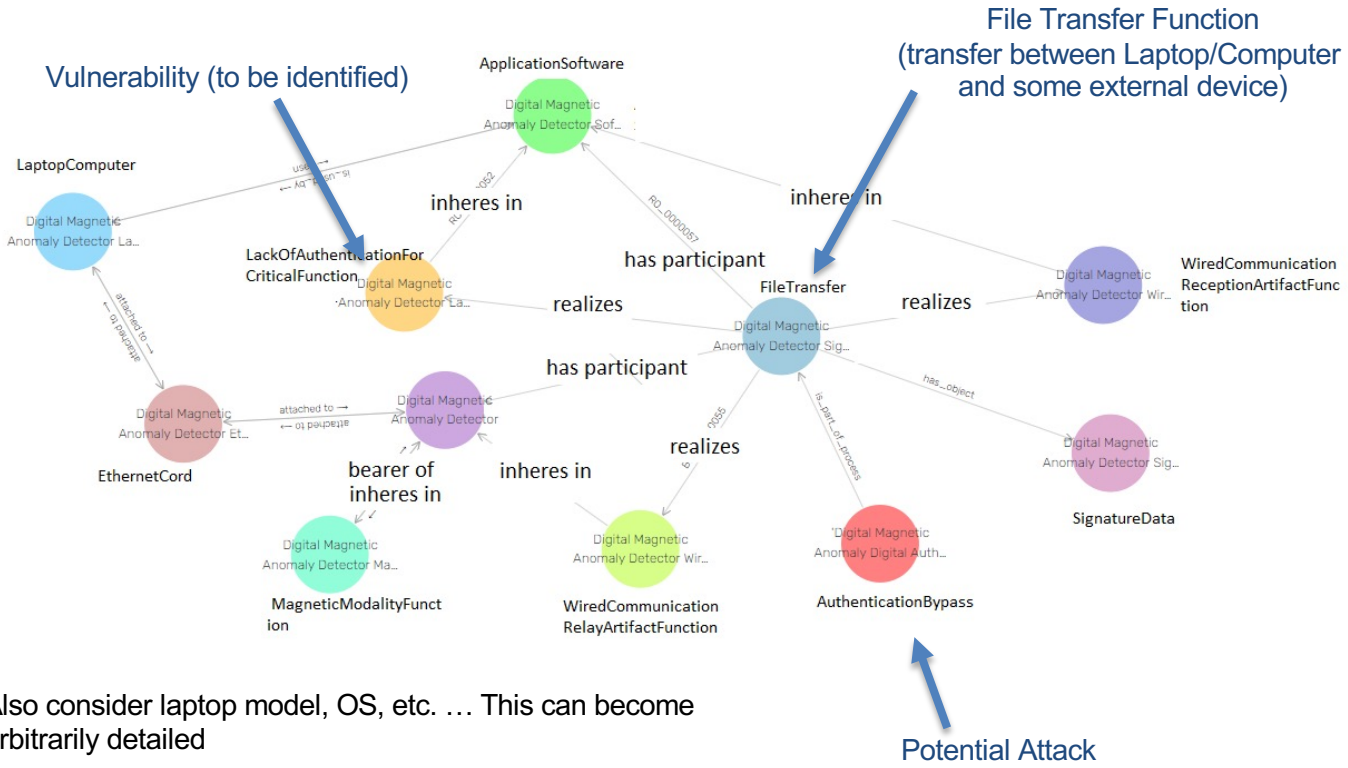
Triple Store Repository for Linked Data from Different Ontologies Initialized

rdf4j

Compliant

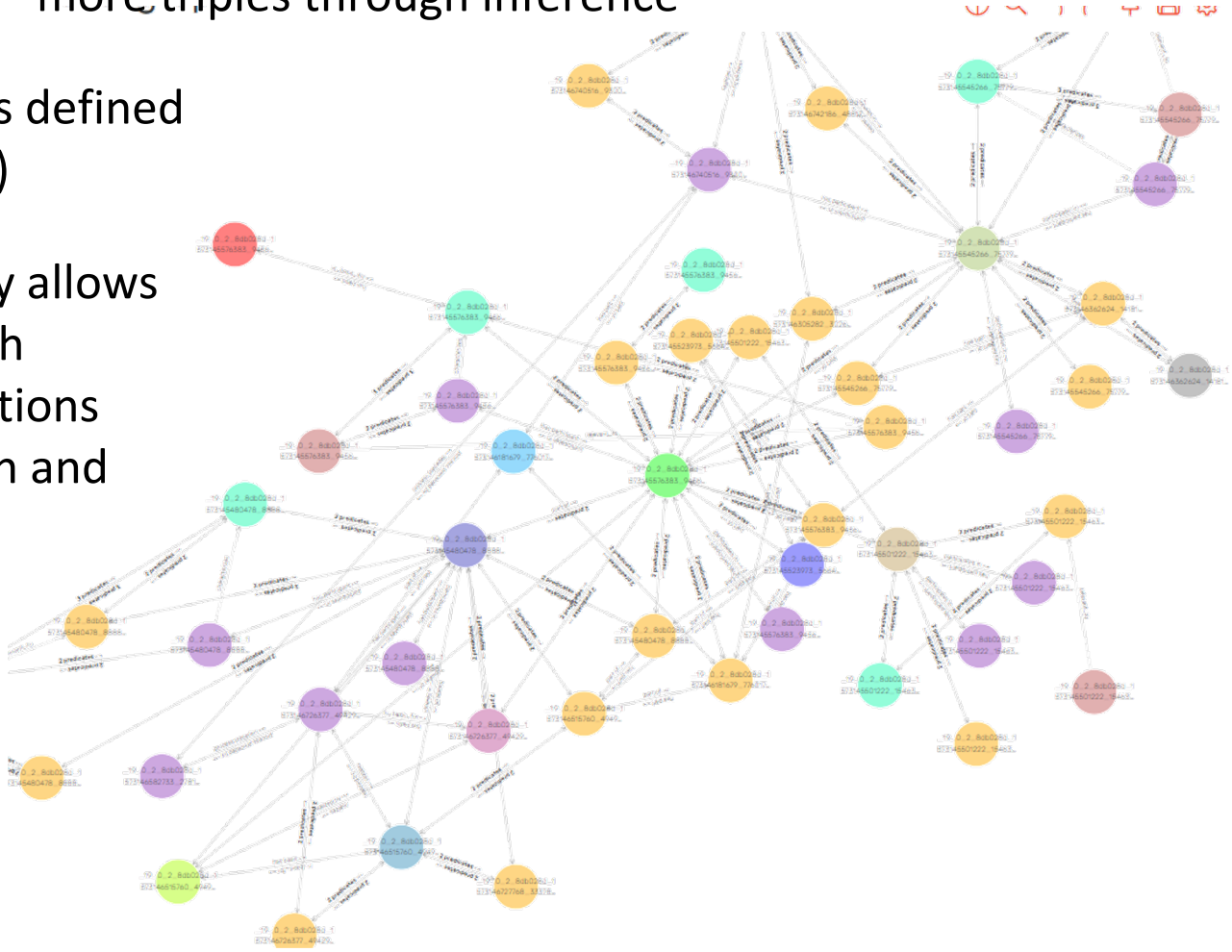
IoIF Cybersecurity Demo: Ontology

- Ontology data (RDF) is store as triples (Subject Predicate Object) as a graph in a Triplestore Repository



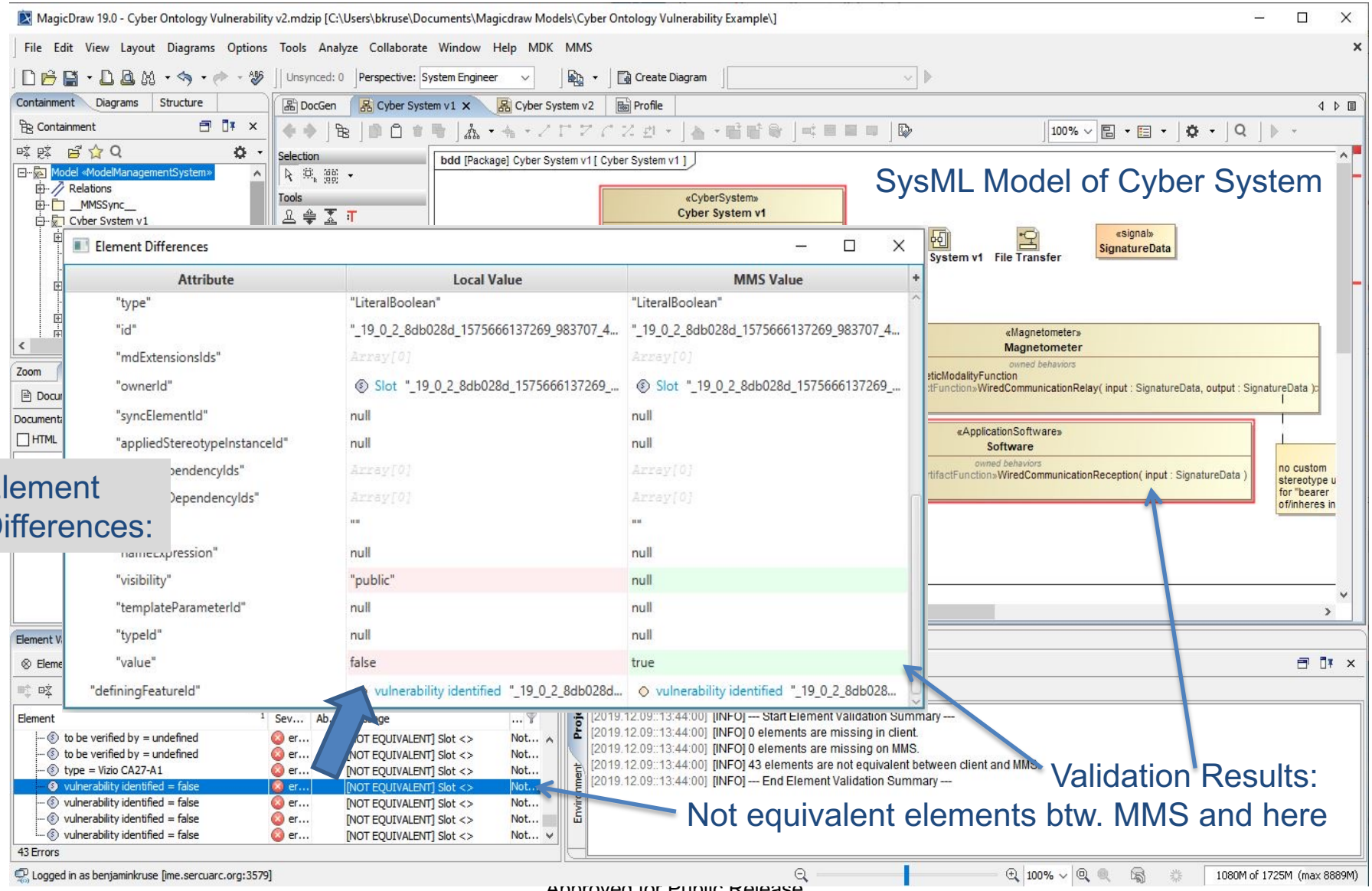
IoIF Conducts Reasoning to Expand Graph

- Reasoners "generate" more triples through inference
- Search vulnerabilities defined in RDF graph (CVAST)
- IoIF + Cyber Ontology allows us to rapidly find such vulnerable configurations and update the graph and synchronize back into model



SYSTEMS ENGINEERING
Research Center

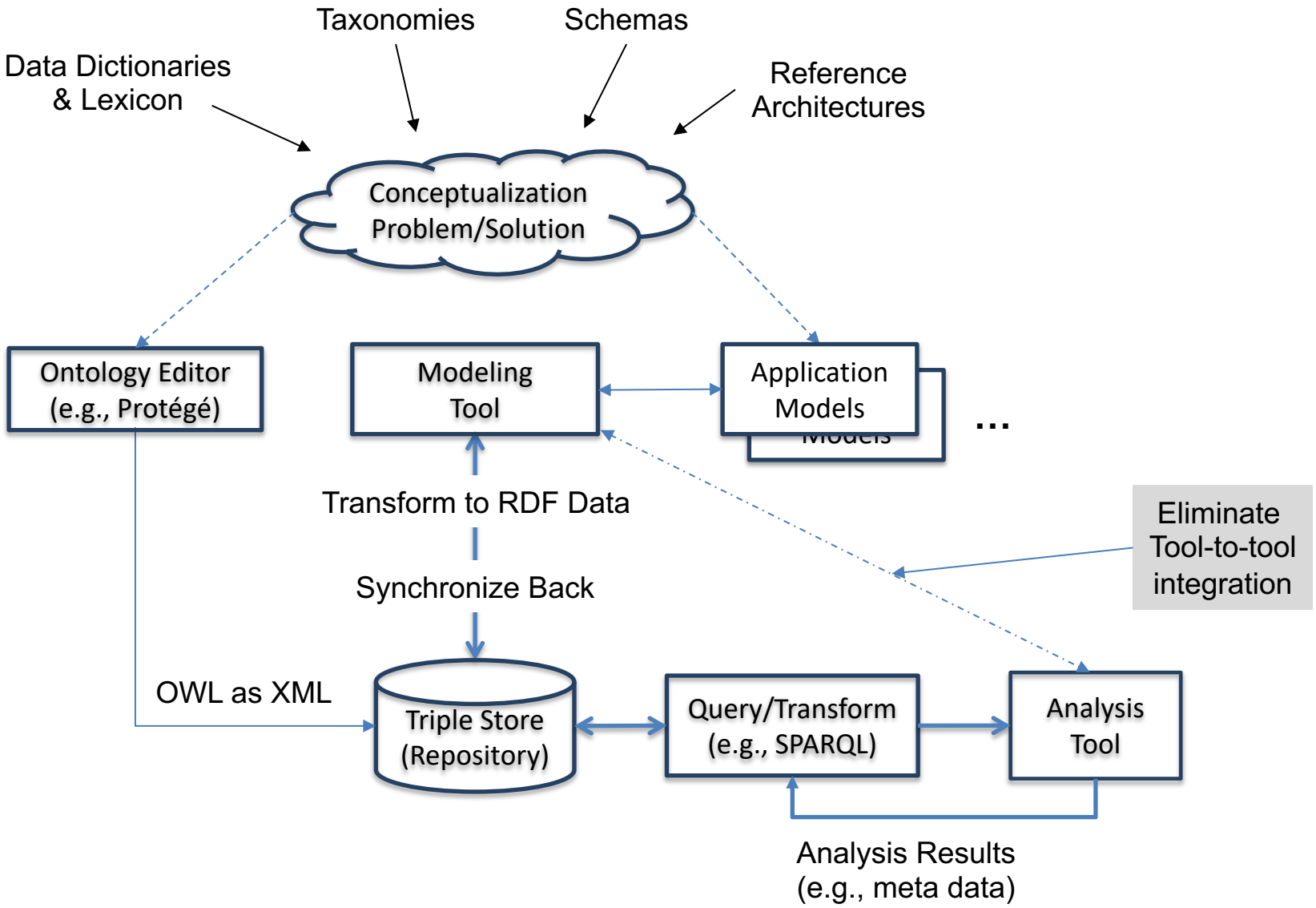
Magicdraw/Cameo Systems Modeler – Data Pushed Back



Summary and How Ontologies and Semantic Technologies Enable DE Infrastructure

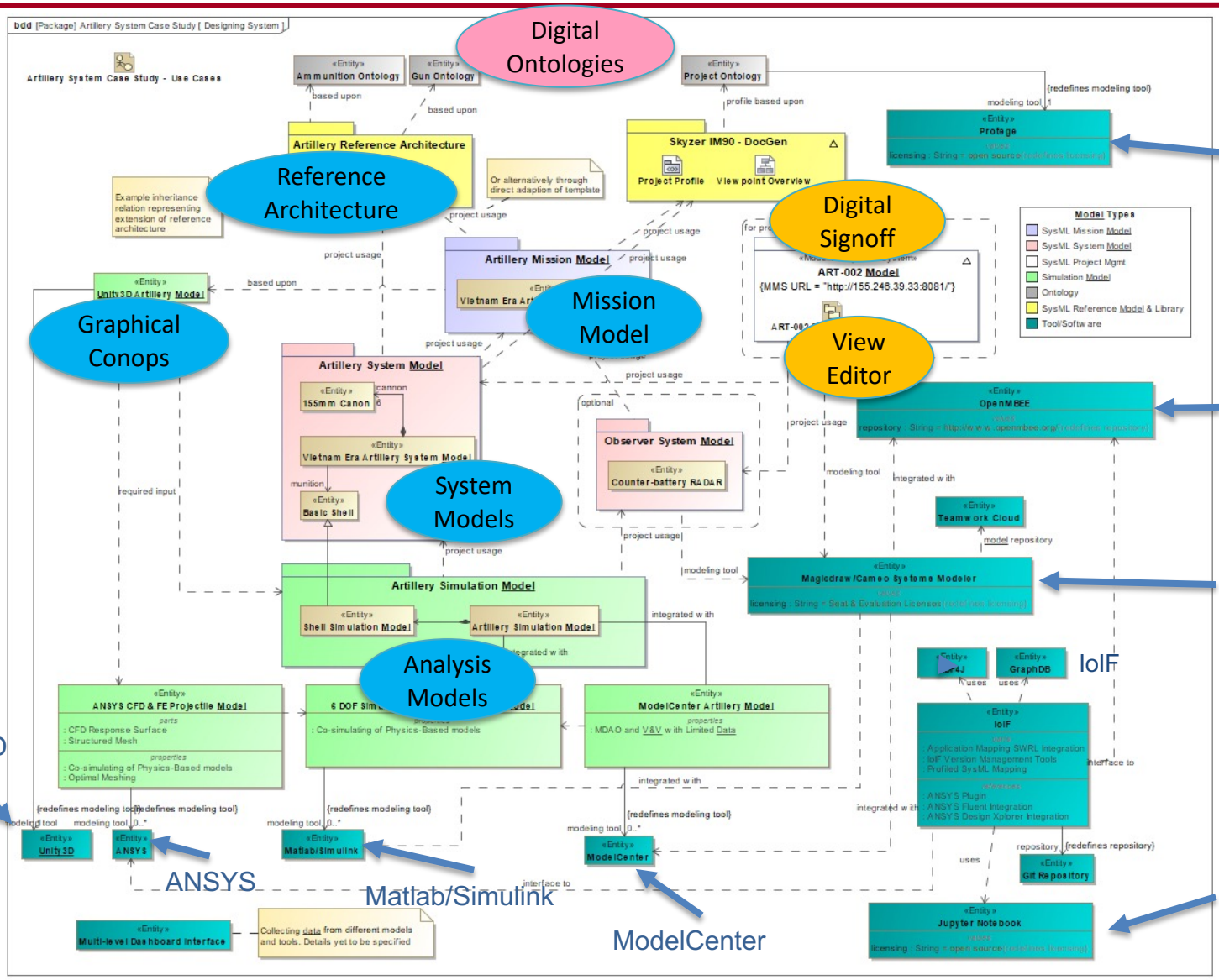
Approved for Public Release

Generalization for Mapping for Using Ontologies to support Interoperability vs. Tool-to-tool Integration



SYSTEMS ENGINEERING
Research Center

Example Reference Architecture "Full Stack"



Distribution Statement A: Approved for public release. Distribution is unlimited.

Primary Takeaways

- This approach has been readily adapted to other Application Domains
- We are looking for opportunities to scale this to a Program of Record to understand any impedance factors to full scale transition
- We plan to have follow on briefings on other Use Cases and additional deep dives into the enabling technologies and concepts

Thank you!

- Dr. Mark Blackburn
- Senior Research Scientist
- Principal Investigator
- Member of SERC Research Council
- Member of OpenMBEE Leadership Team
- School of Systems & Enterprises
- Systems Engineering Research Center
- Stevens Institute of Technology

Advancing the State of R&M Engineering Practice

R. Chris DeLuca
Director Specialty Engineering
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
Orlando, Florida
December 2021

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

Approved for public release. DOPSR Case # 22-S-0310.

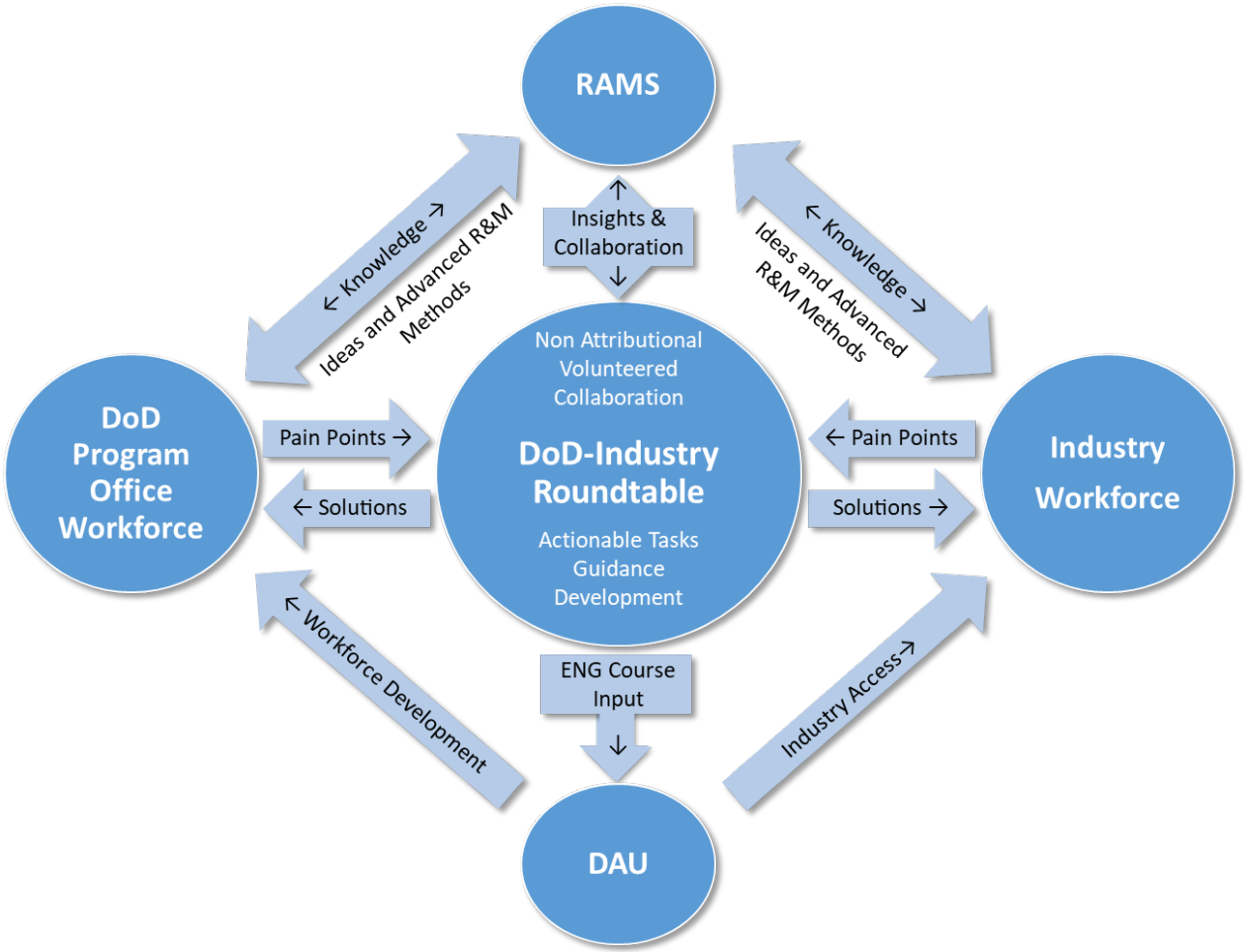
Agenda

- Reliability and Maintainability (R&M) Engineering Relationships and Interactions
- R&M Engineering Roundtable
- R&M Engineering Pain Points (Topics, Challenges)
  - Model-Based Engineering (MBE) Failure Modes, Effects, and Criticality Analysis (FMECA)
  - Instantiate Digital Engineering into R&M Practices
  - Deliver Reliable Software
  - Reducing Risk with Better R&M Estimates Throughout the Lifecycle
- Summary

Approved for public relelase. DOPSR Case # 22-S-0310.

R&M Engineering Relationships and Interactions

- Annual Reliability and Maintainability Symposium (RAMS)
  - RAMS Advisory Board
  - Paper: Challenges and Lessons Learned from Implementing an MBE FMECA in the DoD
  - DoD 'Reverse' Panel
- R&M Engineering Service Leads
- DoD – Industry R&M Engineering Roundtable



Approved for public relelase. DOPSR Case # 22-S-0310.

DoD - Industry R&M Engineering Roundtable

- Hosted annually in conjunction with RAMS with ongoing work activities throughout the year
- Volunteer DoD R&M practitioners and their industry counterparts
- Sharing knowledge, fostering interaction, identifying pain points
- Advancing state-of-the-practice within the R&M community to resolve R&M engineering pain points

RAMS®

Reliability & Maintainability Symposium

SPONSORS

THE INTERNATIONAL SYSTEM SAFETY SOCIETY

SOCIETY OF RELIABILITY ENGINEERS

IISE

SAE INTERNATIONAL

IEEE Reliability Society

ASQ Reliability & Risk Division The Global Voice of Quality®

ASQ Electronics and Communications Division The Global Voice of Quality®

IEST™

Approved for public relelase. DOPSR Case # 22-S-0310.

R&M Engineering Roundtable Pain Points

FY19/20

- Develop R&M Mid-Tier Acquisition Contract Language
- Map Standards to the R&M Engineering Body of Knowledge
- Transition the FMECA to an MBE Environment (ongoing)

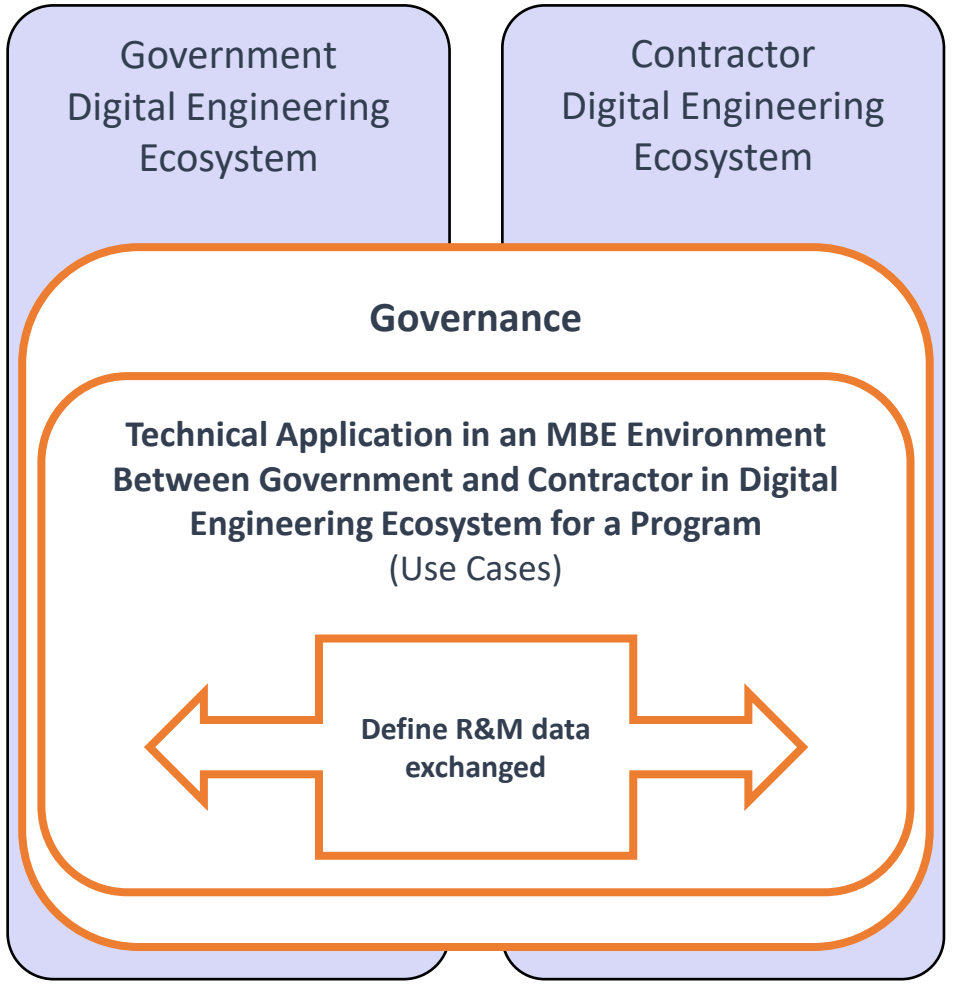
FY21/22

- Instantiate Digital Engineering into R&M Engineering practices
- Deliver Reliable Software
- Reduce Risk with Better R&M Estimates throughout the Lifecycle

Approved for public relelase. DOPSR Case # 22-S-0310.

MBE FMECA

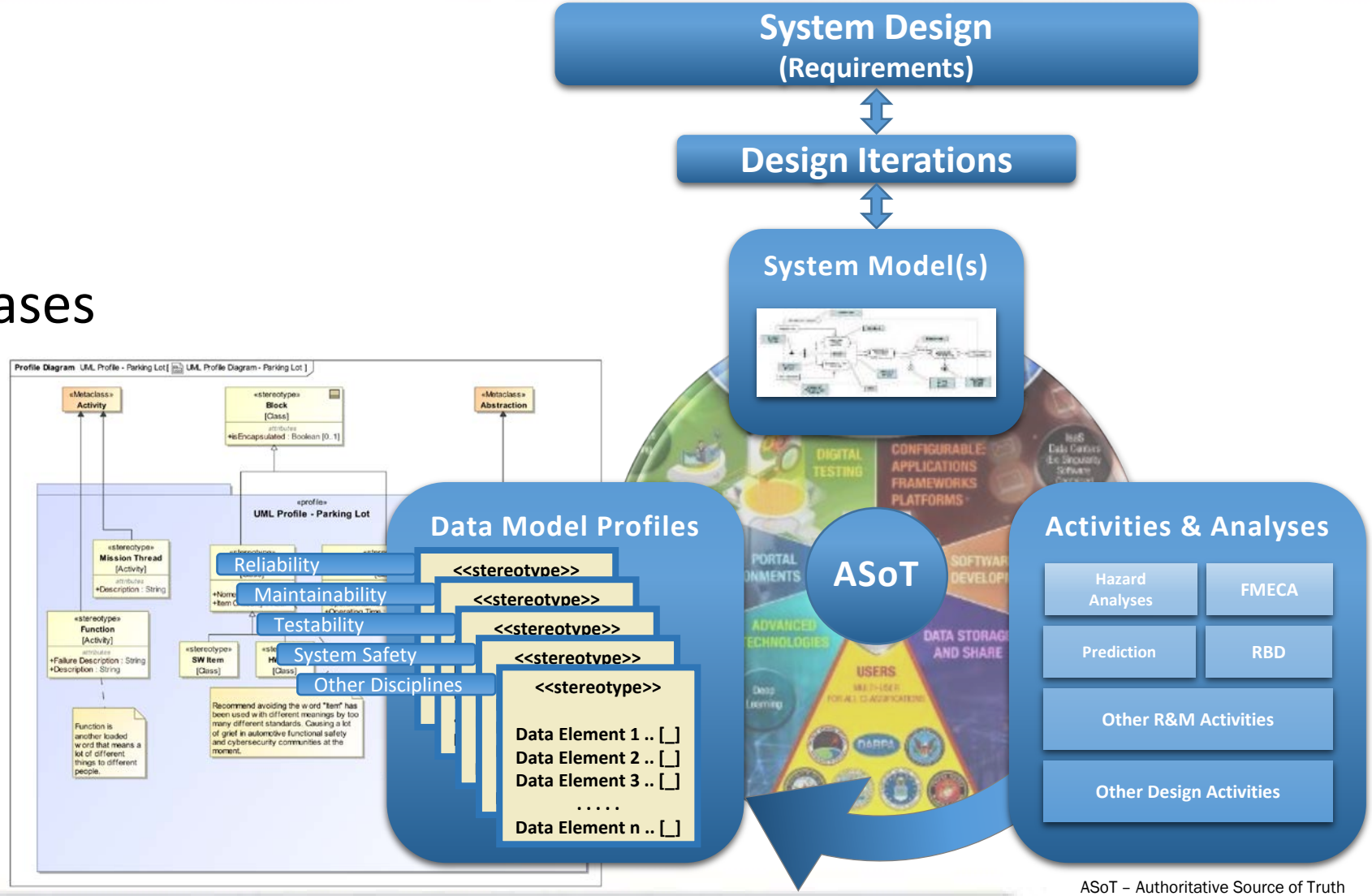
- MBE FMECA divided into three sub-working groups at the August 2019 DoD-Industry Roundtable
  - ☑ Define the R&M Data Exchanged (Elements)
  - ☑ Governance - Defense Standardization Program Office (DSPO)
  - ☐ Technical Application in a Digital Engineering (DE) Ecosystem



Approved for public relelase. DOPSR Case # 22-S-0310.

Technical Application in a DE Ecosystem

- Data Elements
- R&M Data Sources
- Activities and Use Cases
- Analysis Methods
- Reporting
- Government Access



ASoT – Authoritative Source of Truth
ConOp - Concept of Operations

Approved for public relelase. DOPSR Case # 22-S-0310.

FMECA DI-SESS-81495B [Active]

- Objective – Transition current FMECA process to an MBE process

DATA ITEM DESCRIPTION
Title: FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS

Number: DI-SESS-81495B
AMSC Number: N10028
DTIC Applicable: Yes
http://www.dtic.mil/dtic/submit
Preparing Activity: AS
Applicable Forms: N/A

Approval Date: 20190516
Limitation: N/A
GIDEP Applicable: Yes
http://www.gidep.org/data/submit.htm
Project Number: SESS-2019-016

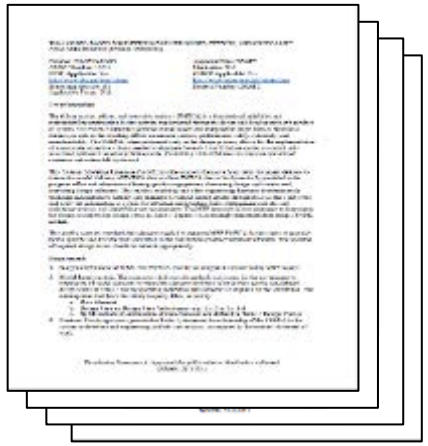
2. Content. These data shall explicitly show and document the relationship of the FMECA to the systems architecture and engineering artifacts and analysis, as required by the contract statement of work, and shall include:

a. Identification of how the FMECA aligns to the digital systems engineering environment.

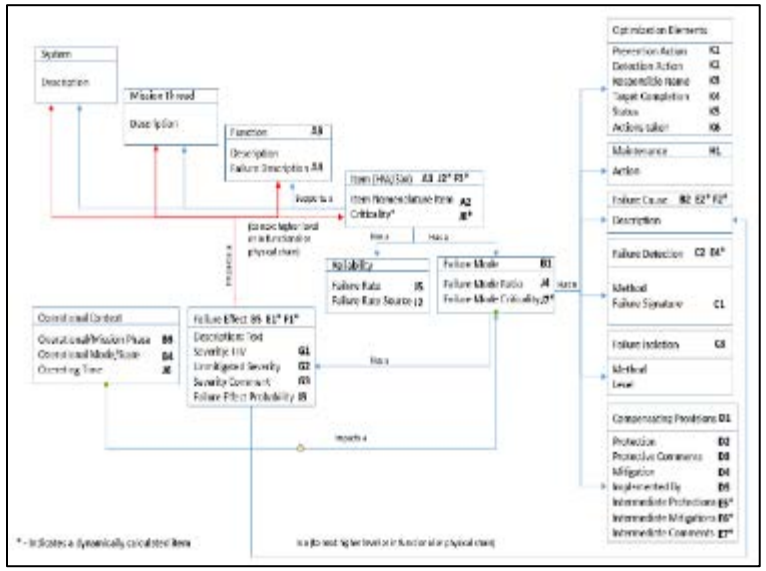
Approved for public relelase. DOPSR Case # 22-S-0310.

Transition to an MBE FMECA Profile

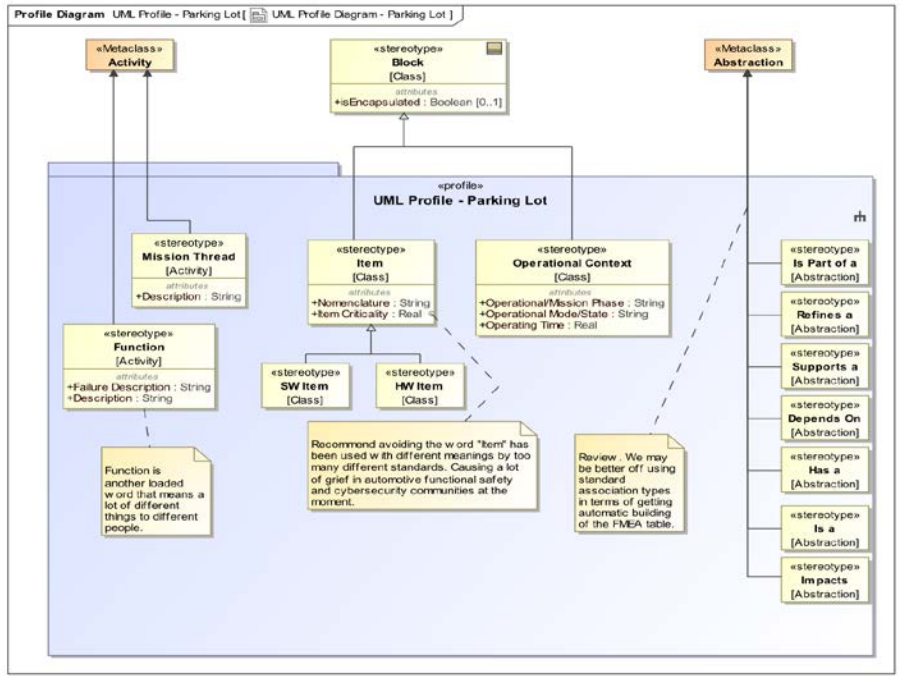
From Human Readable



To Representation



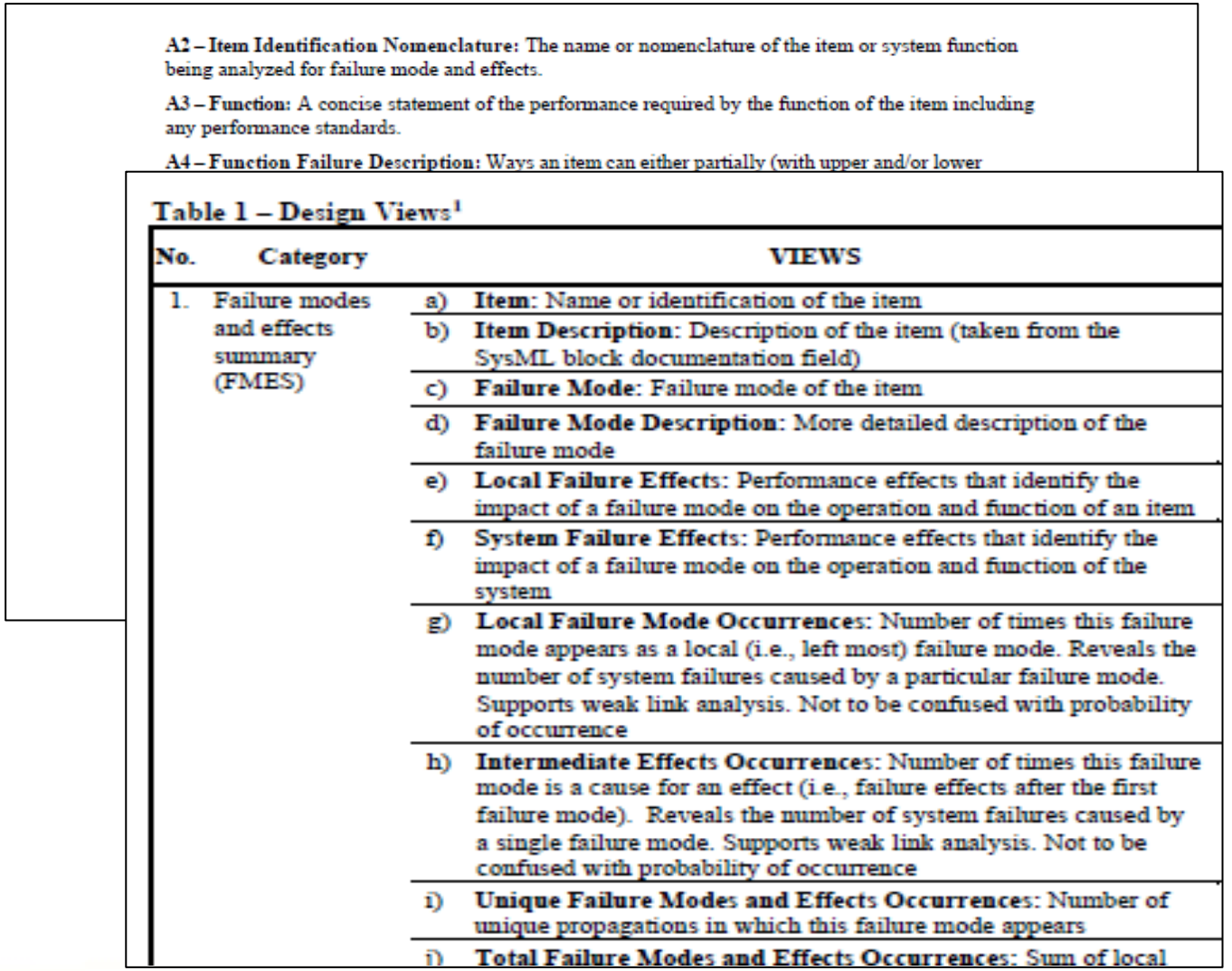
To Machine Readable (SysML)



Approved for public relelase. DOPSR Case # 22-S-0310.

Standard Data Elements and Views - Profile

- Establish Contract Language
  - Data Item Description (DID) Process
  - Data Elements
  - Design Views
- Develop Draft MBE FMECA DID
- Pilot on DSPO ASSIST Database
  - Human Readable PDF
  - Machine Readable XML



A2 – Item Identification Nomenclature: The name or nomenclature of the item or system function being analyzed for failure mode and effects.

A3 – Function: A concise statement of the performance required by the function of the item including any performance standards.

A4 – Function Failure Description: Ways an item can either partially (with upper and/or lower

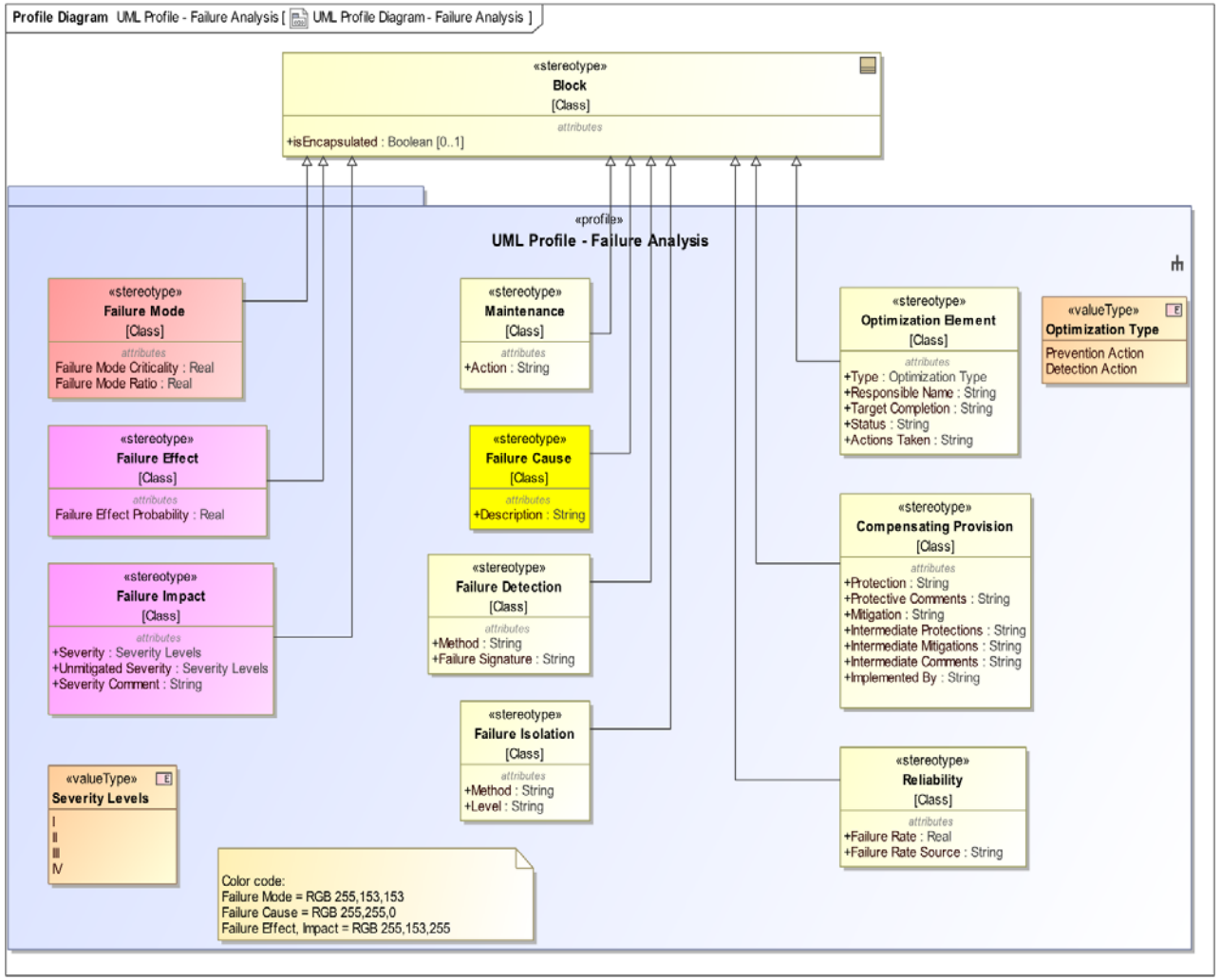
Table 1 – Design Views[1]

No.	Category	VIEWS
1.	Failure modes and effects summary (FMES)	a) **Item**: Name or identification of the item
		b) **Item Description**: Description of the item (taken from the SysML block documentation field)
		c) **Failure Mode**: Failure mode of the item
		d) **Failure Mode Description**: More detailed description of the failure mode
		e) **Local Failure Effects**: Performance effects that identify the impact of a failure mode on the operation and function of an item
		f) **System Failure Effects**: Performance effects that identify the impact of a failure mode on the operation and function of the system
		g) **Local Failure Mode Occurrences**: Number of times this failure mode appears as a local (i.e., left most) failure mode. Reveals the number of system failures caused by a particular failure mode. Supports weak link analysis. Not to be confused with probability of occurrence
		h) **Intermediate Effects Occurrences**: Number of times this failure mode is a cause for an effect (i.e., failure effects after the first failure mode). Reveals the number of system failures caused by a single failure mode. Supports weak link analysis. Not to be confused with probability of occurrence
		i) **Unique Failure Modes and Effects Occurrences**: Number of unique propagations in which this failure mode appears
		j) **Total Failure Modes and Effects Occurrences**: Sum of local

Approved for public relelase. DOPSR Case # 22-S-0310.

MBE FMECA Process

- Load the profile into SysML
- Populate blocks with data
  - Failure modes
  - Failure causes
  - Failure rates
- “Push a button” and generate the desired views
- Challenges
  - Trade-off: SysML model vs External R&M tools, data, and models
  - Scalability
  - Model overload with other disciplines
  - External access, Data Rights (IP)



Approved for public relelase. DOPSR Case # 22-S-0310.

Policy Directs R&M Digital Representations

- DoDI 5000.88 – Engineering of Defense Systems
- "…integral part of the overall engineering process and the digital representation of the system"
- "…strategy consisting of…digital artifacts"

b. Reliability and Maintainability (R&M).

(1) For all defense acquisition programs, the LSE, working for the PM, will integrate R&M engineering as an integral part of the overall engineering process and the digital representation of the system being developed.

(a) The LSE will plan and execute a comprehensive R&M program using an appropriate strategy consisting of engineering activities, products, and digital artifacts, including:

1. R&M allocations, block diagrams, and predictions.
2. Failure definitions and scoring criteria.
3. Failure mode, effects, and criticality analysis,
4. Maintainability and built-in test demonstrations.
5. Reliability testing at the system and subsystem level.
6. A failure reporting, analysis, and corrective action system maintained through design, development, test, production, and sustainment.

Approved for public relelase. DOPSR Case # 22-S-0310.

Instantiate DE into R&M Engineering Practices

- Number 1 (out of 14) Pain Points Identified by the R&M Engineering Community in FY21
- Informed by the MBE FMECA efforts and advancing the flow of failure mode and effects analysis (FMEA) data
  - Design FMEA
  - Process FMEA
  - Supportability FMEA (Logistics Product Data)
- Expanding to all R&M Engineering Activities
- Including the flow from Model-Based Systems Engineering to Model-Based Product Support

Approved for public relelase. DOPSR Case # 22-S-0310.

DE into R&M Engineering Goals

- Educate and train R&M engineers on the application of MBE
- Move from current static document delivery to interactive model delivery of R&M data
- Leverage interfaces to authoritative 3D engineering models (sources of truth) for components and systems
- Allow efficient and continuous engagement of R&M engineers with designers to increase design influence
- Decrease design cycle times
- Ensure R&M models to support weapon systems during Operations and Support phase (MBSE to MBPS)

Approved for public relelase. DOPSR Case # 22-S-0310.

DE into R&M Engineering Path Forward

- R&M MBE Use Cases (How SysML models are used in R&M engineering analyses)
- Pilot opportunities in MBE (Based on the Use Cases)
- Guidance
  - Lessons learned
  - Best practices
  - Model and data exchange between R&M engineering and other engineering models
  - Exchange between government program office and prime contractor manufacturers
  - Updated DAU R&M Engineering 08XX courses as necessary
- Initial guidance at the DoD – Industry R&M Roundtable co-located during RAMS, January 2022

Approved for public relelase. DOPSR Case # 22-S-0310.

Deliver Reliable Software

- Number 2 Pain Point within the R&M Engineering Community
- Opinions on software reliability vary – Why Reliable Software
  - "There is no such thing as software reliability"
  - "You can observe it but it is difficult to predict"
  - "You can track defects with software quality and maturity"
  - "It is either zero or one"
  - "Why not use IEEE-1633-2016"
  - "You can do a software FMEA but not a FMECA because the 'CA' requires quantitative prediction of software reliability"

Approved for public relelase. DOPSR Case # 22-S-0310.

Deliver Reliable Software – Path Forward

- Develop guidance and contract language
  - Use of DevSecOps
  - Metrics (allocate? measure, test, observe)
  - Requirements (restore time, frequency of restarts, availability)
  - Failure definition and scoring criteria
  - Failure mode identification, risk assessment, severity
  - Data collection methods
  - Roles (who is responsible software, reliability, quality, safety, others?)
- Initial guidance at the DoD – Industry R&M Roundtable co-located during RAMS, January 2022

Approved for public relelase. DOPSR Case # 22-S-0310.

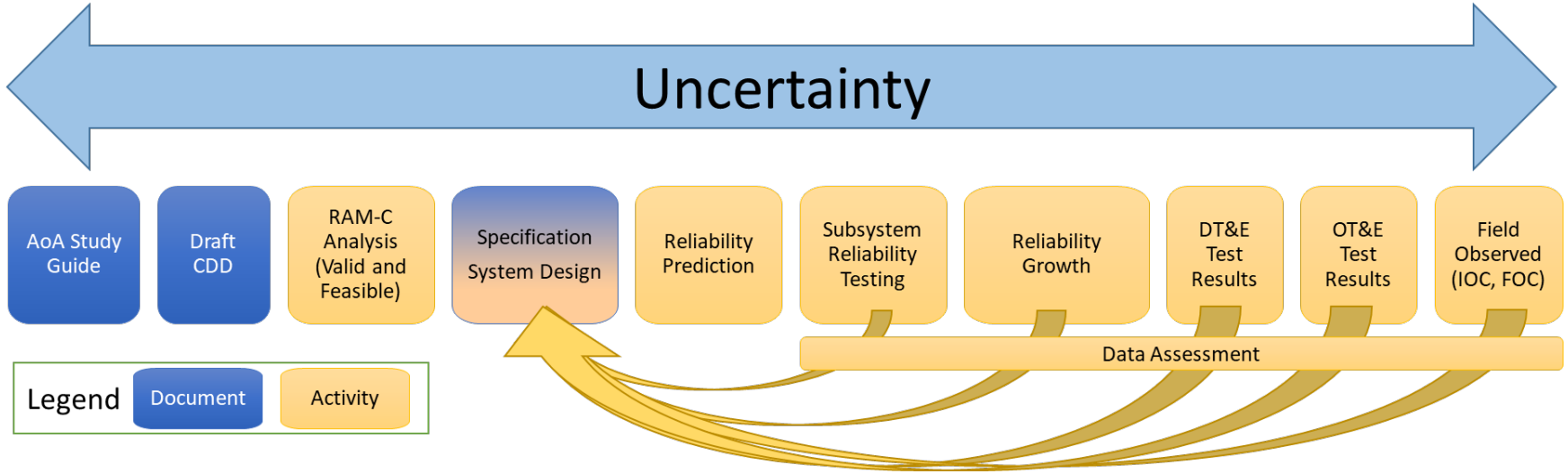
Reduce Risk with Better R&M Estimates

- Number 3 Pain Point within the R&M Engineering Community
- Why? R&M estimates inform many products throughout the lifecycle
  - Allocations and predictions
  - Criticality Analysis
  - Spares Analysis….to name a few
- Not just “better” estimates, help with understanding
  - Incorrect usage
  - Purpose of estimates change throughout the lifecycle
  - Source of data change
  - Fidelity, accuracy, and cleanliness of data
  - Feedback from test and operational usage to inform better up front estimates

Approved for public relelase. DOPSR Case # 22-S-0310.

Better R&M Estimates Path Forward

- Understand all estimates have uncertainty
- Understand what R&M value to use for each activity
- Use modern data analytic techniques
- Initial guidance at the DoD – Industry R&M Roundtable co-located during RAMS, January 2022



Approved for public relelase. DOPSR Case # 22-S-0310.

Summary

- Anyone want to join our R&M Engineering Roundtable?
  - Government (DoD, NASA) ?
  - Industry DoD Manufacturers ?
- Transitioning to a MBE FMECA is leading the R&M community to a DE ecosystem
- Instantiating DE into R&M is helping to flow engineering design to manufacturing and product support
- Delivering reliable software with DevSecOps methods is minimizing the occurrence of software failures that would occur in operations
- Reducing the risk with better R&M estimates ultimately increases the readiness of our systems for the warfighter
- Collaborating on the combined pain points helps deliver Reliable, Maintainable, and Supportable Advanced Capabilities to the Warfighter

Approved for public relelase. DOPSR Case # 22-S-0310.

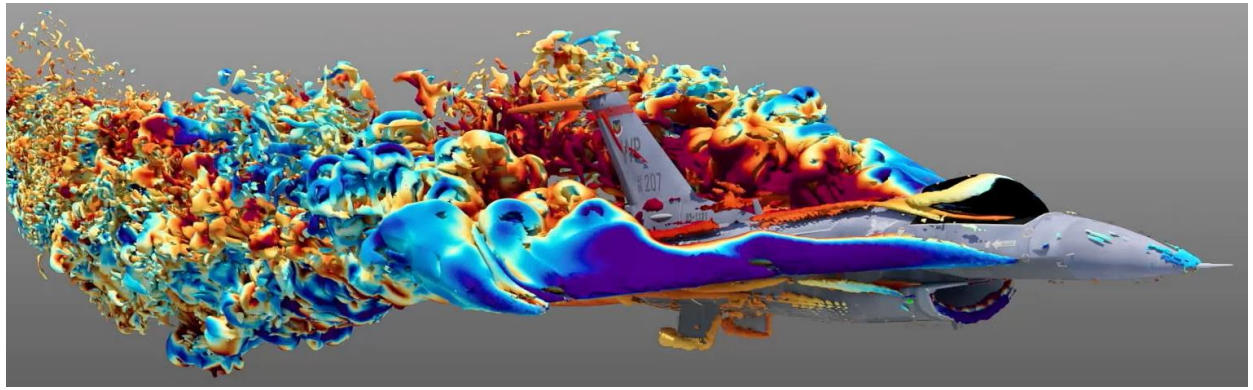
Contact

Office of the Deputy Director for Engineering

osd.r-e.comm@mail.mil
Attention: R&M Engineering

ac.cto.mil/engineering

Approved for public relelase. DOPSR Case # 22-S-0310.



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

National Defense Industry Association
Systems and Mission Engineering Conference
6-8 December 2021

Dr. Scott A. Morton, Associate Director for CREATE
DoD HPCMP, US Army ERDC/Information Technology Laboratory
Scott.a.morton3.civ@mail.mil

Distribution Statement A: Approved for public release, distribution unlimited.

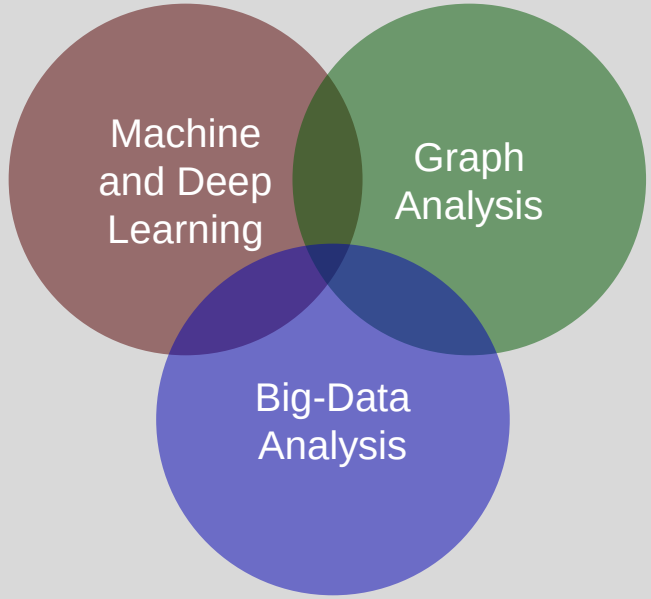
Definition: High-End Computing *(HEC)*

Compute-Intensive	
Difficult	**Easy**
Tightly-coupled *100s to 1000s of nodes in lock-step*	**Embarrassingly parallel** *independent task / node*
Fast / low-latency network	**Slow / high-latency network**
Fast / large memory and storage	**Slow / small memory and storage**
High Performance Computing	**Basic Computing**

Data-Intensive	
Difficult	**Easy**
10s to 1000s of accelerators	**Few accelerators**
10s to 1000s of information feeds	**Few information feeds**
Large graphs	**Small graphs**
Large data sets	**Small data sets**
High Performance Data Analysis	**Basic Data Analysis**

High-End Computing (HEC) = **High Performance Computing (HPC)** + **High Performance Data Analysis (HPDA)**

Data-Intensive Methods: a computer science approach to understanding phenomena and exploiting uncovered information



- Building artificial intelligence (AI) models *(machine and deep learning)*
- Uncovering relationships *(graph analysis)*
- Understanding large volumes of data *("big data" analysis)*

Distribution Statement A: Approved for public release, distribution unlimited.

Definition: Digital Engineering vs. MBSE

- **Model-based systems engineering (MBSE) –** a formalized methodology used to support the requirements, design, analysis, verification, and validation associated with the development of complex systems *(Nataliya Shevchenko, "An Introduction to Model-Based Systems Engineering (MBSE)," Software Engineering Institute (SEI), 21 Dec 2020)*

- **Digital engineering (DE)** – 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.** *(Defense Acquisition University)*
  - Integrated digital approach → a monolithic solution that suggests there can be no R&E / A&S divide
  - Data → must be regularly managed/updated/curated at each stage of the process
  - Models → both compute and data-intensive; range from basic analysis to high-end computing (HEC)
  - Availability → accessible to anyone in the design, test, evaluation, sustainment, mission planning pipeline
  - Duration → from concept through disposal (and possibly beyond); decades to centuries
  - Extensity → continuum across disciplines; simultaneous accounting of all assets at all lifecycle stages to facilitate projection of current and future forces in a full range of scenarios, to determine gaps, to advise the characteristics of future platforms, and to build preventive maintenance plans for individual assets

Distribution Statement A: Approved for public release, distribution unlimited.

Definition: Digital Engineering vs. MBSE

- **Model-based systems engineering (MBSE) –** a formalized methodology used to support the requirements, design, analysis, verification, and validation associated with the development of complex systems *(Nataliya Shevchenko, "An Introduction to Model-Based Systems Engineering (MBSE)," Software Engineering Institute (SEI), 21 Dec 2020)*

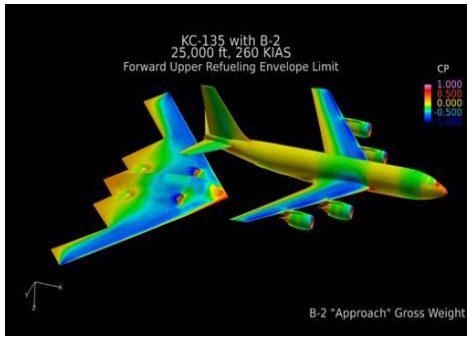
- **Digital engineering (DE)** – an **integrated digital approach** that uses authoritative sources of systems' **data** and **models** as a **continuum across disciplines** to support life cycle activities **from concept through disposal.** *(Defense Acquisition University)*
  - Integrated digital approach → a monolithic solution that suggests there can be no R&E / A&S divide
  - Data → must be regularly managed/updated/curated at each stage of the process
  - Models → both compute and data-intensive; range from basic analysis to high-end computing (HEC)
  - Availability → accessible to anyone in the design, test, evaluation, sustainment, mission planning pipeline
  - Duration → from concept through disposal (and possibly beyond); decades to centuries
  - Extensity → continuum across disciplines; simultaneous accounting of all assets at all lifecycle stages to facilitate projection of current and future forces in a full range of scenarios, to determine gaps, to advise the characteristics of future platforms, and to build preventive maintenance plans for individual assets

Distribution Statement A: Approved for public release, distribution unlimited.

HEC Impacting Digital Engineering

HEC and High Fidelity Physics (Physics Based Analytics-PBA) used for Deficiency Diagnosis

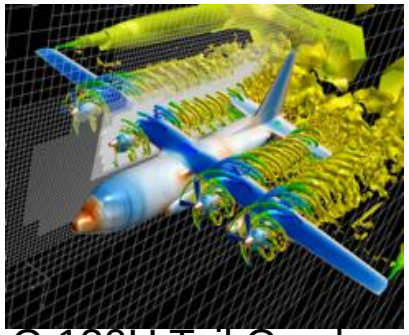
- **Single Point Calc's (days/100k CPUHrs)**
- **Typically Occurs After Wind/Flight Test discoveries**
- **Fixes can be very costly since the vehicle is far into the design timeline**
- **Payoff for Programs ($M's)**
- **Postdictive/Early Predictive**



B-2/KC-135 Refuel



Light Weight Prec Munition



C-130H Tail Crack

Increasing Program Relevance and Impact on Program Cost, Schedule, and Performance

Current Simulation Capability/Increasing Resources

Distribution Statement A: Approved for public release, distribution unlimited.

HEC Impacting Digital Engineering

HEC and High Fidelity Physics (Physics Based Analytics-PBA) used for Deficiency Diagnosis

- Single Point Calc's (days/100k CPUHrs)
- Typically Occurs After Wind/Flight Test discoveries
- Fixes can be very costly since the vehicle is far into the design timeline
- Payoff for Programs ($M's)
- Postdictive/Early Predictive

HEC and PBA used earlier in Design to Downselect From a Few Configurations

- Many More Single Point Calcs/ Maneuvers (days/1Ms CPUHrs)
- Targets Specific Flight Cond's Mnvrs for Comparison and Risk Reduction
- Chosen Vehicle Better Meets Req's
- Higher payoff for Programs ($10M's)
- Early Predictive

Increasing Program Relevance and Impact on Program Cost, Schedule, and Performance

Current Simulation Capability/Increasing Resources

Distribution Statement A: Approved for public release, distribution unlimited.

HEC Impacting Digital Engineering

HEC and High Fidelity Physics (Physics Based Analytics-PBA) used for Deficiency Diagnosis

- Single Point Calc's (days/100k CPUHrs)
- Typically Occurs After Wind/Flight Test discoveries
- Fixes can be very costly since the vehicle is far into the design timeline
- Payoff for Programs ($M's)
- Postdictive/Early Predictive

HEC and PBA used earlier in Design to Downselect From a Few Configurations

- Many More Single Point Calcs/ Maneuvers (days/1Ms CPUHrs)
- Targets Specific Flight Cond's Mnvrs for Comparison and Risk Reduction
- Chosen Vehicle Better Meets Req's
- Higher payoff for Programs ($10M's)
- Early Predictive

Accurate Surrogates built using HEC and PBA across the Life-Cycle

- Faster than real time Models
- Explore the Design Space
- Enable Mission Length Multiphysics Analysis
- Optimized Designs with Models of Many Disciplines Interacting
- Higher payoff for Programs ($100M's)
- Predictive

Increasing Program Relevance and Impact on Program Cost, Schedule, and Performance

Current Simulation Capability/Increasing Resources

Revolutionary Approach to Building Accurate Models

Distribution Statement A: Approved for public release, distribution unlimited.

HEC Impacting Digital Engineering

HEC and High Fidelity Physics (Physics Based Analytics-PBA) used for Deficiency Diagnosis

- Single Point Calc's (days/100k CPUHrs)
- Typically Occurs After Wind/Flight Test discoveries
- Fixes can be very costly since the vehicle is far into the design timeline
- Payoff for Programs ($M's)
- Postdictive/Early Predictive

HEC and PBA used earlier in Design to Downselect From a Few Configurations

- Many More Single Point Calcs/ Maneuvers (days/1Ms CPUHrs)
- Targets Specific Flight Cond's Mnvrs for Comparison and Risk Reduction
- Chosen Vehicle Better Meets Req's
- Higher payoff for Programs ($10M's)
- Early Predictive

Accurate Surrogates built using HEC and PBA across the Life-Cycle

- Faster than real time Models
- Explore the Design Space
- Enable Mission Length Multiphysics Analysis
- Optimized Designs with Models of Many Disciplines Interacting
- Higher payoff for Programs ($100M's)
- Predictive

System Level Models Built with Surrogates

- System Models with Associated Confidence Bounds
- Use AI/ML to Search Design Space for Deficiencies
- Virtual Flight Test Accomplished and Validated with Targeted FT
- Continual Model Updates Through Life Cycle
- Higher payoff for Programs ($B's)
- Fully Predictive

Increasing Program Relevance and Impact on Program Cost, Schedule, and Performance

Current Simulation Capability/Increasing Resources

Revolutionary Approach to Building Accurate Models

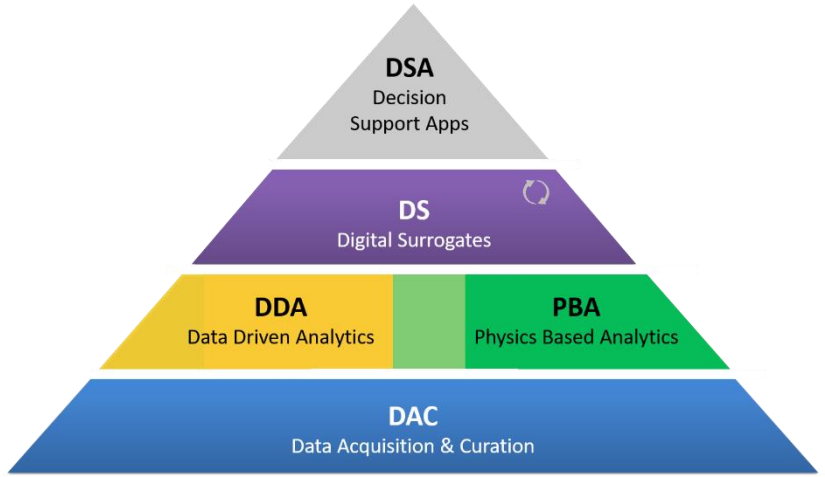
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Digital Engineering

- **Combat Air Vehicle Example**



- **Look at example Apps, Physics Informed Surrogates, Physics Based Analytics, Data Driven Analytics, and Data Acquisition and Curation**



Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics - Aerodynamics

- **Models are built to impact decision making in air vehicle design, development, and sustainment**
  - Examples – Aerodynamics, Stability and Control (S&C), Propulsion, Structures



- **High Fidelity CFD Models typically…**
  - Take supercomputer resources to run depending on the fidelity of the mesh
  - Take flight conditions, surface and external volume meshes with boundary condition attributions as inputs
  - Compute the surface and volume aerodynamics of the vehicle using a finite volume or finite element solution algorithm
  - May be coupled with a structural solver, propulsion module, 6DOF solver, chemistry solvers for non-ideal gases, and conjugate gradient heat transfer solver to compute multiphysics simulations



- **Reduced Order Loads Models typically…**
  - Are derived from simulations using the high fidelity CFD solver, sometimes coupled with other physics models (e.g. S&C 6DOF, Structures, Propulsion)
  - Run faster than real time and can span the air vehicle envelope

Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics – S&C



- **The Stability and Control Model is typically a 6 Degree of Freedom (6DOF) solver that…**
  - Runs faster than real time and spans the vehicle envelope
  - Takes mass properties, vehicle configuration, and desired flight trajectory (e.g. stick inputs) or conditions as inputs
  - Uses information about vehicle aerodynamics, structures, and propulsion and the equations of motion to determine a vehicle's trajectory
  - Can incorporate "feedback control laws"
  - Can easily be improved for accuracy by replacing aerodynamics, structures, and propulsion data as higher fidelity information is known
- **Stability and Control Model can be used for…**
  - Stability and Control analysis and handling qualities
  - Sensitivity studies
  - Mission performance – fuel burn, available payload weight, etc.
  - Driver for "Pilot in the Loop" Simulators





Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics - Propulsion

- **The Propulsion Model has two variants**
  - High fidelity turbomachinery integrated into a CFD solver
  - Engine cycle deck



- **Turbomachinery are geometry/mesh components (e.g. compressor or turbine rotor/stators, combustor) in the flowfield path of a high fidelity simulation tool**

- **The Engine Cycle Deck typically…**
  - Runs faster than real time and spans the vehicle envelope
  - Takes flight conditions, compressor face conditions, exit nozzle conditions, and vehicle configuration as inputs
  - Uses information about the engine and with one-dimensional engine pressure and temperature ratios through the engine stations, along with bleed losses and installation losses, determines compressor face and exit nozzle mass flow, velocity, and temperature data, as well as fuel burn and installed thrust
  - Can be run offline, integrated into a high fidelity simulation tool (FORTRAN or NPSS Model) with pseudo-time accuracy with or without transient behavior, or integrated into an S&C 6DOF Model to provide thrust



Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics - Structures

- **Two variants of Structures Models**
  - Finite Element Structural Model with a High Fidelity Simulation Tool
  - Modal Structural Model



- **The Finite Element Structures Model typically…**
  - Takes from work station to supercomputer resources to run depending on the fidelity of the mesh
  - Takes flight conditions, internal structure meshes with material property attributions, and external loads as inputs
  - Computes the structural deformation, as well as, internal stress and strain of the structure using a finite element solution algorithm
  - It may be coupled with an aerodynamic solver and/or a conjugate gradient heat transfer solver to compute fluid-structure, thermal-structure, or fluid-thermal-structural interactions



- **The Modal Structural Model typically…**
  - Is a linearized Reduced Order Model derived from the Finite Element Model through an eigenvalue analysis
  - Runs orders of magnitudes faster than the Finite Element Model

Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)

Kestrel

Outer Mold Line OML



Increasing Multi-disciplinary

Increasing Detail/Accuracy

Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**

Increasing Multi-disciplinary

Kestrel

Outer Mold Line OML

Inlet/Exit Geometry



Increasing Detail/Accuracy

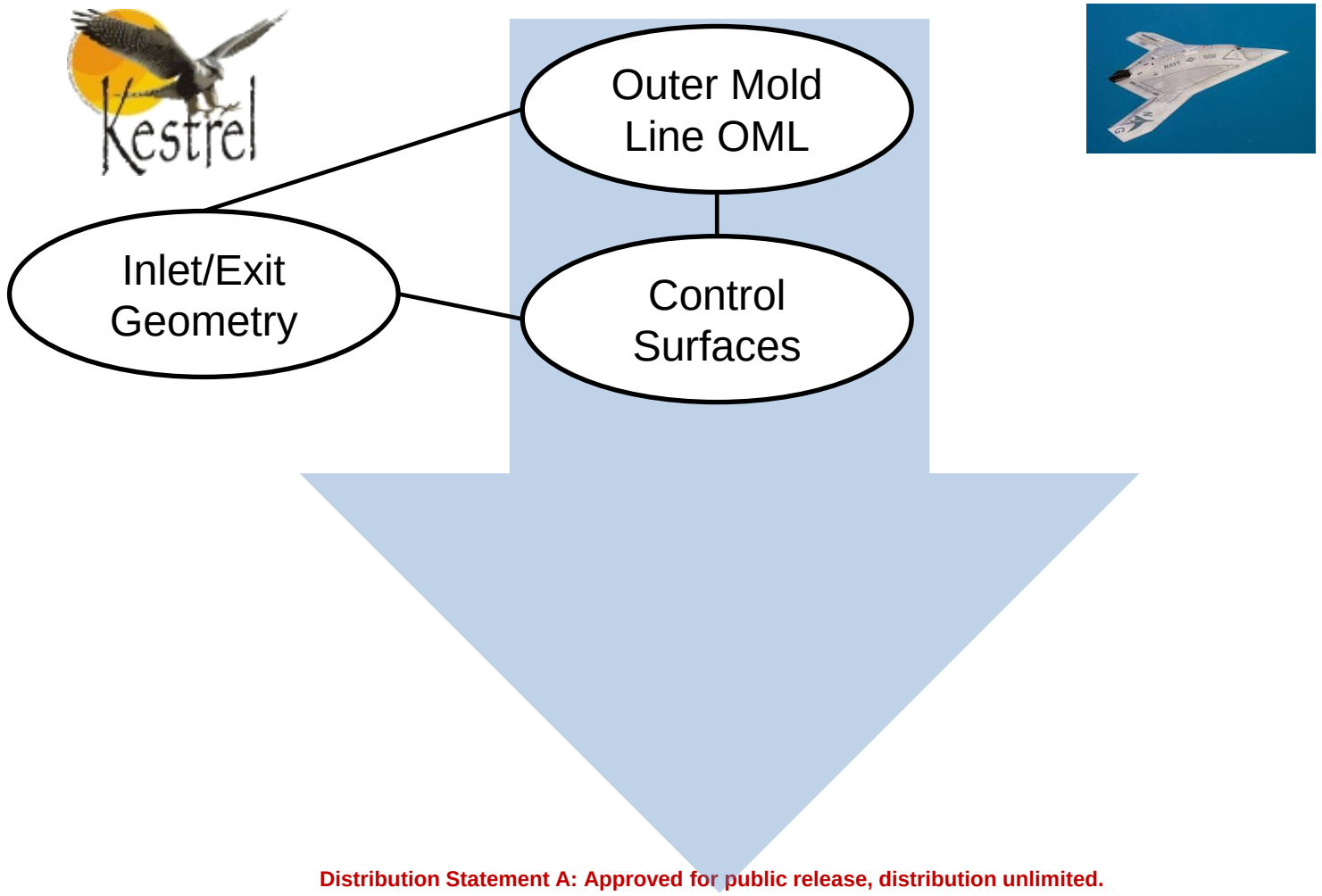
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



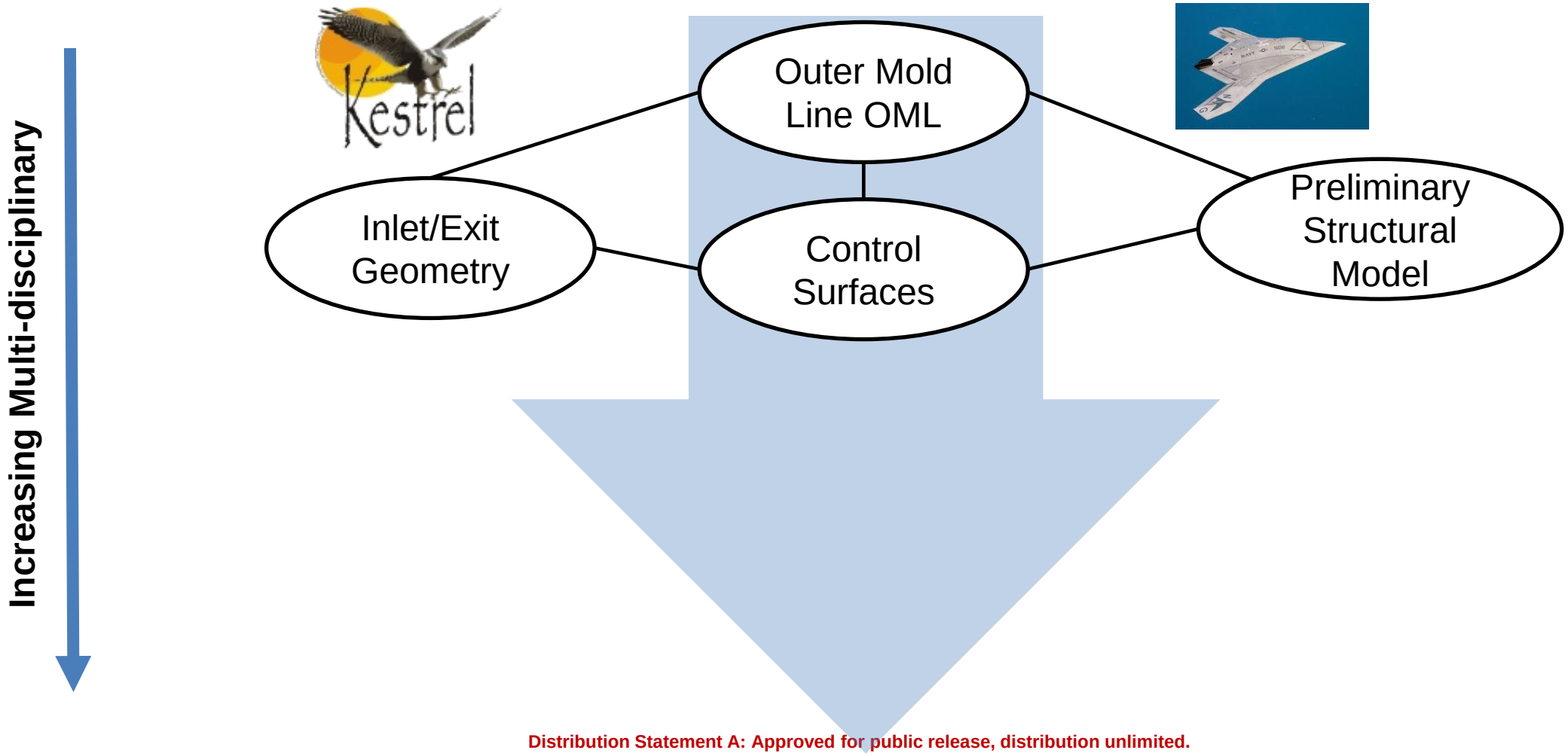
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



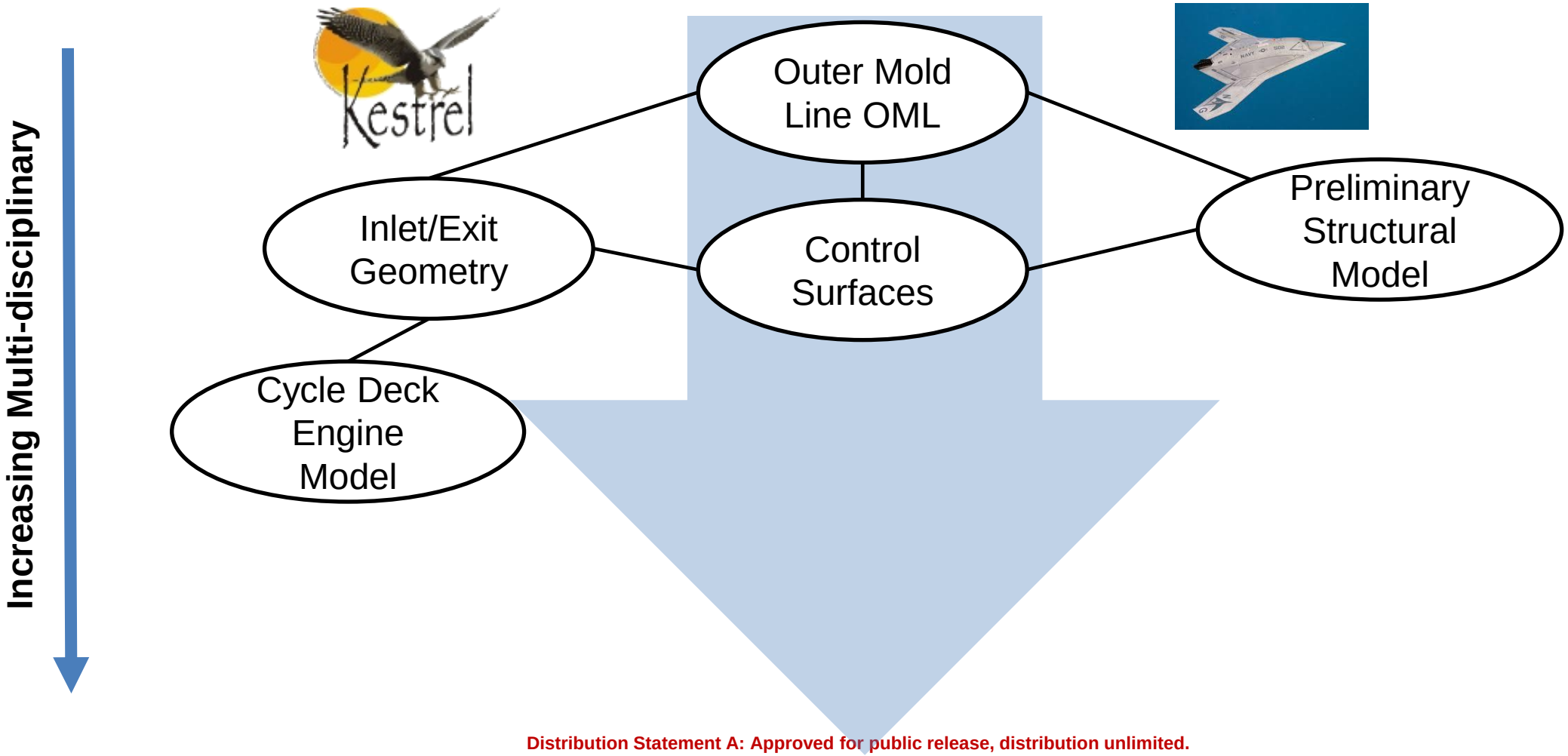
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



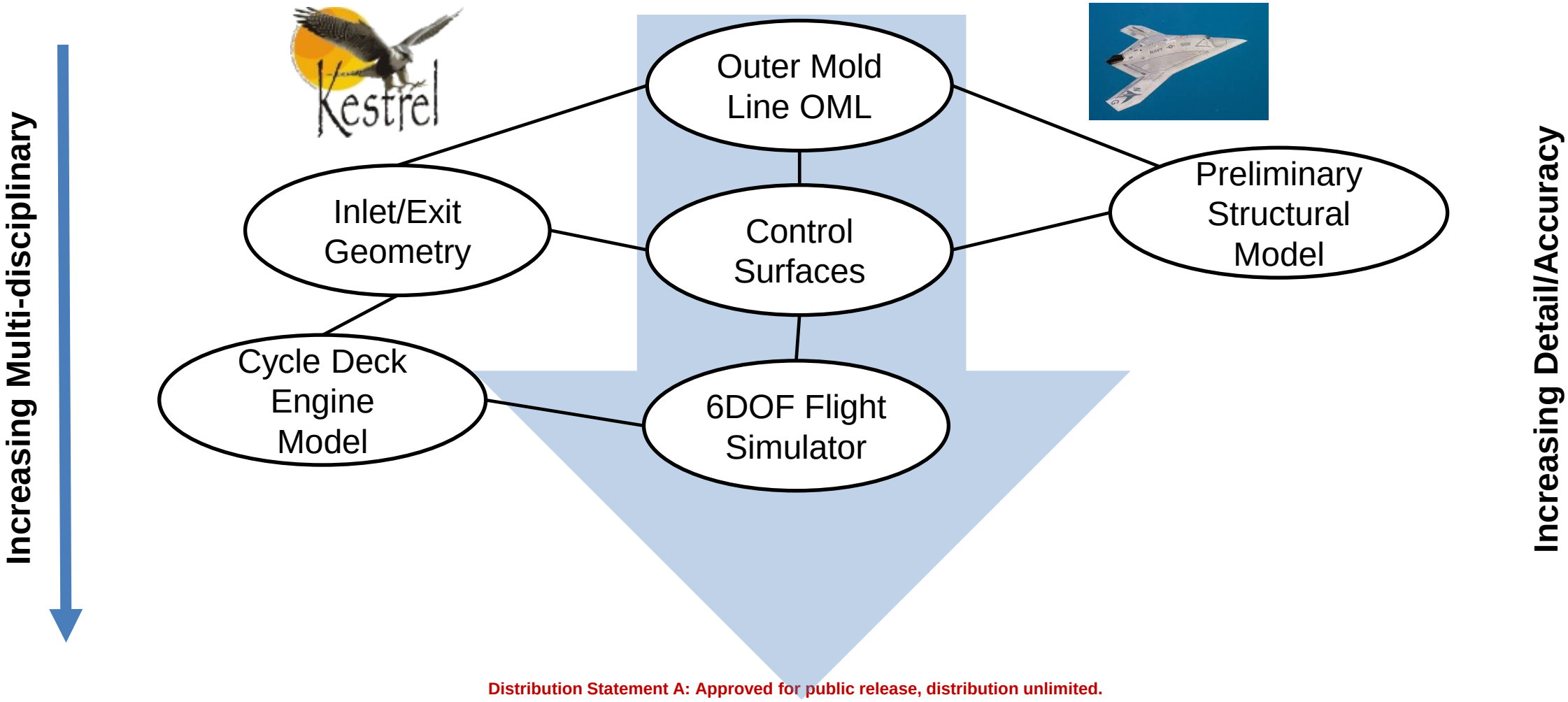
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

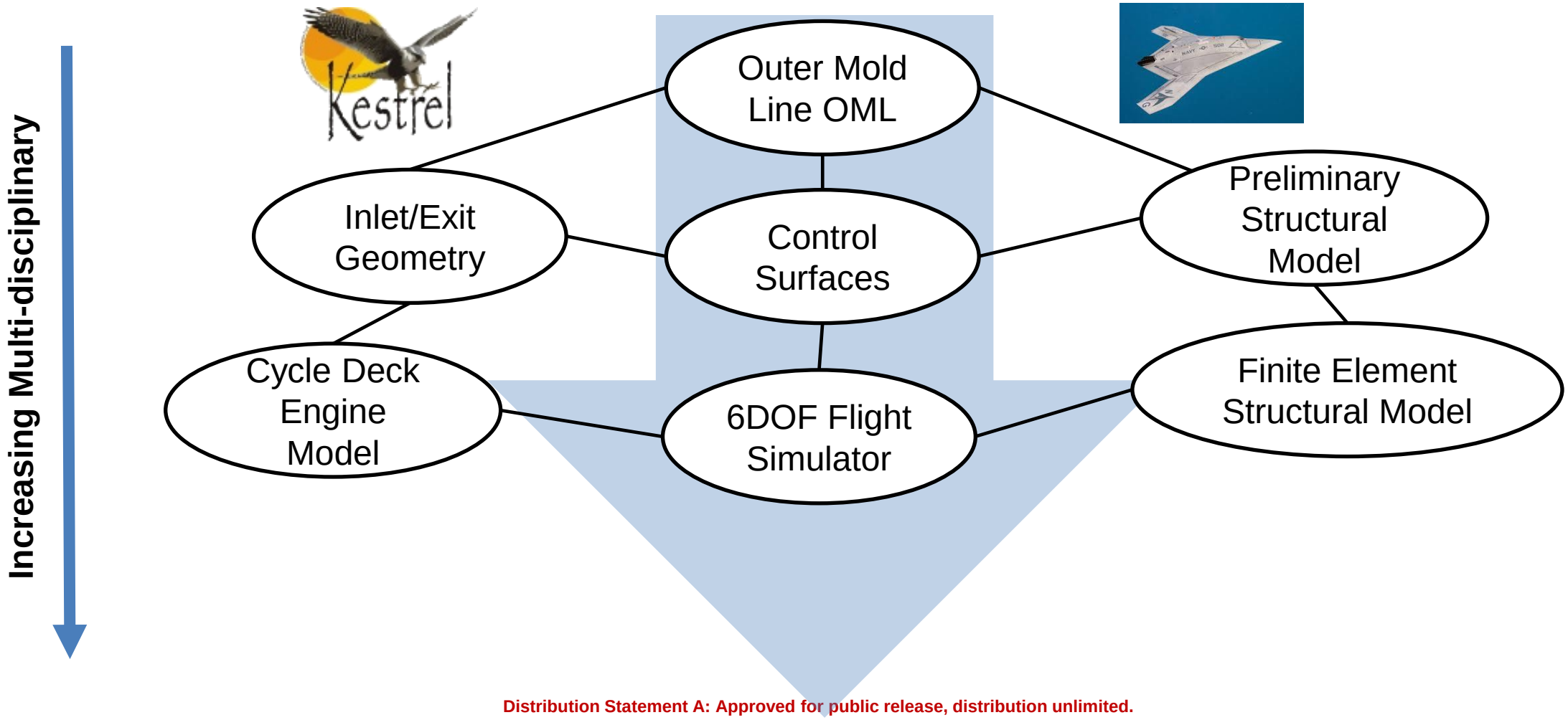
- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



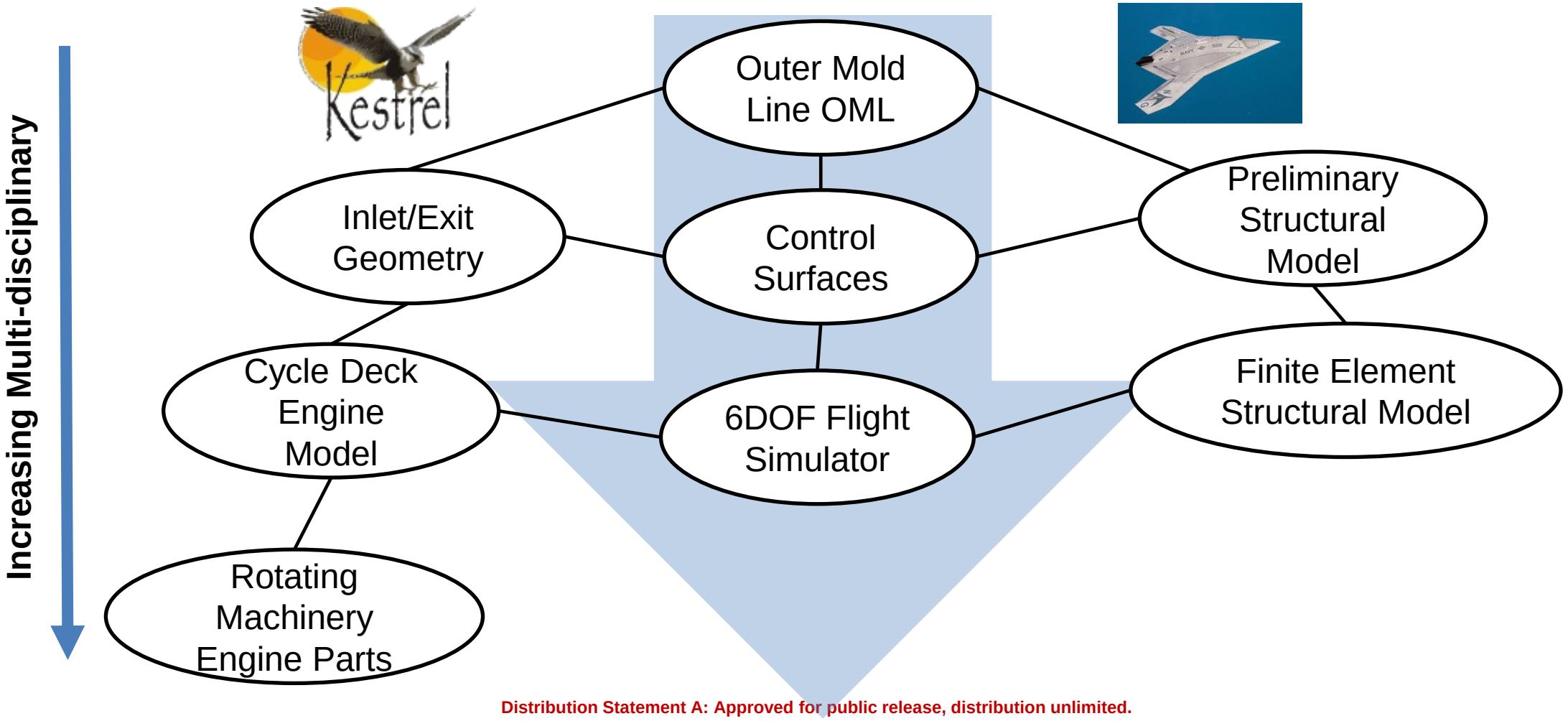
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



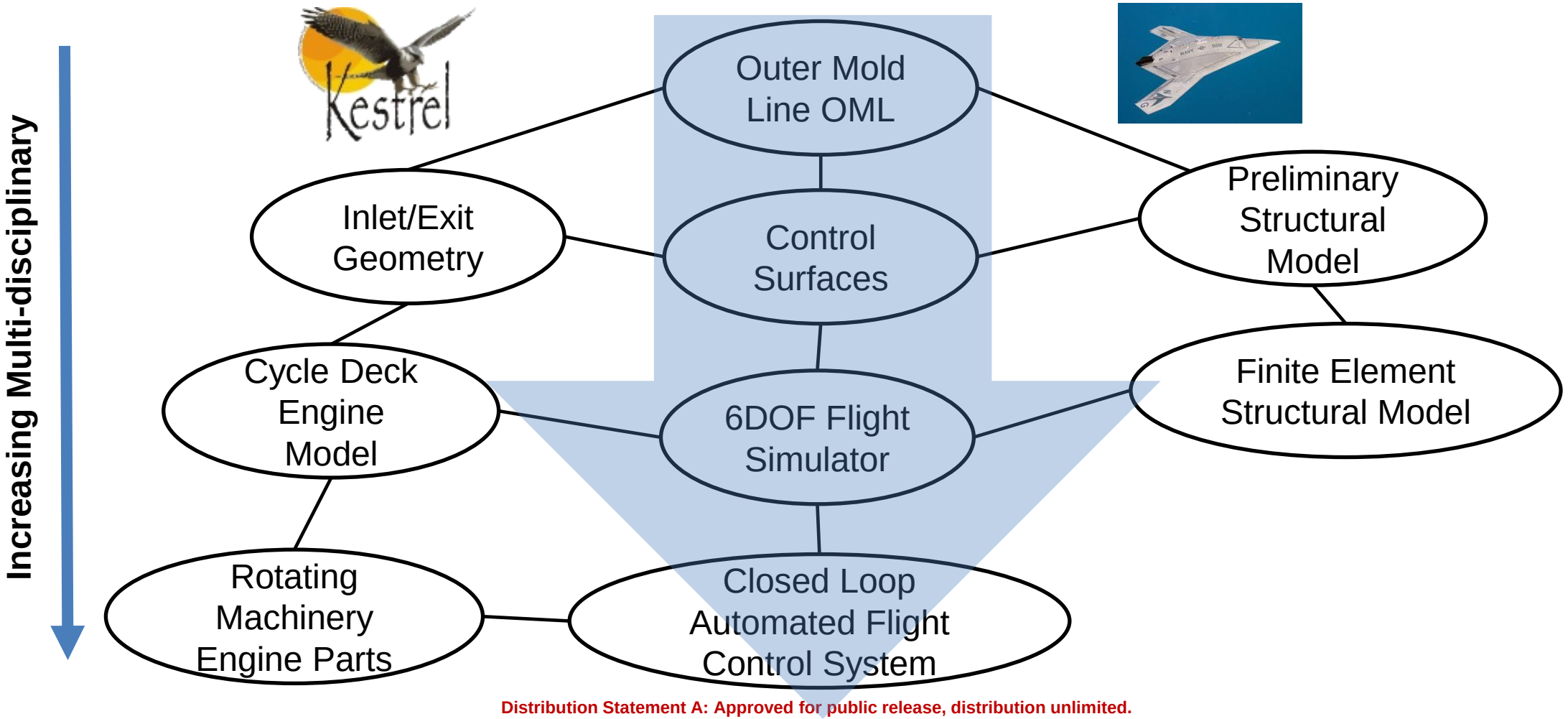
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



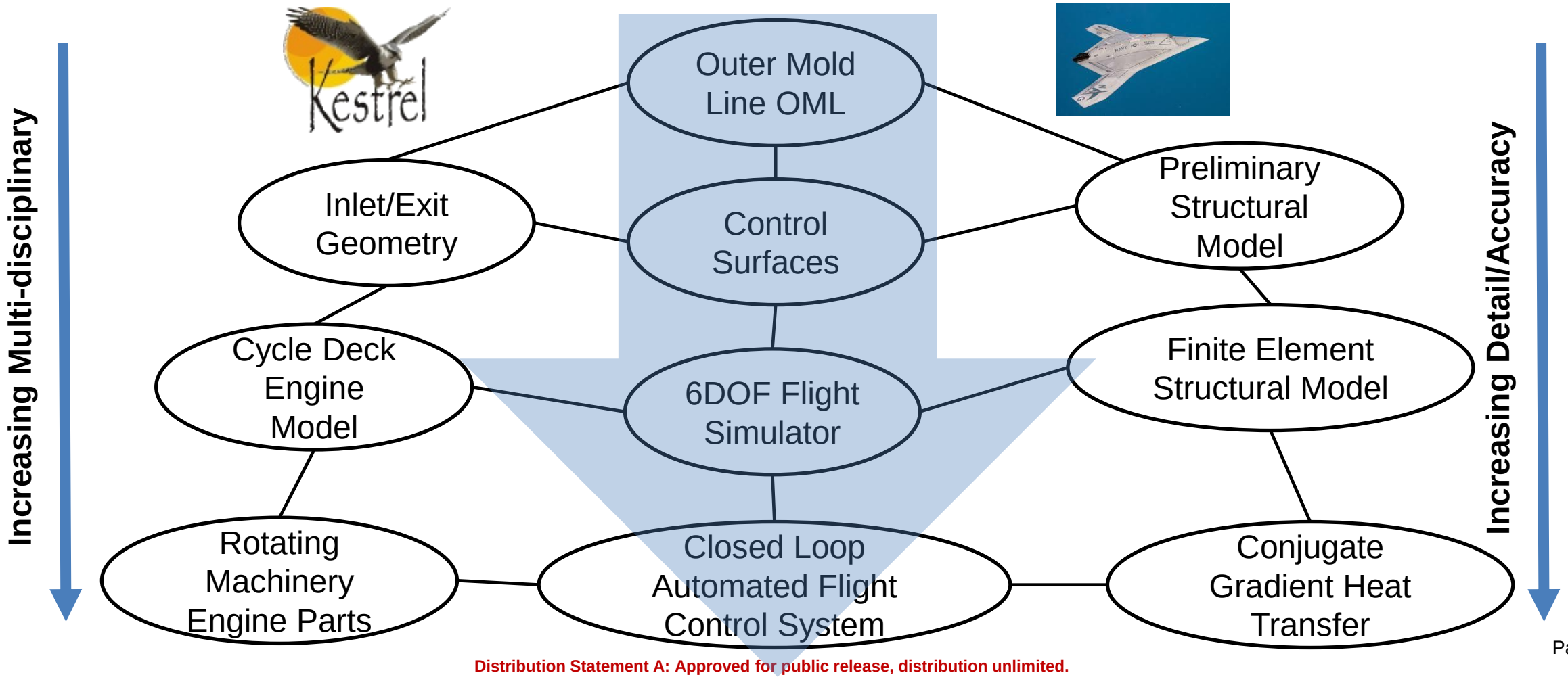
Distribution Statement A: Approved for public release, distribution unlimited.

Physics Based Analytics

PBA
Physics Based Analytics

DOD HPC MODERNIZATION PROGRAM

- **During the design process we can eliminate poor design choices by increasing the fidelity of the PBAs as more information is known (objects and connection notional)**



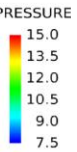
Distribution Statement A: Approved for public release, distribution unlimited.

Reduced-Order Modeling

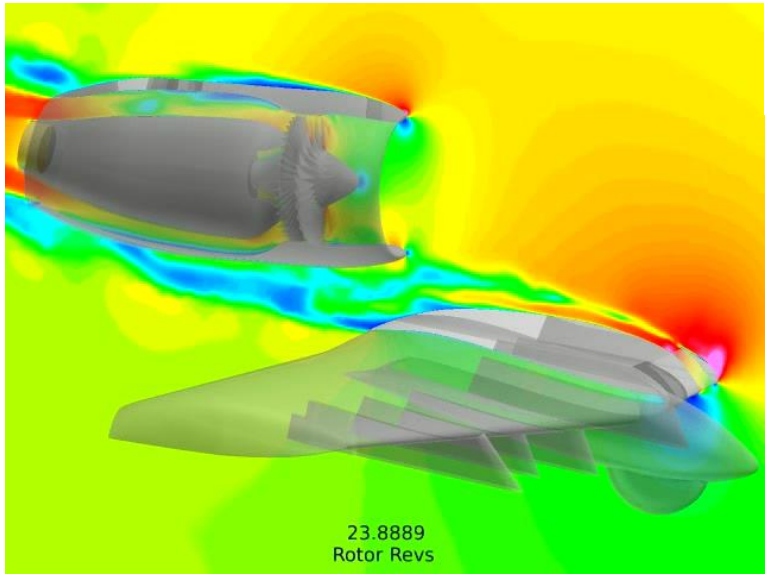
PBA
Physics Based Analytics

DS
Digital Surrogates









CFD

Flight Direction

ROM



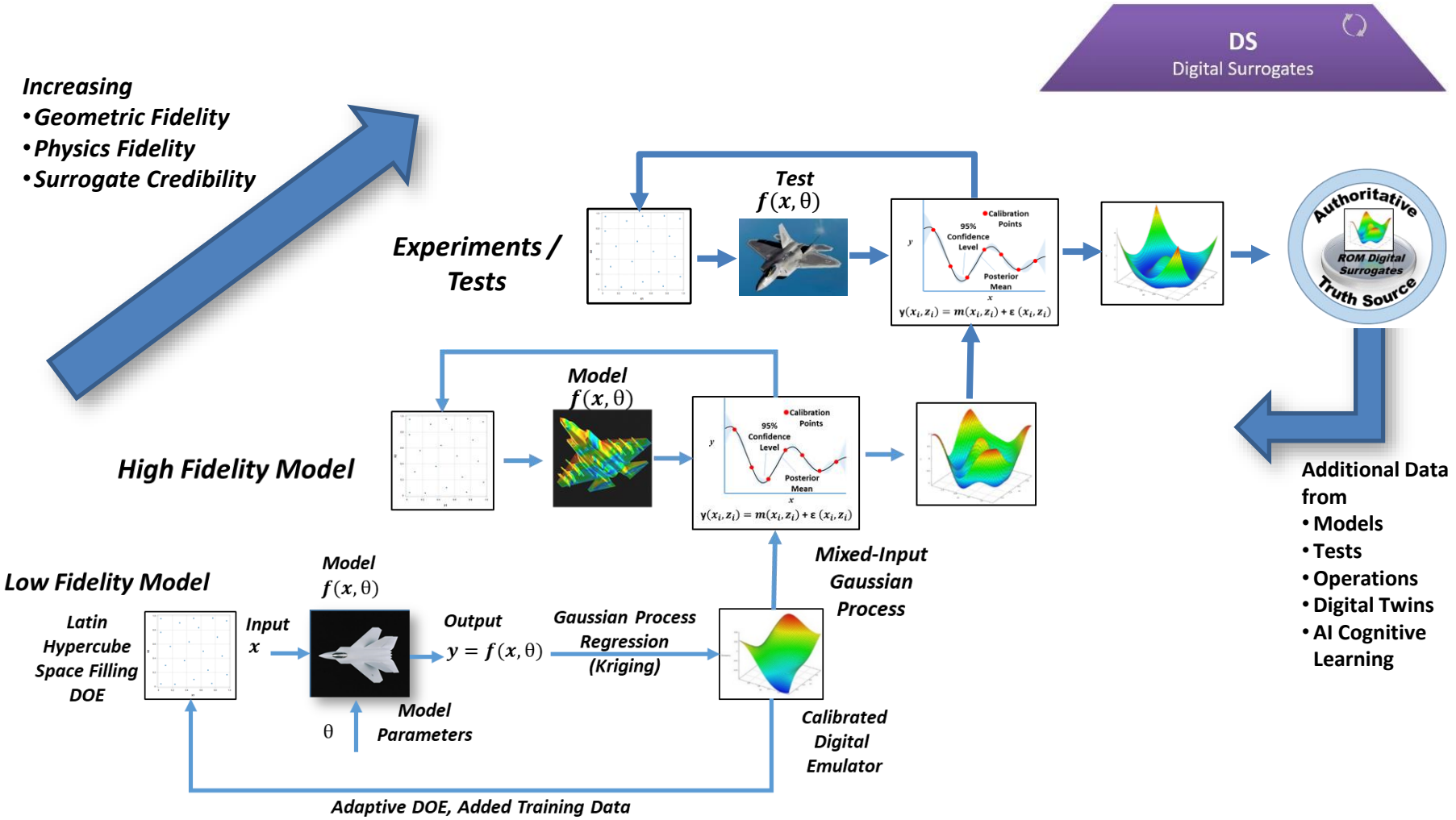


Mach = 0.800
Time = 0.000 s. c_P



Distribution Statement A: Approved for public release, distribution unlimited.

Example of Developing an Authoritative Digital Surrogate Reduced Order Model for Aerodynamics



Edward M. Kraft, "Development and Application of a Digital Thread / Digital Twin Aerodynamic Performance Authoritative Truth Source," AIAA-2018-4003. Aviation Systems Conference, Atlanta, GA, June 25-29, 2018

Distribution Statement A: Approved for public release, distribution unlimited.

Enhanced Surrogates through Data Driven Analytics

- **Surrogates shown up to this point have been based on PBA**



Distribution Statement A: Approved for public release, distribution unlimited.

Enhanced Surrogates through Data Driven Analytics

- **Surrogates shown up to this point have been based on PBA**
- **There is also a wealth of information available (E.g. Ground test data, flight test data, fleet maintenance data)**



Distribution Statement A: Approved for public release, distribution unlimited.

Enhanced Surrogates through Data Driven Analytics

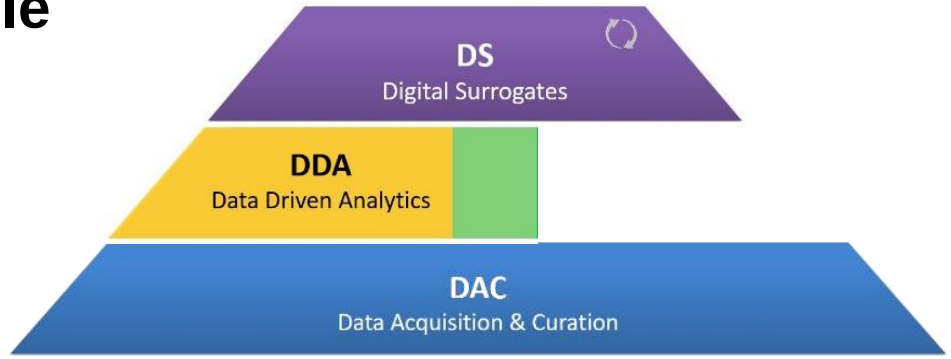
- Surrogates shown up to this point have been based on PBA
- There is also a wealth of information available (E.g. Ground test data, flight test data, fleet maintenance data)
- Data can be curated/analyzed for use in surrogate generation



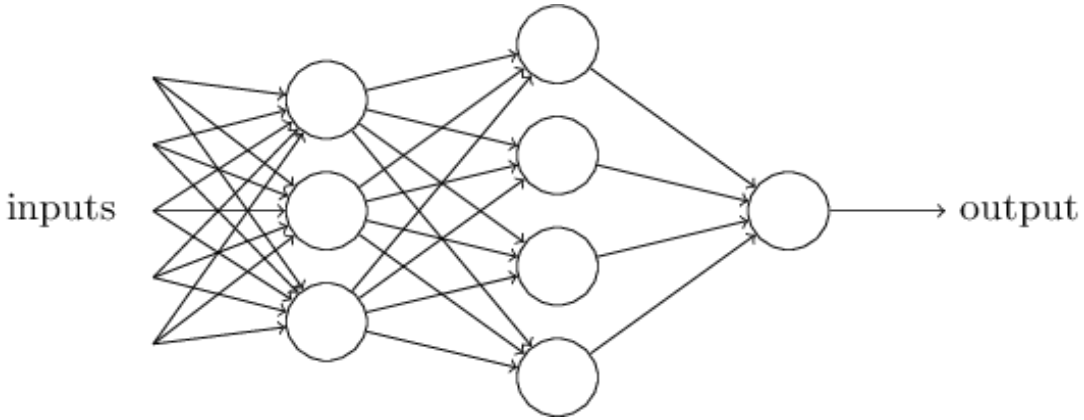
Distribution Statement A: Approved for public release, distribution unlimited.

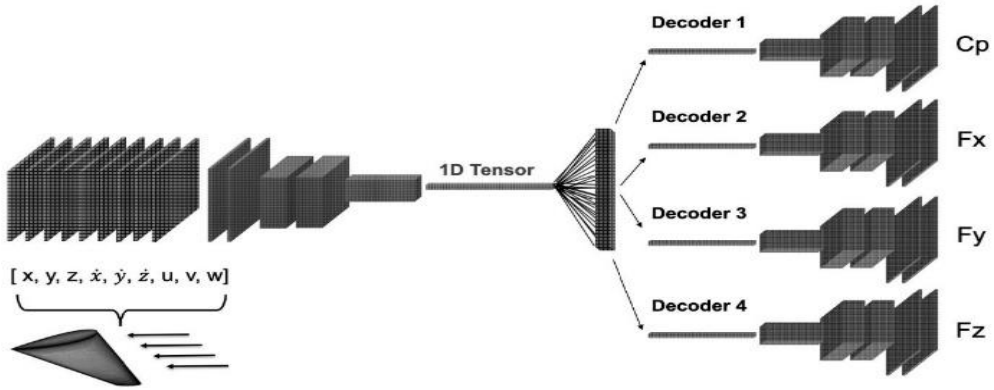
Enhanced Surrogates through Data Driven Analytics

- Surrogates shown up to this point have been based on PBA
- There is also a wealth of information available (E.g. Ground test data, flight test data, fleet maintenance data)
- Data can be curated/analyzed for use in surrogate generation



- Machine Learning/Deep Learning (ML/DL) can be used to create surrogates (requires a significant amount of data)

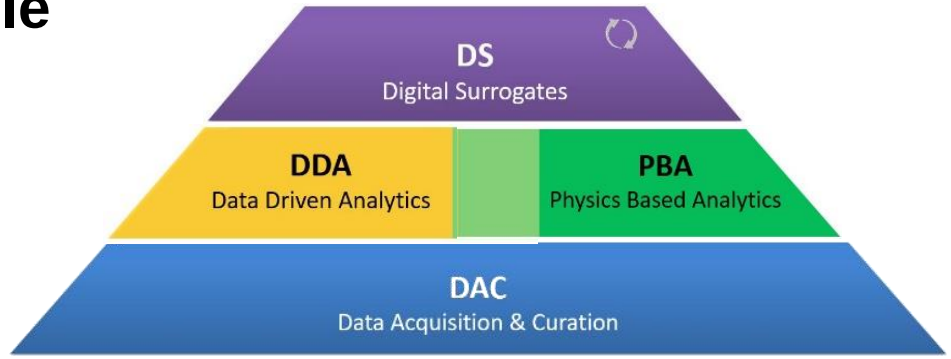




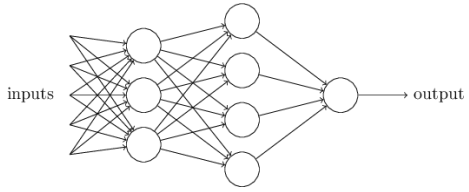
Distribution Statement A: Approved for public release, distribution unlimited.

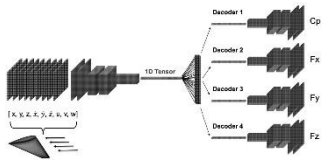
Enhanced Surrogates through Data Driven Analytics

- Surrogates shown up to this point have been based on PBA
- There is also a wealth of information available (E.g. Ground test data, flight test data, fleet maintenance data)
- Data can be curated/analyzed for use in surrogate generation



- Machine Learning/Deep Learning (ML/DL) can be used to create surrogates (requires a significant amount of data)
- The most powerful surrogates are “constrained” by the physics to create a combined DDA/PBA surrogate that accounts for the un-modeled physics/tail number specifics





Kestrel

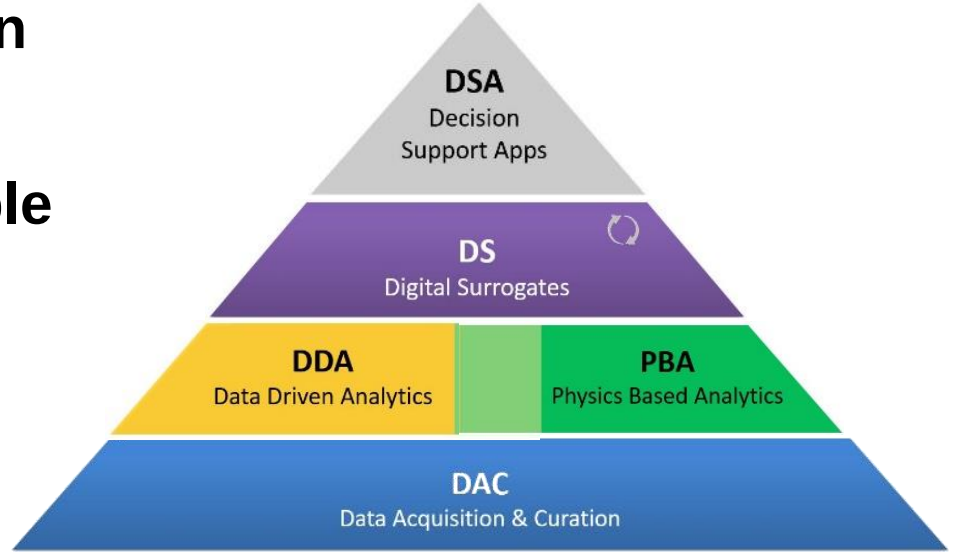
Helios

SENTRi

Distribution Statement A: Approved for public release, distribution unlimited.

Enhanced Surrogates through Data Driven Analytics

- Surrogates shown up to this point have been based on PBA
- There is also a wealth of information available (E.g. Ground test data, flight test data, fleet maintenance data)
- Data can be curated/analyzed for use in surrogate generation



- Machine Learning/Deep Learning (ML/DL) can be used to create surrogates (requires a significant amount of data)
- The most powerful surrogates are “constrained” by the physics to create a combined DDA/PBA surrogate that accounts for the un-modeled physics/tail number specifics
- Decision Support Apps can be built on this foundation of DDA/PBA – Mission Analysis, Structural Failure Analysis, etc.

Distribution Statement A: Approved for public release, distribution unlimited.

Concluding Remarks and Discussion

- The Physics Based Digital Engineering (PBDE) vision, such as described here, is the inevitable progression of technology (viz., high performance computing, physics, data analytics, and software engineering)
- The union of Machine Learning and Digital Surrogate Training via Physics-Based virtual test is what will deliver decision support data at the speed of relevance
- Machine Learning and Physics-Based virtual test both require HPC resources that can be reliably delivered by the HPC Modernization Program
- This PBDE vision can be applied to next generation combat air vehicle development through its Life-Cycle and specific examples have been shown
- Decision Support App software based on physics and system data can be pushed UP the leadership chain to aid in fast, accurate, decision making with high impact

Distribution Statement A: Approved for public release, distribution unlimited.

Acknowledgements

- Material presented in this presentation is a product of the CREATE-AV element of the Computational Research and Engineering for Acquisition Tools and Environments (CREATE) Program sponsored by the U.S. Department of Defense HPC Modernization Program Office
- ***Huge*** thanks to Dr. Robert Meakin, Dr. Saikat Dey, the CREATE-AV Development Team, the CREATE-AV Quality Assurance Team and all of our collaborators for their contributions to this presentation
- Thanks to the CREATE Management Team, the 96th Test Wing RNCS/RNCE, and AEDC for their financial management and facility support and the DoD HPCMP DSRC's for their computational resource support

Distribution Statement A: Approved for public release, distribution unlimited.

Questions?

Distribution Statement A: Approved for public release, distribution unlimited.

Lessons Learned in the Creation of a Digital Thread

Steven H. Dam, Ph.D., ESEP
President, SPEC Innovations
571-485-7805
steven.dam@specinnovations.com

Public Release Approved

Presentation Overview

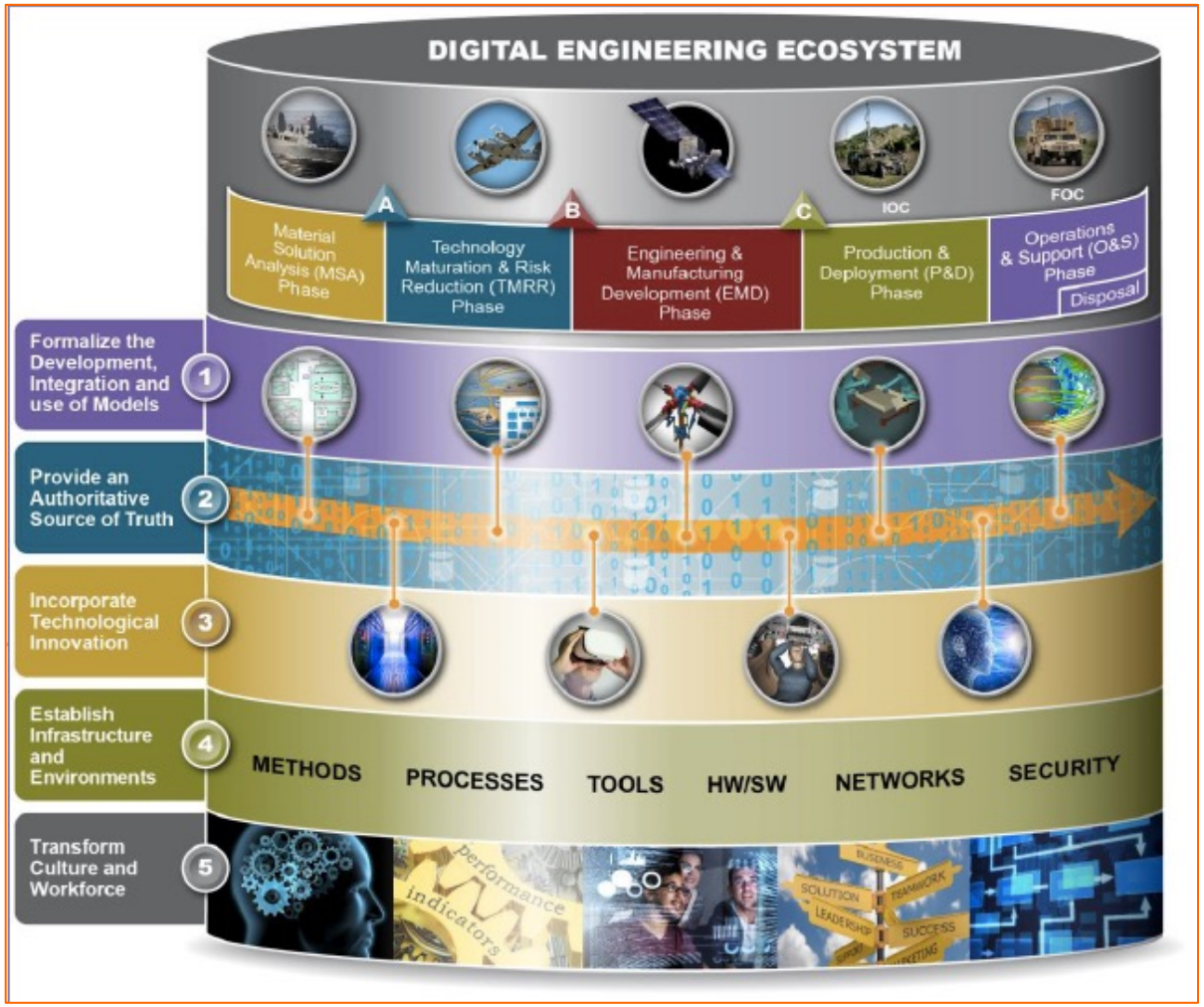
- Key Elements of the Digital Thread
- Research Conducted in Tool Integration and Model Curation
- Resulting Digital Engineering Development Environment
- Application: NASA “Break the Ice” Challenge
- Key Lessons Learned

Key Elements of the Digital Thread

What is the "Digital Thread?"

- Defined in the DoD's Digital Engineering Strategy
- Objectives:
  - Deliver high payoff solutions to the warfighter at the "speed of relevance"
  - Reform business practices
    - Digital enterprise connects people, processes, data, and capabilities
    - Improves technical, contract, and business practices through an authoritative source of truth and digital artifacts

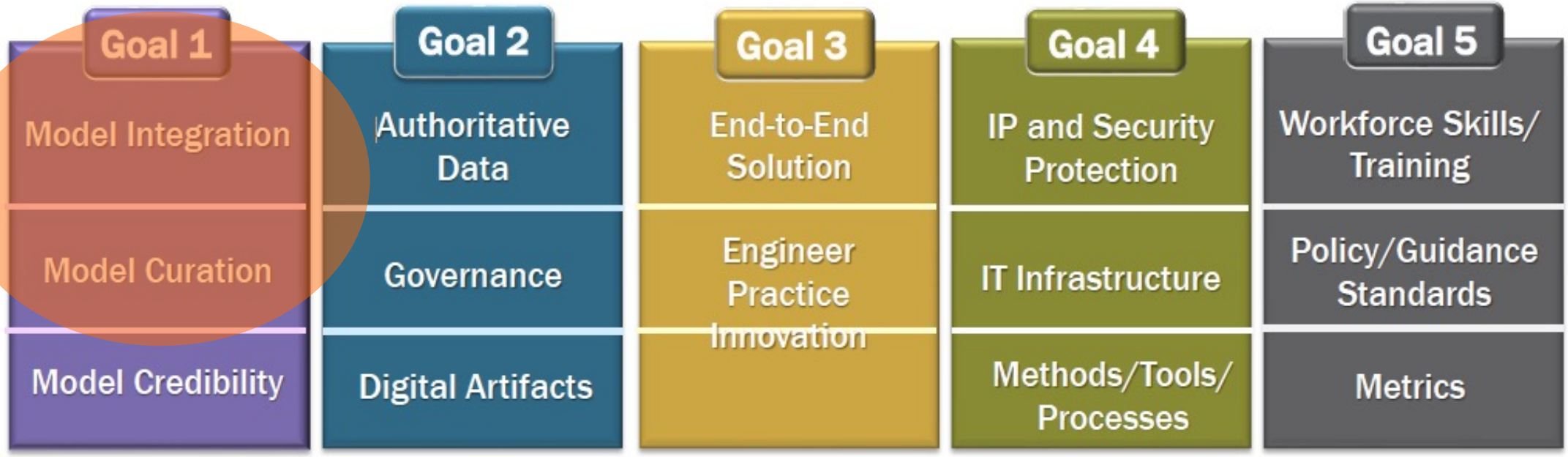
From NDIA Presentation by Philomena Zimmerman. October 24, 2018



Combines model-based techniques, digital practices, and computing infrastructure.

Why Do We Want to Integrate Tools?

- Model integration and Model Curation are key goals of the Digital Engineering
- Tool interoperability has been a historic problem



But is it model integration we need or data interoperability?

Research Conducted in Tool Integration and Model Curation

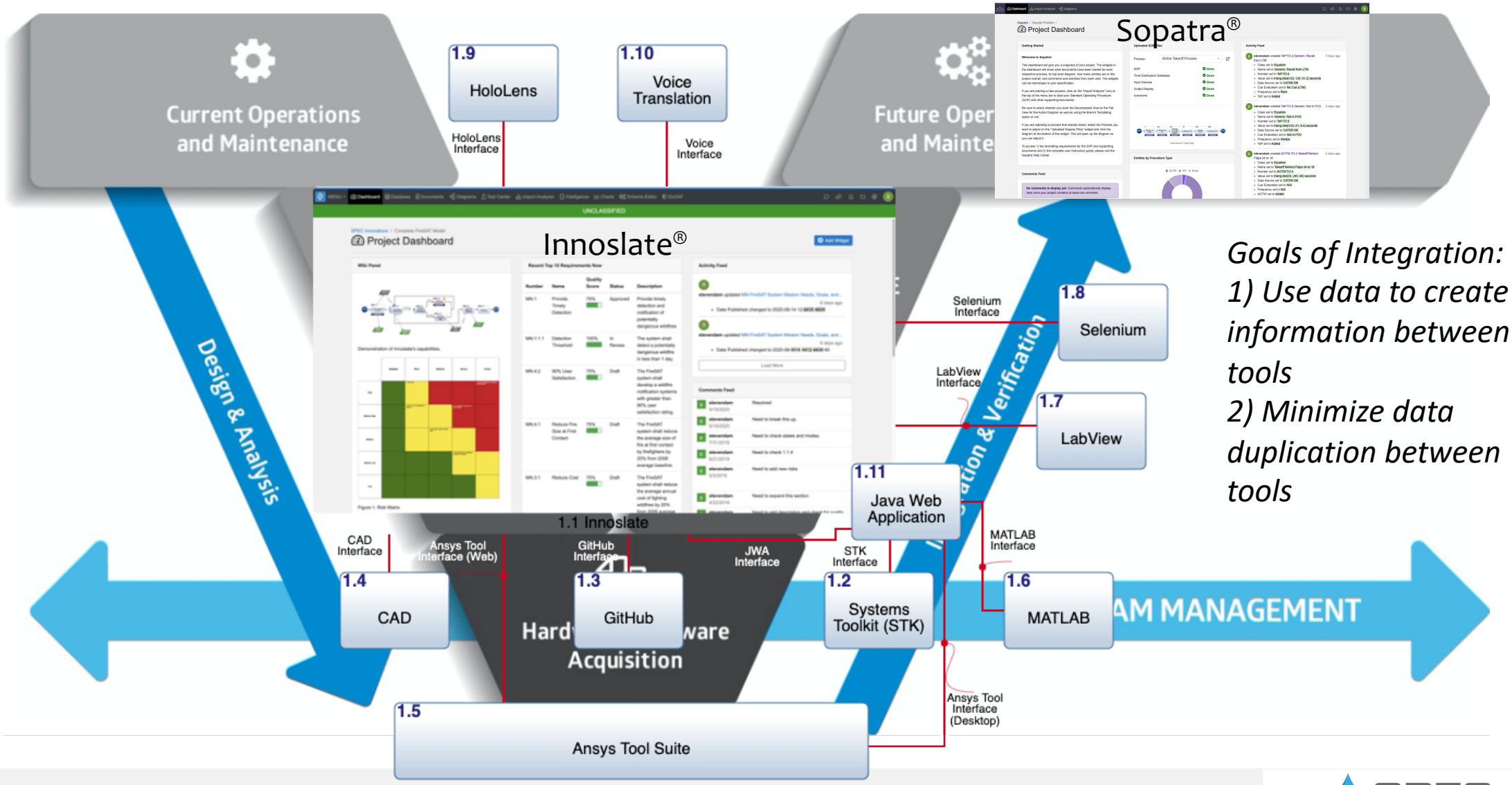
Research Performed

- Extensive research into was performed for the last two years in:
  - Use of APIs and Java Web Applications for interface with other tools
  - Advanced NLP technologies for automated diagram generation from natural language
  - Program and Portfolio Management
  - CAD integration and visualization
  - Code requirements and visualization
  - Software repository integration (GitHub, Jira, and GitLab)
  - Automated software (and hardware) testing and design of experiments
  - Mixed Reality technologies
- Much of this research has already been productized in Innoslate® and Sopatra®
- More is planned for near future releases

Resulting Digital Engineering Development Environment

BLUF: A well integrated system that moves appropriate data between tools

We Have the Future Digital Engineering Environment Today

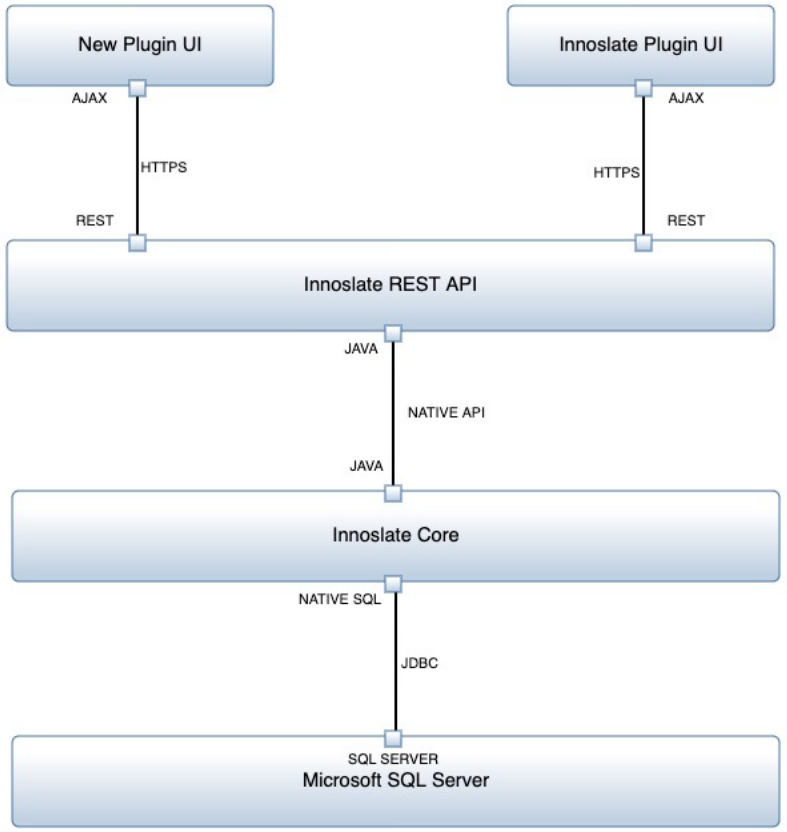


Goals of Integration:
1) Use data to create information between tools
2) Minimize data duplication between tools

Integration Enabled Using Innoslate®'s MOSA Architecture

- Plugins are viewpoints of the Innoslate database
- Plugin features
  - Not a standalone application (requires Innoslate Core)
  - All authentication is through Innoslate Core with the options for:
    - Single-Sign-On CAC (Default)
    - Native Email/Password (Optional)
    - LDAP (Optional)
  - All data is stored in the U.S. Government managed MSSQL database using Innoslate Core (***no data lock***)
  - Innoslate REST API facilitates plugin data exchange

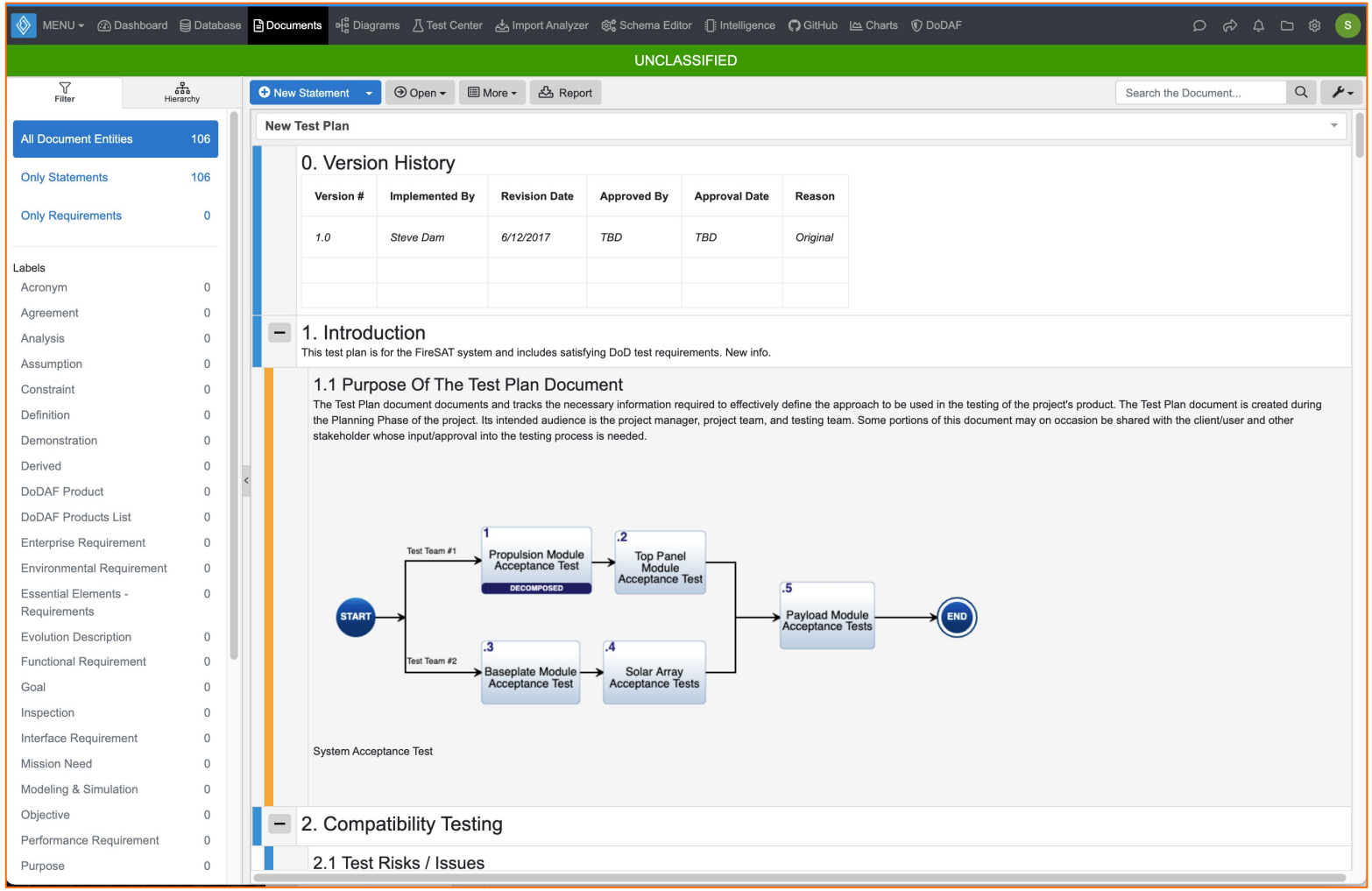
Note: SPEC Innovations' instance on GovCloud uses the PostgreSQL Server instead.



Modular Open Systems Approach (MOSA) Architecture Enables Architecture to Operations (DEVOPS)

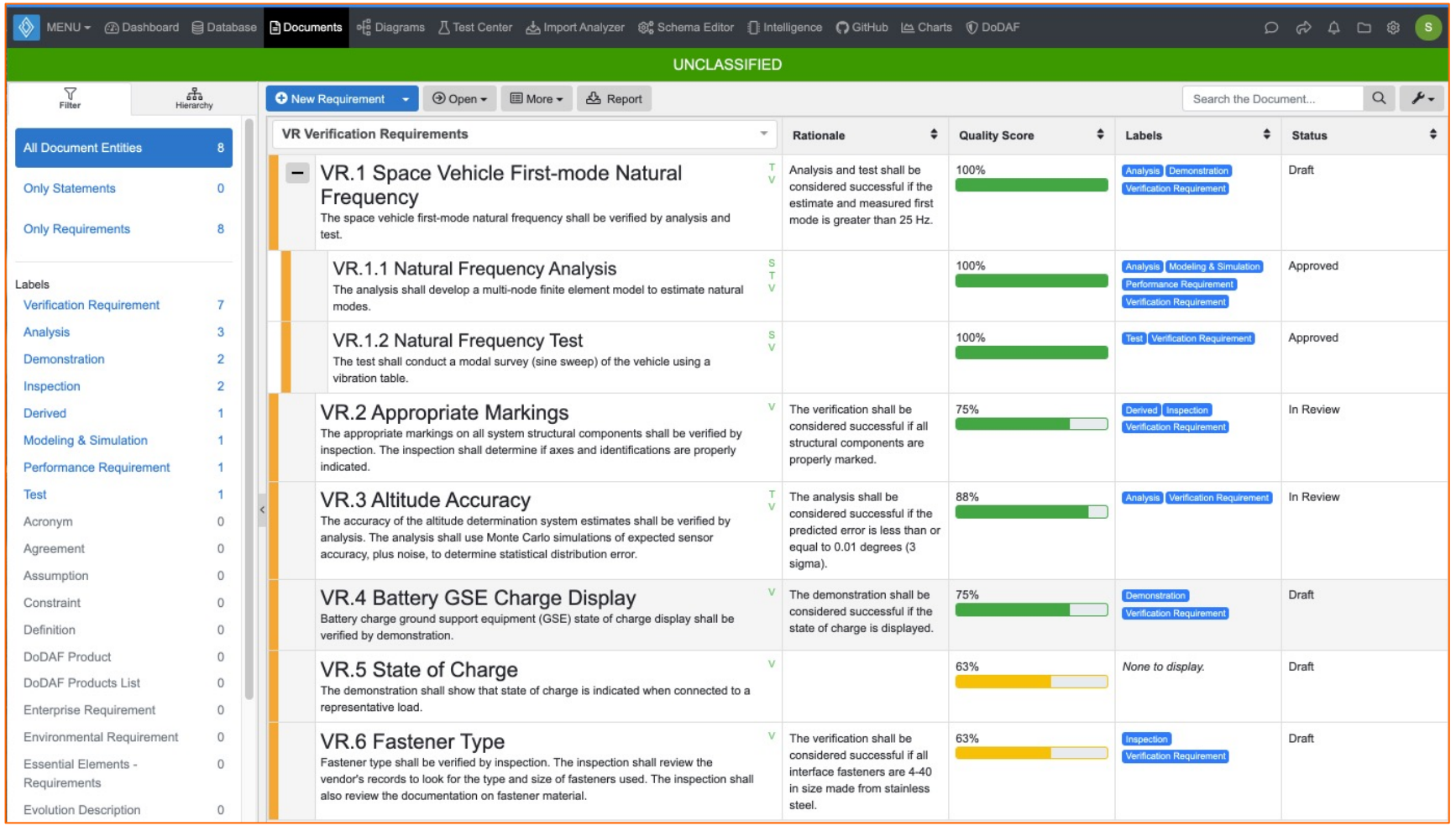
Documents View

- Innoslate enable you to capture and develop your documentation
- It provides the means to capture pictures, create table, use diagrams and charts from Innoslate, and create live tables
- You can develop your own custom template or pick from a number of built-in templates
- You can use these to perform model-based reviews
- The Benefit: show users and customers information in a simple form they can easily understand, yet be reusable and traceable to other parts of the design



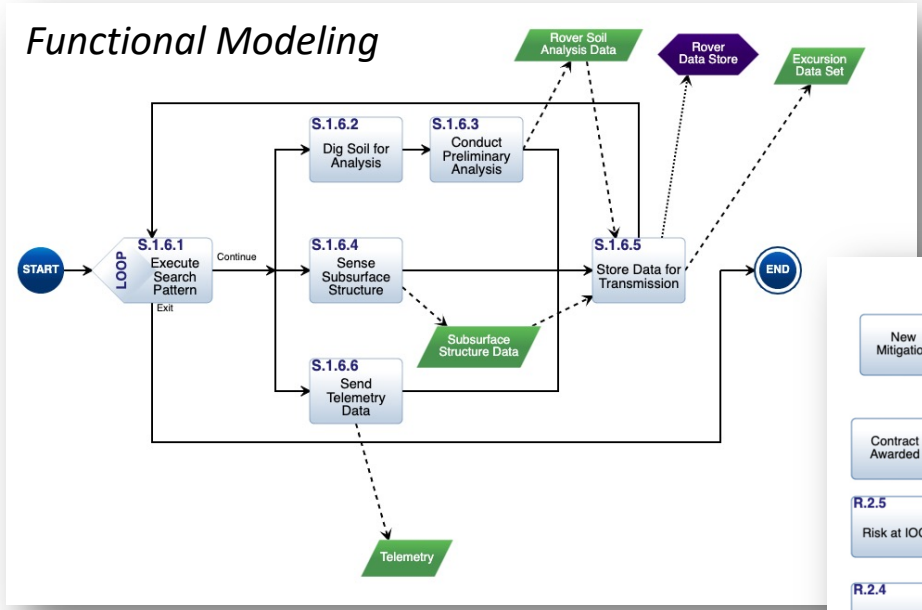
Requirements View

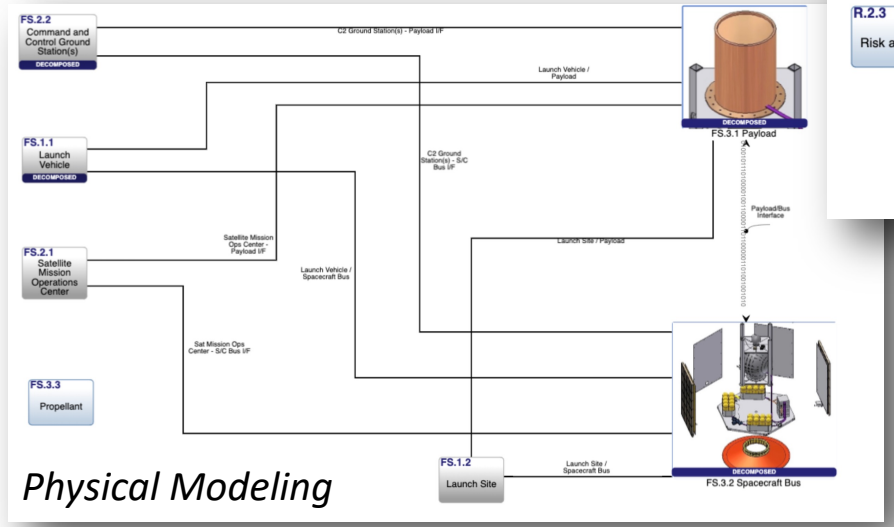
- A special type of document that includes by default, the rationale field, quality score and quality checker
- Can also see indicators for key traceability relationships
- Has all the benefits of any document in Documents View, including baselining, formatting, acronym extraction, find & replace, etc.
- Uses workflow to manage requirements
- Use labels for sorting and identifying verification methods
- The Benefit: A digital document for your living requirements

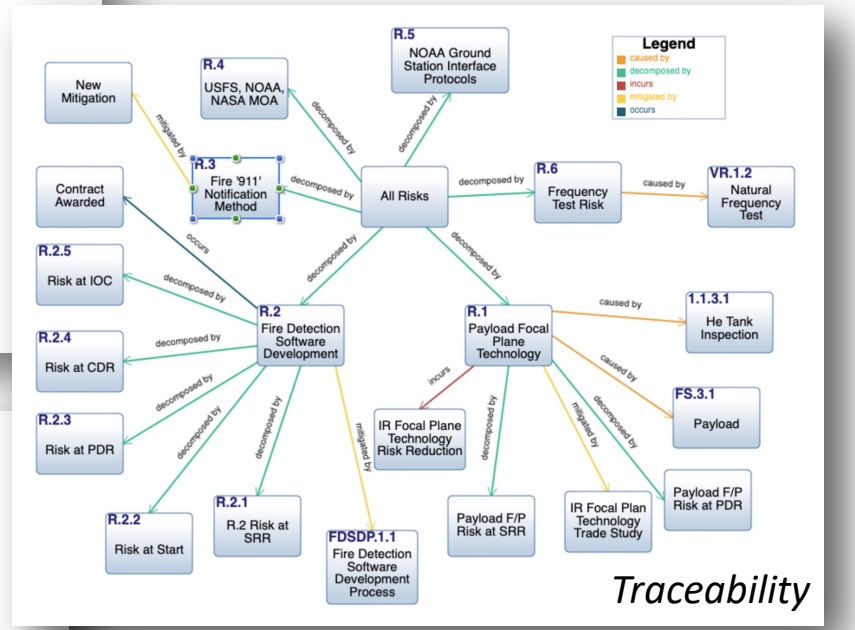


Modeling

- Create high level to detailed models of functional and physical elements of the design
- Functional model (Action Diagram) provides means to allocate decision points and use Resources explicitly
- Allocates Actions to Assets automatically (functional to physical mapping)
- View/use models in many different formats, including SysML, IDEF, etc.
- Reuse portions of models in other models, including across Innoslate projects
- The Benefit: Develop the functional requirements and physical constraints



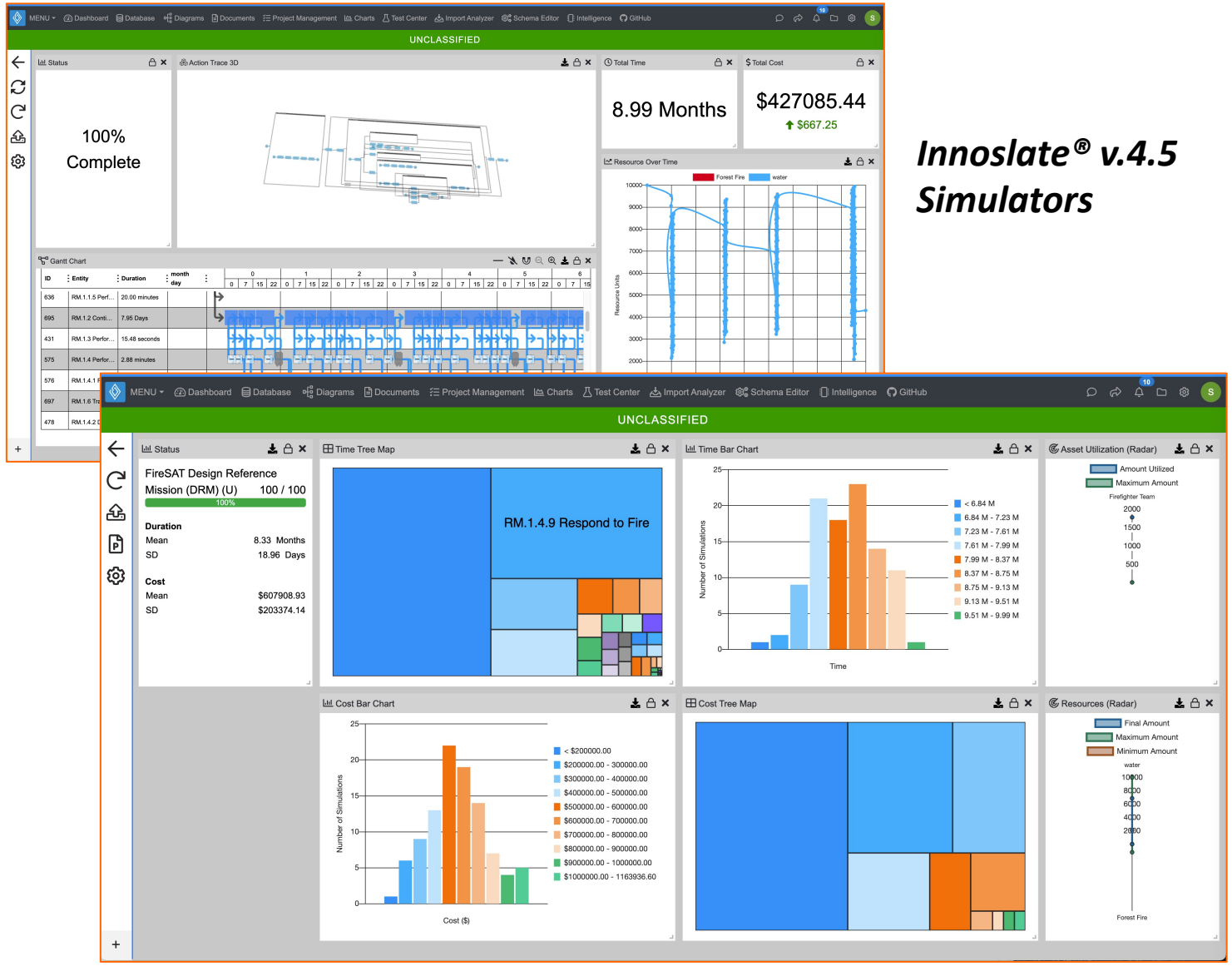




26 Diagram types, 2 Charts, and counting. All the 9 SysML diagrams.

Simulation

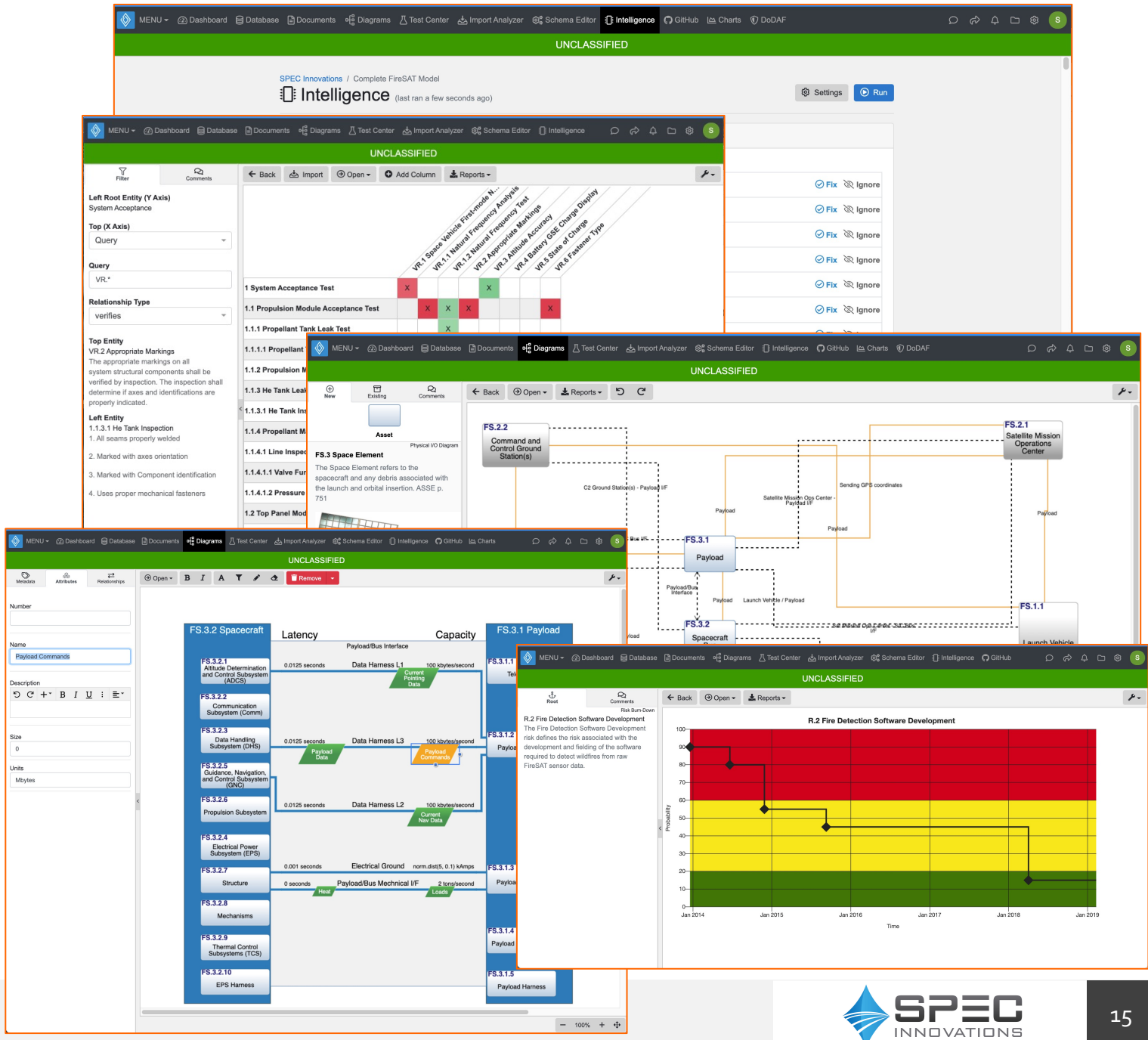
- Innoslate® provides built-in discrete event and Monte Carlo simulators
- Decision points come with pre-built scripts for probability and Resource selection, as well as iterations for loops
- JavaScript can be used to enhance the simulation execution
- Can access web resources using APIs
- Integration with MATLAB/Simulink and STK through special APIs
- Major enhancements to simulators developed in v4.5
- The Benefit: derive performance requirements for timeliness and quantity using distributions and Resources



Innoslate® v.4.5 Simulators

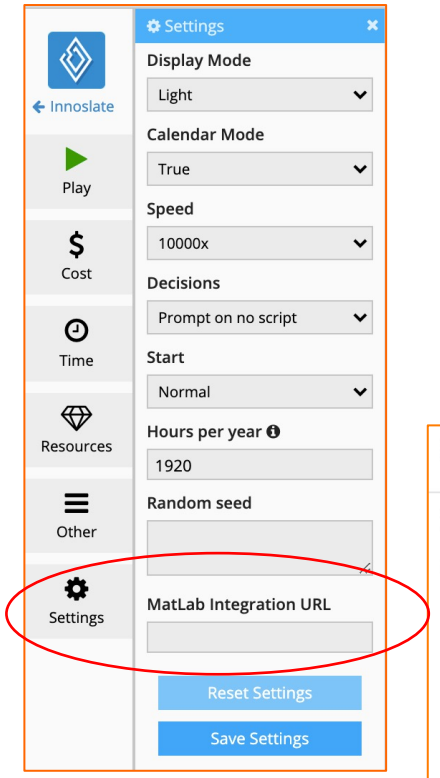
Analysis

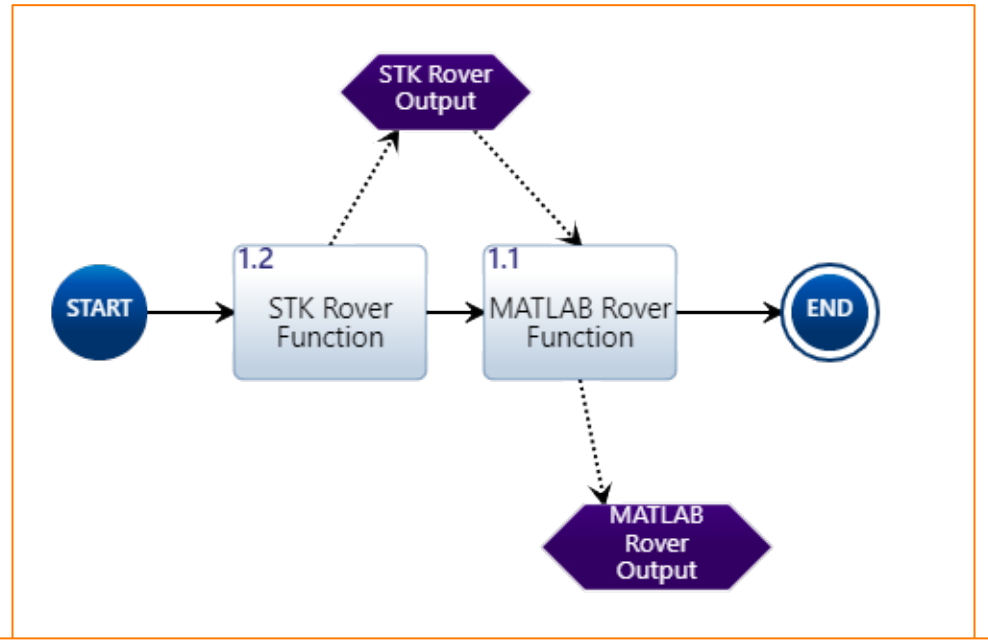
- Innoslate® supports various types of analyses:
  - Textual analysis (using Natural Language Processing (NLP) algorithms)
    - Requirements quality analysis
    - Traceability assistance
    - Modeling heuristics (Intelligence View)
  - Dynamic Analysis
    - Discrete event simulation
    - Monte Carlo simulation
  - Static Analysis
    - Attribute roll-up
    - Diagram warnings (errors, unit mismatch)
  - Risk and Cost Analysis
- Integration with other tools adds to Innoslate®'s capabilities
  - MathWorks® MATLAB/Simulink
  - Ansys/AGI Systems Tool Kit (STK)



Mathematical Analytics with MATLAB

- Use the MATLAB APIs to interoperate with MATLAB/Simulink models that perform detailed calculations
  - Simple GET and POST commands move data between Innoslate and MATLAB
- Use Setting option to show pathway to MATLAB on desktop
- The Benefit: Reuse models created in MATLAB to perform more detailed calculations





MATLAB Rover Function Script

Edit Script

Script

```
function onStart(){
  var roverInput = Sim.getResourceByName("STK Rover Output"); //Obtain Resource value for STK output
  var matlabCommand = "runRoverFunction("+roverInput+")"; //set up MATLAB Command
  matlab.post("roverOutput", matlabCommand); //Send Command to MATLAB
  var matlabRoverOutput = matlab.get("roverOutput"); //?Get output from matlab
  Sim.setResourceByName("MATLAB Rover Output", matlabRoverOutput); //Set Resource value for MATLAB

}
```

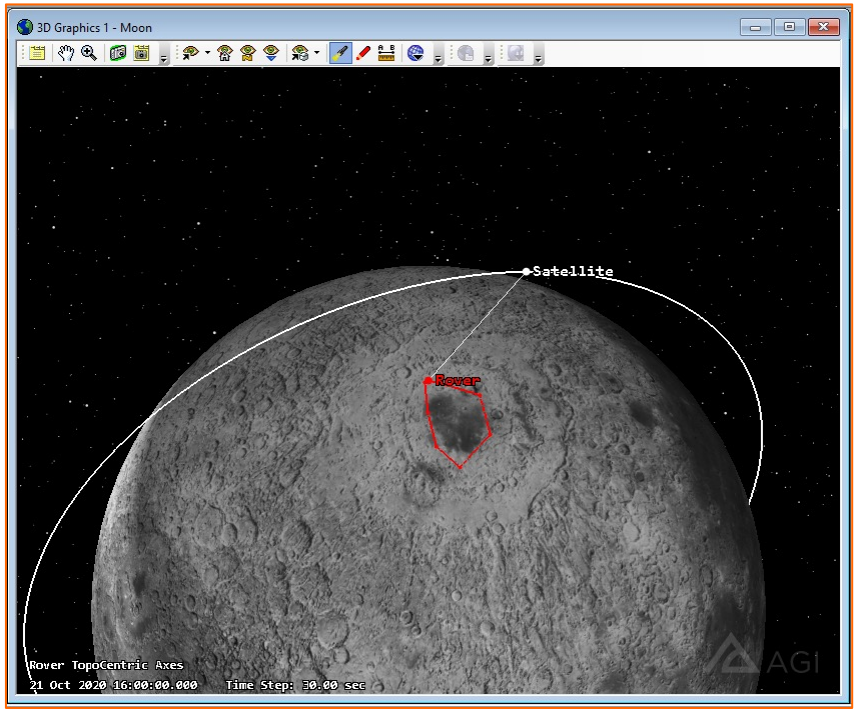
New APIs: matlab.post and matlab.get

Cancel Submit

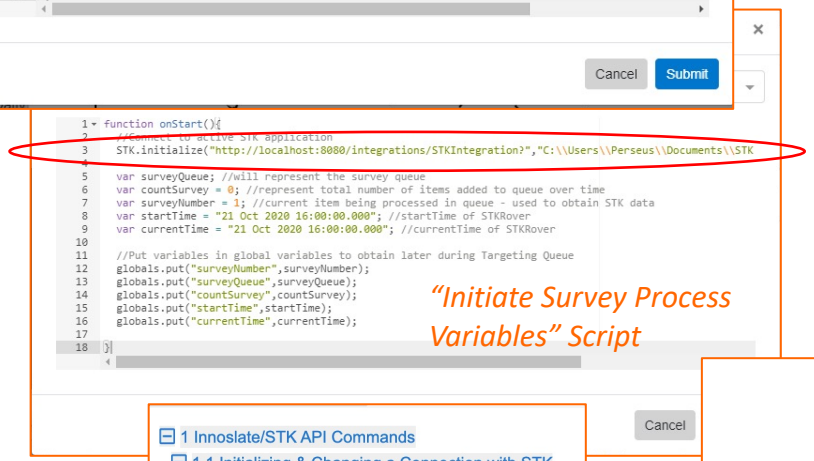
Geospatial Visualization and Analysis with STK

- Use the STK integration to visualize and take advantage of the STK analysis tools
- APIs designed to get to the critical parameters in STK
- Use the information to alter the simulation performance in co-simulation
- The Benefit: Includes geo-spatial constraints in the discrete event simulation for more realistic analyses

STK Rover Model with Search Pattern and Communications Satellite



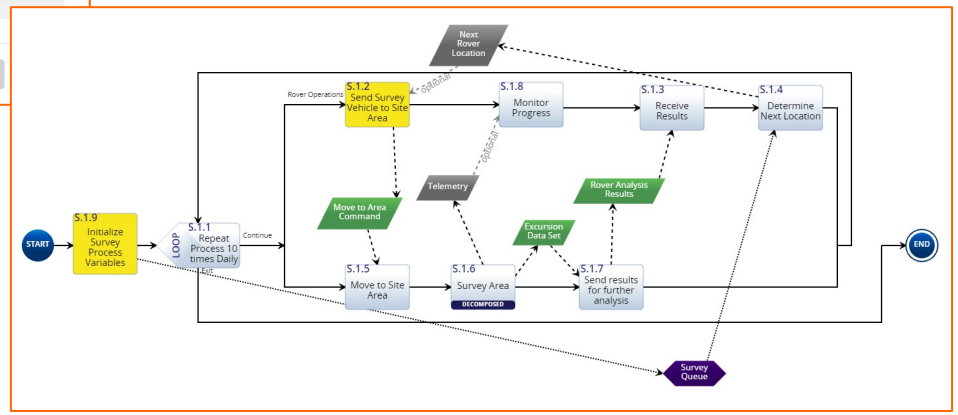




"Initiate Survey Process Variables" Script

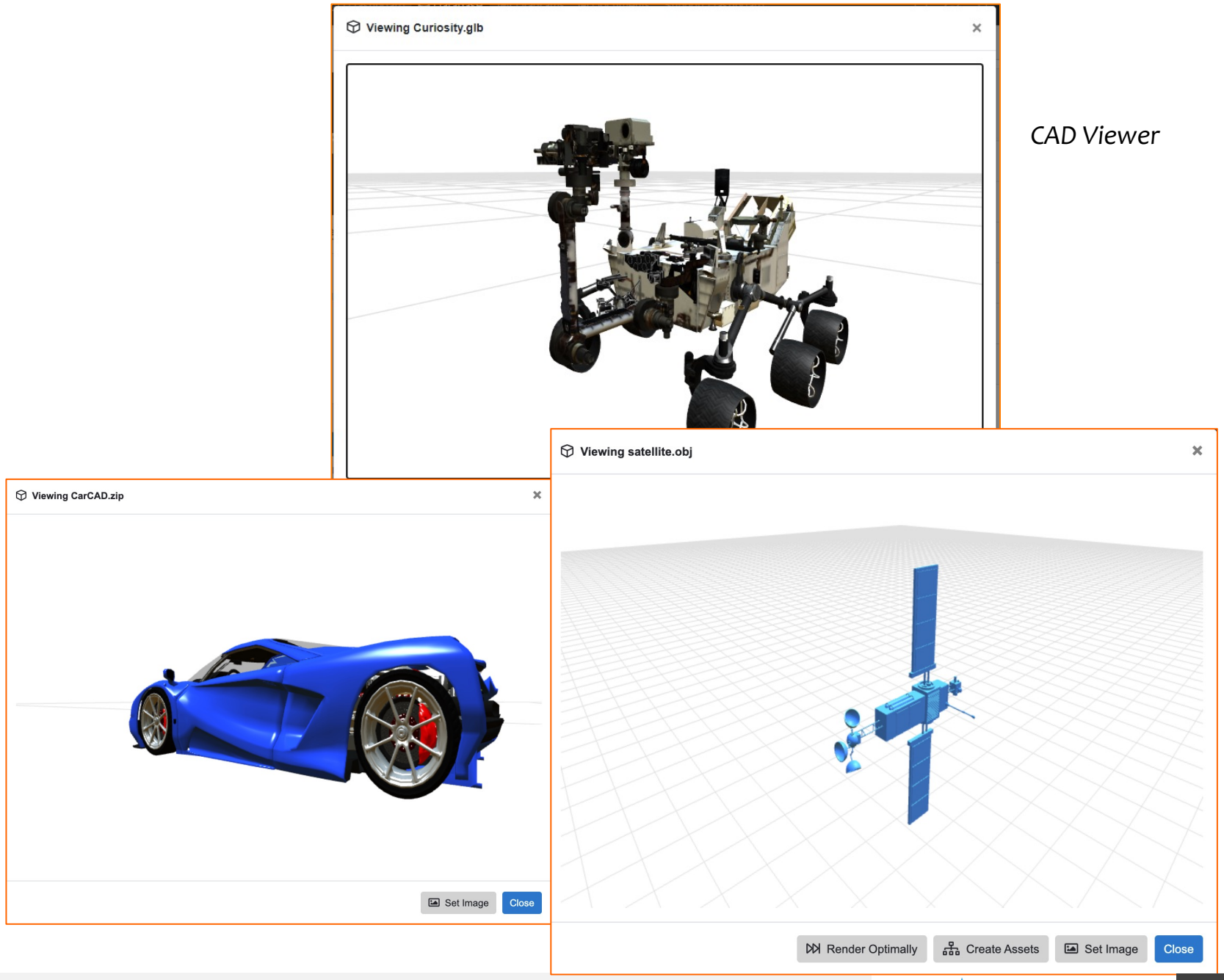


New APIs for STK



CAD/CAM

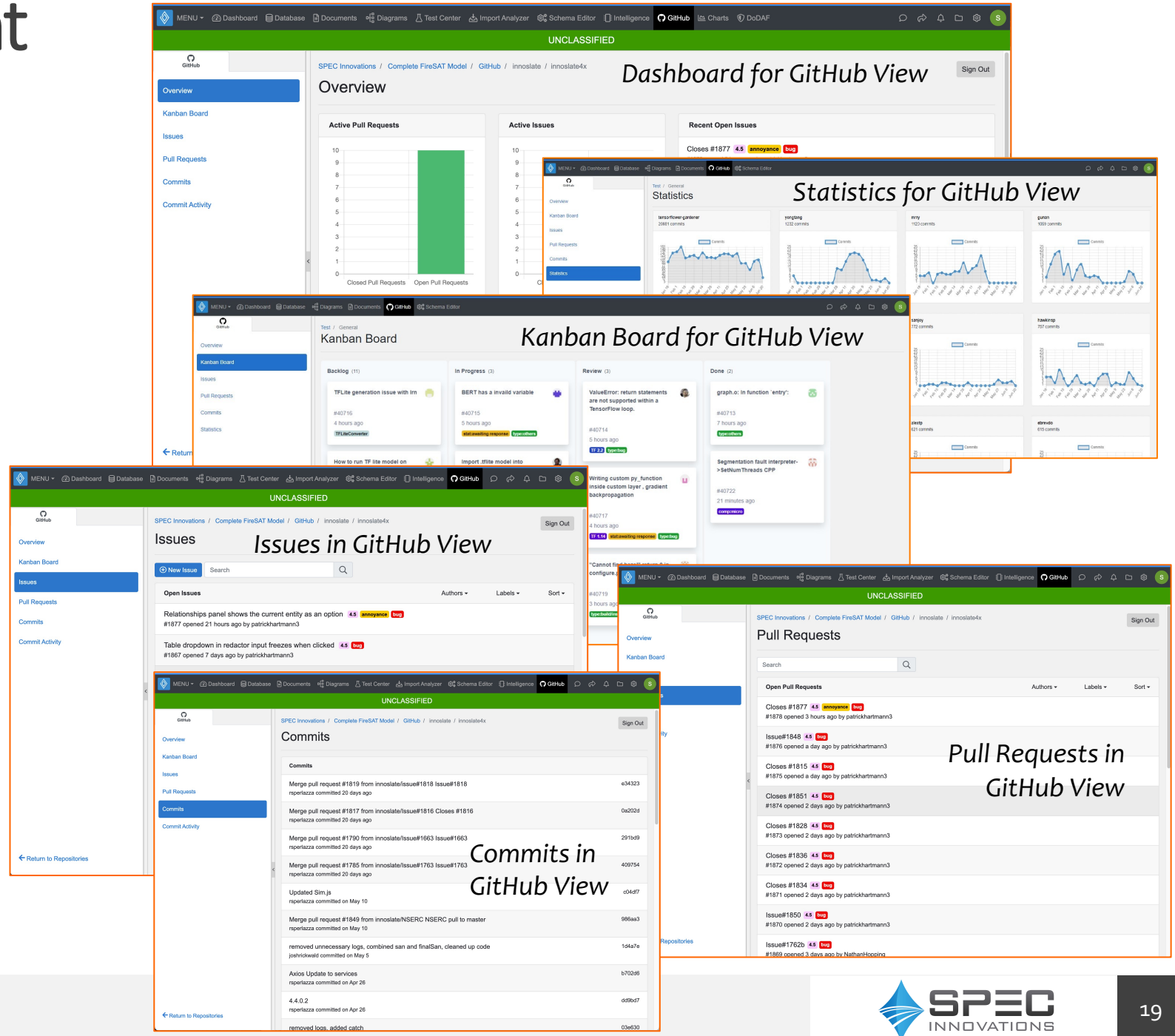
- New CAD Viewer provides capability to view CAD files and convert CAD data into Innoslate objects/BOM
- Export other information from CAD tools using CSV and import into Innoslate® for further analysis
- Added other filetypes: STL, GLB, gITF, 3DS, PLY and ZIP (with OBJ and MTL combined)
- The Benefit: Enables verification of the design and links back to requirements



CAD Viewer

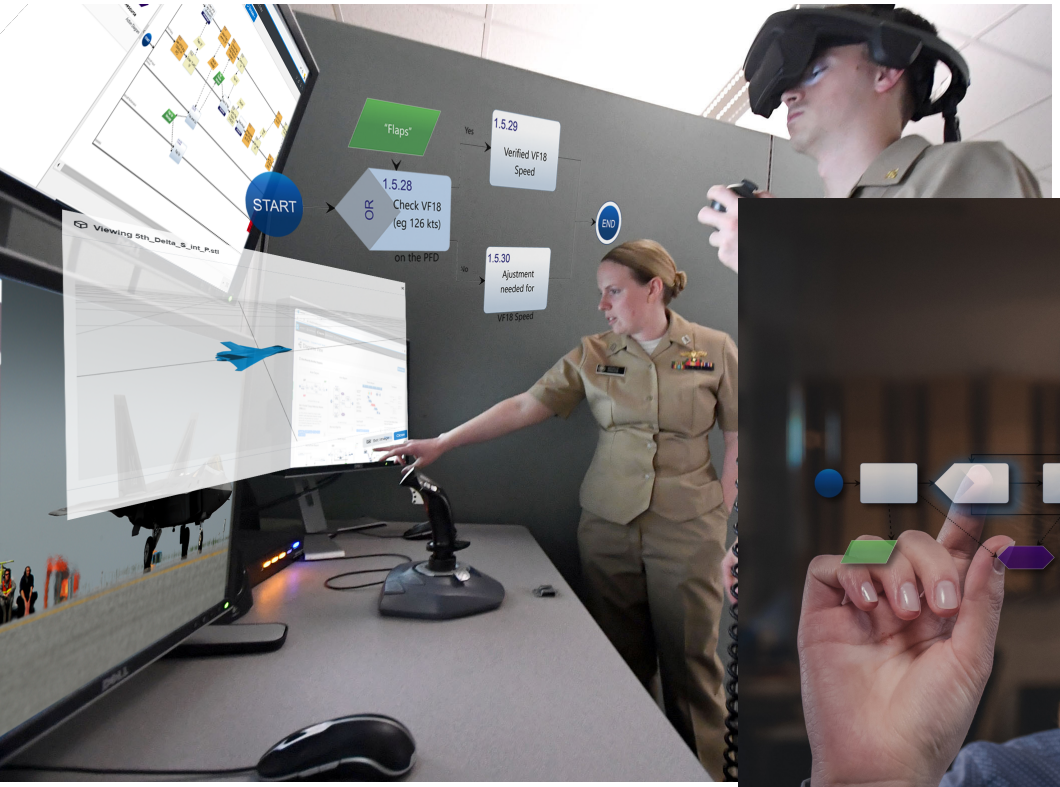
Software Development Integration

- GitHub View provides capability to directly interface with GitHub using a special set of dashboards
- Provides entire new viewpoint to enable program managers and systems engineers to more effectively monitor software development progress and capture results
- Version 4.5 included capability to create Class Diagrams from code to enhance traceability between requirements and code
- The Benefit: Capability to monitor software development progress and verify code meets requirements



AR/VR

- Innoslate is browser-based making it easy to use with AR/VR technologies such as Hololens
- Useful when field operatives need to be able to view the digital information such as standard operating procedural diagrams, test plans, or metrics
- The Benefit: Enhanced visualization of design elements during operations





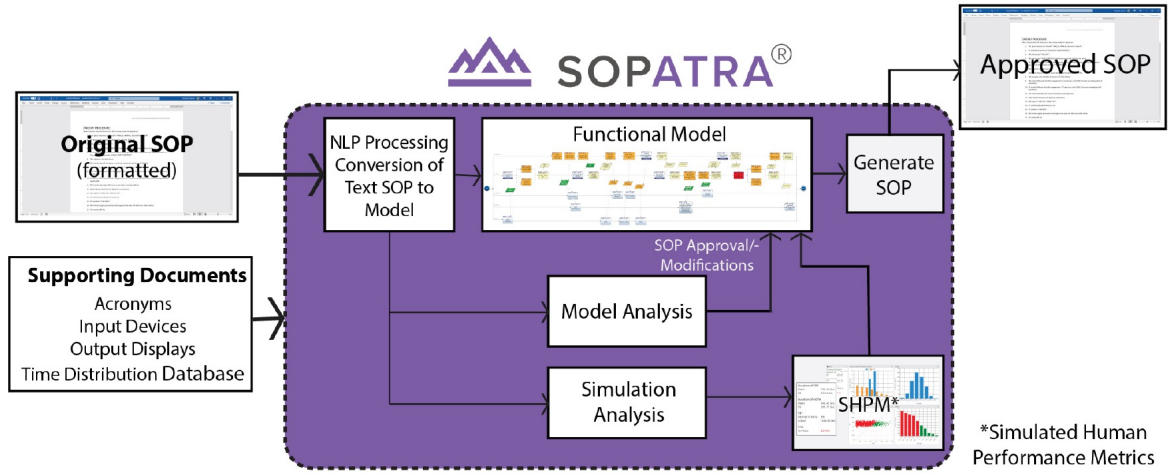


Operations Support

- Sopatra®, powered by Innoslate®
- Text to Diagram autogeneration used to transform written standard operating procedures (SOP) to Action Diagrams for analysis
- Advanced NLP algorithms developed
- Automatically adds best practice actions, such as “See and Decide”
- Special Monte Carlo Analysis of the Allowable Operational Time Window (AOTW) and Time of Procedure (ToP)
- Advanced analytics to calculate the Procedure Buffer Time (PBT)
- The Benefit: More accurate SOPs

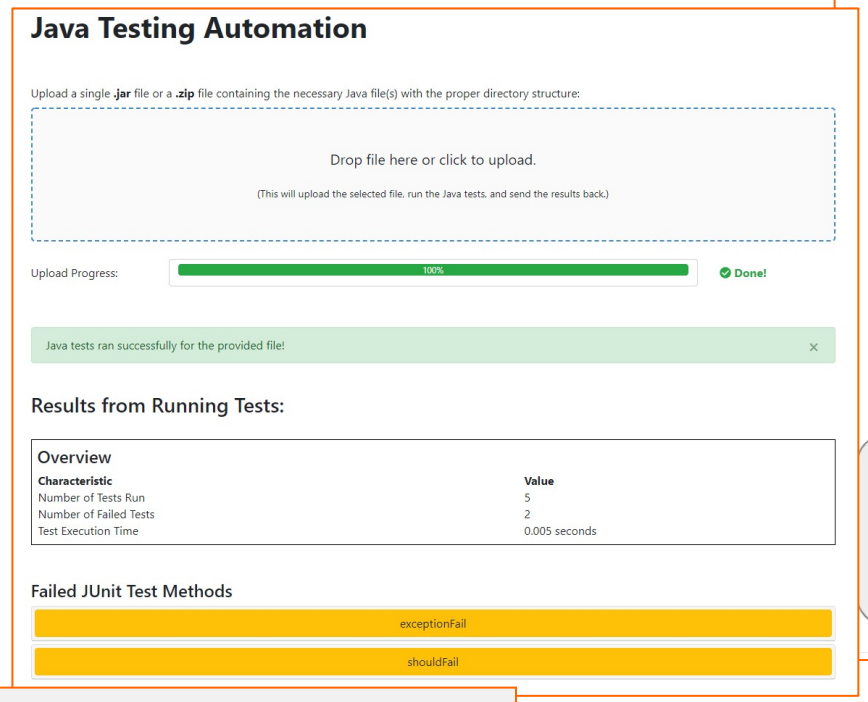
SOPATRA®
powered by Innoslate

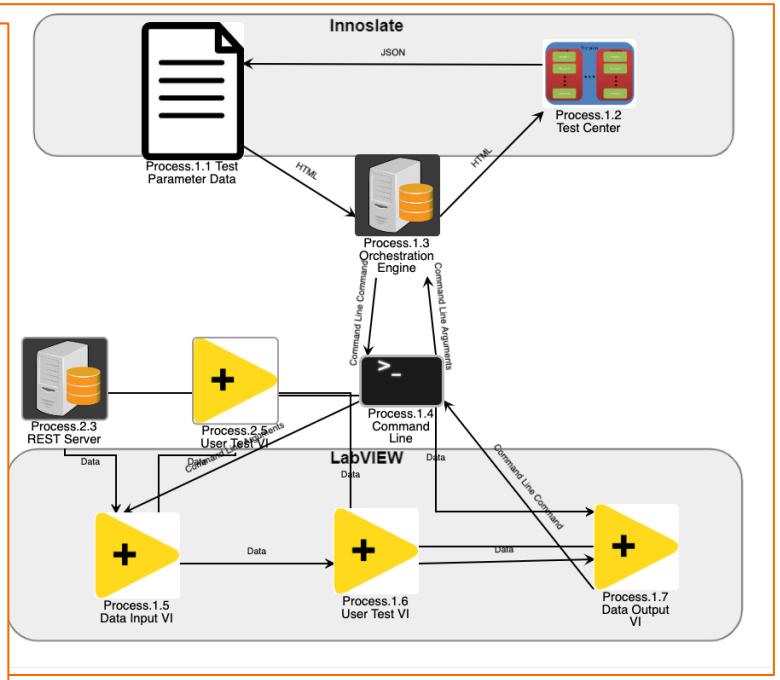
How Sopatra Works

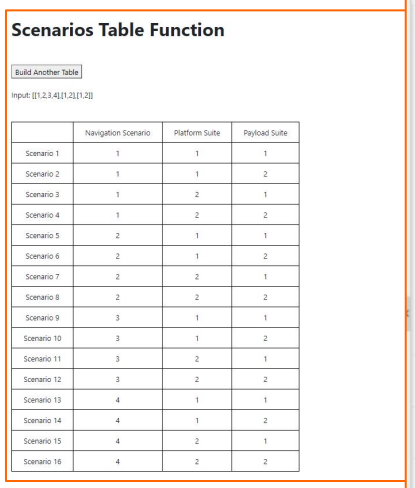


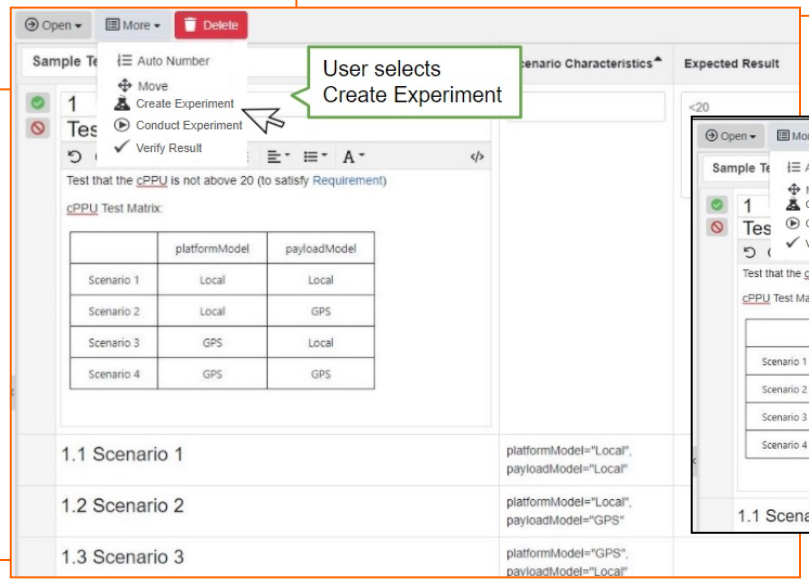
Plans for Version 4.7

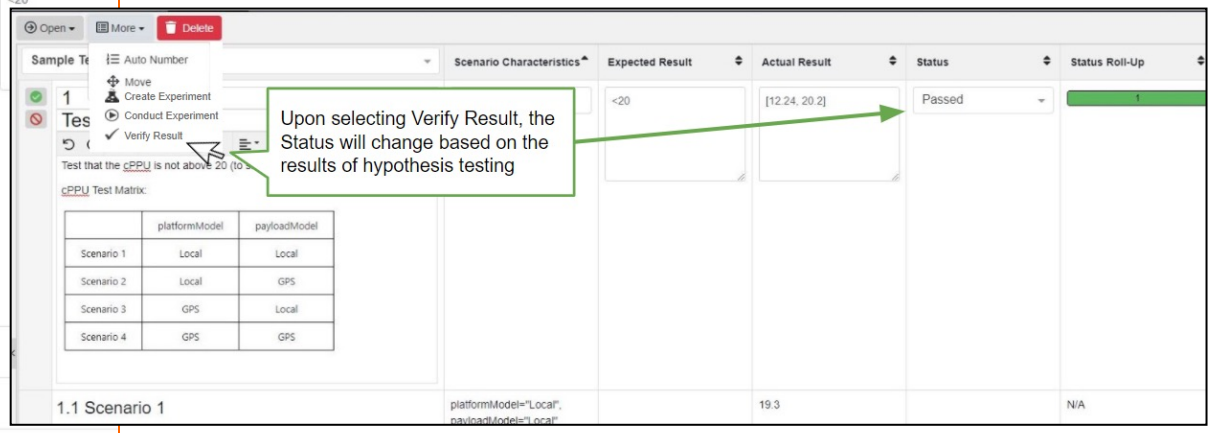
- Add automated testing using Selenium and LabView
- Add design of experiments capability
- Reviewer Tool







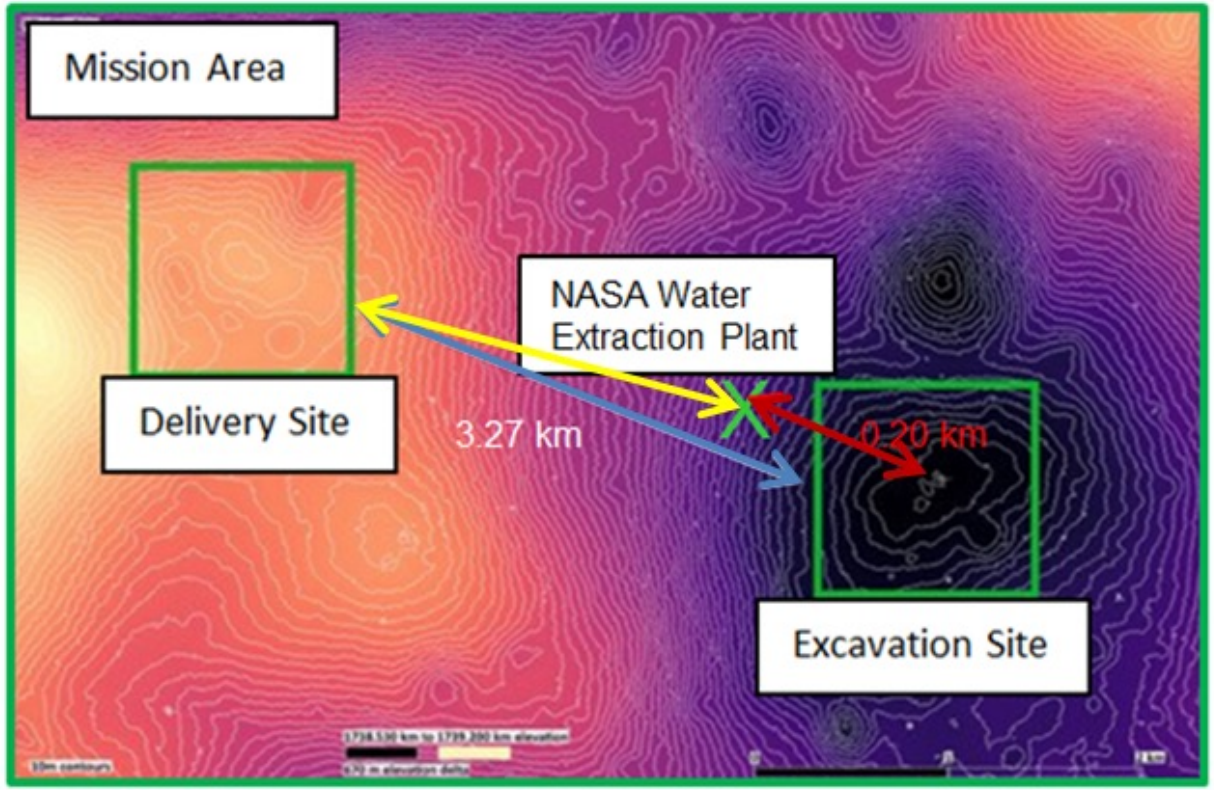




Application: NASA "Break the Ice" Challenge

Break the Ice Challenge

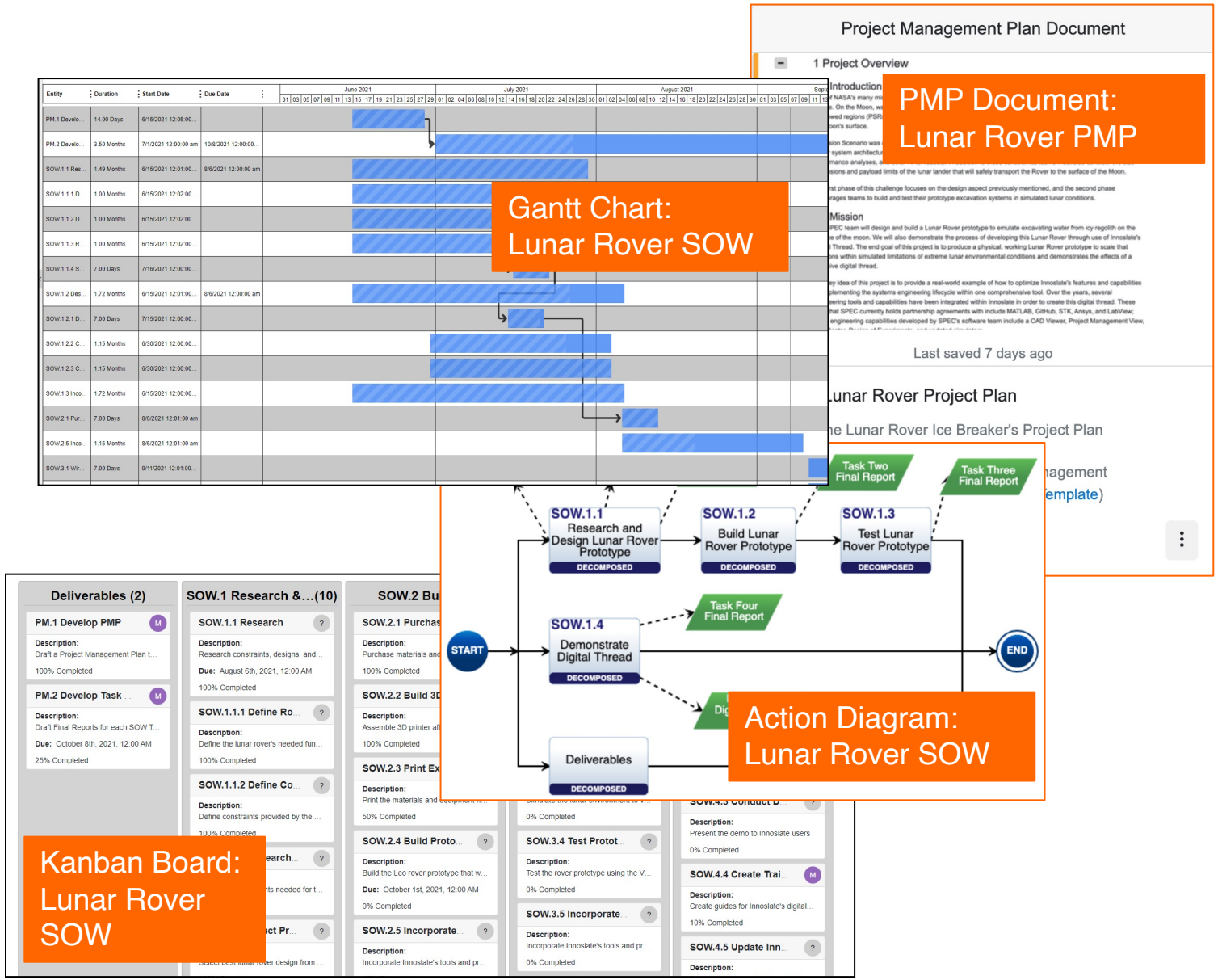
- Competition hosted by NASA
- Solutions sought for:
  - Excavating regolith
  - Maximizing water delivered
  - Minimizing mass of equipment
  - Minimizing power consumption



- Goal: Extract 10,000 kg of water from regolith in 365 days

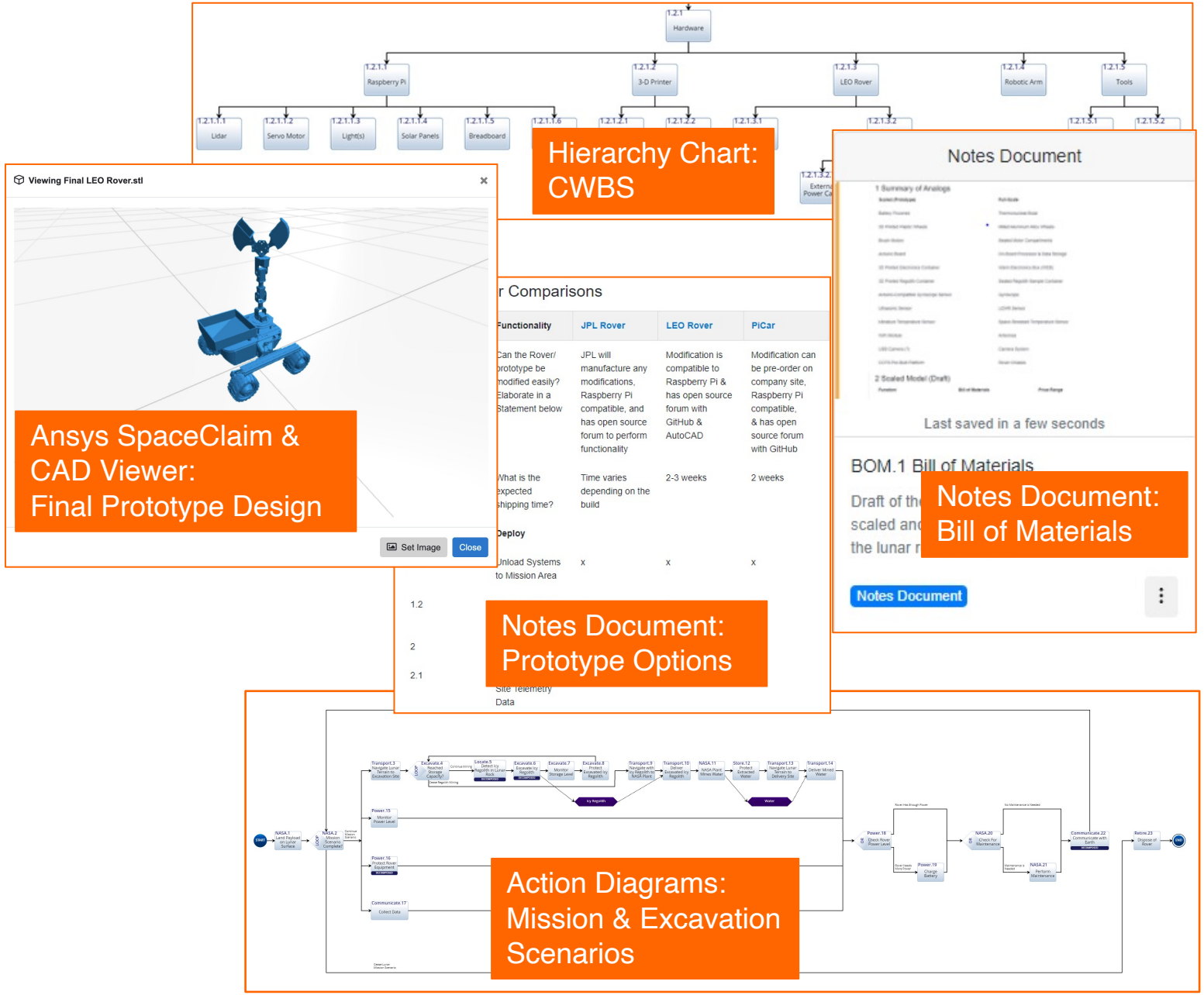
Project Planning

- Defines the project's:
  - Scope
  - Schedule
  - Budget
  - Technical execution
  - Statement of Work
  - Timelines



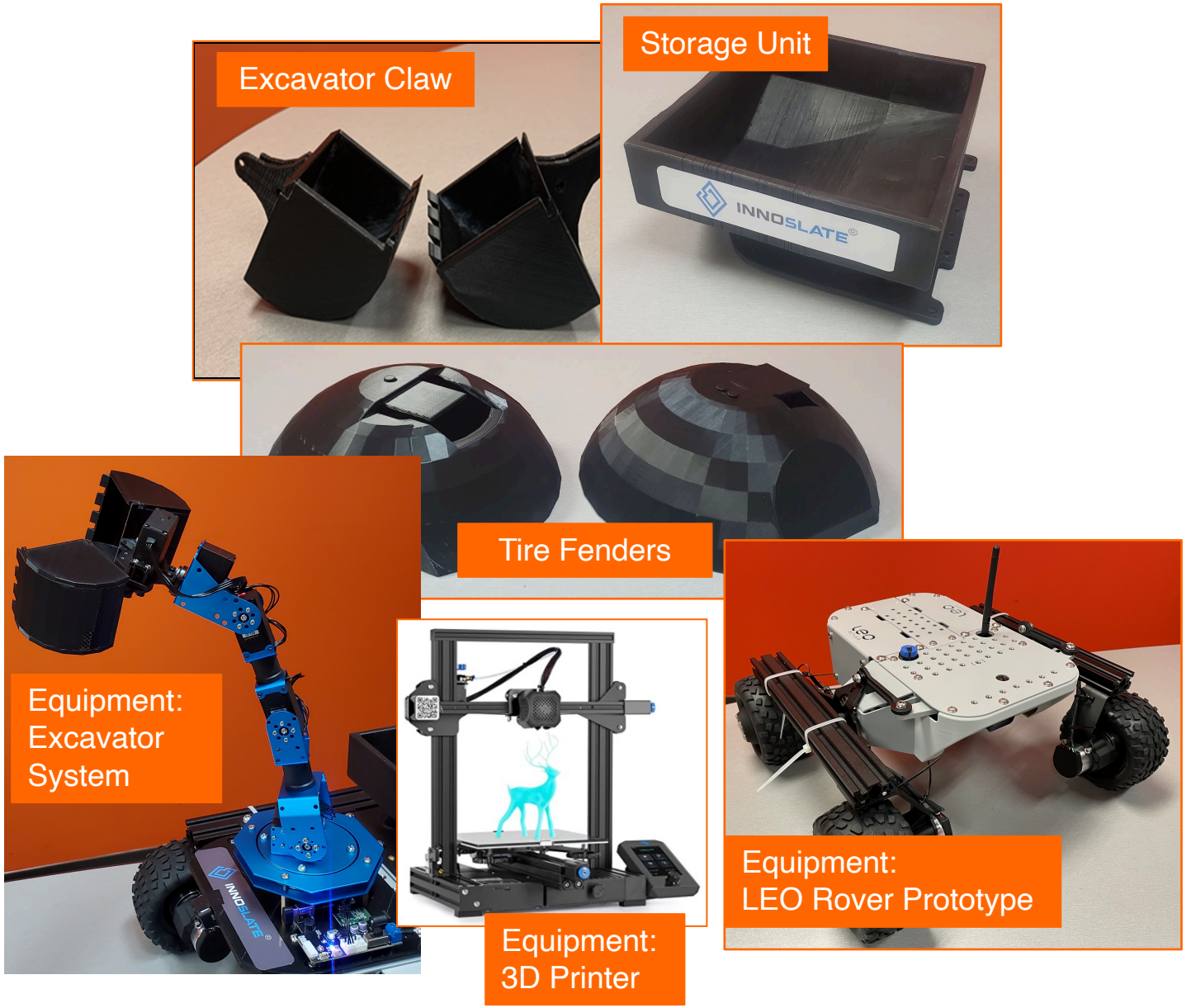
Research and Design

- Research included: Terms and definitions, Technical Constraints, Environmental Conditions, Mission Requirements, Technical Goals, Supporting Assets and Equipment
- Design included: Mission Analysis, Scenario Development and Analysis, COTS Selection, Design of Additional Equipment, Cost Analysis, Prototype Design



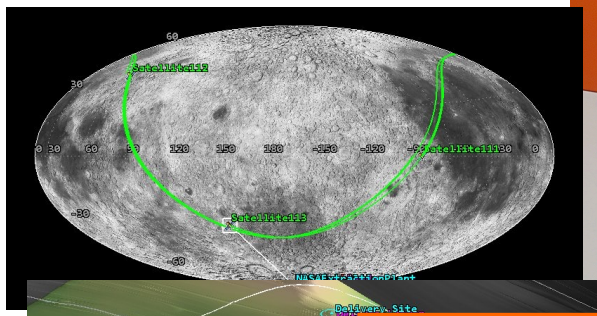
Build Phase

- Build included: assembly of COTS rover, assembly and HW/SW integration of robotic arm for excavation of regolith, Ansys SpaceClaim and 3-D printer to fabricate additional components, added LiDAR (for navigation) and LEDs (lights for improved visuals in darkness)



System Verification and Validation

- System V&V included:
  - in-house testing field testing, demonstration
  - capturing results in TestCenter
  - STK and MATLAB co-simulation analysis using lunar terrain of rover route and comms
  - Ansys SpaceClaim for static load capacity metrics
  - pressure tolerances using Ansys Mechanical Platform with SpaceClaim model
  - landed mass analysis





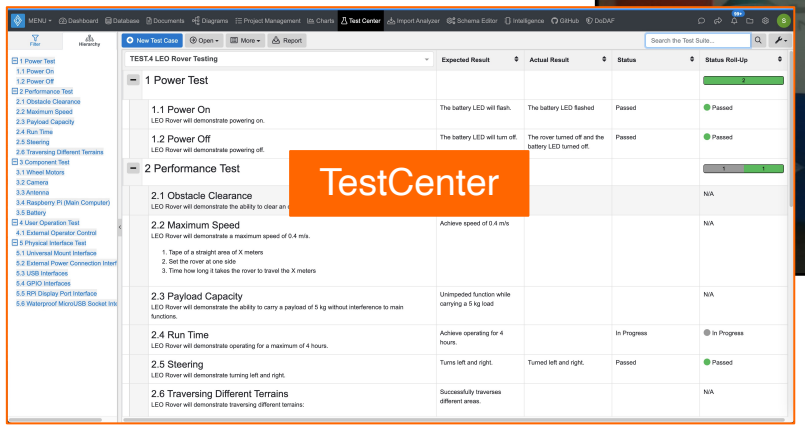
STK Model: Rover Route



Test Object: SPECTER



SPECTER UI: SPECTER Camera View and Control



TestCenter

Key Lessons Learned

BLUF: A well integrated system that moves appropriate data between tools

Key Lessons Learned

- Having a well integrated systems and design engineering environment reduces prototype development time and cost significantly
  - SPECTER developed and tested in less than 6 months: ½ the time of other competitors, many of whom did not create a prototype
- Inexpensive 3D printing made enhancing available COTS feasible on a small budget
- Many software tools do not have modern APIs for integration
- Many software tools are still essentially desktop tools (difficult to integrate with cloud computing tools – Java Web App workaround)
- Access to tools – many vendors ignore requests for teaming/partnership; Ansys partnership enabled complete design lifecycle



Questions and Answers

Contact us on Linked In (https://www.linkedin.com/groups/7415373/) or at support@innoslate.com

SYSTEMS ENGINEERING RESEARCH CENTER

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Integrating Digital Engineering Technical Models with MBSE Cost Models

Sponsors: NAVAR, CCDC-AC

Presented by: Dr. Mark Blackburn SET Research, SERC, Stevens
Co-authors: Mr. Donald P. Allen, Mr. Taylor Fields, Dr. Selcuk Cimtalay

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Copyright and Disclaimer

Certain commercial software products are identified in this material. These products were used only for demonstration purposes. This use does not imply approval or endorsement by Stevens, SERC, or CCDC-AC/DEVCOM, NAVAIR, nor does it imply these products are necessarily the best available for the purpose. Other product names, company names, images, or names of platforms referenced herein may be trademarks or registered trademarks of their respective companies, and they are used for identification purposes only.

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Research Tasks and Collaborator Network

RT-48 (2013)
- Mark Blackburn (PI), Stevens
- Rob Cloutier (Co-PI) - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-118 (2104)
- Mark Blackburn (PI), Stevens
- Rob Cloutier - Stevens
- Eirik Hole - Stevens
- Gary Witus – Wayne State

RT-141 (2015)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Gary Witus – Wayne State

RT-157 (2016)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Roger Blake - Stevens
- Mark Austin – Univ. Maryland
- Leonard Petnga – Univ. of Maryland

RT-170 (2016)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Deva Henry - Stevens
- Paul Grogan - Stevens
- Steven Hoffenson - Stevens
- Mark Austin – Univ. of Maryland
- Leonard Petnga – Univ. of Maryland
- Maria Coelho (Grad) – Univ. of Maryland
- Russell Peak – Georgia Tech.
- Stephen Edwards – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.

RT-168 – Phase I & II (2016)
- Mark Blackburn (PI), Stevens
- Dinesh Verma (Co-PI) – Stevens
- Ralph Giffin
- Roger Blake - Stevens
- Mary Bone – Stevens
- Andrew Dawson – Stevens (Phase I)
- Rick Dove
- John Dzielski, Stevens
- Paul Grogan - Stevens
- Deva Henry – Stevens (Phase I)
- Bob Hathaway - Stevens
- Steven Hoffenson - Stevens
- Eirik Hole - Stevens
- Roger Jones – Stevens
- Benjamine Kruse - Stevens
- Jeff McDonald – Stevens (Phase I)
- Kishore Pochiraju – Stevens
- Chris Snyder - Stevens
- Gregg Vesonder – Stevens (Phase I)
- Lu Xiao – Stevens (Phase I)
- Brian Chell (Grad) – Stevens
- Luigi Ballarinni (Grad) – Stevens
- Harsh Kevadia (Grad) – Stevens
- Kunal Batra (Grad) – Stevens
- Khushali Dave (Grad) – Stevens
- Rob Cloutier – Visiting Professor
- Robin Dillon-Merrill – Georgetown Univ.
- Ian Grosse – Univ. of Massachucetts
- Tom Hagedorn – Univ. of Massachusetts
- Todd Richmond – Univ. of Southern California (Phase I)
- Edgar Evangelista – Univ. of Southern California (Phase I)

RT-195 (2018)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- Ralph Giffin - Stevens
- Benjamin Kruse - Stevens
- Russell Peak – Georgia Tech.
- Stephen Edwards – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.
- Donna Rhodes - MIT
- Mark Austin – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

WRT-1008 (2019)
- Mark Blackburn (PI), Stevens
- Mary Bone - Stevens
- John Dzielski- Stevens
- Benjamin Kruse - Stevens
- Bill Rouse – Stevens/Georgetown
- Russell Peak – Georgia Tech.
- Selcuk Cimtalay – Georgia Tech.
- Adam Baker (Grad) – Georgia Tech.
- Marlin Ballard (Grad) – Georgia Tech.
- Alanna Carnevale (Grad) – Georgia Tech.
- William Stock (Grad) – Georgia Tech.
- Michael Szostak (Grad) – Georgia Tech.
- Donna Rhodes - MIT
- Mark Austin – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

WRT-1025 (2020)
- Mark Blackburn (PI), Stevens
- Mark Austin (Co-PI) – Univ. Maryland
- Maria Coelho (Grad) – Univ. Maryland

ART-002 (2018) – ART-022 (2021)
- Mark Blackburn (PI), Stevens
- Dinesh Verma (Co-PI) – Stevens
- Kunal Batra – Stevens
- Mary Bone - Stevens
- John Dzielski, Stevens
- Steven Hoffenson - Stevens
- Steve Hespelt - Stevens
- Roger Jones - Stevens
- Benjamin Kruse - Stevens
- Annie Yu
- Chris Snyder - Stevens
- Brian Chell – Stevens
- Daniel Dunbar (PhD) - Stevens
- Andrew Underwood (Ungrad) – Stevens
- Cory Phillipe (Grad) - Stevens
- Ian Grosse – Univ. of Massachucetts
- Tom Hagedorn – Univ. of Massachusetts
- Joe Gabbard – Virginia Tech
- Jared Van Dam (PhD) – Virginia Tech
- Kelsey Quinn (PhD) – Virginia Tech

WRT-1036 (2020)
- Mark Blackburn (PI), Stevens
- John Dzielski- Stevens
- Russell Peak – Georgia Tech.
- Selcuk Cimtalay – Georgia Tech.
- Taylor Fields – Georgia Tech.
- William Stock (Grad) – Georgia Tech.
- Sahil Panchal – Georgia Tech
- Jake Sisavath – Georgia Tech
- Gabriel Rizzo – Georgia Tech

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Acknowledgements

- Special thanks to NAVAIR Cost Modeling:
  - Don Allen
  - Alexandra (Lexi) Kilmon
- Special thanks to Master's Student:
  - Scott Schmidt, Stevens Institute of Technology
    - Performed this effort for Stevens Master's Project
  - William Stock, Georgia Tech
- Research Collaborators
  - Dr. Selcuk Cimtalay
  - Dr. John Dzielski
  - Jake Sisavath
  - Sahil Panchal
  - Gabriel Rizzo
  - Dr. Russell Peak (PI – Georgia Tech)

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Organization

- **INTRO:** Context and Scope of NAVAIR SE Transformation & Skyzer Pilot
- **WHAT:** Integrating Digital Engineering Technical Models with MBSE Cost Models
- **HOW:** Surrogate Pilot & Experiments to Demonstrate Art-of-the-Possible
  - Authoritative Source of Truth
  - ”Full Stack” Graphical CONOPS, Mission, System, Multi-physics, Ontologies, Ref. Architectures
  - Stakeholder Analysis Models such as MBSE Cost Model
  - Modeling Methods
  - Digital Signoffs – Transformation From CDRLs
- **HOW WELL:** Contributing Modeling Examples transitioning to Support Workforce Development demonstrating Art-of-the-Possible
  - Video of demonstration coming soon: https://www.youtube.com/c/SERCUARC

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

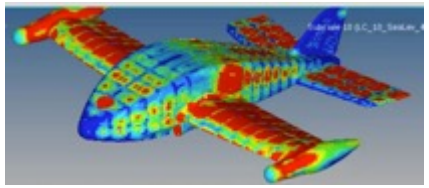
Surrogate Pilot Scenario: Skyzer UAS Search and Rescue Mission

Doing Everything in Models to Demonstrate Art-of-the-Possible

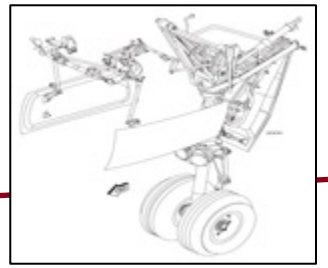
Graphical CONOPS Scenario: Search & Rescue



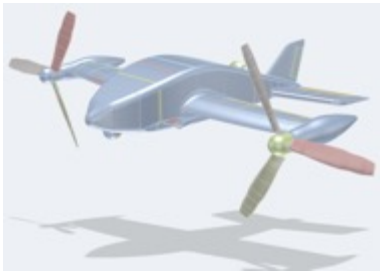
Deep Dives by Phases



P1: Multi-physics



P2: Airworthiness



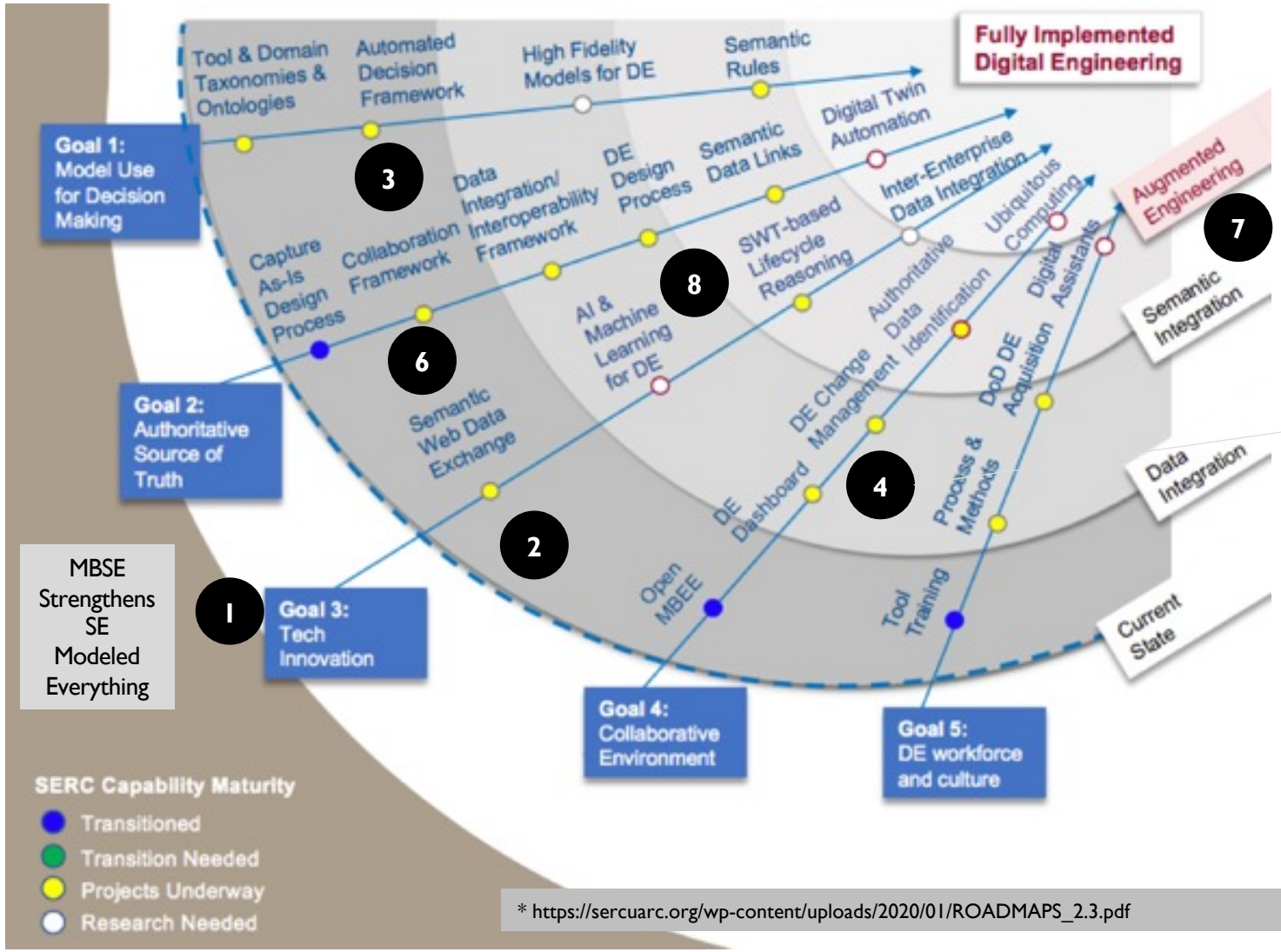
P3: Cost Modeling

Performance constraints force Multi-physics Design considerations – similar to Bell Eagle Eye



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Digital Engineering for Systems Engineering Roadmap





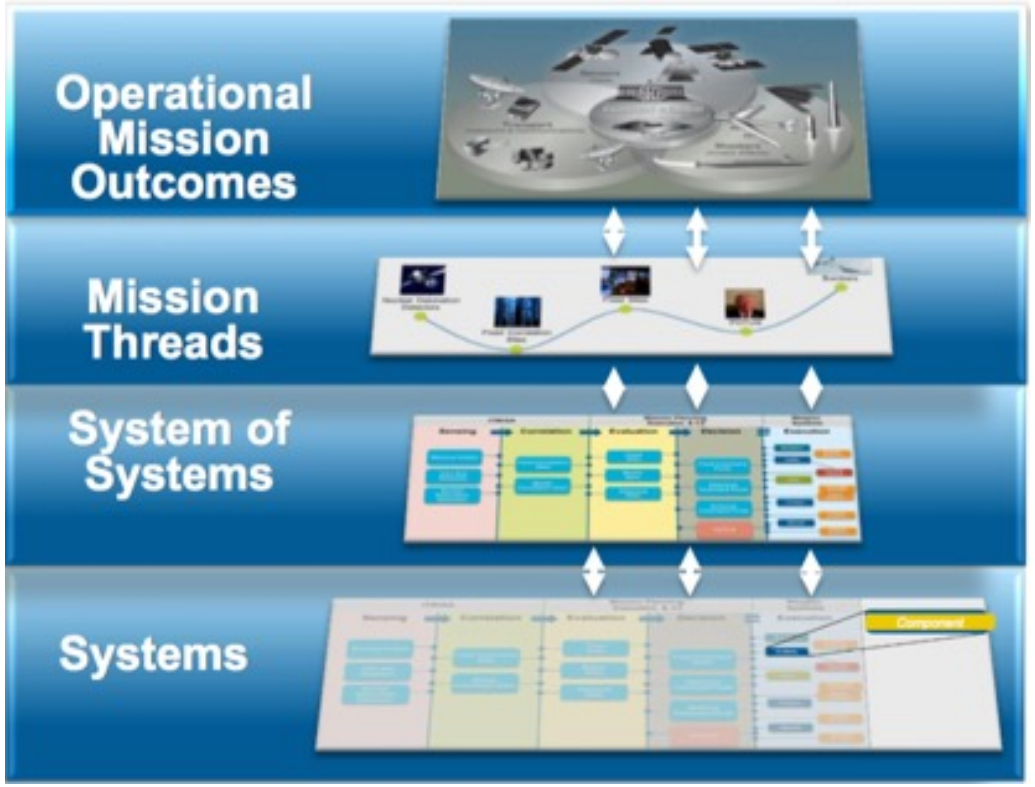
* https://sercuarc.org/wp-content/uploads/2020/01/ROADMAPS_2.3.pdf



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Context Related to DoD Digital Engineering Strategy Goals

- MBSE Strengthens Systems Engineering (Goal 3)
  - Represent Structure, Behavior, Interfaces, Requirements and related interactions
  - Can characterize different levels of abstraction – Mission, System, Subsystem where different types of **methods** are needed
  - Can generate "documents/specifications" based on stakeholder-relevant views
- Need to formalize representation that links information in an Authoritative Source of Truth (Goal 2 – distributed like Internet)
- Need computing infrastructure to access and visualize on need-to-know basis (Goal 4)
- Need to semantically link information from different modeling levels and types to enable tradespace analyses and **decision making** (Goal 1)
- Skyzer models are unclassified examples and are being transformed to support workforce development (Goal 5)



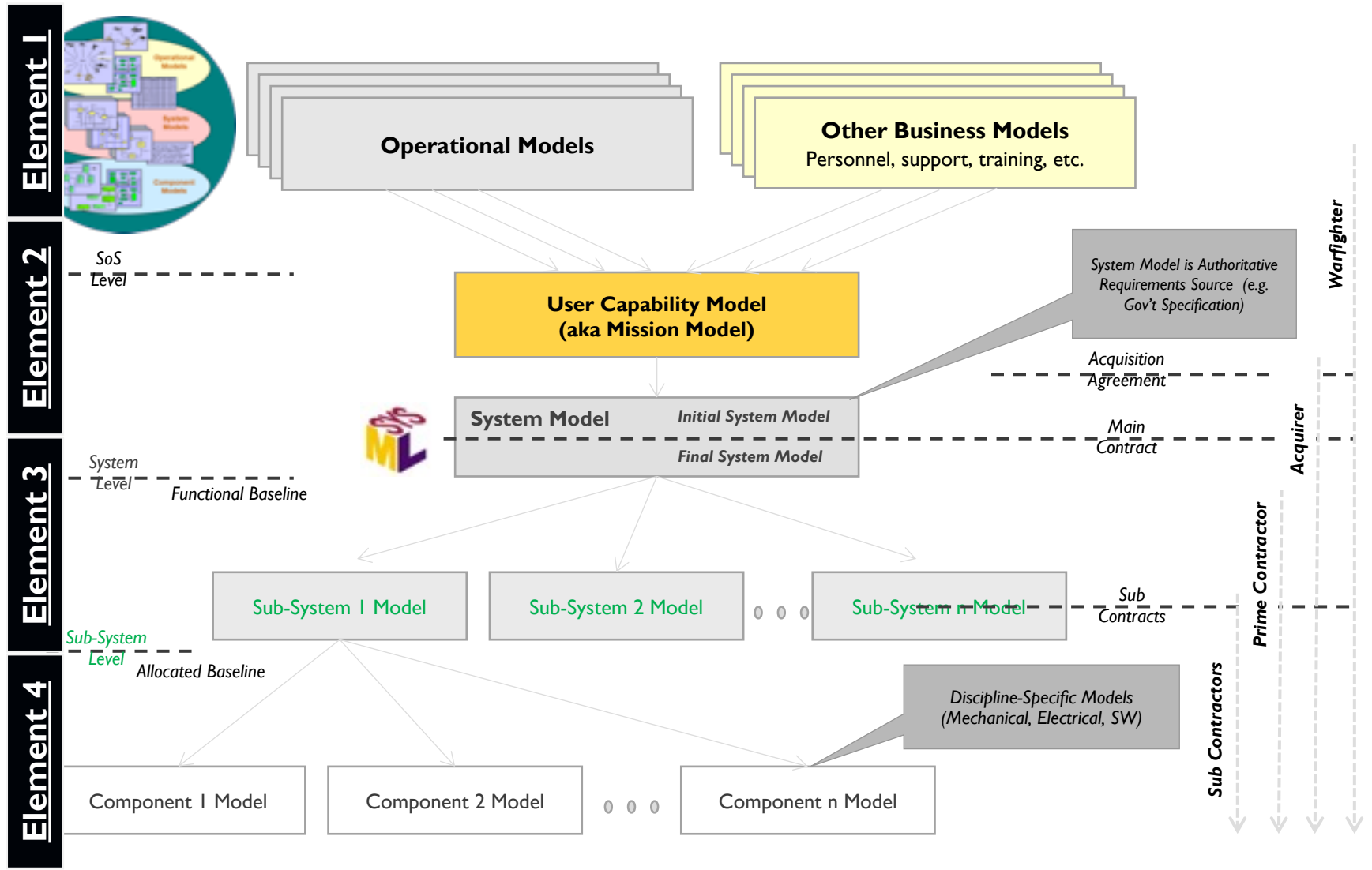
Extending the DoD Digital Engineering Strategy to Missions, Systems of Systems, and Portfolios
P. Zimmerman, T. Gilbert, J. Dahmann
22nd Annual NDIA Systems and Mission Engineering Conference Tampa, FL| 23 October 2019

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Skyzer Demonstrates Modeling Methods for SET Framework Elements at Different Abstraction Levels

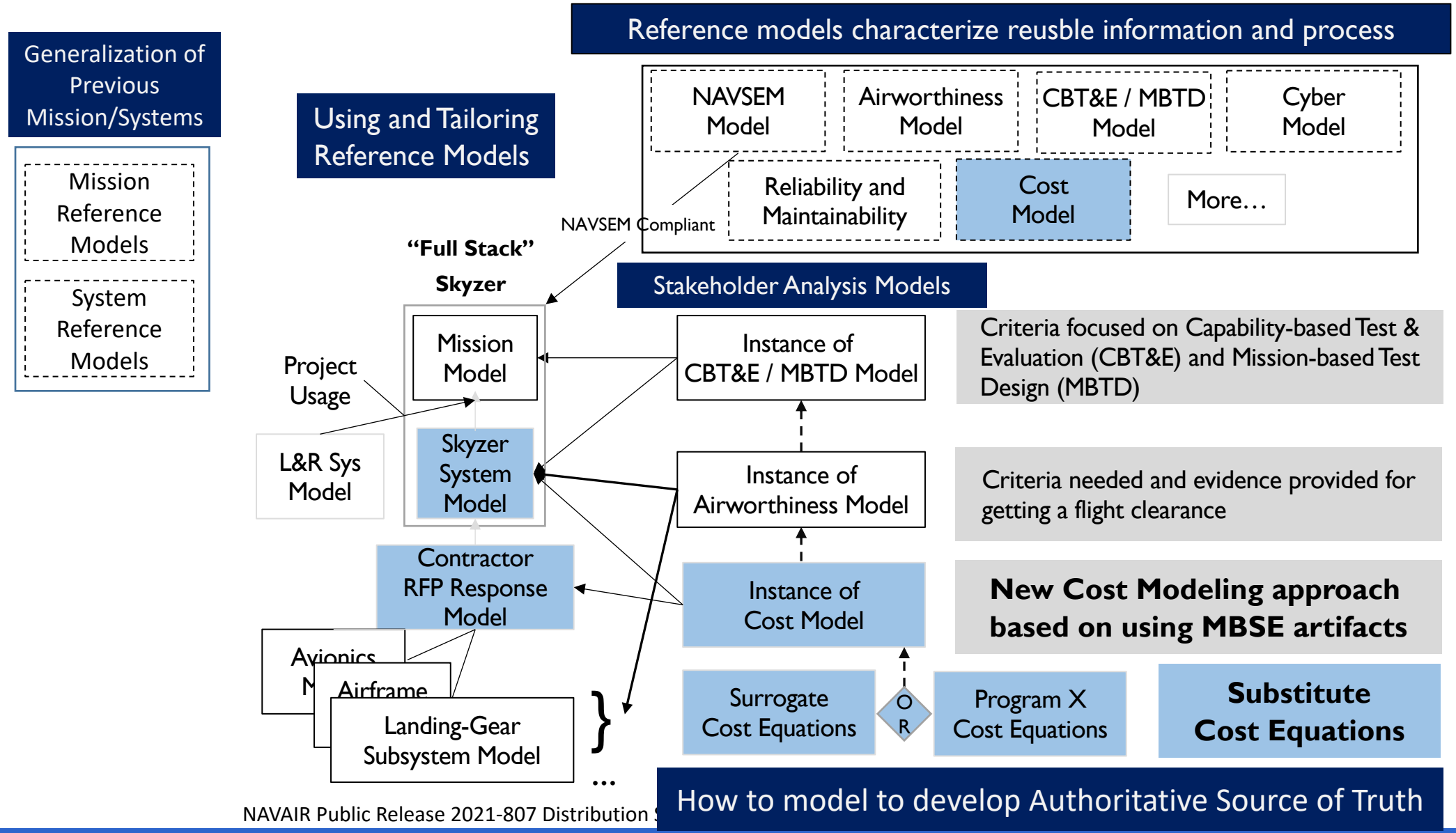
MBSE tools & languages applicable

MBE tools & languages applicable



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

“Full Stack” of Skyzer Models



NAVAIR Public Release 2021-807 Distribution S

Cost Modeling

INPUTS

Cost Parameters
- Hours (Mfg, Tool, QC, Eng, etc.)
- Dollars (Mfg, Tool, QC, Eng, RM / PP,PE, etc.)
- Labor Rates (Direct, Indirect, OH, Wrap, etc.)
- Etc.

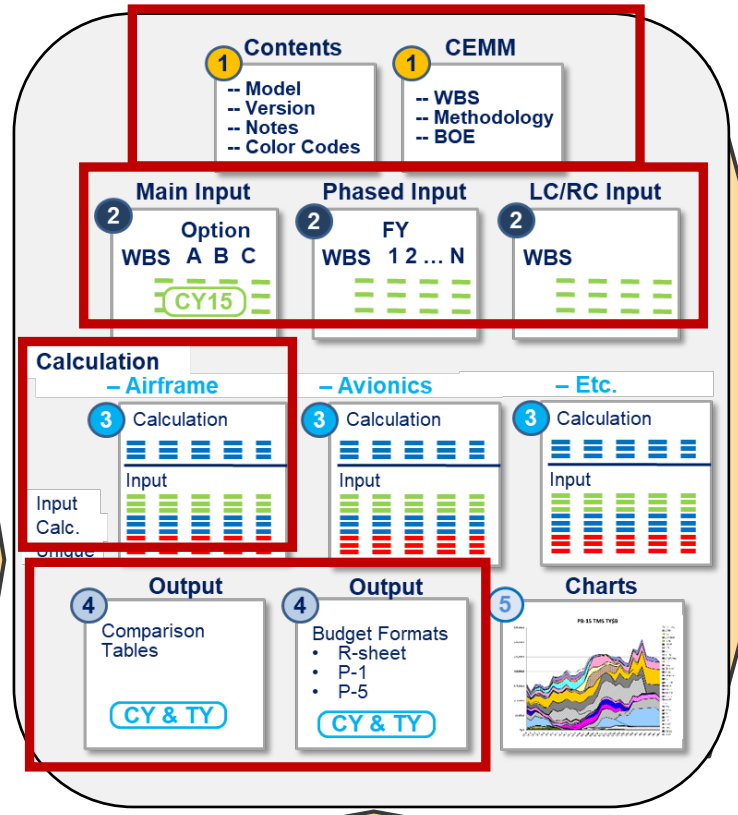
Technical Parameters (ETAB)
- Weight: WE, AUW, Structure, A/B Kit[lbs]
- Material Distribution :
  - Al, Steel, Ti, Composites, Other [%]
- Avionics:
  - CNI, EW, FC, Survivability, etc.
- Software: ESLOC, S/W language
- Propulsion: T/W Ratio , Airflow [lbs / sec]
- Flight Test: Hours, Points, Type
- Risk
- Etc.

Programmatic Parameters (ETAB)
- Acquisition Assumptions
- Prime / Sub Work Split
- Dates: Milestone, Contract Award, First Flight
- Schedules: Dev., Flight Test , Prod.
- ILS Elements: Data, Trainers, Spares
- O&S Assumptions
  - Maintenance Concept, Spares, Personnel, Reliability
- Risk
- Etc.

Input Suppliers
- PMAs
- IPTs
- AIR-00
- PEOs
- ASN
- OSD
- Industry
- Academia
- Etc.

Policy & Guidance
- DoDD 5000 Series
- CSDR Manual
- OSD Cost Guidebook
- ECNAV INST 5000.2B
- MIL-STD- 881D
- DoD ACQ Guidebook
- ETAB NAVAIRINST 5223.2
- Naval Systems Engineering Guide
- Etc.

Cost Model



Analytical Tools
- MS Excel, Cost Analysis ToolPak, NEMO, AIR-4.2 Regression Tool, ACEIT (ACE, CO$TAT), Tableau, Qlik,, Etc.

Data
- CADE (DAMIR, DACIMS, EVM), JCARD (CSDRs, Expenditures, Programmatic, Weights), BANK Datasets. eDocs, CBAR, Inflation (OSD, GI), Etc.

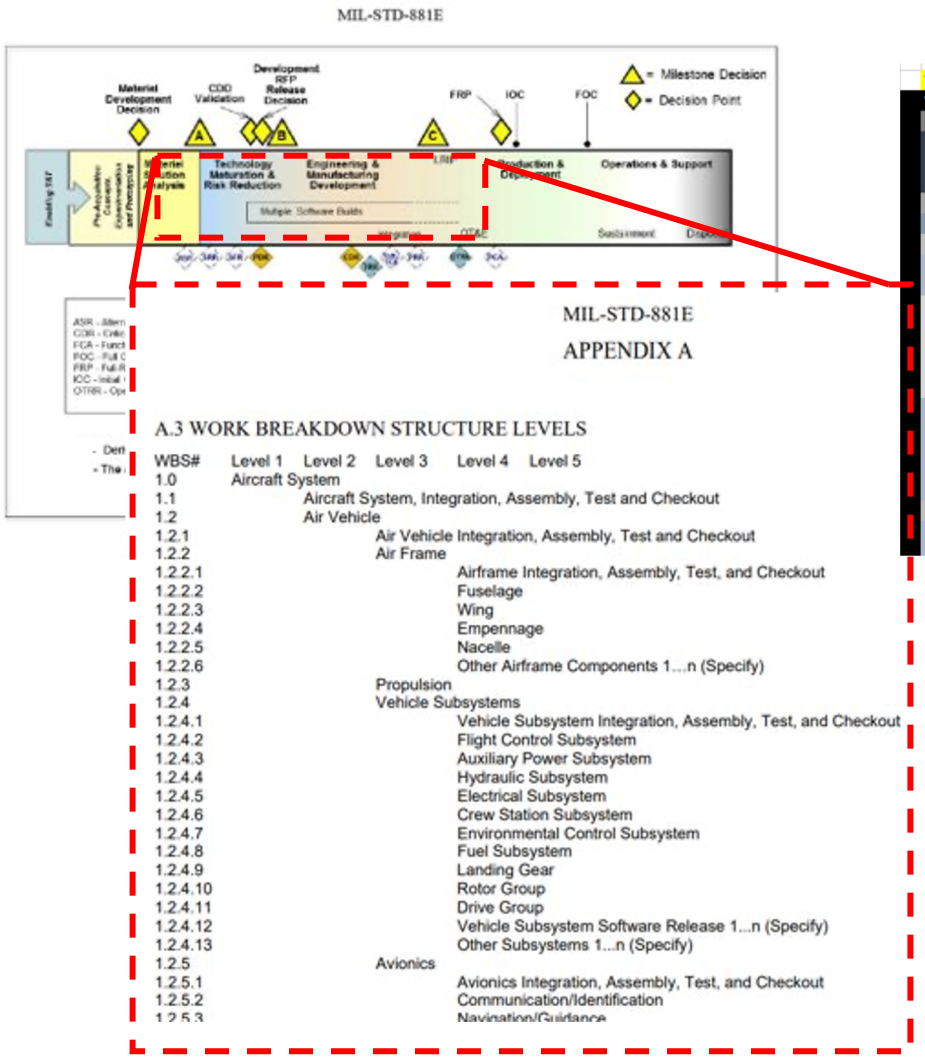
OUTPUTS

Products
- Budgets (DON, OSD, PB, POM)
- M/S LCC Estimates
- Naval Aviation Plan
- Will Cost / Should Cost
- Total Ownership Cost
- Special Studies (AOAs, CAIV, DAS, EAs, Trade Studies)
- Affordable Readiness
- What-if Drills
- Sensitivity Analysis
- Risk Analysis
- Briefings
- IBR's
- Claims / Litigation
- Negotiation Support

Customers
- PMAs
- PEOs
- AIR-00
- ASN
- NAVCOMPT
- NCCA
- OSD CAPE
- Etc.

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Total Ownership Cost – As-Is Process



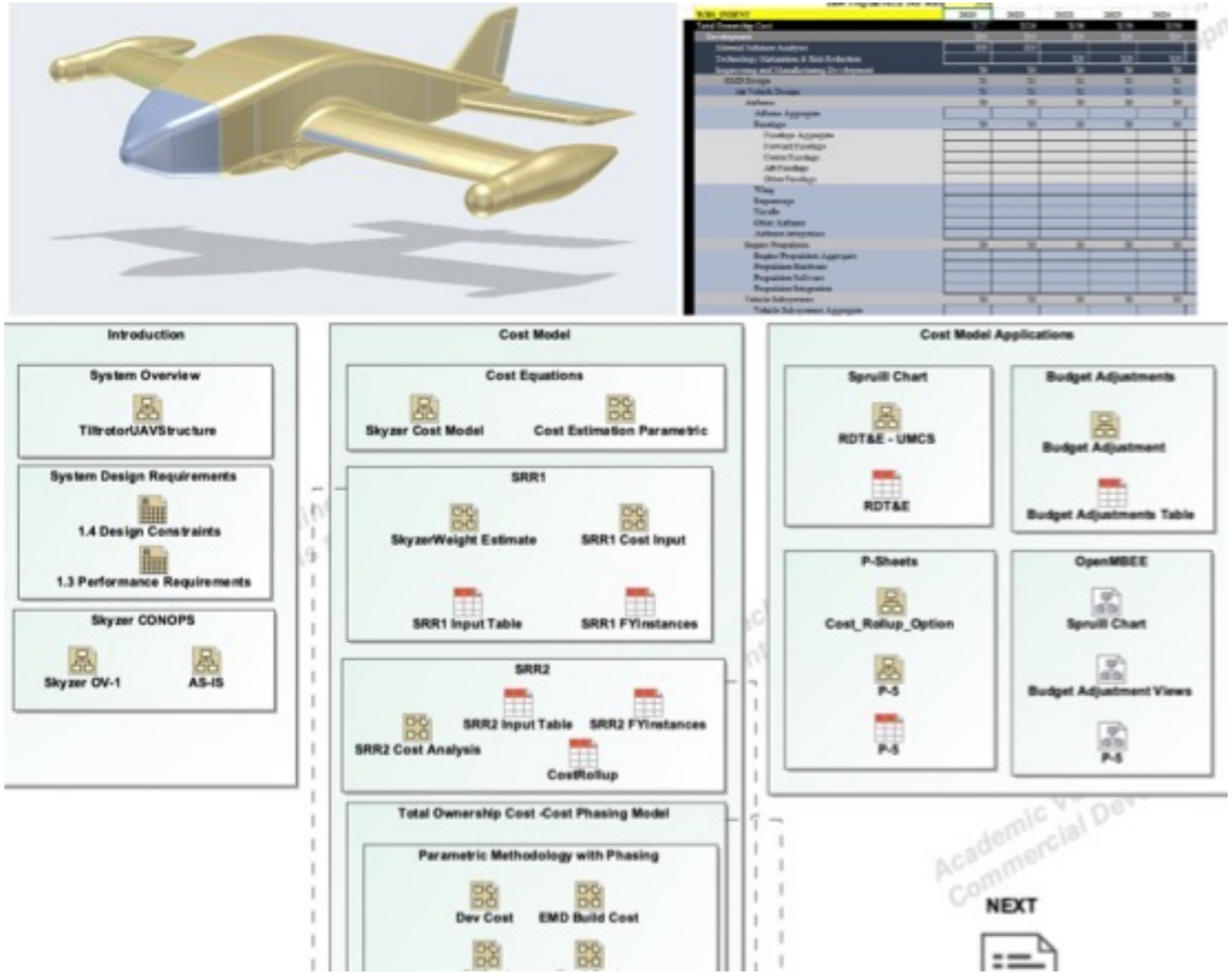
WBS_INDENT	2020	2021	2022	2023	2024
Total Ownership Cost	$127	$126	$136	$136	$136
Development	$14	$14	$24	$24	$24
Material Solution Analysis	$10	$10			
Technology Maturation & Risk Reduction			$20	$20	$20
Engineering and Manufacturing Development	$4	$4	$4	$4	$4
EMD Design	$1	$1	$1	$1	$1
Air Vehicle Design	$1	$1	$1	$1	$1
Airframe	$0	$0	$0	$0	$0
Aiframe Aggregate					
Fuselage	$0	$0	$0	$0	$0
Fuselage Aggregate					
Forward Fuselage					
Center Fuselage					
Aft Fuselage					
Other Fuselage					
Wing					
Empennage					
Nacelle					
Other Airframe					
Airframe Integration					
Engine/Propulsion	$0	$0	$0	$0	$0
Engine/Propulsion Aggregate					
Propulsion Hardware					

Standard WBS structure defined and leveraged to complete consistent cost and technical analysis

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

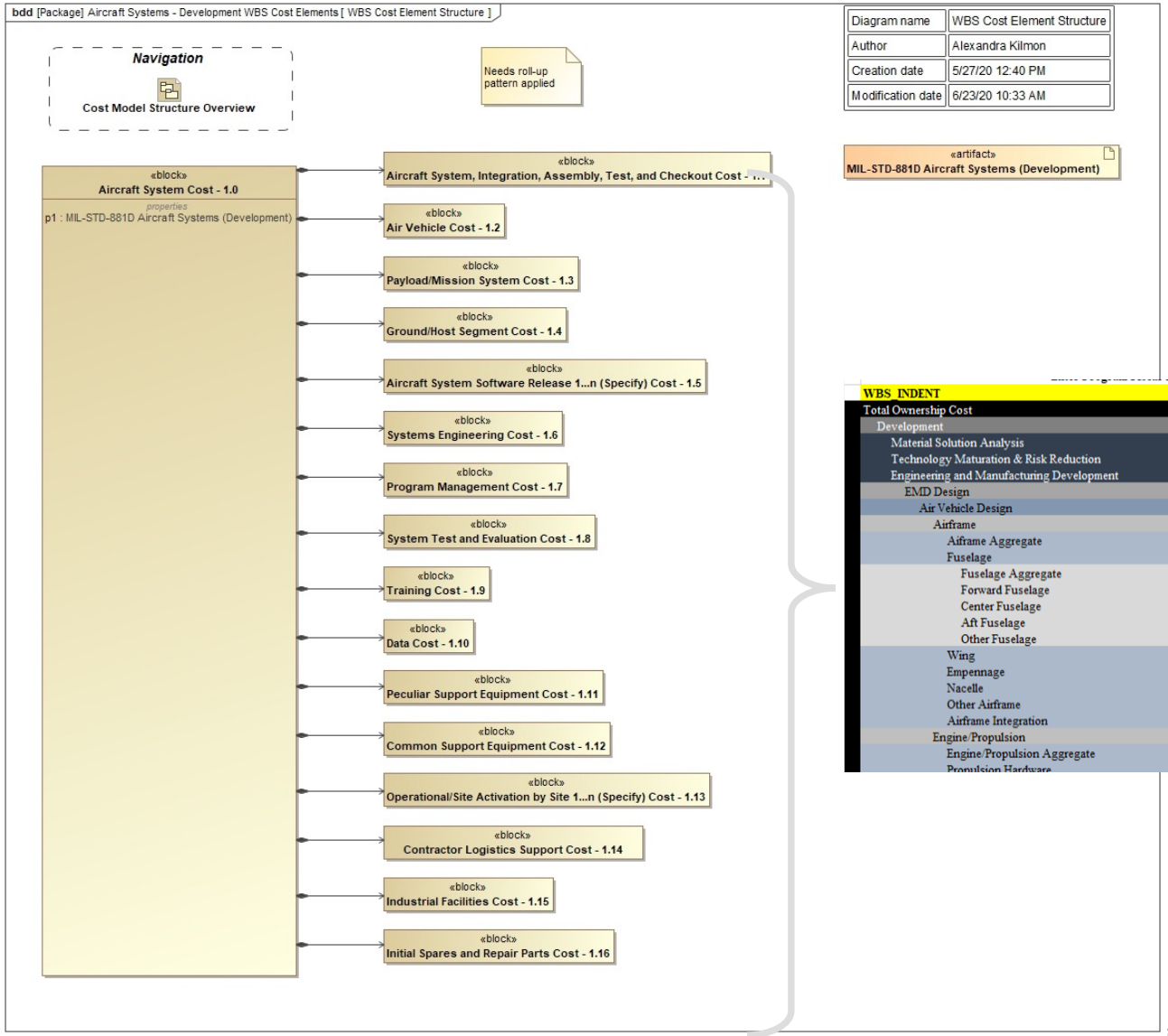
Cost Model Organization

Aircraft Characteristics Deep Dive



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Aircraft System Cost Model – Structure Aligns with Mil-STD 881

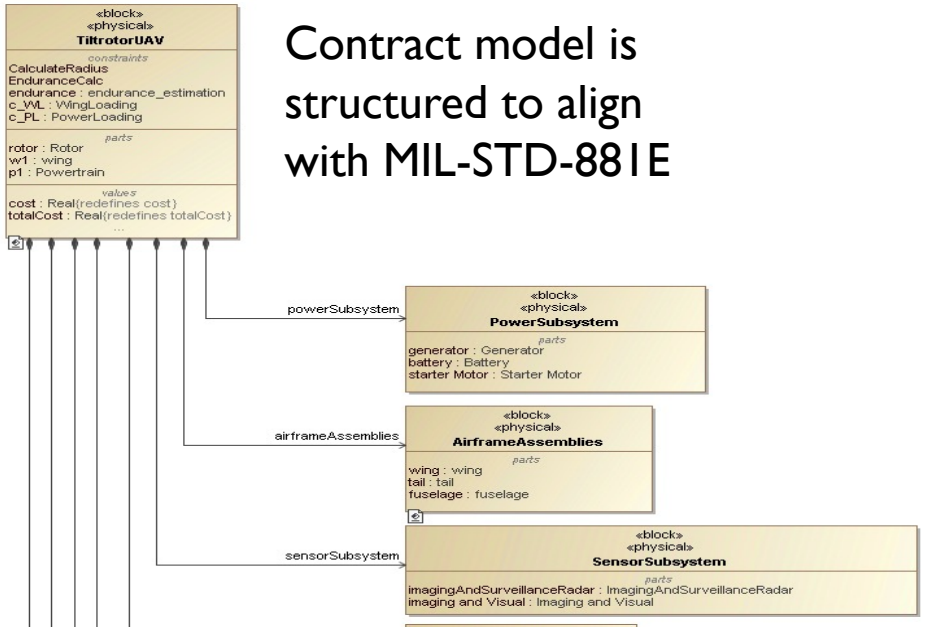


WBS_INDENT	2020	2021	2022	2023	2024
Total Ownership Cost	$127	$126	$136	$136	$136
Development	$14	$14	$24	$24	$24
Material Solution Analysis	$10	$10			
Technology Maturation & Risk Reduction			$20	$20	$20
Engineering and Manufacturing Development	$4	$4	$4	$4	$4
EMD Design	$1	$1	$1	$1	$1
Air Vehicle Design	$1	$1	$1	$1	$1
Airframe	$0	$0	$0	$0	$0
Aiframe Aggregate					
Fuselage	$0	$0	$0	$0	$0
Fuselage Aggregate					
Forward Fuselage					
Center Fuselage					
Aft Fuselage					
Other Fuselage					
Wing					
Empennage					
Nacelle					
Other Airframe					
Airframe Integration					
Engine/Propulsion	$0	$0	$0	$0	$0
Engine/Propulsion Aggregate					
Propulsion Hardware					

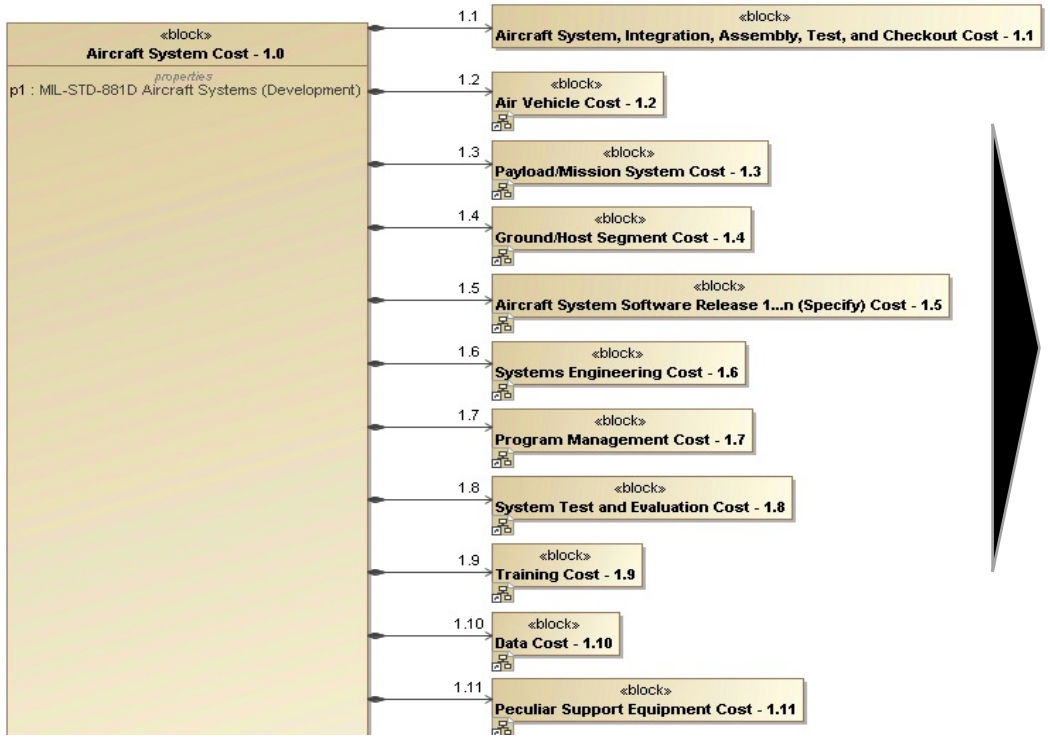
NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Total Ownership Cost – To-be Process

Contract model is structured to align with MIL-STD-881E



Government cost model rollup patterns MIL-STD-881E from AURA Cost Model

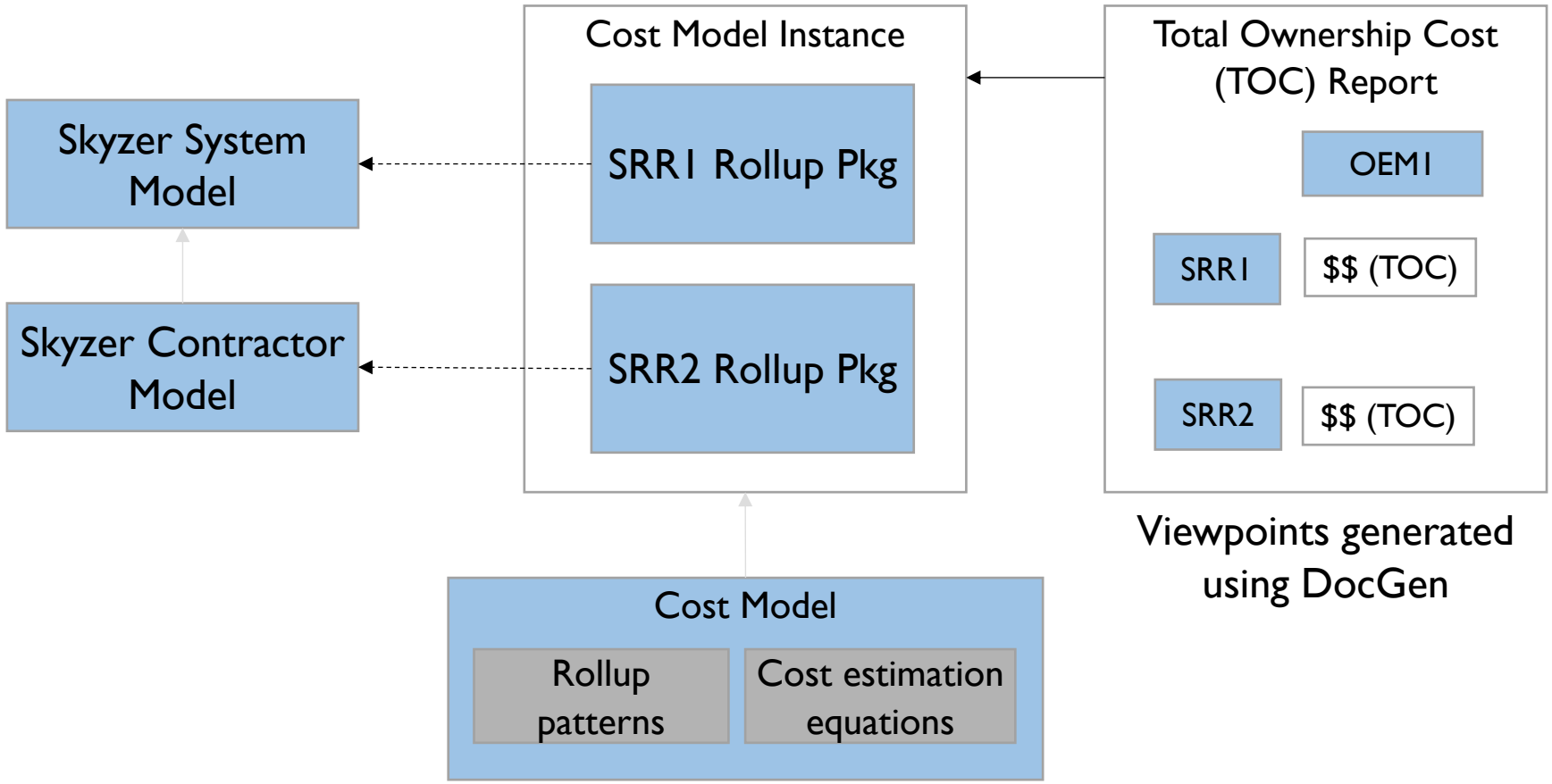


Benefits

- Improve ability to rapidly access change impacts in Authoritative Source of Truth
- Enable comparison of contractor model to government model
- Relate technical data to cost data

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Generate Cost Data based on Airframe Weight Rollups



Goal: Leverage the system design data to gain insights into total ownership cost

Goal: Reduce the burden to navigate the system model

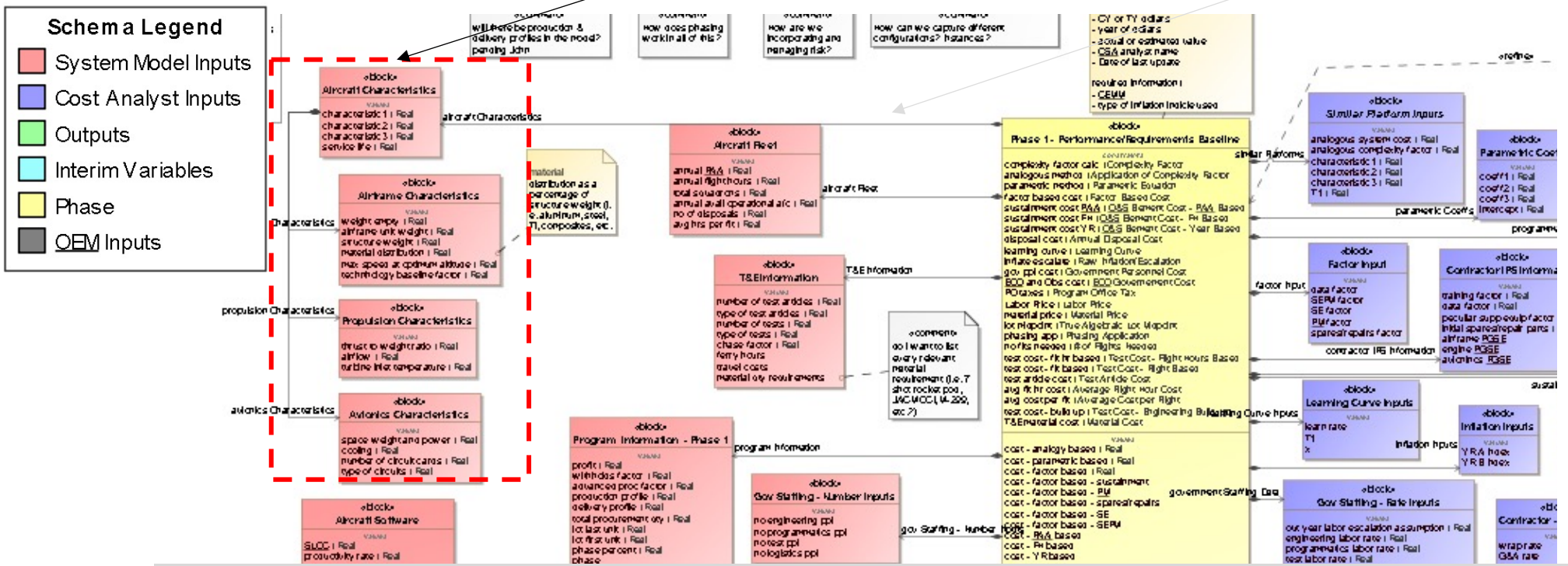
Automate Cost Estimates as Technical Data Changes

- Cost rollup changes based on the fidelity of the data, generally related to overall program phase
  - Phase 1: Simple analogy and historical (SRR1)
  - Phase 2: Analogy and parametric (SRR2)
  - Phase 3: Engineering buildup (PDR/CDR)
  - Phase 4: Extrapolation of actuals (Prod)
- Approach
  - Use cost analysis patterns which relate to technical data fidelity, tracking contractor cost over the program lifecycle
  - Cost estimation approach is tailored by the fidelity of data on hand

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Cost Model Schema (v58)

Deep Dive on Aircraft Characteristics
(see next slide for details)



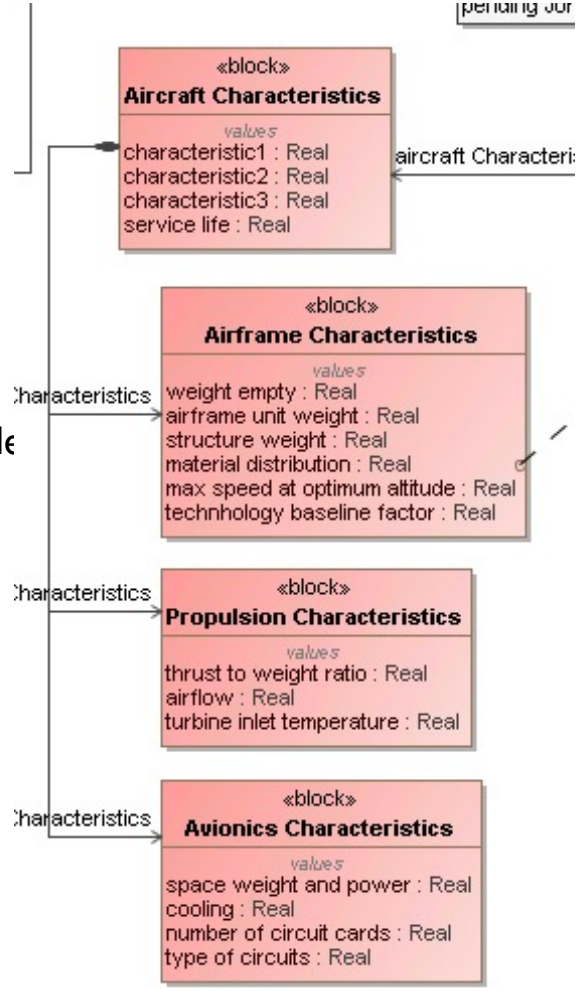
Observations based on Version #58 of AURA MBSE Cost Model

- Schema captured, identify cost analysis inputs, outputs, and phases
- Approach documented MIL-STD-881 relationships
- Rollup patterns were early in concept, not high in fidelity

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

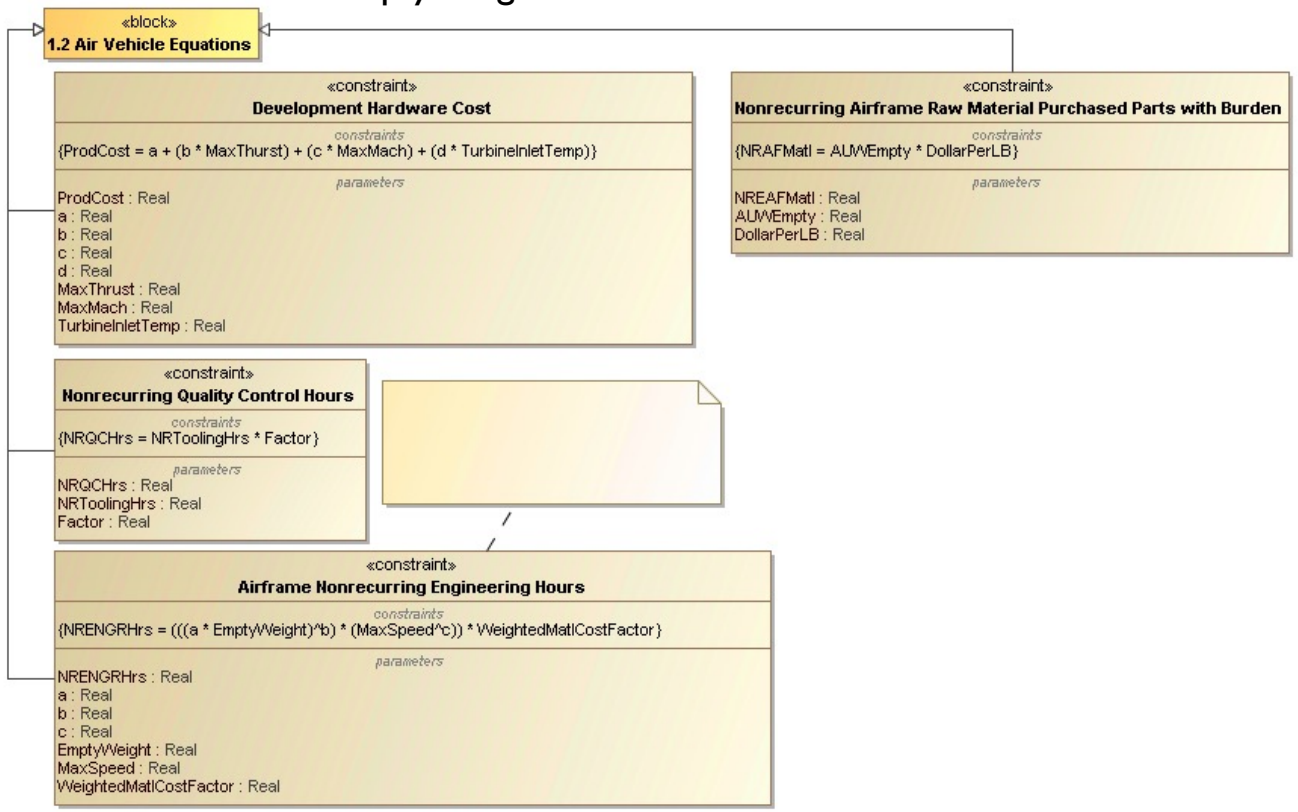
Deep Dive Focused on Aircraft Characteristics and Equations

- Airframe characteristics
  - Weight empty
  - Airframe unit weight
  - Structure weight
  - Material distribution
  - Max speed at optimum altitude
- Propulsion characteristics
  - Thrust to weight ratio
  - Airflow
  - Turbine inlet temperature
- Avionics characteristics
  - Space weight and power
  - Cooling
  - Number of circuit cards
  - Type of circuits



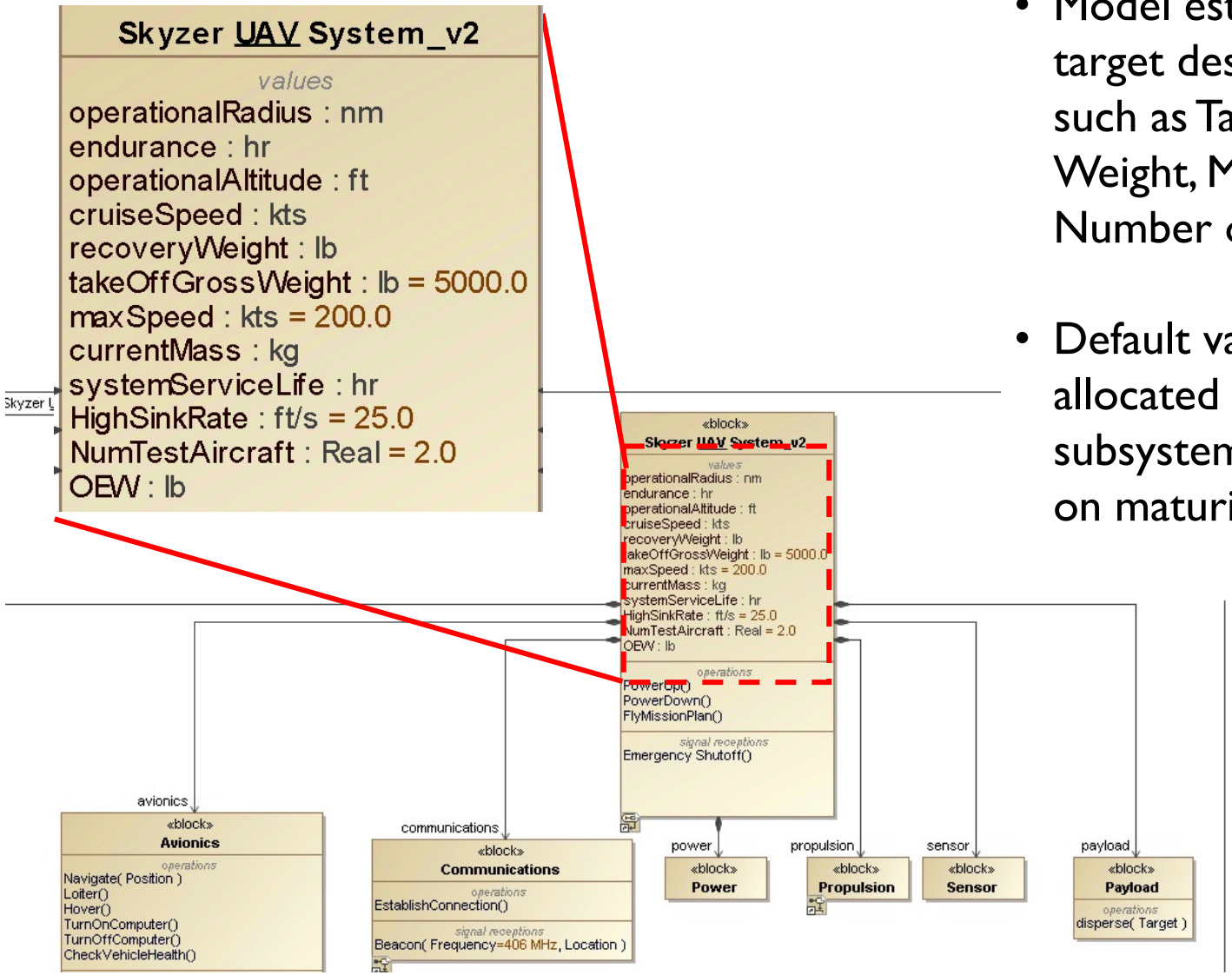
Air vehicle parameters of interest

- MaxMach
- MaxSpeed
- MaxThrust
- EmptyWeight



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

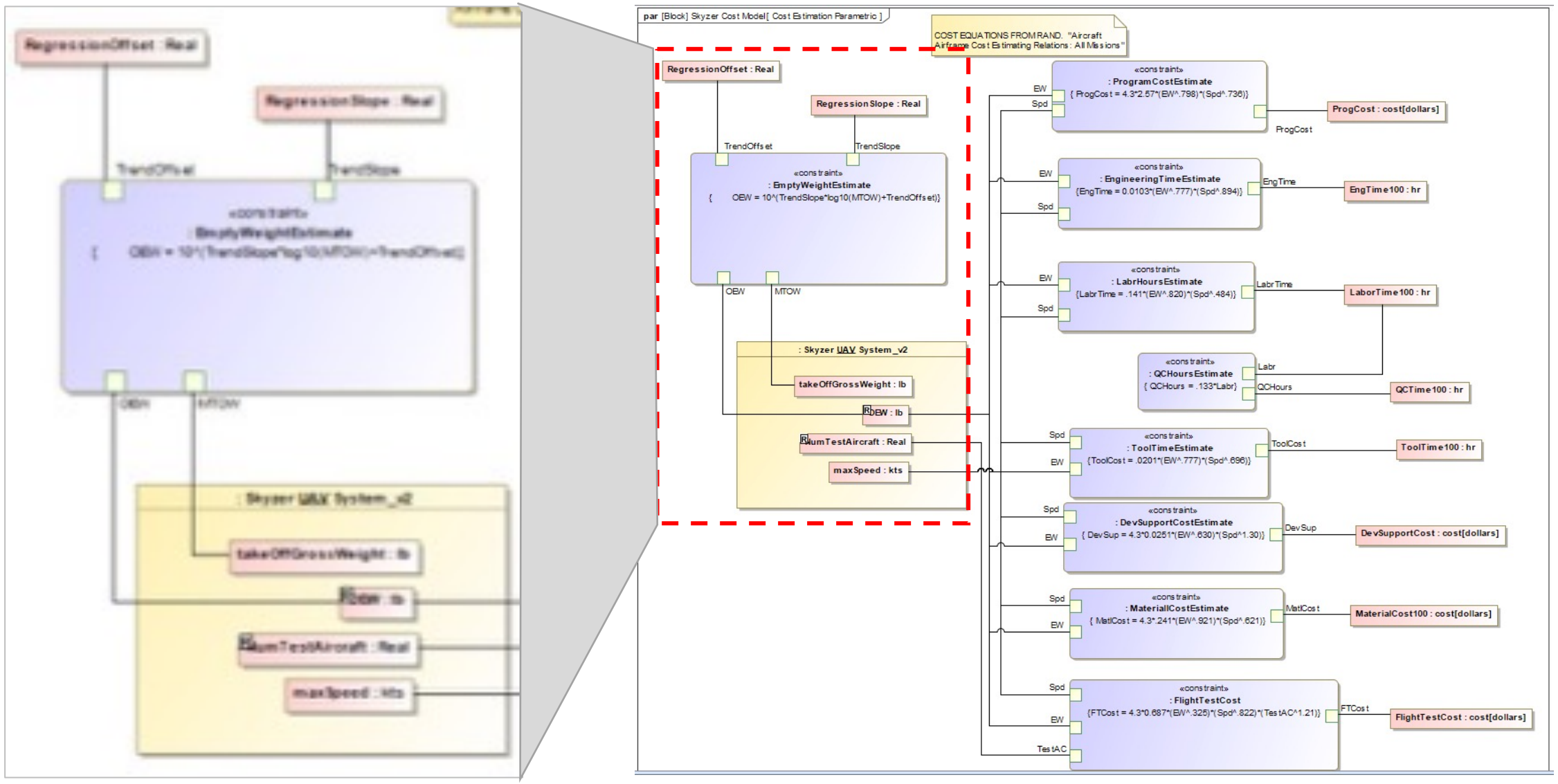
SRR1 - Model Development



- Model established with target design constraints, such as Take Off Gross Weight, Max Speed, and Number of Test Aircraft
- Default values can be allocated or inherited from subsystem blocks, depending on maturity of the design

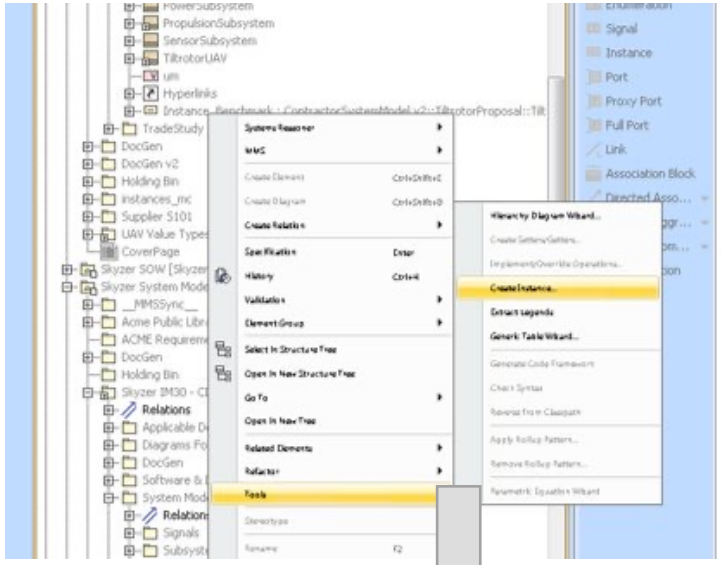
NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Cost Equations (Surrogate or Actual)



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

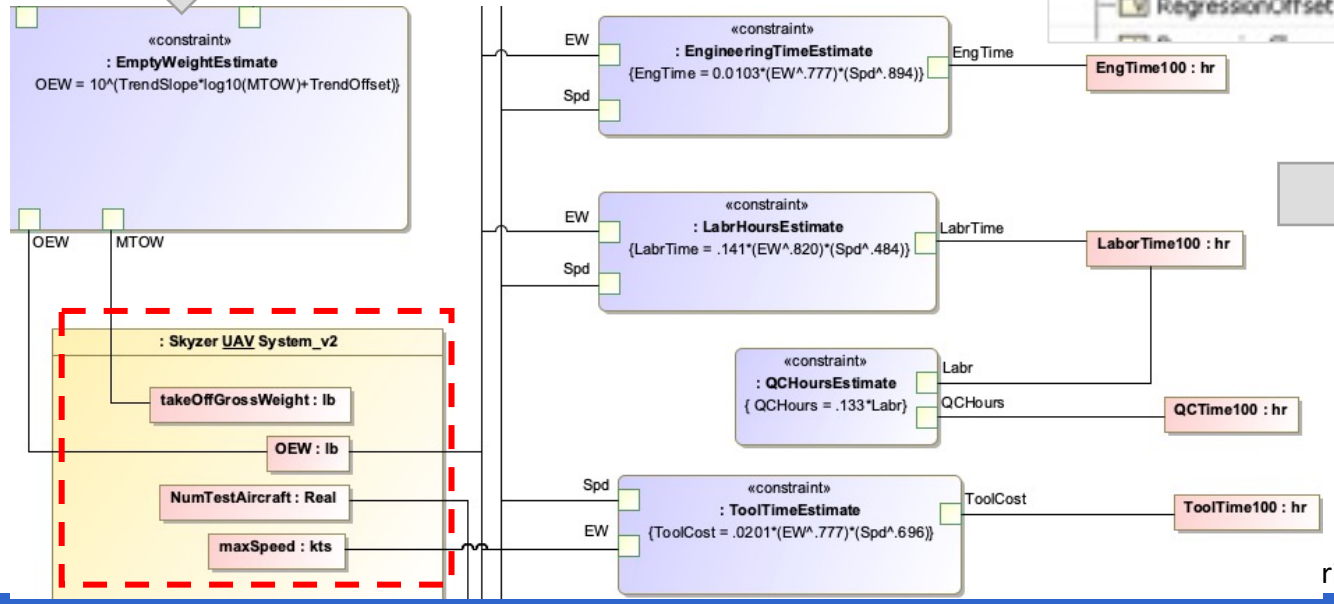
SRR1 – Model Instance in Cost Model



Create instances of for technical model in Cost Model, establishing source of truth data for cost model

Name	Value
Skyzer Cost Model	Skyzer Cost Model
DevSupportCost : cost[dollars]	14740.4671
EngTime100 : hr	517.9189
FlightTestCost : cost[dollars]	6794.6236
LaborTime100 : hr	1131.2535
MaterialCost100 : cost[dollars]	37913.4148
ProgCost : cost[dollars]	2.8362E5
QCTime100 : hr	150.4567
RegressionOffset : Real	-0.0870

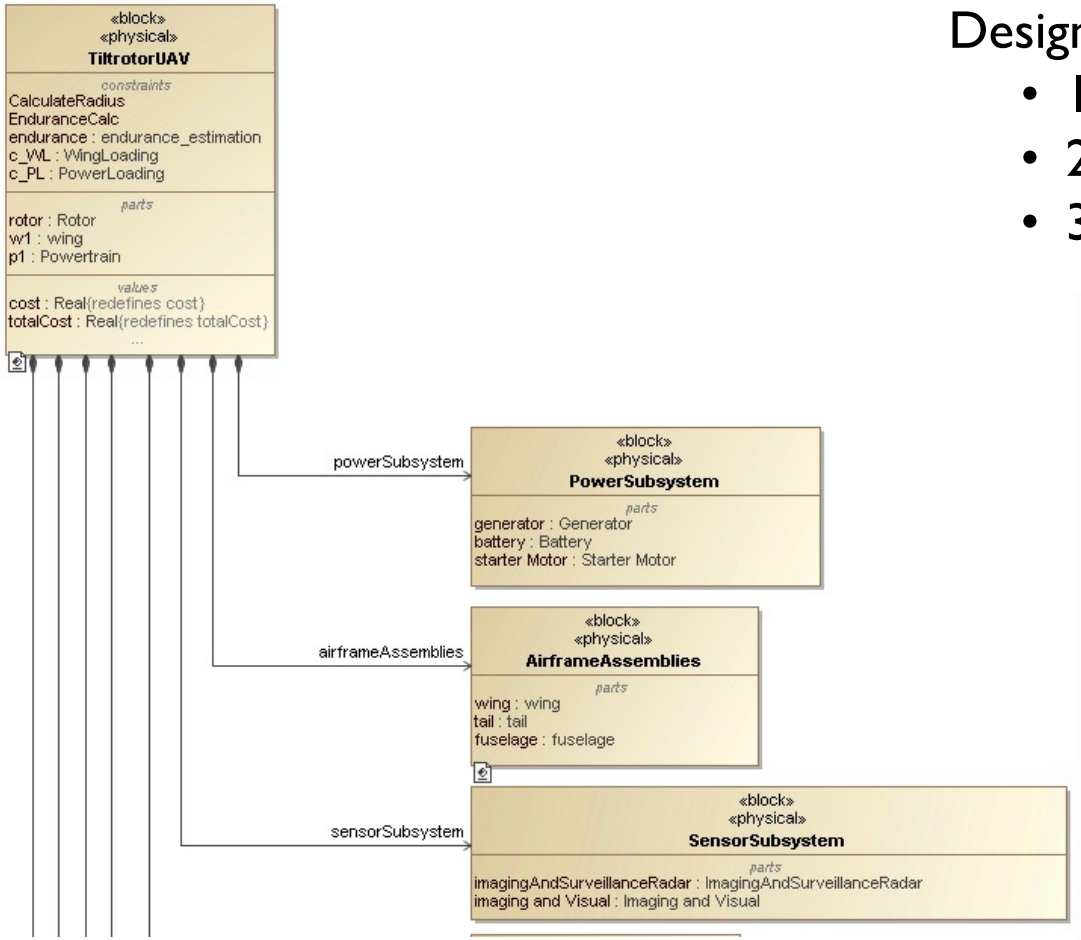
Parametric Rollup



Run parametric simulation for cost methodology model to determine system cost estimates, such as development support cost

ribution is unlimited"

SRR2 – Cost Rollup Pattern based on RFP Model



Design trades

- 1) Subsystem/component cost data organization
- 2) Project use relationship
- 3) Rollup cost pattern ownership

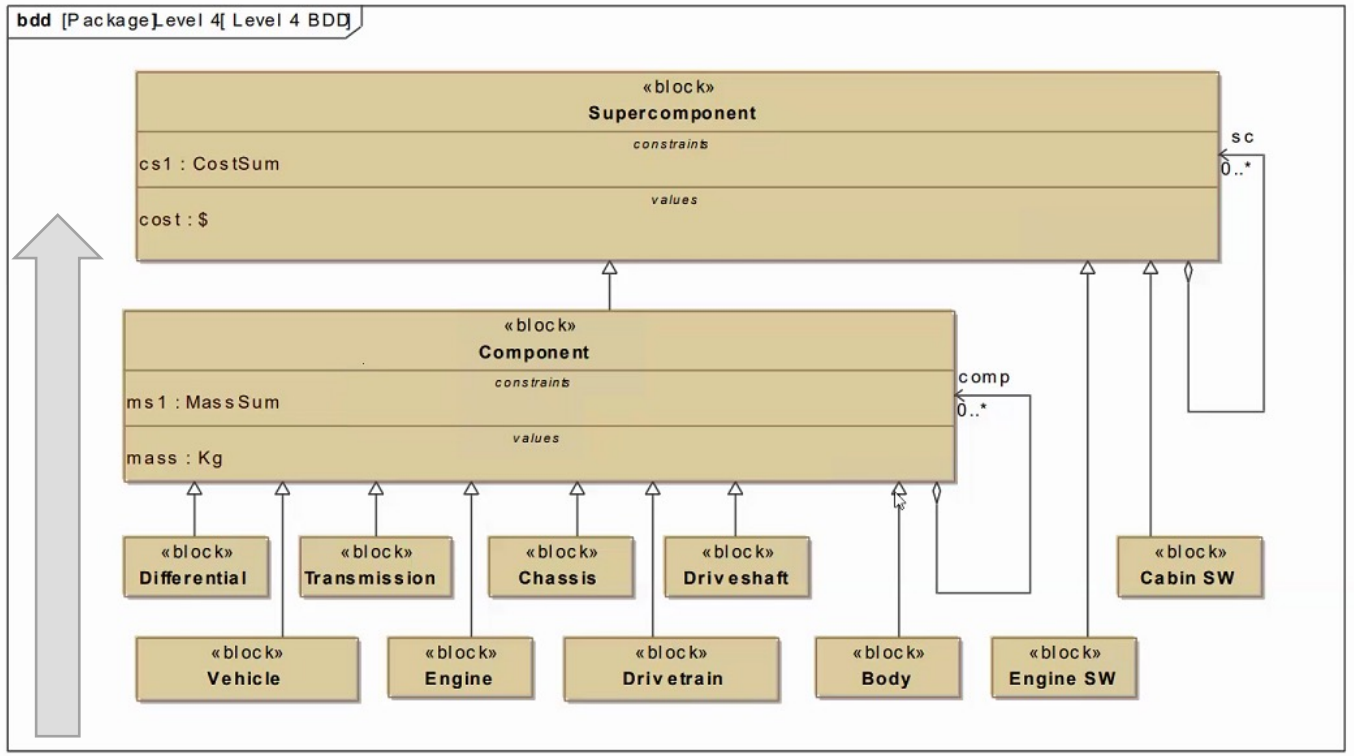
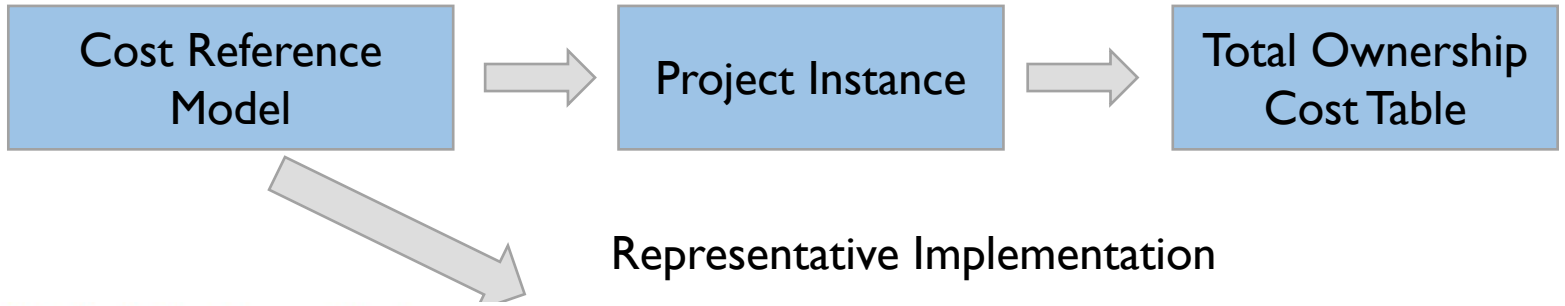


Figure 16 Two levels of Inheritance for Roll-up Calculations

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Total Ownership Cost Approach



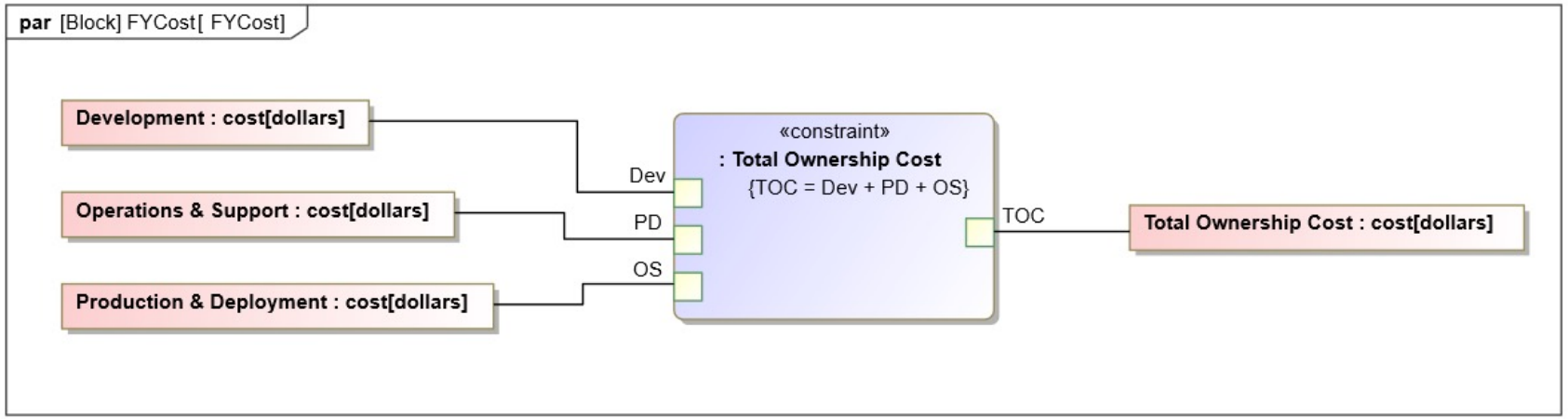
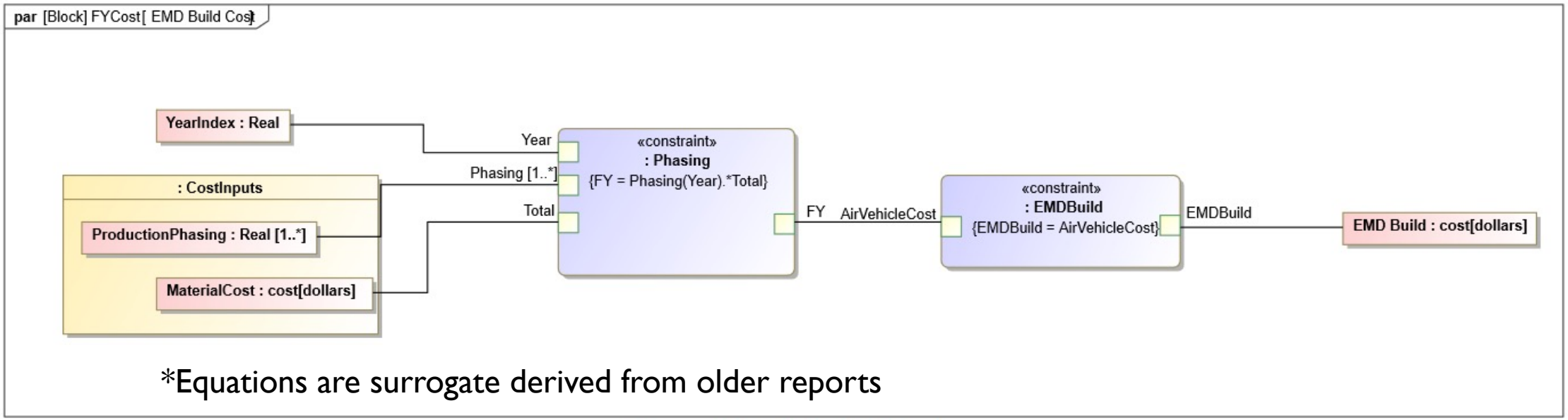


Figure 12. Methodology

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

EMD Build Cost – Example Parametric Equation*

Inputs link back to contractor model



*Equations are surrogate derived from older reports

Figure 14. EMD Build Cost

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

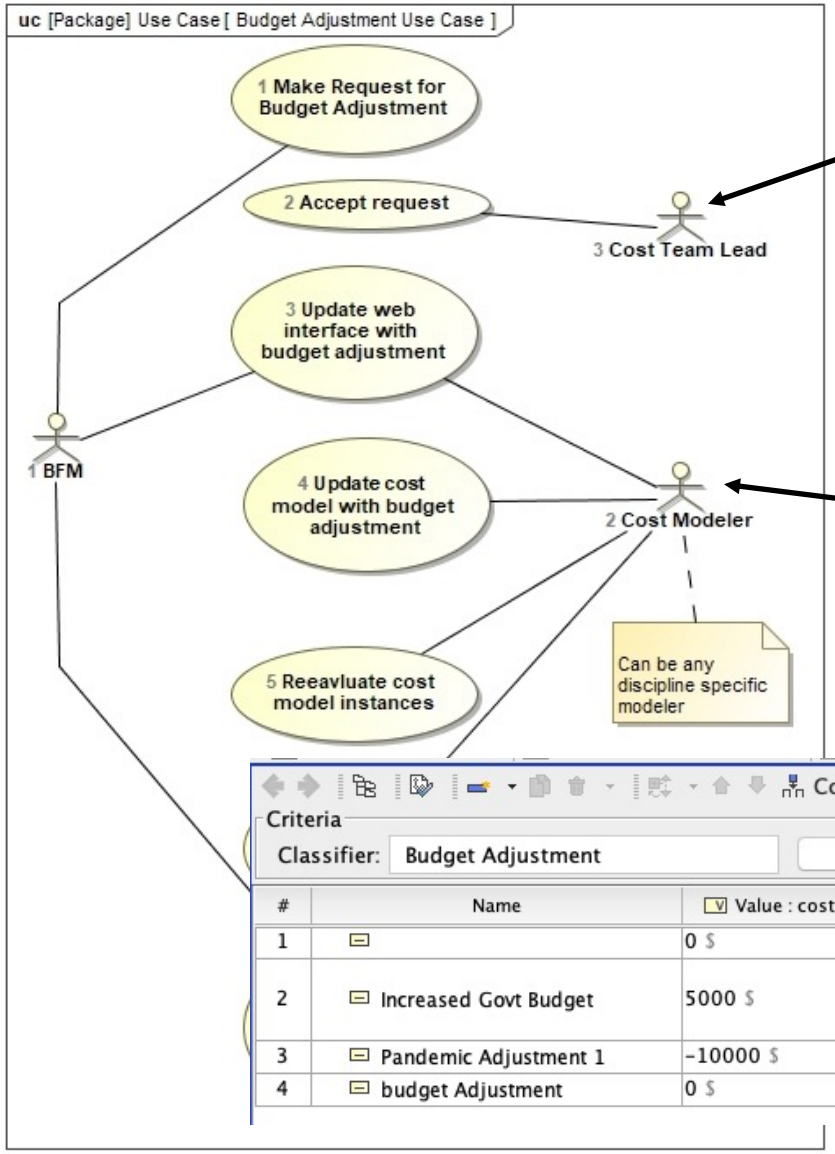
Generation of Total Ownership Cost Table

#	Name	Total Ownership Cost : cost[dollars]	Development : cost[dollars]	EMD Design : cost[dollars]	EMD Build : cost[dollars]	Production & Deployment : cost[dollars]	Test & Evaluation : cost[dollars]	Operations & Support : cost[dollars]
1	FY2020	69411.66 $	31109.62 $	29003.46 $	1516.54 $	38302.05 $	589.62 $	0 $
2	FY2021	173529.15 $	77774.04 $	72508.65 $	3791.34 $	95755.11 $	1474.05 $	0 $
3	FY2022	240877.15 $	106819.99 $	101512.11 $	5307.88 $	134057.16 $	0 $	0 $
4	FY2023	275288.17 $	122079.99 $	116013.84 $	6066.15 $	153208.18 $	0 $	0 $
5	FY2024	275288.17 $	122079.99 $	116013.84 $	6066.15 $	153208.18 $	0 $	0 $
6	FY2025	240877.15 $	106819.99 $	101512.11 $	5307.88 $	134057.16 $	0 $	0 $
7	FY2026	189260.62 $	83929.99 $	79759.52 $	4170.48 $	105330.62 $	0 $	0 $
8	FY2027	120438.58 $	53410 $	50756.06 $	2653.94 $	67028.58 $	0 $	0 $
9	FY2028	86027.55 $	38150 $	36254.33 $	1895.67 $	47877.56 $	0 $	0 $
10	FY2029	51616.53 $	22890 $	21752.6 $	1137.4 $	28726.53 $	0 $	0 $

TOC reviewable from ViewEditor, removing stakeholder navigation of containment tree (NOT Actual Data)

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Budget Adjustment Use Case - (See Video)



The Actors are Roles

(Discipline-Specific Modeler)

Walkthrough scenario for demo

Columns | Export

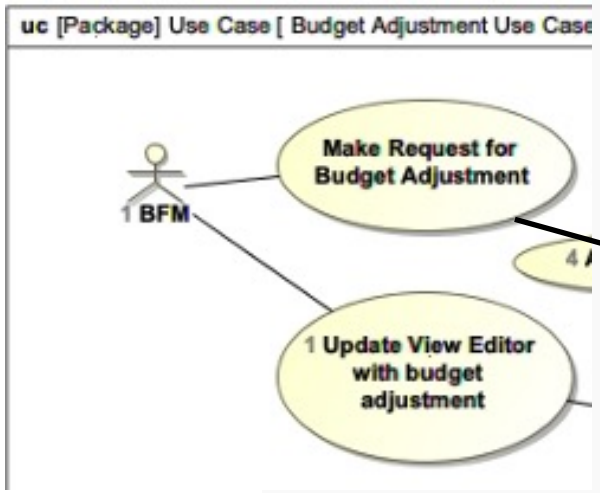
Criteria

Classifier: Budget Adjustment ... Scope (optional): Budget Adjustment Instances ... Filter:

#	Name	Value : cost[dollars]	Reasoning : String	Date : String	Adjustor : String	From : String	To : String
1		0 $					
2	Increased Govt Budget	5000 $	Increased Government Spending	2022	Program	2024	2026
3	Pandemic Adjustment 1	-10000 $	COVID-19 Pandemic	2020	Taylor Fields	2020	2022
4	budget Adjustment	0 $					

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Budget Financial Manager



Surrogate Pilot Switch Org | Search selected project | UAT

oject: Skyzer Cost Model › Budget Adjustments | Branc

Filter table of contents

- Budget Adjustments
  - 1 Adjustment Summary Table

DOCLIB

Document Last Modified: 2/11/21 5:04 PM

Budget Adjustments

Last Modified: 2/9/21 2:40 PM by **taylor.fields**

1 Adjustment Summary Table

Last Modified: 2/11/21 5:04 PM by **taylor.fields**

EXPORT CSV | FILTER TABLE

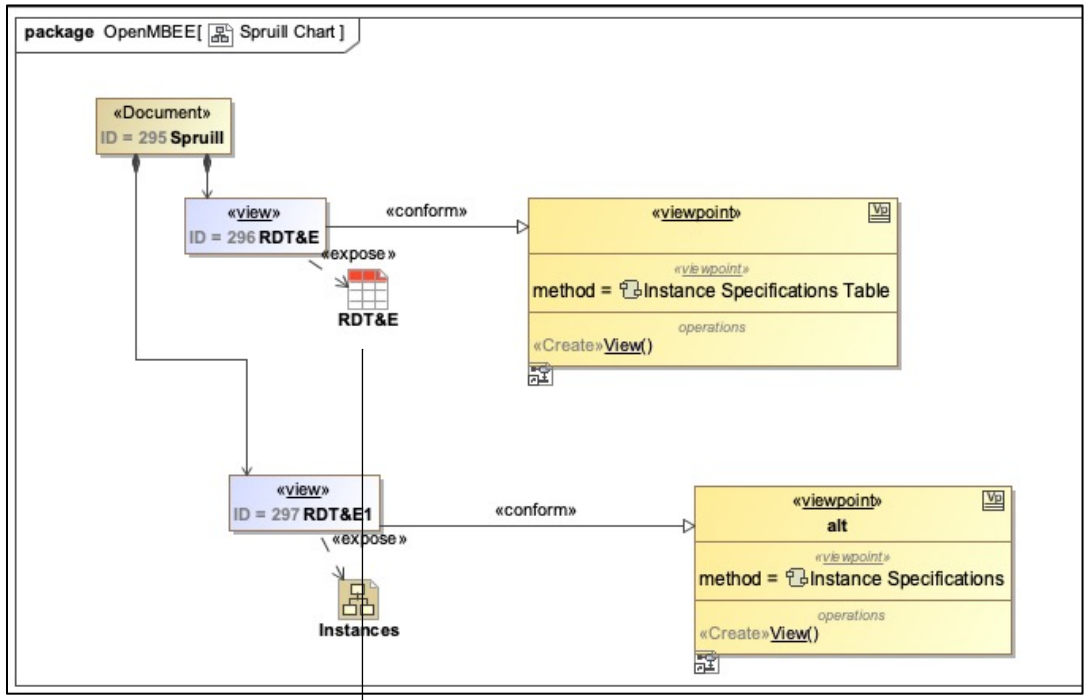
Table 1. <>

Budget Adjustment	Adjustor	Date	Reasoning	Value	From	To
(no name)	(no value)	(no value)	(no value)	0.0		
budget Adjustment	(no value)	(no value)	(no value)	0.0	(no value)	(no value)
Increased Govt Budget	Program	2022	Increased Government Spending	5000.0	Value : 2024 ADD	2026
Pandemic Adjustment 1	Taylor Fields	2020	COVID-19 Pandemic	-10000.0	2020	2022

Used DocGen and Excel for Synchronization

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

OpenMBEE DocGen/Cameo Publisher



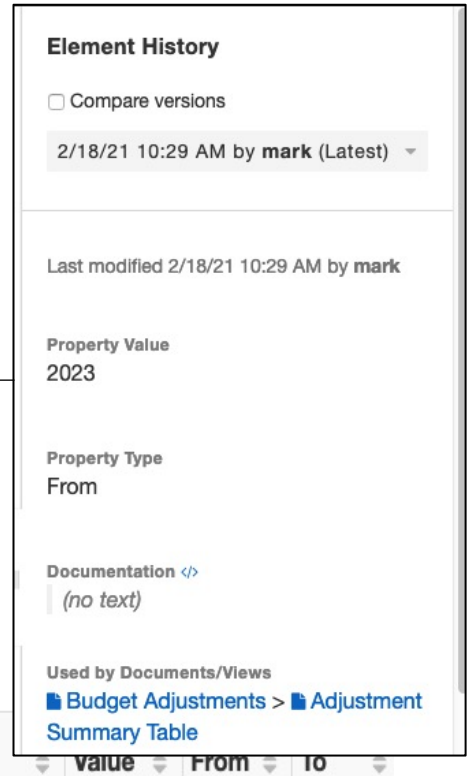


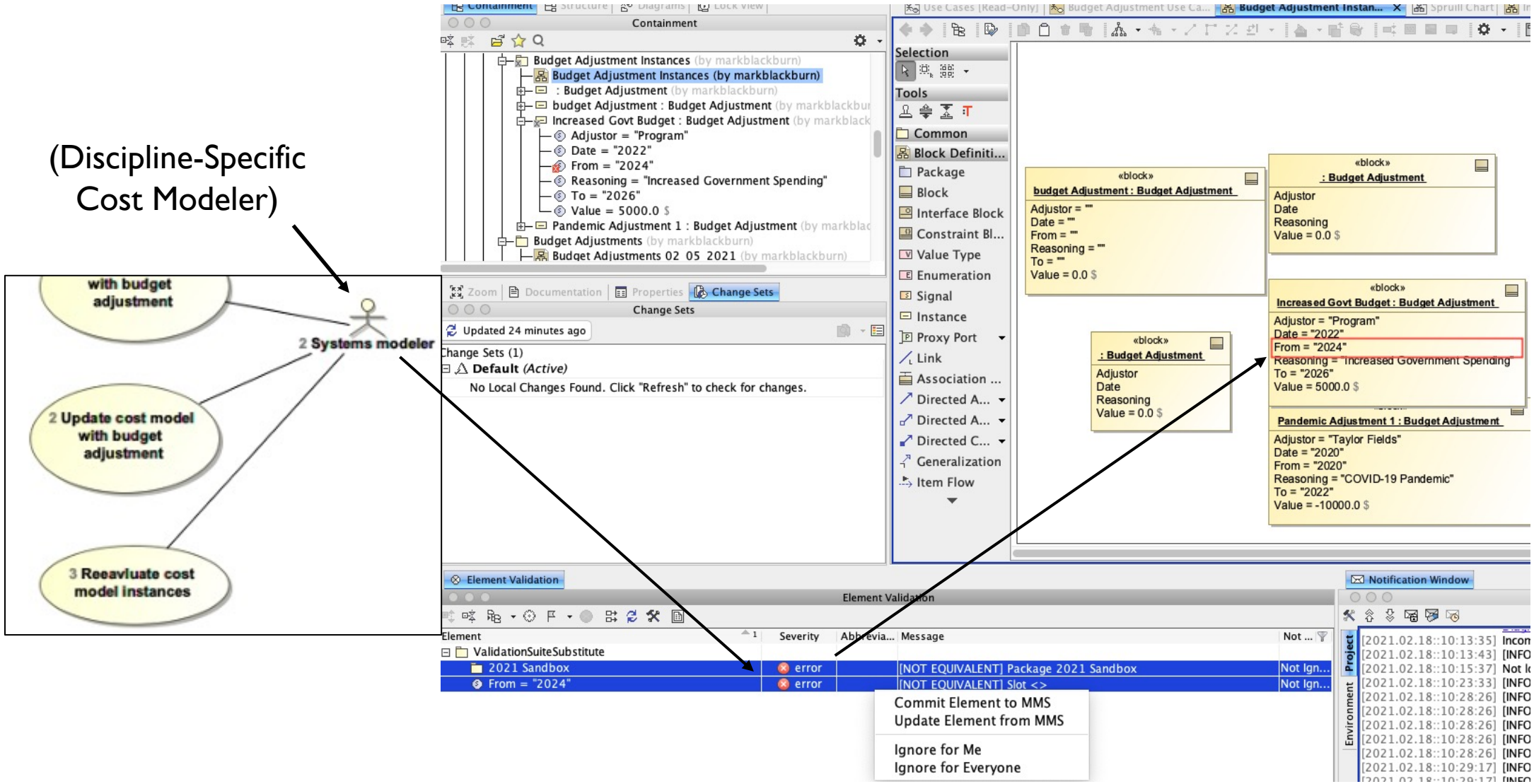
Table 1. <>

Budget Adjustment	Adjustor	Date	Reasoning	Value	From	To
(no name)	(no value)	(no value)	(no value)	0.0		
budget Adjustment	(no value)	(no value)	(no value)	0.0	(no value)	(no value)
Increased Govt Budget	Program	2022	Increased Government Spending	5000.0	2023	2026
Pandemic Adjustment 1	Taylor Fields	2020	COVID-19 Pandemic	-10000.0	2020	2022

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

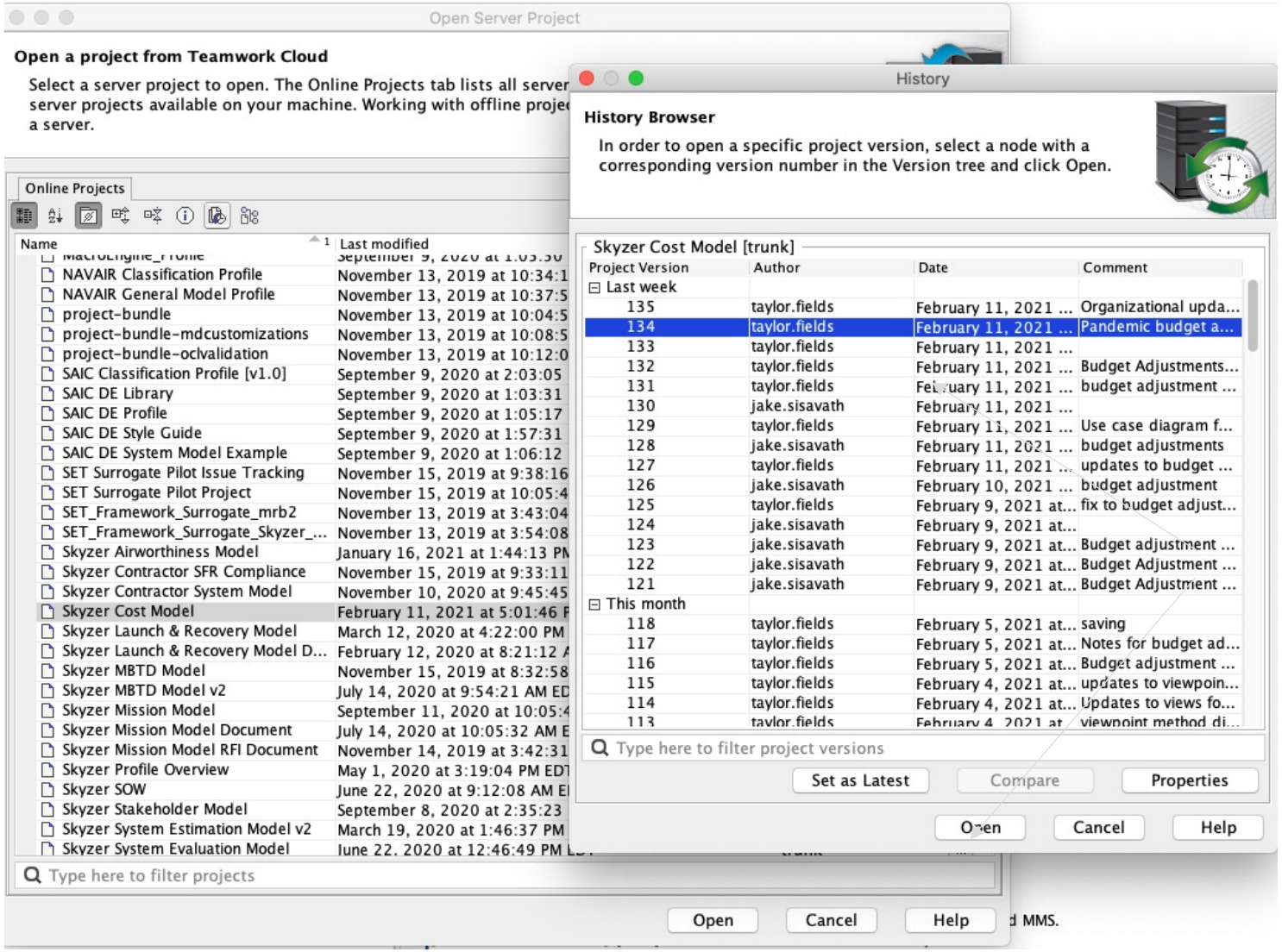
Final Synchronization Done in Model to Establish Authoritative Source of Info

(Discipline-Specific Cost Modeler)



NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Actual Commit by Role With Additional/Appropriate Privileges

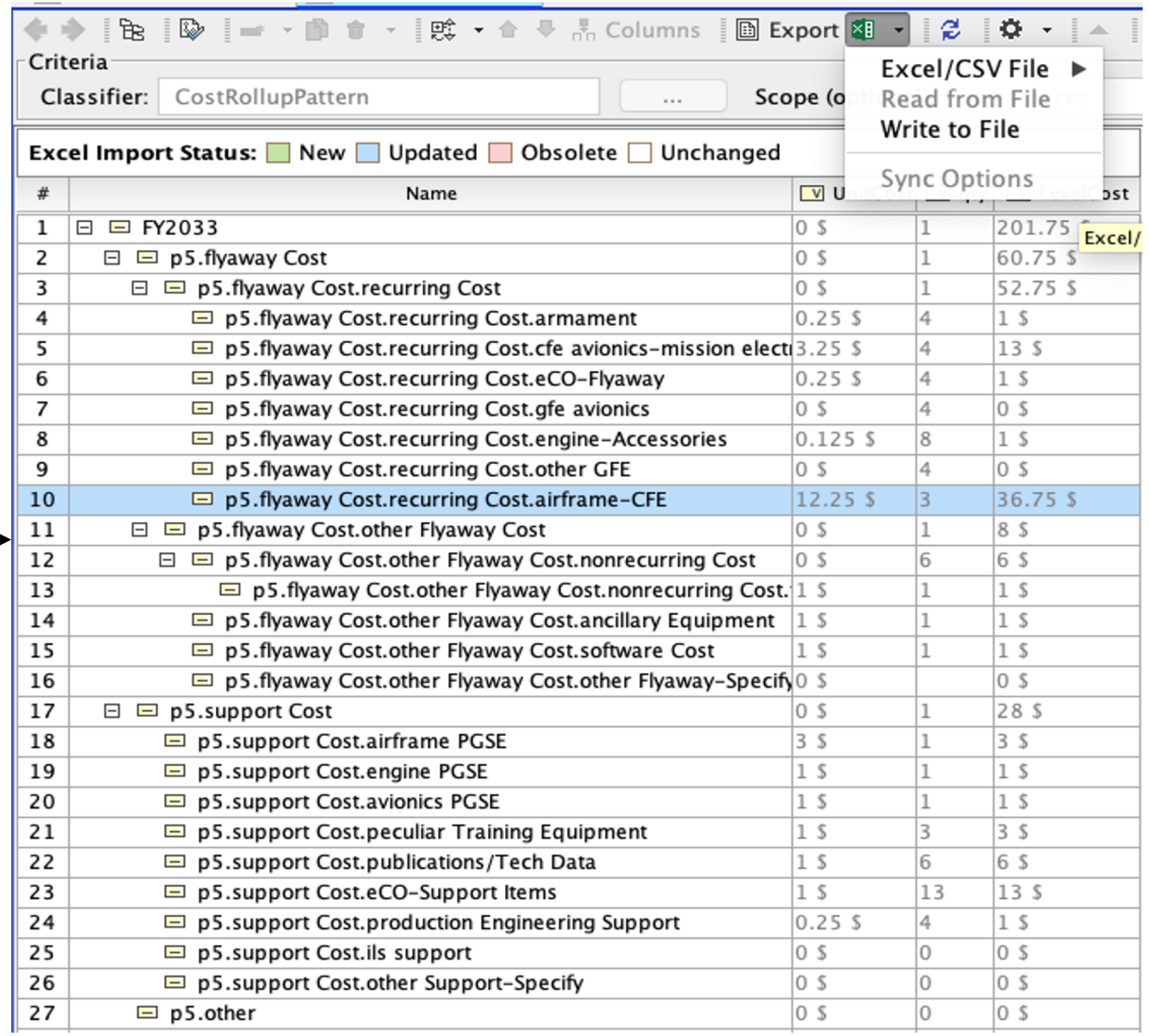


We can rollback

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Update to P-5 Rollup

Can do updates in exported Excel Spreadsheet and Synchronize back into Model for Commit



#	Name	U		ost
1	FY2033	0 $	1	201.75 $
2	p5.flyaway Cost	0 $	1	60.75 $
3	p5.flyaway Cost.recurring Cost	0 $	1	52.75 $
4	p5.flyaway Cost.recurring Cost.armament	0.25 $	4	1 $
5	p5.flyaway Cost.recurring Cost.cfe avionics-mission electi	3.25 $	4	13 $
6	p5.flyaway Cost.recurring Cost.eCO-Flyaway	0.25 $	4	1 $
7	p5.flyaway Cost.recurring Cost.gfe avionics	0 $	4	0 $
8	p5.flyaway Cost.recurring Cost.engine-Accessories	0.125 $	8	1 $
9	p5.flyaway Cost.recurring Cost.other GFE	0 $	4	0 $
10	p5.flyaway Cost.recurring Cost.airframe-CFE	12.25 $	3	36.75 $
11	p5.flyaway Cost.other Flyaway Cost	0 $	1	8 $
12	p5.flyaway Cost.other Flyaway Cost.nonrecurring Cost	0 $	6	6 $
13	p5.flyaway Cost.other Flyaway Cost.nonrecurring Cost.	1 $	1	1 $
14	p5.flyaway Cost.other Flyaway Cost.ancillary Equipment	1 $	1	1 $
15	p5.flyaway Cost.other Flyaway Cost.software Cost	1 $	1	1 $
16	p5.flyaway Cost.other Flyaway Cost.other Flyaway-Specify	0 $		0 $
17	p5.support Cost	0 $	1	28 $
18	p5.support Cost.airframe PGSE	3 $	1	3 $
19	p5.support Cost.engine PGSE	1 $	1	1 $
20	p5.support Cost.avionics PGSE	1 $	1	1 $
21	p5.support Cost.peculiar Training Equipment	1 $	3	3 $
22	p5.support Cost.publications/Tech Data	1 $	6	6 $
23	p5.support Cost.eCO-Support Items	1 $	13	13 $
24	p5.support Cost.production Engineering Support	0.25 $	4	1 $
25	p5.support Cost.ils support	0 $	0	0 $
26	p5.support Cost.other Support-Specify	0 $	0	0 $
27	p5.other	0 $	0	0 $

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Video Shows Demonstration for Several Scenarios

- Walkthrough Skyzer Cost Model
- Discuss Model Organization and Navigation
- Look at a few scenarios
  - Cost roll-up pattern
  - Mechanisms that allow subject matter experts to adjust cost values through using Export/Import spreadsheet that are synchronized back into the Cost Model
  - Automated cost equation substitution
- Check *Systems Engineering Research Center YouTube* for Video to be posted

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Accomplishments

- Demonstrated Cost Model Stakeholder Analysis Model linked to Skyzer technical models for cost model criteria, relationships and to generate various reports
- Demonstrated how standard cost-estimating relationships (CERS) and methodologies (CEMs) are applied to these models
- Used technical data for parametric total ownership cost (TOC) estimates
- Aligned MBSE Cost Model with with MIL-STD-881E
- Automatically generated reports (e.g., P-5 sheet, Spruill Charts)
- Demonstrated approach for Cost Model modularization (e.g., Project Usages) for access and control
- Ready to initiate on small number of DoD programs as trials

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Thank you!

- Dr. Mark Blackburn
- Senior Research Scientist
- Principal Investigator
- Member of SERC Research Council
- Member of OpenMBEE Leadership Team
- School of Systems & Enterprises
- Systems Engineering Research Center
- Stevens Institute of Technology

NAVAIR Public Release 2021-807 Distribution Statement A - "Approved for public release; distribution is unlimited"

Technology and Program Protection Resilient Systems Overview

Melinda Reed
Director, Resilient Systems
Office of the Under Secretary of Defense for Research and Engineering

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

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

The Challenge

The Challenge

Problem: Cyber threats are outpacing weapon system designs for safe, effective, resilient, secure operations; lack engineering bench for secure cyber resilient engineering design decisions

- Policy compliance / requirements derivation
- Cyber risk aversion / technical implication
- Legacy system compatibility

The Portfolio

Strategic and Tactical

Legislation: Inform cybersecurity/supply chain actions

Regulation: Influence outcomes to reduce burden

Policy: Enable tailoring to support warfighter needs

Procedures: Inclusive of engineering requirements

Guidance: Expand S&T manager and engineer knowledge

Workforce: Grow engineering cyber expertise

Risk Assessment: Refine technical assessment approaches



PARTNERS
Industry
Interagency
International
OSD Stakeholders
Military Services
PEO
PM

Key Engineering Cyber/Program Protection Initiatives

- Secure cyber resilient engineering primer and standards
- Influence EO 14028 Enhancing Software Supply Chain Security
- Safeguarding unclassified controlled technical information implementation
- Enhance software supply chain security, including through the Joint Federated Assurance Center
- Provide tools to tailor technology and program protection planning for technical workforce
- Creation of Secure Cyber Resilient Engineering Credential Program / updates to program protection courseware at DAU
- Expand safeguarding requirements for critical programs



Ideal End State

1. Knowledgeable engineering bench
2. Measurable test outcomes
3. Informed technical design decisions across levels of application
4. Tailored to operational needs with clear, concise implications
5. Reduced burdensome compliance activities
6. Innovative mitigations for fielded systems

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Strategic Technology Protection & Exploitation



Deputy Director
Strategic Technology Protection & Exploitation (STP&E)
Dr. Robert Irie

D, Maintaining Technology Advantage
Dr. Jesse Appler



Maintain Leadership in Critical Technology Modernization Areas

- Implement new procedures for Technology Area Protection
- Update DoD and Government-wide procedures to strengthen U.S. research enterprise
- Mitigate exploitation in academia, labs, FFRDCs, and UARCs
- Focus security, counterintelligence, and law enforcement actions to deter adversaries

D, Resilient Systems
Ms. Melinda Reed



Foster Assured Resilient Missions, Systems and Components

- Set the technical and policy direction for technology and program protection
- Grow DoD capability/capacity to evaluate and mitigate software component vulnerabilities
- Establish secure cyber resilient weapons, engineering methods and workforce competency

D, Technology and Manufacturing Industrial Base
Mr. Robert Gold



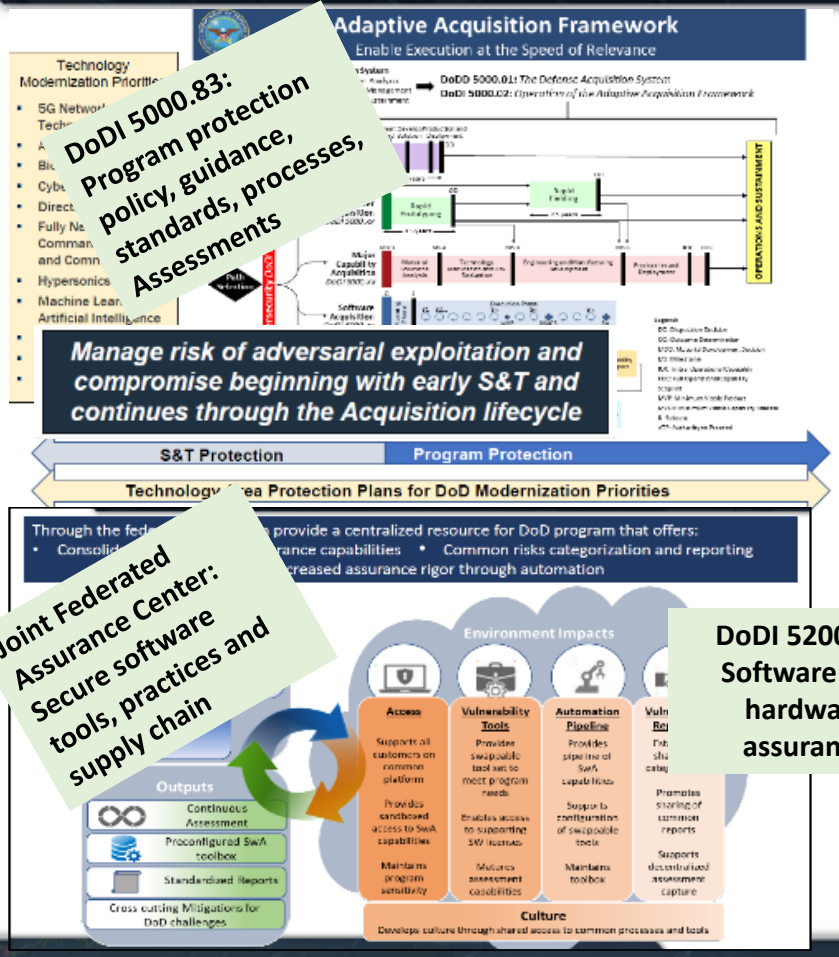
Advance Domestic Innovation Base to Deliver Modernization Goals

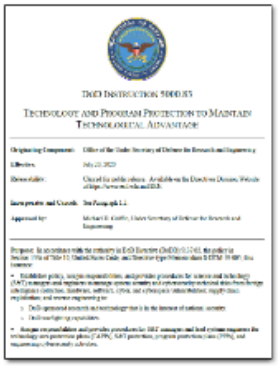
- Assess and monitor emerging technology, workforce, engineering, test, & infrastructure base
- Facilitate USG mechanisms and tools to close gaps, foster enabling domestic technology development and manufacturing capability, and counter strategic competitor actions
- Manage the OSD Manufacturing Technology program and Manufacturing Innovation Institutes

MISSION: Promote and protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through superior, assured, secure and resilient systems, and a healthy viable national security innovation base.

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Resilient Systems Initiatives

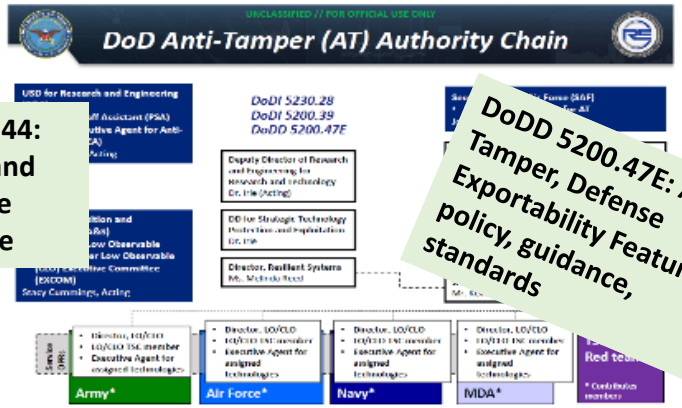




- Safeguard inform
- Control DoD-s research
- Design for s cyber resili
- Protect the s cyber attacks from enabling and supporting systems
- Protect fielded systems
- Enhance protection for critical programs and technologies

Secure Cyber Resilient Engineering (SCRE): requirements derivation, standards and workforce

Ability to deliver required capability in a secure manner under the presence of adverse conditions

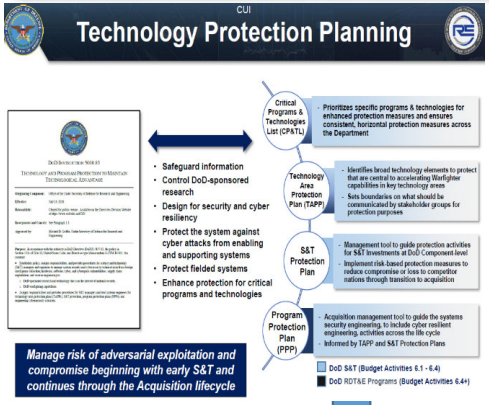


DoDI 5200.44: Software and hardware assurance

DoDD 5200.47E: Anti-Tamper, Defense Exportability Features: policy, guidance, standards

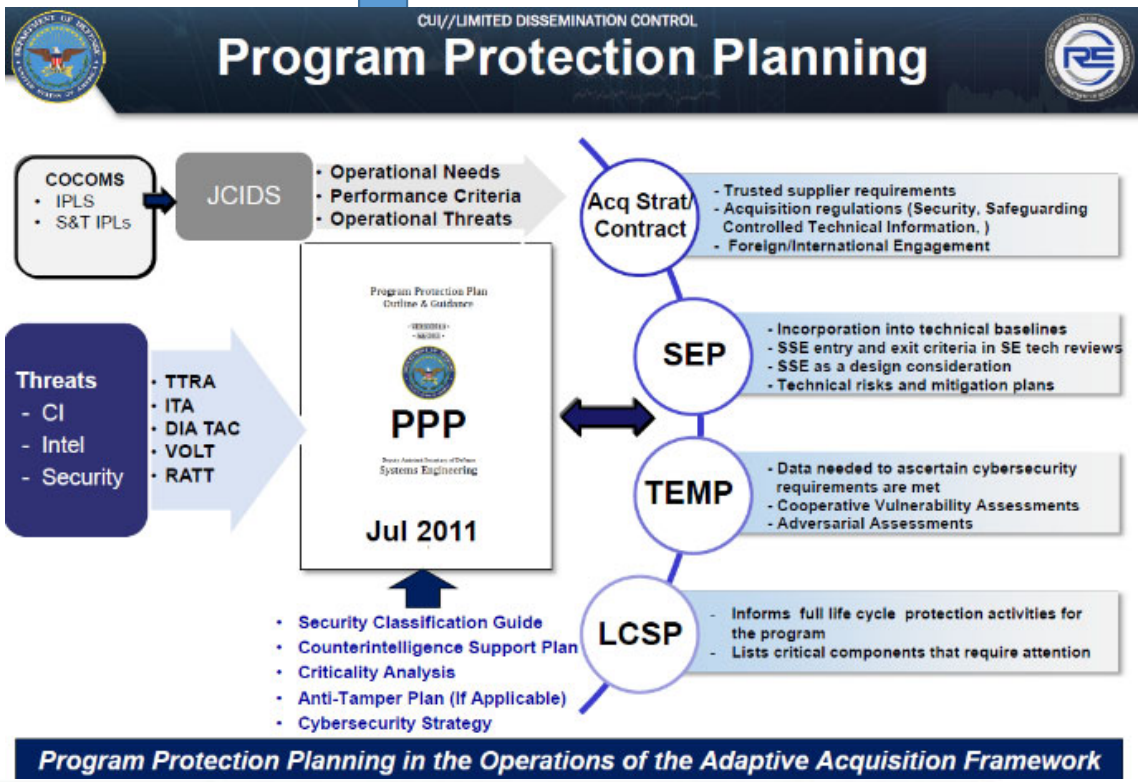
Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Program Protection
S&T and Acquisition Activities



- Provides mechanism to maintain and transition implemented protections applied in S&T
- Informs Secure Cyber Resilient Engineering Design trade off decisions

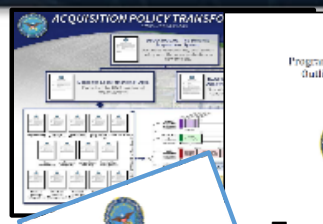
- Informs S&T protections



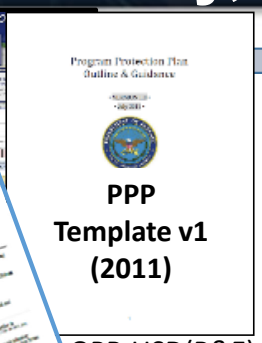
Program Protection Planning in the Operations of the Adaptive Acquisition Framework

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

DoDI 5000.83: Policy, Guidance, Transformation

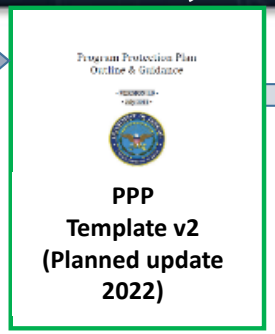


DoDI 5000.83: OPR: USD(R&E)/RS (2020)



PPP Template v1 (2011)

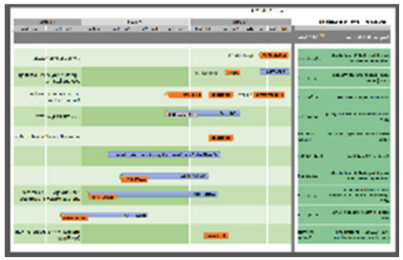
OPR:USD(R&E)/RS



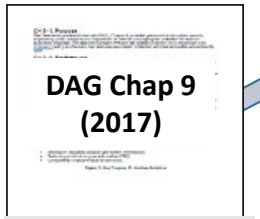
PPP Template v2 (Planned update 2022)

OPR:USD(R&E)/RS

PPP Review and Approval Process



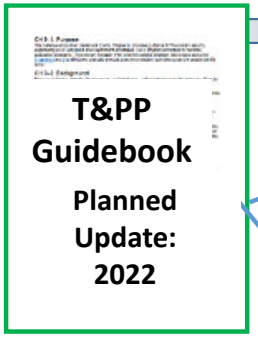
USD(R&E) Assessments for program protection and cyber technical risks



DAG Chap 9 (2017)

Guidance for DoDI 5000.02 Enclosure 13

OPR:USD(R&E)/RS



T&PP Guidebook

Planned Update: 2022

OPR:USD(R&E)/RS

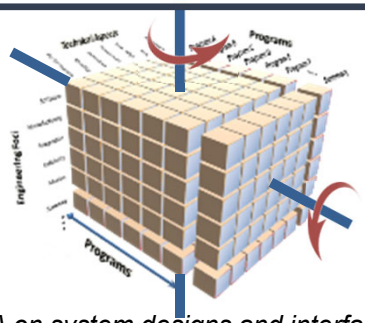
Guidance for S&T Managers and Engineers

OPR:USD(R&E)/MTA

S&T Protection Plan Outline and Guidance under development

Secure Cyber Resilient Engineering Primer under development

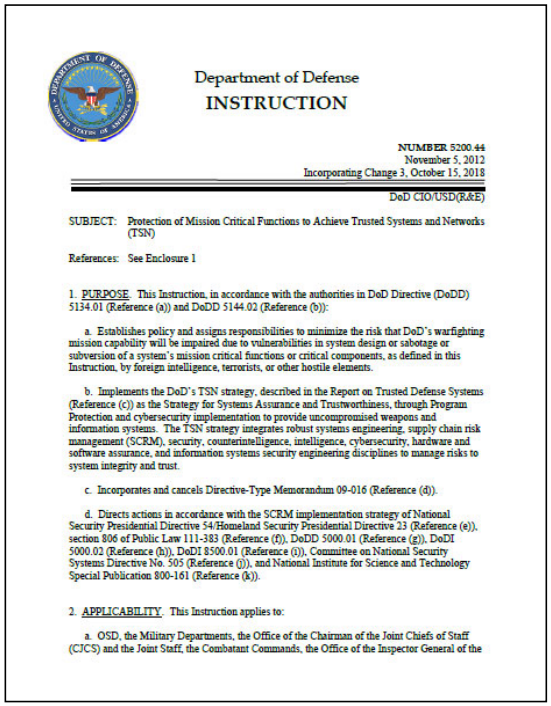
OPR:USD(R&E)/RS



"ITRA on system designs and interfaces for adversarial risks, program protection, and cyber vulnerabilities; results inform technical baselines and risk management activities."

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

DoDI 5200.44: Trusted Systems and Networks



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 3, October 15, 2018

DoD CIO/USD(R&E)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoDD 5000.01 (Reference (g)), DoDI 5000.02 (Reference (h)), DoDI 8500.01 (Reference (i)), Committee on National Security Systems Directive No. 505 (Reference (j)), and National Institute for Science and Technology Special Publication 800-161 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

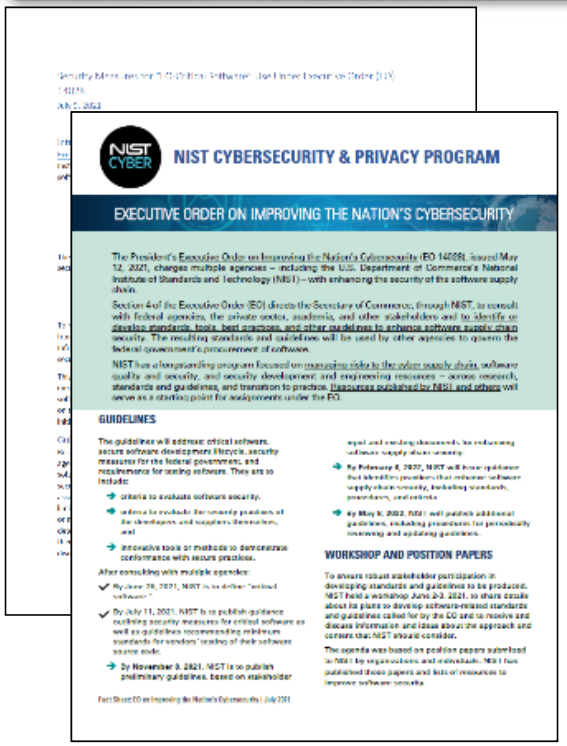
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing:**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
  - Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document planning and accomplishments in program protection and information assurance activities**

Draft update incorporates procedures to implement information communication technology (ICT) exclusion authorities, and quantitative assurance approach

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Executive Order (EO) 14028
Improving the Nation's Cybersecurity

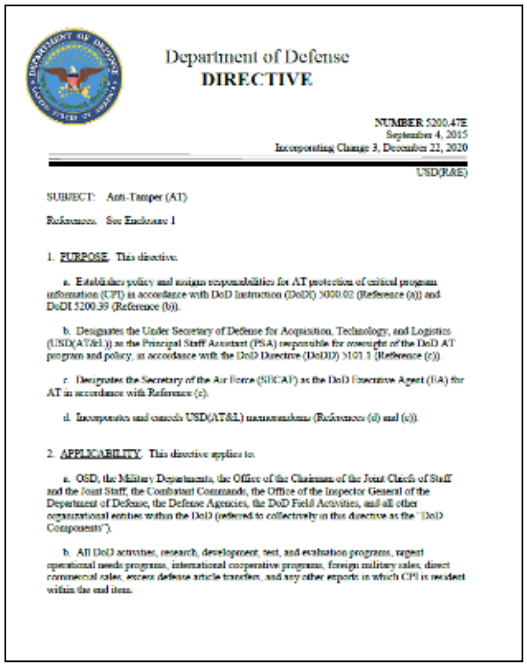


Partnerships with DHS and NIST

- **Section 4. Enhancing Software Supply Chain Security**
- **Sec. 4(n)**. Within 1 year of the date of this order, the **Secretary of Homeland Security**, in consultation with the **Secretary of Defense**, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language *requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section*.
- Resources published by NIST and others will serve as a starting point for assignments under the EO
  - Security Measures for "EO-Critical Software" use under EO 14028
  - Guidance/practices to enhance software supply chain security
  - The Minimum Elements For a Software Bill of Materials (SBOM)
  - Revision to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations; public comments due December 3, 2021

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

DoDD 5200.47E: Anti-Tamper/Defense Exportability Features



Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015
Incorporating Change 3, December 22, 2020
USD(R&E)

SUBJECT: Anti-Tamper (AT)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoD Instruction (DoDI) 5000.02 (Reference (a)) and DoDI 5200.39 (Reference (b)).

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, in accordance with the DoD Directive (DoDD) 5101.1 (Reference (c)).

c. Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with Reference (c).

d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

2. APPLICABILITY. This directive applies to:

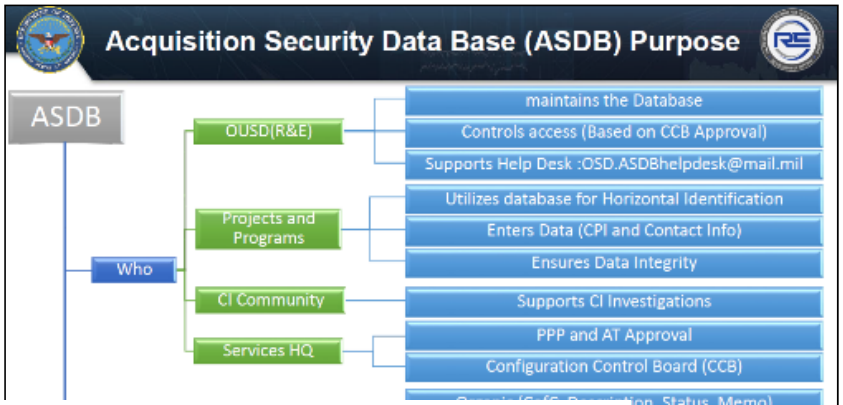
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD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

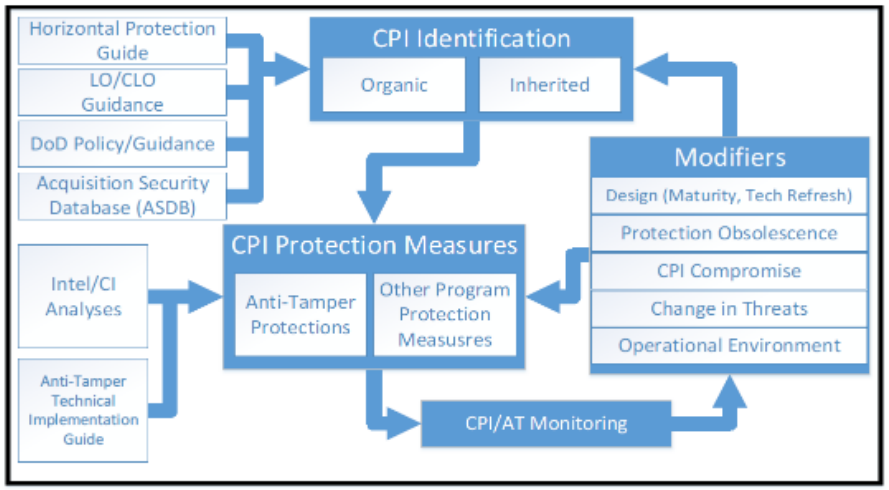
b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, export defense article transfers, and any other exports in which CPI is resident within the end item.

USD(R&E) is the PSA for Anti-Tamper

SECAF is the DoD Executive Agent for Anti-Tamper

Partnership with OUSD(A&S) International Cooperation





Draft update clarifies critical program information as technology advantage elements

Secure Cyber Resilient Engineering

Background

Goal: Improve resiliency of weapons system designs to cyber attack*

- ✓ **Action: Develop a new enclosure to DoD Instruction 5000.02 Operation of the Defense Acquisition System***
  - DoDI 5000.02, Enclosure 14 Cybersecurity in the Defense Acquisition System, 26 Jan 2017
- **Action: Review system security engineering design processes and methods and recommend standardization or other approaches to improve cybersecurity of designs***
  - DASD(SE), in partnership with the Services, Chief Information Officer (CIO), other stakeholders have identified multiple activities to improve security of engineering designs. An opportunity exists to collaborate, mature efforts, and move toward common approaches

Key Objectives:

- Determine set of engineering design patterns, standards and methods for cyber resilient weapon systems, addressing both systems in development and systems in sustainment
- Establish a foundation to grow the engineering practices and strengthen engineering agility

*extract from Better Buying Power 3.0 Implementation Guidance

DoD w

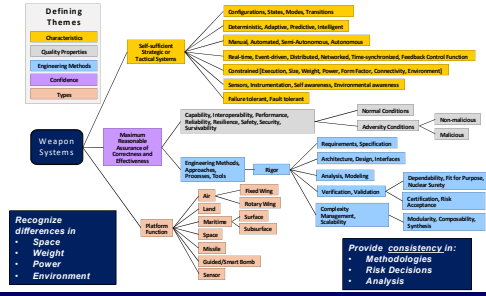
Implementing Cybersecurity into Weapons System Programs: Summary of Observations

- **PEOs, PMs are reporting that implementation is problematic**
  - Acquisition programs are seeking clear and specific cyber resiliency guidance
  - Risk Management Framework (RMF) for Information Technology (IT) governance and compliance schemes don't possess weapons and tactical domain expertise
- **Services and Agencies, PEOs/Programs, and Industry partners are each working to determine cyber resiliency solutions**
  - No common implementation of rules or principles; Solutions beginning to diverge
- **Operational Test community, Red Teams, COCOM exercises continue to identify vulnerabilities**
  - Findings in legacy systems indicate that cybersecurity must be designed in, not tested in, nor patched in
  - Developmental T&E is shifting left, Engineering needs to lay the foundation for the shift

Core Recurring Challenges		
Design Guidelines	Engineering Assessment	Implementation

Distribution Statement A – Approved for public release by DOPSR on 7/26/2018, SR Case # 18-S-1986 applies. Distribution is unlimited.

Weapon Systems Characteristics



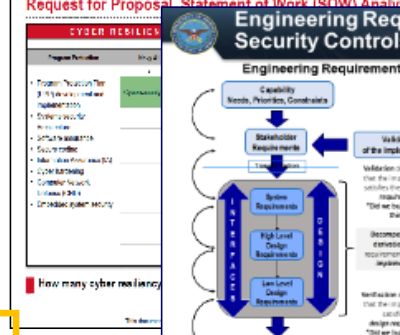
Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

A secure and cyber resilient system is one that can deliver required capability in a secure manner under the presence of adverse conditions

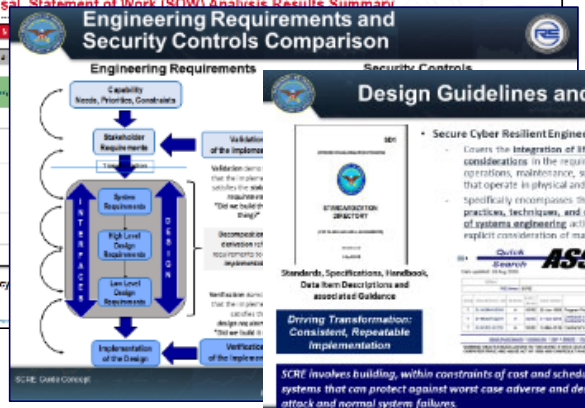
RFP SOW Analysis Results Summary

Raytheon

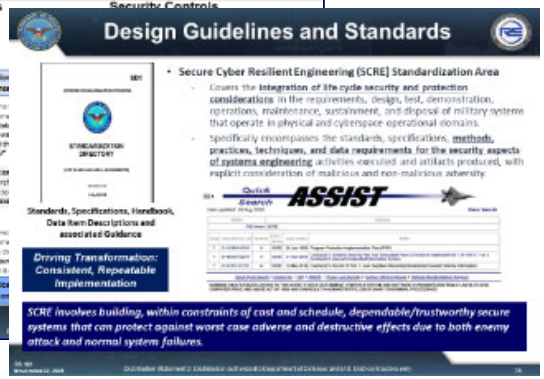
Request for Proposal, Statement of Work (SOW) Analysis Results Summary



Engineering Requirements and Security Controls Comparison



Design Guidelines and Standards



Addressing Recurring Challenges: Processes, Standards, Workforce

Implementation: Engineering Cyber Resilient Weapon Systems Workshop Series

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

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

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

4 Engineering Methods
1. Cyber effects on Technical Performance Measures and Metrics
2. Examine cyber requirements and SETR criteria
3. Leverage System Safety
4. Identify considerations for embedded software
5. Inform RIO based on cyber effects

5 Supply Chain Risk Management
1. Integrate supply chain mitigation approaches in standards, guidance and assessment methods
2. Consider approach for systems in sustainment
3. Plan for sustainment
4. Use available validated Intel and CI to make risk informed decisions

6: Cybersecurity Engineering
Identify skill sets and curriculum needs for our current and future engineering workforce
1. Develop a BoK
2. Establish a cyber engineering competency model
3. Establish a practice

7: Move the Ball, Move the Chain
Establish roadmap for engineering standardization of J6 Cyber Survivability Endorsement
1. Fundamental challenge is preventing losses
2. Establish a cyber engineering competency model
3. Scope of cyber loss

8: Engineering Design Activities
Identify skill sets and curriculum needs for our current and future engineering workforce
1. Need Loss Control Objectives
2. Refine Design Materials
3. System Analysis of Loss Guidance

Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

9: Technical Exchange
Virtual sharing of ongoing activities to shape the landscape
1. Army Practices
2. Air Force Practices
3. Navy Practices

9a: CYBER Mission Forces
Planning for integration of CYBER Mission Forces capability
1. Mission Level / System Level
2. Actionable Mission information needed
3. CYBERCOM requirements / system requirements

10: Fill the "Building Code"| Void
Establish roadmap for secure cyber resilient engineering practice to for standardization
1. Define building code criteria,
2. Identify secure cyber resilient engineering activities
3. Inform SCRE Credential Program

In development

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Secure Software Supply Chain
Joint Federated Assurance Center

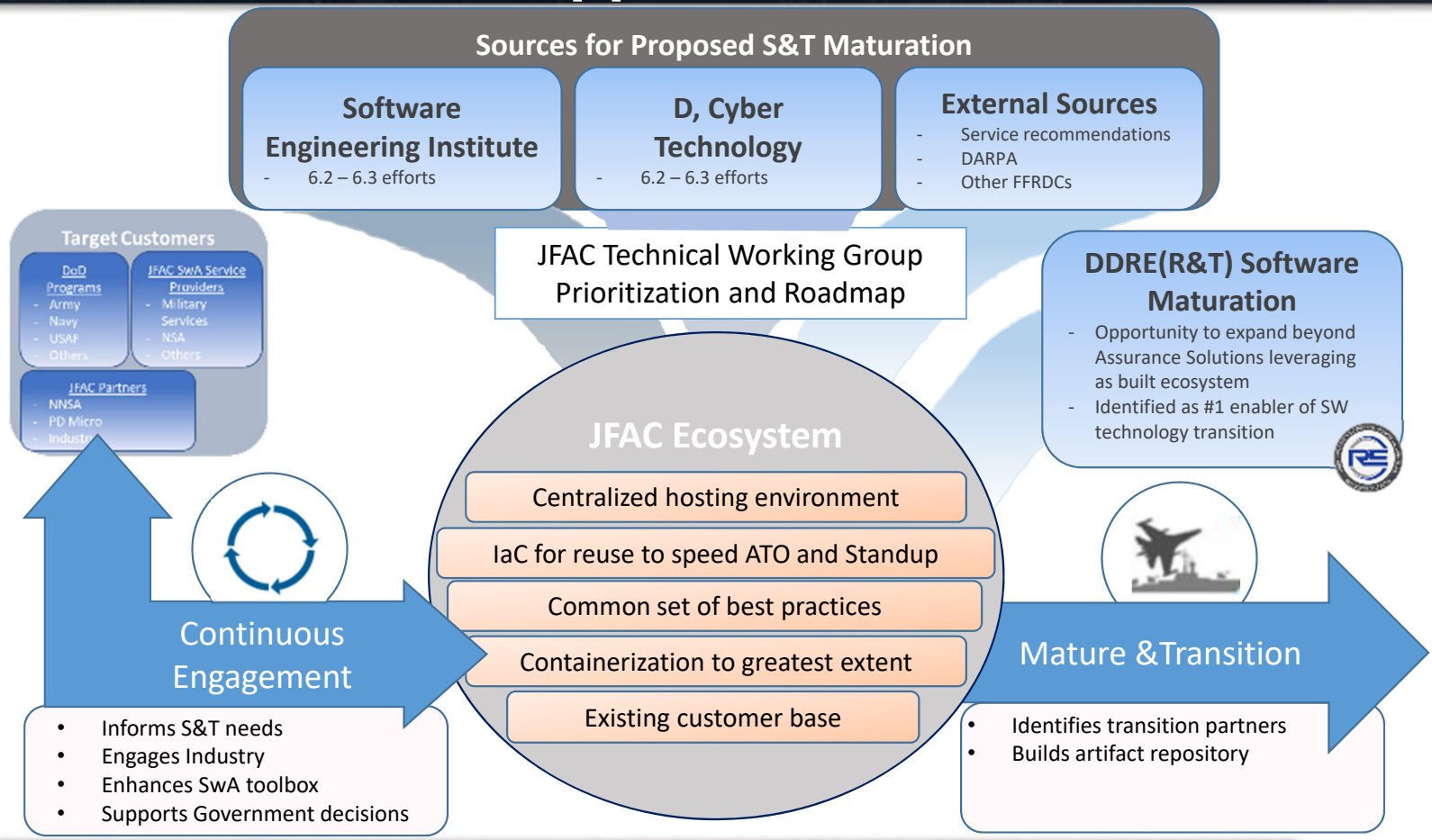
- **The Joint Federated Assurance Center (JFAC) was established to ensure the security of software and hardware developed, acquired, maintained, and used by the Department through the federation of existing DoD software and hardware assurance resources, expertise, and capabilities.**
- **Federal and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

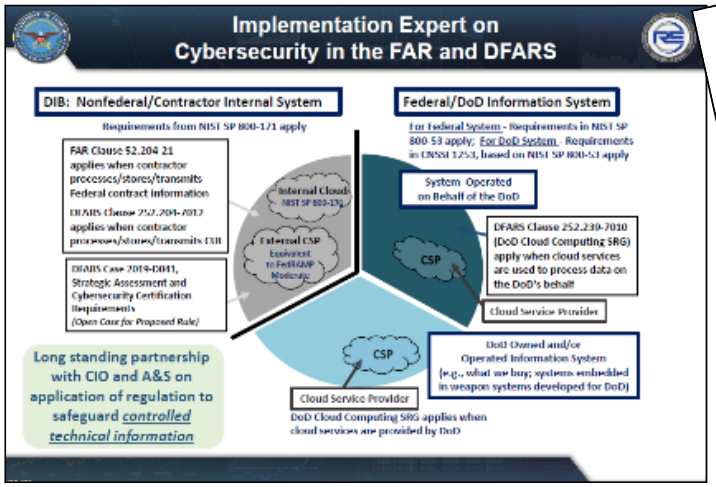
Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

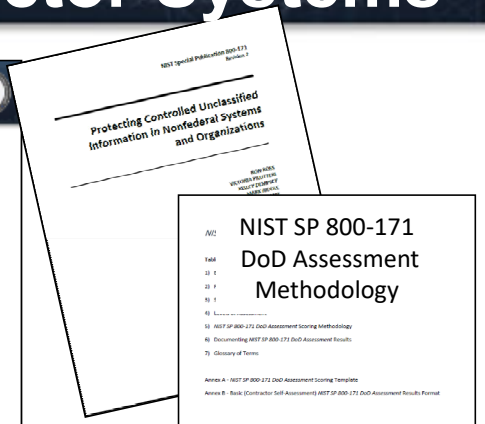
Software Assurance Technology Transition Opportunities



Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

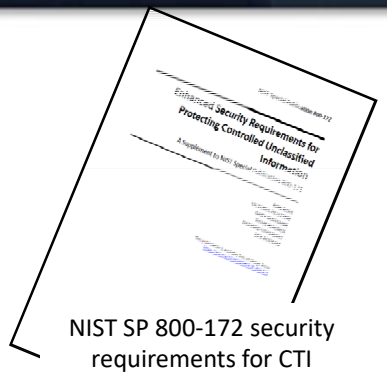
Protection of Controlled Technical Information on Contractor Systems



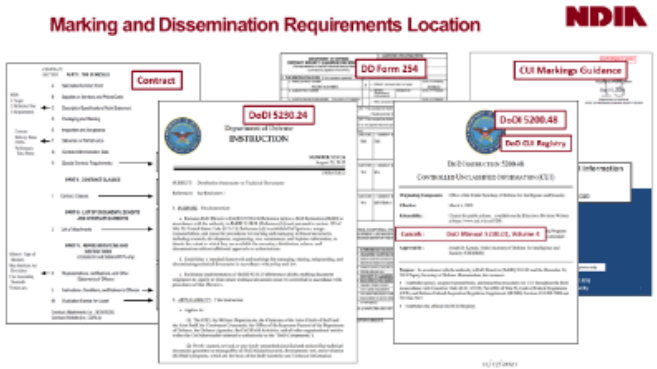


NIST SP 800-171 DoD Assessment Methodology

Standardized procedures to strategically assess NIST SP 800-171 implementation



NIST SP 800-172 security requirements for CTI associated with critical programs and technologies



Working with NDIA, DTIC and DAU to develop guidance for S&T managers and engineers to apply marking and dissemination statements and safeguard Controlled Technical Information (CTI)

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Workforce Competency

- Defense Acquisition University
  - ACQ 160*: Program Protection Planning Awareness
  - ENG 260*: Program Protection for Practitioners

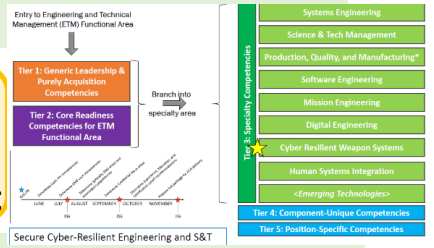
Program Protection Credential Program In place

***Update required to align with AAF**

Curriculum includes: Anti-Tamper, safeguarding CTI in the Defense Industrial Base, information communications technology supply chain risk management (ICT SCRM), software assurance and hardware assurance

- Defense Acquisition University
  - Draft Secure Cyber Resilient Engineering competency model approved by Engineering and Technical Management (E&TM) Task Force

SCRE Credential Program Under Development



Planned to include life cycle protection considerations for engineering secure, resilient, and trustworthy DoD systems, networks, and communications

- **Partnering with NDIA System Security Engineering Committee and DAU**
  - CTI Tabletop Tutorial
  - Hardware Assurance and Microelectronics Quantitative Assurance Tabletop Tutorial

Controlled Technical Information Credential Program future request

Proposal to include methods to identity, apply marking and dissemination statements to CTI; and to carve out information that is not controlled

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Resilient Systems End State

- **DoDI 5000.83 establishes roles and responsibilities for the S&T manager and the engineering workforce**
  - **Updates to guidance, standards, education and training are pending to make more consistent implementation**
- **Improve the efficiency and effectiveness of weapon systems engineering practice to deliver, and modernize, systems with the required capability in a secure manner under the presence of adverse conditions**
- **Increase consistency and repeatability of secure cyber resilient engineering methods and standards**
- **Improve the communication between government, industry, and operational stakeholders**

Customer-Focused: Outcome-Based

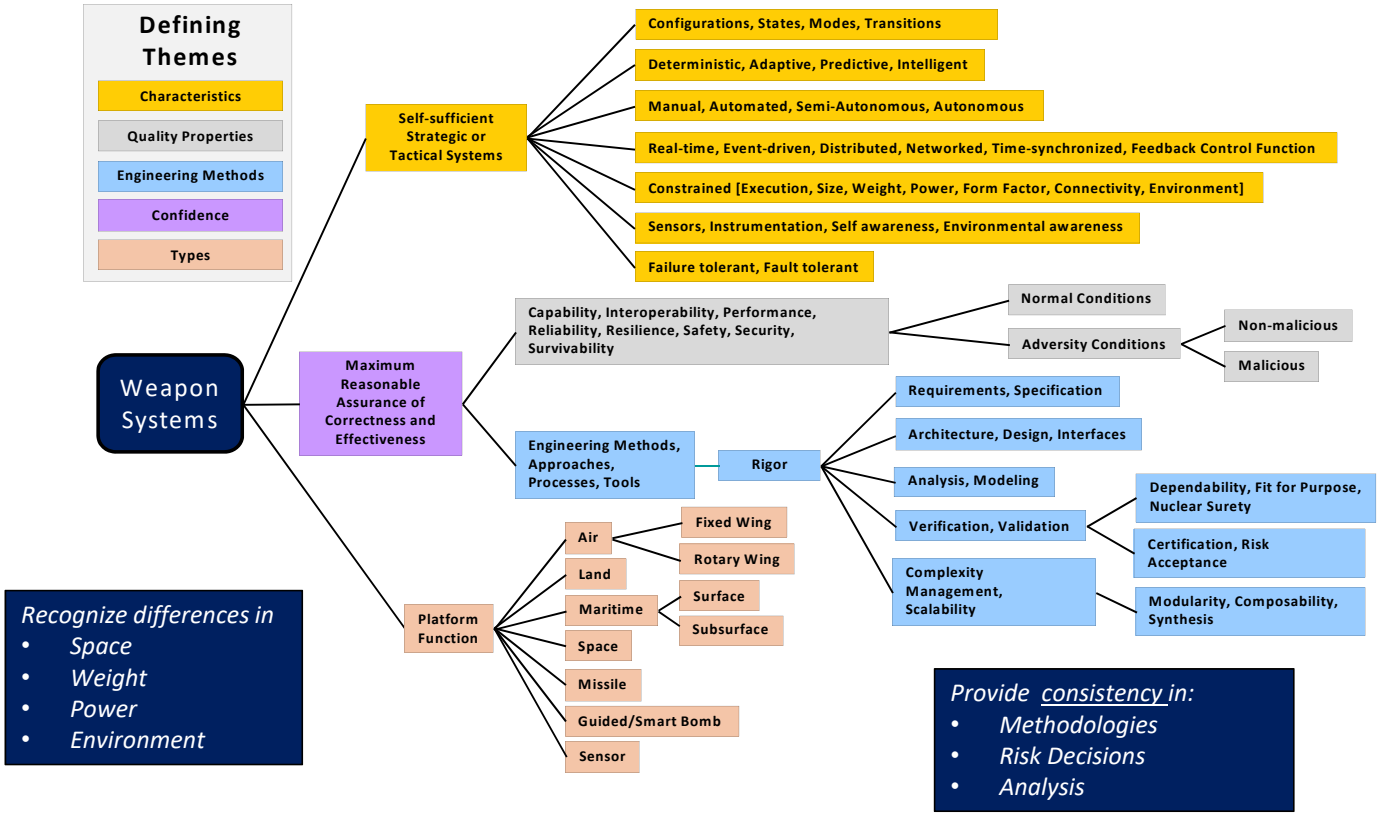
Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Questions

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Backup

Weapon Systems Characteristics



Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Technology, Program Protection & Cybersecurity Related Policies

Technology

Key Protection Activities:

- Export Control
- Anti-Tamper
- Defense Exportability Features
- DoD Horizontal Protection Guide
- Acquisition Security Database

Goal: Prevent compromise or loss of critical technology transfer

- **DoDI 5200.39 Critical Program Information**
- **DoDD 5200.47E Anti-Tamper**

Mission Components

Key Protection Activities:

- Software Assurance
- Hardware Assurance
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center

Goal: Protect mission-critical components (hardware, software) from malicious exploitation

- **DoDI 5200.44 Trusted Systems & Networks**
- **PL 113-66 Sec 937 (FY14 NDAA) JFAC**
- **DFARS 239.73 Requirements for information relating to supply chain risk**
- **10USC 2339a; Requirements for Information Relating to Supply Chain Risk**
- **NDAA FY18 Sec 1659. Supply Chain Risk Management of Critical Missions**
- **NDAA FY19 Sec 1655, Mitigation of Risks to National Security Posed by Providers of IT products and services who have obligations to foreign governments**

Information

Key Protection Activities:

- Classification
- Information Security
- Cybersecurity Protections and Technology Solutions
- Joint Acquisition Protection & Exploitation Cell (JAPEC)
- Damage Assessment Management

Goal: Safeguard system and technical data from adversary collection and disruption

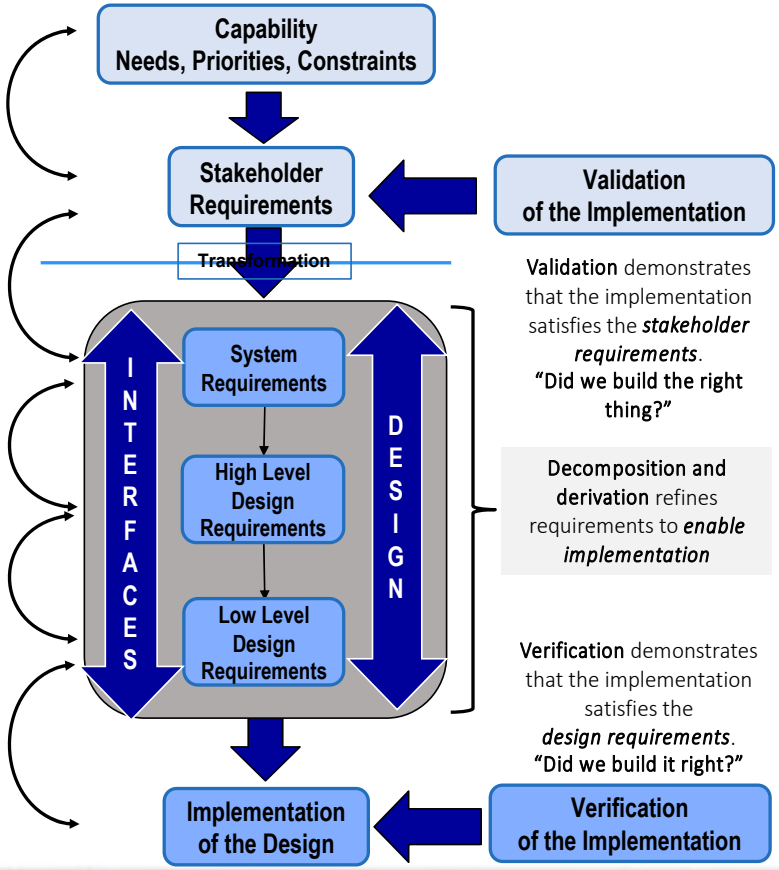
- **DoDI 5230.24 Distribution Statements on Technical Information**
- **DoDI 5200.48 Controlled Unclassified Information**
- **DFARS 252.204-7012 Safeguarding covered defense information and cyber incident reporting (includes requirement to implement NIST SP800-171)**
- **DCMA NIST SP 800-171 Strategic Assessments**
- **32 CFR 2002: Controlled Unclassified Information**
- **Secure Cyber Resilient Engineering**
- **DoDI 8500 series**

Goal: Ensure warfighter dominance through superior, assured, and resilient systems

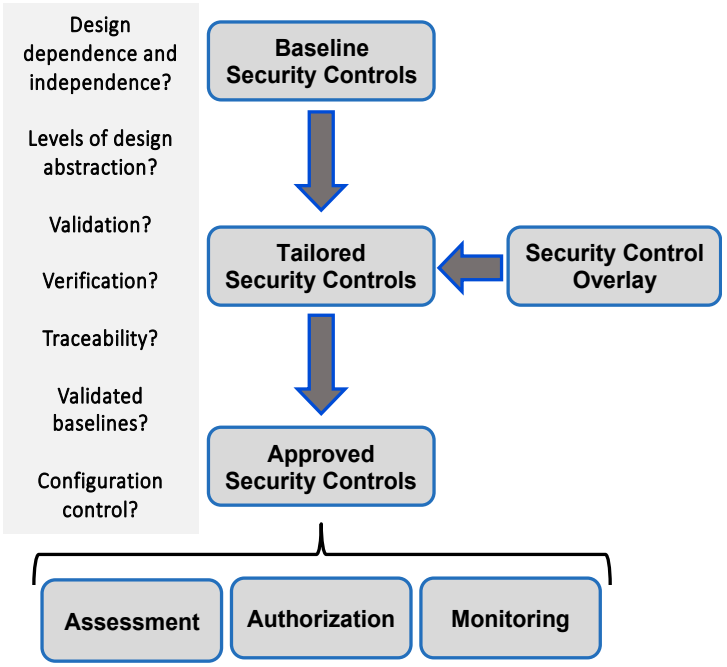
Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Engineering Requirements and Security Controls Comparison

Engineering Requirements

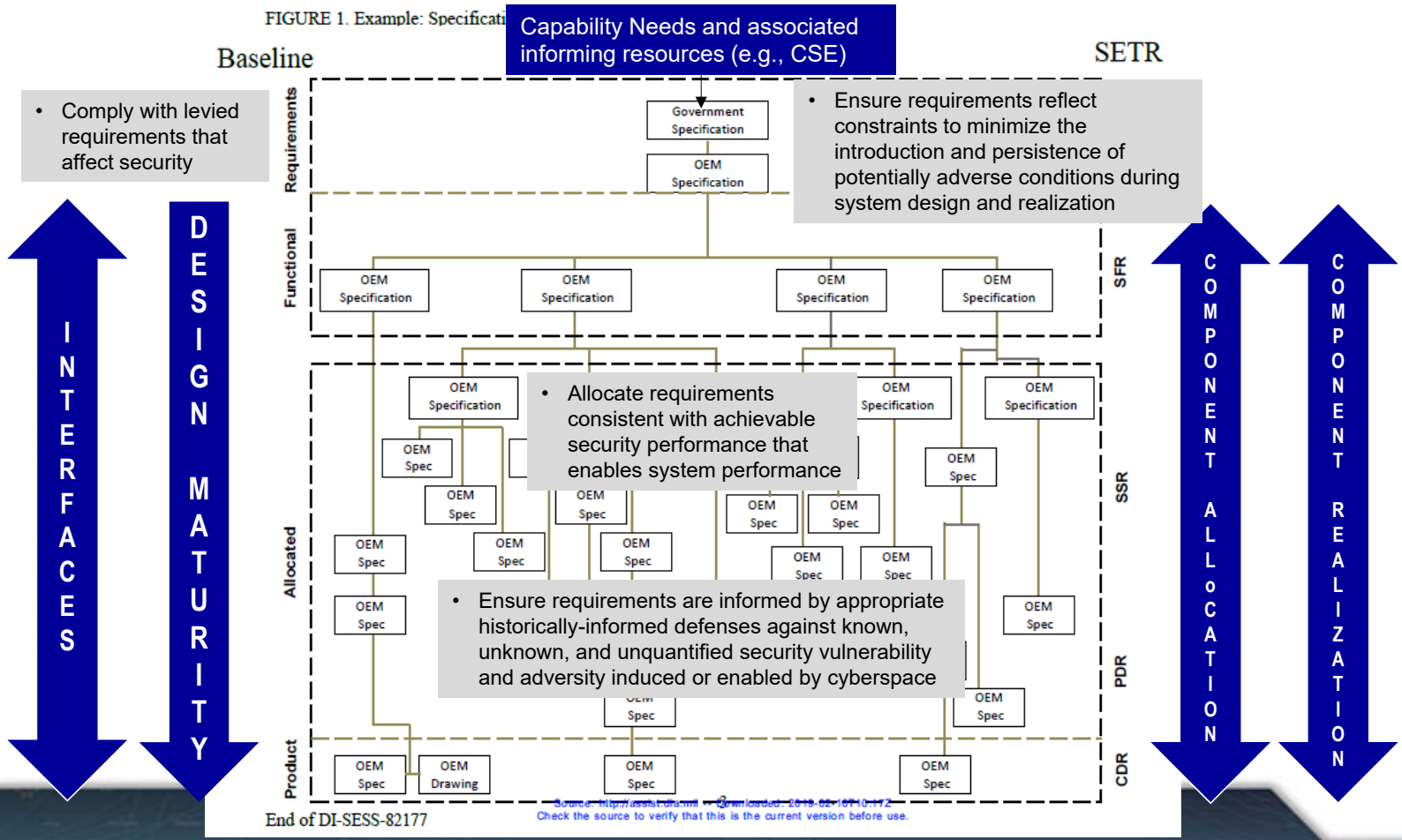


Security Controls



Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Secure Cyber Resilient Engineering Practice Requirements and Design Maturity





Distribution Statement A: Approved for public release. DOPSR case #22-S-0455 applies. Distribution is unlimited.

Department of the Air Force

Integrity - Service - Excellence

Operation Vulcan Logic (OVL): Risk Management with Agility

Daniel C. Holtzman, HQE
Director, Cyberspace Innovation (A);
Cyber Technical Director;

Authorizing Official for:
JSF F-35 ALIS;
F-35 Cloud & DevSecOps;
DAF Cloud & DevSecOps
GBSD Cloud and DevSecOps;
Command & Control Systems;
Rapid Cyber Acquisitions (RCA);
Enterprise IT as a Service (EITaaS);
SAP Command and Control Systems;
SAP Rapid Cyber Acquisitions (RCA);
SAP Enterprise IT as a Service (SEITaaS)

6 December 2021
NDIA

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic

VULCANLOGIC@US.AF.MIL

Handout



OPERATION VULCAN LOGIC

PHASE 1

PROGRAM MANAGEMENT

PHASE 2

COLLABORATIVE EXECUTION

PHASE 3

ENABLERS

FAST-TRACK AID PROCESS: WHAT IS IT?

OPERATION VULCAN LOGIC

COMMUNITY FEEDBACK

SAMPLE ONBOARDING MODULES

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

Be around the light-bringers,
the magic makers,
the world shifters.

They challenge you,
break you open,
uplift and expand you.

They don't let you play small
with your life.

These heartbeats are your people.
These people are your tribe.

- Danielle Doby

Areas of Responsibility (AOR)
Perspective across AF Weapon systems

AF Cyber Technical Director AFLCMC/EN

Cyber Security Engineering and Resilience (CSER) Senior Leader.

Technical authority for:

- Security engineering, cyber resiliency and systems, and mission assurance.
- Engineering resilient systems.
- Defensive security engineering.

AF Authorizing Official, SAF/CN

Authorization Boundaries:

- Cloud and DevSecOps.
- Command and Control Systems.
- SAP Command and Control Systems.
- Rapid Cyber Acquisition.
- SAP Rapid Cyber Acquisitions.
- Enterprise IT as a Service (EITaaS).
- SAP Enterprise IT as a Service (SEITaaS).
- F-35 (JSF); Cloud and DevSecOps.
- F-35 ALIS;
- Ground-Based Strategic Deterrent (GBSD); Cloud and DevSecOps.

AF Director, Cyberspace Innovation, SAF/CN

- Innovation thought leadership of risk-based cyber security across the DAF (USAF and USSF).
- Accelerate DAF understanding and mastery of commercial best practices.
- Collaborate across Government, Industry, Allies, and Partners.
- Manage DAF technical standard setting and adoption process.
- Represent DAF/DoD interests in the international standard-setting process.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Data is current as of 01 May 2021.

Authorization Boundary at a Glance:
Cross-Section of Air Force Programs

CRC



- JADC2/ABMS
- Kessel Run/AOC
- Cloud One/Platform One
- E3 AWACS and JSTARS
- F-35 ALIS
- F-35 Cloud and DevSecOps
- GBSD Cloud and DevSecOps

E-3



- ShOC-N
- Wide-Area Surveillance
- RADSIL
- BACN
- ACBN
- C2IMERA

cUAS



- EITaaS
- SEITaaS
- RDT&E DREN
- NGAD
- Commercial UAS
- TORCC

TAC-P



- PRC2
- WaRTAK
- GCCS / DCGS
- Pocket-J
- TBMCS
- Mission Planning
- Special Programs

AOC



Authorizations as of 1 Nov 2021 = 260

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

Cyber Security

and

Resiliency

is a journey,

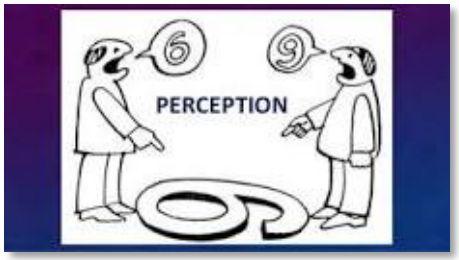
not a destination.

- D.C. Holtzman

Culture Change Challenge
Unperceived Bias

“Cool, you 3D-printed the save icon!”







Do you know the answers to these?

Do you realize your own bias?

Communication is key to culture change.

Change your thoughts and you change your world. ***– Norman Peale***

Authorizing Official North Star:
Exercising Agile Risk Management

- **Objectives:**
  - Render decisions faster: Being Transparent, foster reciprocity;
  - Enable Program Managers: More Secure Tomorrow than today;
  - Facilitate risk management: Acquisition, operations, and sustainment.

- **Enablers:**
  - Setting clear requirements: AO Determination Briefing;
  - Base Risk on Evidentiary analysis and data: Use Standard System Engineering:
  - Focus on Risk of Use: Operational-focused with enterprise view.
  - Move to Single AO for each weapon system: Streamline expectations & Seams.

- **Collaborative Execution:**
  - Cyber Risk Assessors (CRA) (formerly SCA) focus on assessing risks;
  - Authorizing Official informs decision makers on cyber risks;
  - Partnerships with PEOs, DOEs, PMs, users, and sustainers enable holistic view.

Increase decision-making agility by focusing on risk management.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

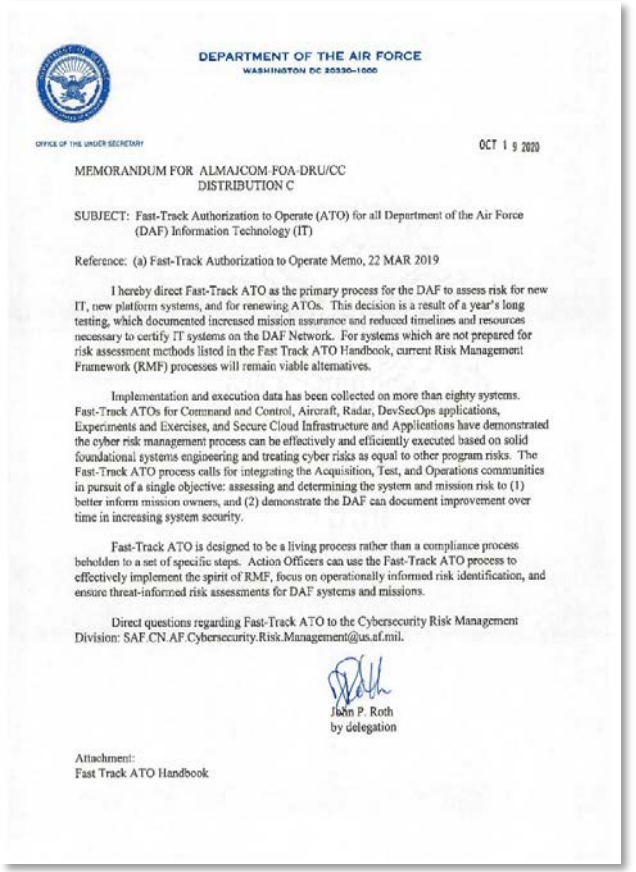
Fast-Track ATO Process: What Is It?

- **Not a "new" process: Focus is on risk management.**
- **Complies with DOD 8510**
- **Provides AOs the ability to make risk-informed determinations: Spirit of RMF.**
- **Does not require anything "new" or compliance to a new process**.

"The Fast-Track process gives [AOs] the discretion to make an authorization determination based on review of the combination of a Cybersecurity Baseline, an assessment (e.g., Penetration Test), and an Information Systems Continuous Monitoring Strategy.

"AOs are expected to make operationally informed risk determinations by working closely with information systems owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment."

- **Fast-Track is NOT an "easy" button; it requires robust systems engineering and "going slow to go fast."**



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

OFFICE OF THE UNDER SECRETARY

OCT 19 2020

MEMORANDUM FOR ALMAJCOM-FOA-DRU/CC
DISTRIBUTION C

SUBJECT: Fast-Track Authorization to Operate (ATO) for all Department of the Air Force (DAF) Information Technology (IT)

Reference: (a) Fast-Track Authorization to Operate Memo, 22 MAR 2019

I hereby direct Fast-Track ATO as the primary process for the DAF to assess risk for new IT, new platform systems, and for renewing ATOs. This decision is a result of a year's long testing, which documented increased mission assurance and reduced timelines and resources necessary to certify IT systems on the DAF Network. For systems which are not prepared for risk assessment methods listed in the Fast Track ATO Handbook, current Risk Management Framework (RMF) processes will remain viable alternatives.

Implementation and execution data has been collected on more than eighty systems. Fast-Track ATOs for Command and Control, Aircraft, Radar, DevSecOps applications, Experiments and Exercises, and Secure Cloud Infrastructure and Applications have demonstrated the cyber risk management process can be effectively and efficiently executed based on solid foundational systems engineering and treating cyber risks as equal to other program risks. The Fast-Track ATO process calls for integrating the Acquisition, Test, and Operations communities in pursuit of a single objective: assessing and determining the system and mission risk to (1) better inform mission owners, and (2) demonstrate the DAF can document improvement over time in increasing system security.

Fast-Track ATO is designed to be a living process rather than a compliance process beholden to a set of specific steps. Action Officers can use the Fast-Track ATO process to effectively implement the spirit of RMF, focus on operationally informed risk identification, and ensure threat-informed risk assessments for DAF systems and missions.

Direct questions regarding Fast-Track ATO to the Cybersecurity Risk Management Division: SAF.CN.AF.Cybersecurity.Risk.Management@us.af.mil.

John P. Roth
by delegation

Attachment:
Fast Track ATO Handbook

Fast-Track is a philosophy of focusing on the Risk of Use vs. compliance.

Cyber Security and Resiliency Enablers:
Systems Engineering

1. What is the system? What does it do? CONOPS? Missions?
2. What is the system architecture? Weapon system (e.g., aircraft, ground systems, maintenance systems, training systems, etc.)?
3. List hardware (LRU) and software and the providences of each (e.g., supply chain); identify Critical Program Information (CPI), Critical Components (CC); technical orders, and operational procedures. Identify technologies being used.
4. Identify all external communications access points.
5. How does data flow into, through, and out of the system? What type of data? How is it protected? Where does it come from? Where does it go? What is it used for?
6. What threat/intel information is available?

Establish the baseline from known data.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Cyber Security and Resiliency Enablers:
Supply Chain

1. **Bill of Material (BOM): As part of the SE process, especially in a legacy system, programs already know all parts (HW and SW).**
2. **Existing supplier management process identifies source of suppliers, End of Life (EOL) analysis, and alternate-part analysis**
   - Document the "As Is"
3. **Is existing criteria, being used by primes and flowed down to subs, known on purchasing of parts?**
4. **What is the supply chain mapping? Does one exist already?**
   - Graphical representation of supply chain down?

- **With the data collected from items 1-4 above, review of the potential risks of the supply chain can be done rather quickly at low cost ("As Is/Known").**
- **Available intel/threat info can be applied against the list of parts or suppliers identified (or technologies) if known.**
- **Provide an assessment of risk of the current supply chain:**
  - Better than we have today.

Establish the baseline from known data.

Operation Vulcan Logic
Fast Track Implementation: Agile Authorizations

1 PHASE 1

Systems/Systems Security Engineering
Evidentiary Data & Analysis

- Architectures
- System Boundries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessents
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

2 PHASE 2

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Previous asessments analysis results
- Operational Use Perspective

Scope the assessment criteria and outcomes

3 PHASE 3

Executive Risk Assessment

- Tool Agnostic - Focus on Evidentirary Data and Analysis
- Clinically deine Risk of Use Posture
- Outline Mitigations for Risks

Provide determination briefing to AO

Phase 3 starts never ending journey of continuous assessment & monitoring

PROGRAM MANAGEMENT

- Facilitate Risk management across S&T, Acquisition, Operations & Sustainment

COLLABORATIVE EXECUTION

- Partnerships with PEO's, DOEs, PMs, S&T, T&E, Sustainers, Users, enables holistic view

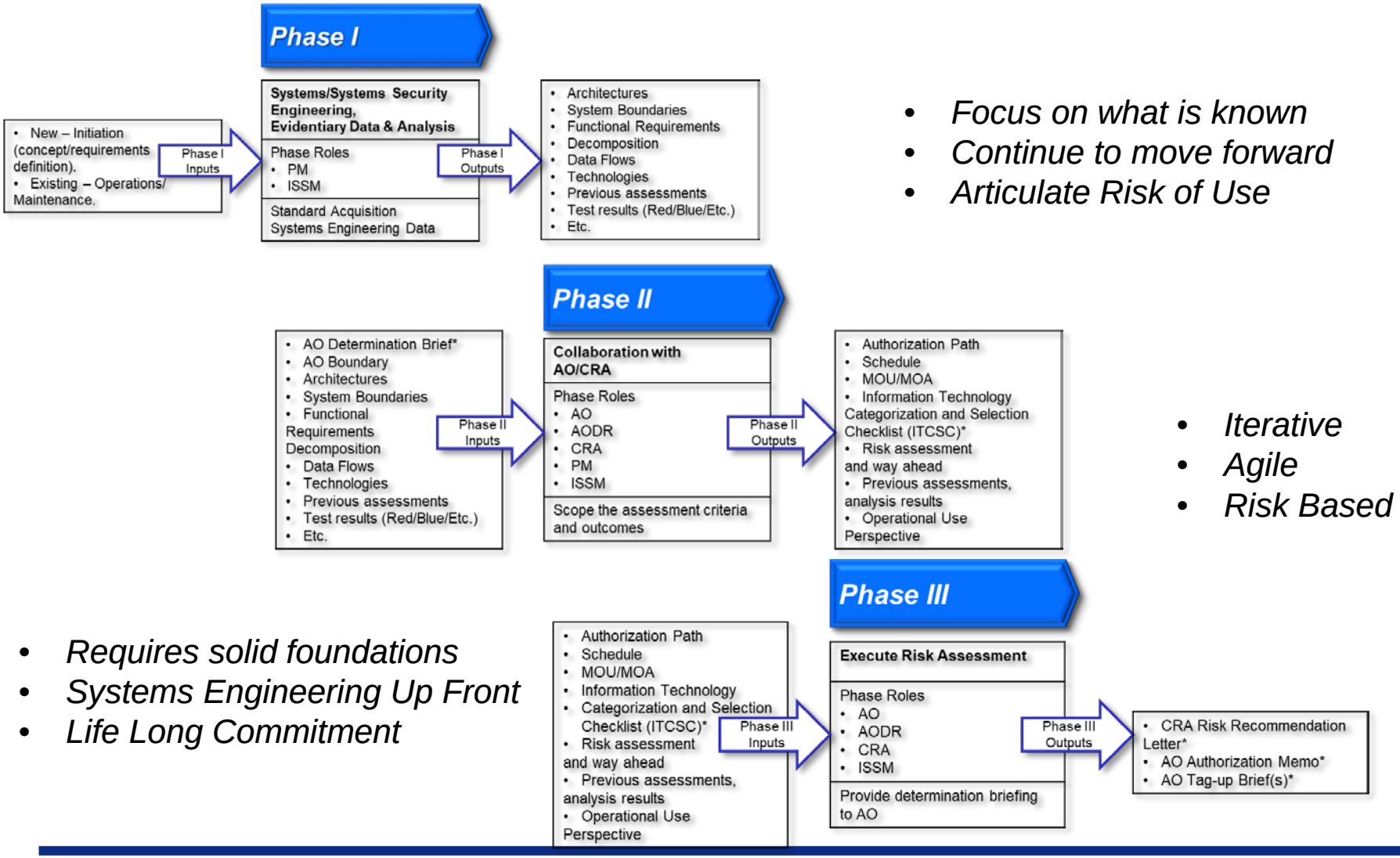
ENABLERS

- Single, Lead AO for each Weapon System
- Streamline expectations and increase Agility

Operationalizing the Fast Track ATO Process

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Agile Authorizations:
Enabled by Disciplined Systems Engineering

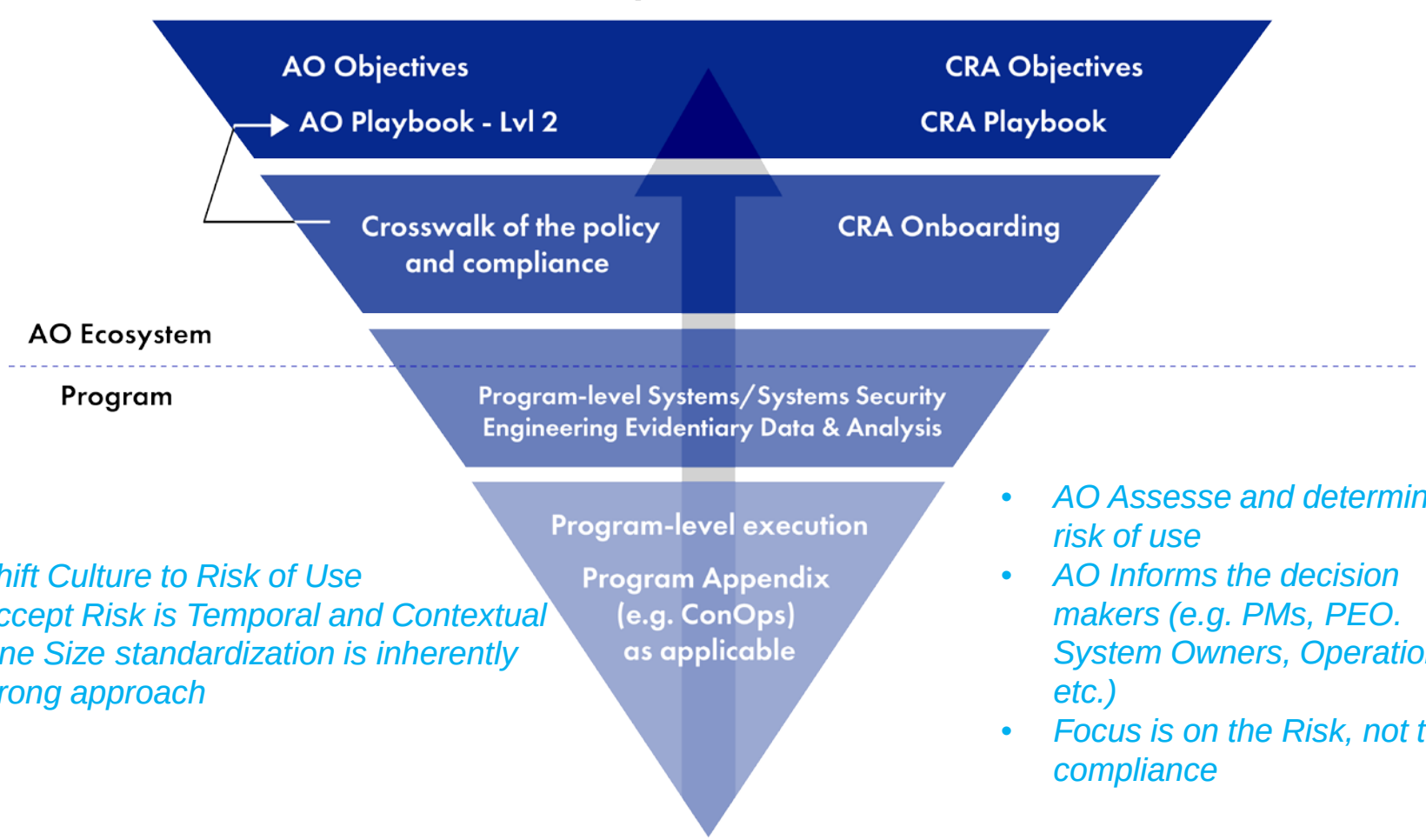


- *Focus on what is known*
- *Continue to move forward*
- *Articulate Risk of Use*

- *Iterative*
- *Agile*
- *Risk Based*

- *Requires solid foundations*
- *Systems Engineering Up Front*
- *Life Long Commitment*

Operation Vulcan Logic: Agile Authorizations Execution NorthStar



- *Shift Culture to Risk of Use*
- *Accept Risk is Temporal and Contextual*
- *One Size standardization is inherently wrong approach*

- *AO Assesse and determines risk of use*
- *AO Informs the decision makers (e.g. PMs, PEO. System Owners, Operations, etc.)*
- *Focus is on the Risk, not the compliance*

The holistic, continuous authorization ecosystem is focused on Risk of Use.

Operation Vulcan Logic
Authorization Templates
Simple, Effective, Agile

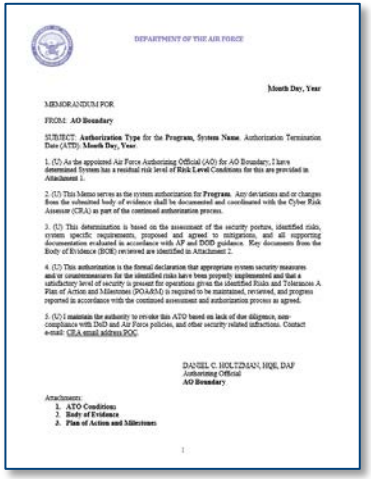
- **Determination Brief**
- **Authorization Package**
- **CRA Risk Recommendation**


U.S. Air Force

Integrity - Service - Excellence

AO Determination Briefing

<State Decision Type, etc.>
<IATT, ATO, etc.>
<Your Program Name>
<Program Type>
<ITIPS ID/PID/eMASS ID>
<Weapons, Logistics, etc.>
SCA/CRA Briefing:
<SCA/CRA Name>
<Briefing Date>


DEPARTMENT OF THE AIR FORCE

Month Day, Year

MEMORANDUM FOR

FROM: AO Boundary

SUBJECT: Authorization Type for the Program, System Name Authorization Termination Date (ATD): Month Day, Year

1. (U) As the appointed Air Force Authorizing Official (AO) for AO Boundary, I have determined System has a residual risk level of Risk Level Conditions for this are provided in Attachment 1.

2. (U) This Memo serves as the system authorization for Program. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the Cyber Risk Assessor (CRA) as part of the continued authorization process.

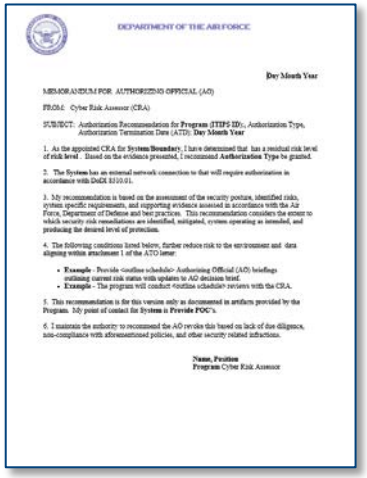
3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are identified in Attachment 2.

4. (U) This authorization is the formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations given the identified Risks and Tolerances. A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed, and progress reported in accordance with the continued assessment and authorization process as agreed.

5. (U) I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with DoD and Air Force policies, and other security related infractions. Contact e-mail: CRA email address POC

DANIEL C. HOLTZMAN, HQE, DAF
Authorizing Official
AO Boundary

Attachments:
1. ATO Conditions
2. Body of Evidence
3. Plan of Action and Milestones


DEPARTMENT OF THE AIR FORCE

Day Month Year

MEMORANDUM FOR AUTHORIZING OFFICIAL (AO)

FROM: Cyber Risk Assessor (CRA)

SUBJECT: Authorization Recommendation for Program (ITIPS ID):, Authorization Type, Authorization Termination Date (ATD): Day Month Year

1. As the appointed CRA for System/Boundary, I have determined that has a residual risk level of risk level . Based on the evidence presented, I recommend Authorization Type be granted.

2. The System has an external network connection to that will require authorization in accordance with DoDI 8510.01.

3. My recommendation is based on the assessment of the security posture, identified risks, system specific requirements, and supporting evidence assessed in accordance with the Air Force, Department of Defense and best practices. This recommendation considers the extent to which security risk remediations are identified, mitigated, system operating as intended, and producing the desired level of protection.

4. The following conditions listed below, further reduce risk to the environment and data aligning within attachment 1 of the ATO letter:

- Example - Provide <outline schedule> Authorizing Official (AO) briefings outlining current risk status with updates to AO decision brief.
- Example - The program will conduct <outline schedule> reviews with the CRA.

5. This recommendation is for this version only as documented in artifacts provided by the Program. My point of contact for System is Provide POC's.

6. I maintain the authority to recommend the AO revoke this based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions.

Name, Position
Program Cyber Risk Assessor

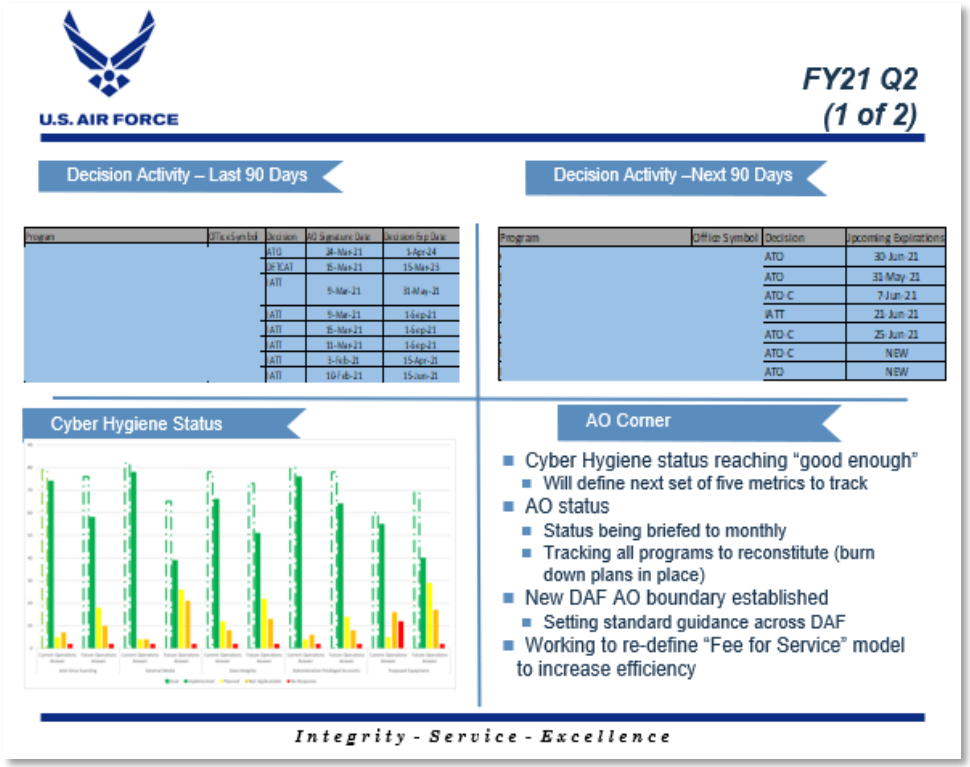
- *Meets all DoDI 8510 and DAF policy requirements for RMF*
- *Authorization Memo has list of BOE that was used to increase reciprocity*
- *Not a work flow or set of "artifacts'*
- *Risk Analysis informed by threat/intel, stakeholder tolerance and operational mission parameters*

- *Provides the AO with an independent Assessment*
- *Not a one time product, developed over time working hand in hand*
- *Authorization starts the life long commitment to improving cyber every day*

Standardization is flexible for authorization packages: There is no one-size-fits-all approach.

Operation Vulcan Logic
AO / PEO Partnership

- **AO provides PEO Quarterly Update.**
  - **Communicate Status.**
  - **Provides Awareness of AOR items & Challenges**
  - **Real time changes communicated by exception**
- **Fosters Collaboration**
  - **Cross PEO challenges**
  - **Opportunities for synergies**
  - **Same Site Picture**
- **PEO AODR-Assigned:**
  - Works for PEO DOE.
  - OPCON to AO.
  - Integrates Cyber into SE/SSE.
- **PEO AODRs collect metrics and status.**



Model works for PEO "Like" (e.g. COCOMs)as well

Cyber is Commanders Business

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic

Risk Adjudication Process: Cyber is a Commander's Business

- **Authorizing Official (AO) determines risk is high:**
  - **AO communicates with Program Manger (PM):**
    - Agree and mitigate = Stop here.
  - **AO and PM jointly present to the PEO:**
    - Agree and mitigate = Stop here.
  - **AO and PEO present to the Risk Board.**
    - Risk Board: CIO, SAE, System Operational Commander.
    - Risk Board weighs risk, tolerance, mission, and enterprise.
- **Agile, Efficient, Effective.**
  - Informs relevant stakeholders quickly, allows for more informed decisions

Risk of Use communicated to: Acquisition, Enterprise, & Operational stakeholders.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic
Collaborative Partnerships

- **DAF CSO, CAO, CEO, CDO, CIO = Leadership Strategic Alignment.**
- **Air Force and Space Force Collaborations.**
- **AF Authorizing Officials:**
  - Weapon Systems AOs: Reciprocity agreement in place.
  - AFRL AO: Collaborating on Fast-Track ATO and reciprocity.
  - HAF/A4 AO: Collaboration and Reciprocity.
  - AF Innovation AO: Collaboration on DevSecOps and cloud migration.
  - AF Global Strike Command: Collaborating on reciprocity.
  - Enterprise AO: Reciprocity across boundary.
  - AF IC AO: Collaboration on reciprocity; ADSV exemplar.
  - 16th AF AO: Collaboration on reciprocity and the AO process.
  - AF OSI/PJ: Collaboration on reciprocity, sharing of resources.
  - DOD CIO: Reciprocity agreement in place.
- **Industry:**
  - Collaboration via AF/Industry Authorization Round Table.
- **External Agencies:**
  - NSA, National Nuclear Security Agency (NNSA), DHS, DLA, USDA, Army RCO, Army NETCOM, DOJ, Navy, etc.

- **Agile execution based on collaborative partnerships, vice policy, and memos.**
- **Building confidence and trust.**

Cyber Risk is Shared – Contextual and Temporal.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

The most dangerous phrase in language is:

"We've always done it this way."

- Admiral Grace Hopper

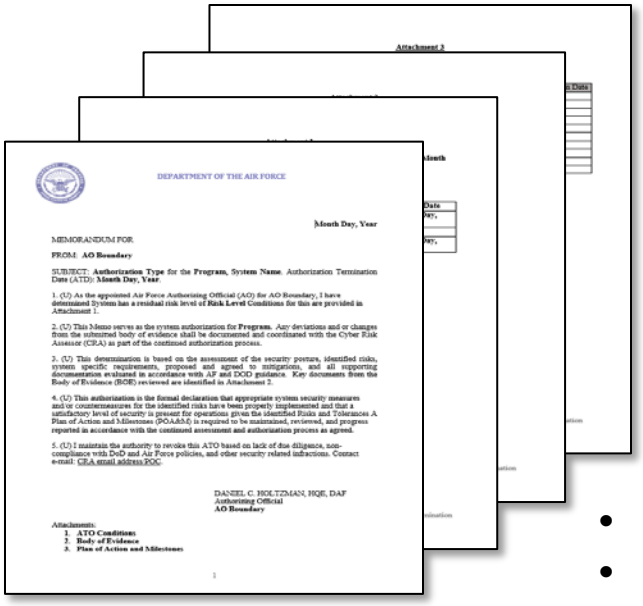
Strategic Challenges

- **Reciprocity:**
  - The myth of the lowest common denominator.
- **Culture of Compliance:**
  - Compliance masquerading as risk management.
- **Operational Risk Integration:**
  - Risk is temporal and context-sensitive.
- **Command and Control:**
  - Too many cooks makes for bad-tasting chili.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

ATO Package of the Future

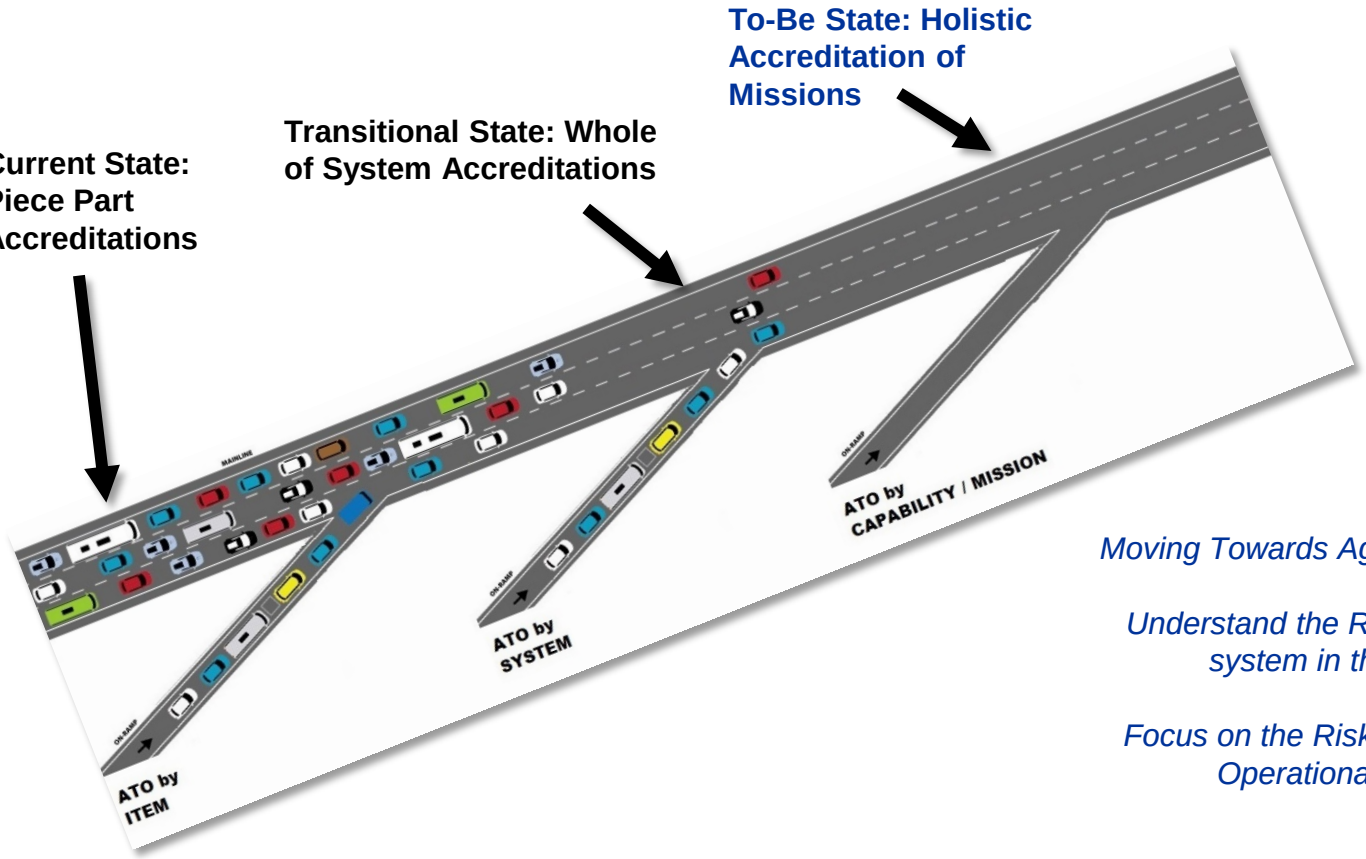
- **Will document the key items needed for reciprocity:**
  - Authorization Memo.
  - Attachment 1: Conditions.
  - Attachment 2: Body of Evidence.
  - Attachment 3: Plan of Action and Milestones.



- **Attachment 1: Conditions**
  - Documents any conditions on the ATO.
  - Security is a journey, never a destination.
- **Attachment 2: Body of Evidence**
  - Key artifacts that supported the authorization.
  - Informs other AOs and consumers to increase reciprocity.
- **Attachment 3: Plan of Action and Milestones.**
  - Can be a Classified appendix.

- *Provided to the requesting consumer as a contract*
- *Documented in enterprise tools (e.g. eMass, XACTA….)*

Highway to Resilient Capabilities



Moving Towards Agile Authorizations.

Understand the Risk of Use of the system in the context.

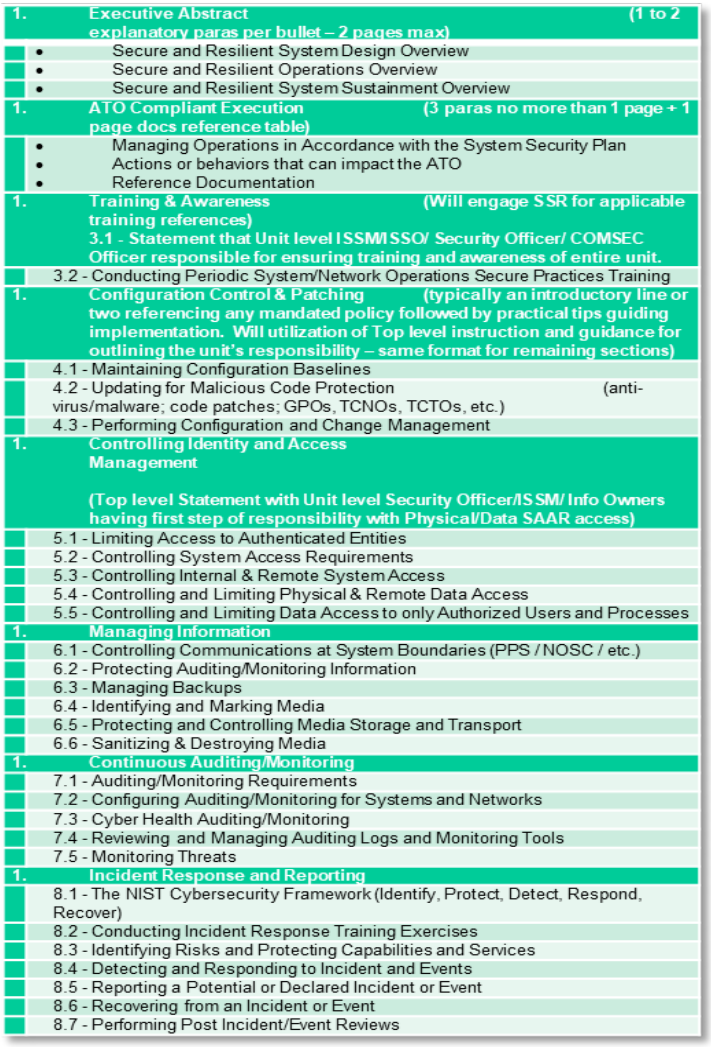
Focus on the Risk Management in Operational Context.

Traditional Boundary Configuration Management is no longer sufficient in a software-defined, ubiquitous, connected environment.

Cyber Tech Order and Continuous Monitoring

- **Cyber Tech Order:**
  - Communicate the "How" to maintain systems for Secure Resiliency.
  - Provide clear operating instructions for users and maintainers.
  - Educate, enable, and execute.

- **Continuous Monitoring:**
  - Recognize that change is constant.
    - New vulnerabilities and threats appear every day.
    - Technology changes.
    - Mitigation effectiveness degrades over time.
  - Integrate Mission Defense Teams into CONMON plans.
    - It is the first line of defense.



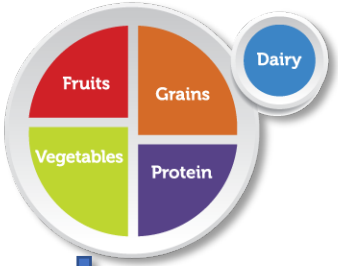
1.	**Executive Abstract (1 to 2 explanatory paras per bullet – 2 pages max)**
•	Secure and Resilient System Design Overview
•	Secure and Resilient Operations Overview
•	Secure and Resilient System Sustainment Overview
1.	**ATO Compliant Execution (3 paras no more than 1 page + 1 page docs reference table)**
•	Managing Operations in Accordance with the System Security Plan
•	Actions or behaviors that can impact the ATO
•	Reference Documentation
1.	**Training & Awareness (Will engage SSR for applicable training references)**
	3.1 - Statement that Unit level ISSM/ISSO/ Security Officer/ COMSEC Officer responsible for ensuring training and awareness of entire unit.
	3.2 - Conducting Periodic System/Network Operations Secure Practices Training
1.	**Configuration Control & Patching (typically an introductory line or two referencing any mandated policy followed by practical tips guiding implementation. Will utilization of Top level instruction and guidance for outlining the unit's responsibility – same format for remaining sections)**
	4.1 - Maintaining Configuration Baselines
	4.2 - Updating for Malicious Code Protection (anti-virus/malware; code patches; GPOs, TCNOs, TCTOs, etc.)
	4.3 - Performing Configuration and Change Management
1.	**Controlling Identity and Access Management**
	(Top level Statement with Unit level Security Officer/ISSM/ Info Owners having first step of responsibility with Physical/Data SAAR access)
	5.1 - Limiting Access to Authenticated Entities
	5.2 - Controlling System Access Requirements
	5.3 - Controlling Internal & Remote System Access
	5.4 - Controlling and Limiting Physical & Remote Data Access
	5.5 - Controlling and Limiting Data Access to only Authorized Users and Processes
1.	**Managing Information**
	6.1 - Controlling Communications at System Boundaries (PPS / NOSC / etc.)
	6.2 - Protecting Auditing/Monitoring Information
	6.3 - Managing Backups
	6.4 - Identifying and Marking Media
	6.5 - Protecting and Controlling Media Storage and Transport
	6.6 - Sanitizing & Destroying Media
1.	**Continuous Auditing/Monitoring**
	7.1 - Auditing/Monitoring Requirements
	7.2 - Configuring Auditing/Monitoring for Systems and Networks
	7.3 - Cyber Health Auditing/Monitoring
	7.4 - Reviewing and Managing Auditing Logs and Monitoring Tools
	7.5 - Monitoring Threats
1.	**Incident Response and Reporting**
	8.1 - The NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
	8.2 - Conducting Incident Response Training Exercises
	8.3 - Identifying Risks and Protecting Capabilities and Services
	8.4 - Detecting and Responding to Incident and Events
	8.5 - Reporting a Potential or Declared Incident or Event
	8.6 - Recovering from an Incident or Event
	8.7 - Performing Post Incident/Event Reviews

Cyber Risks Facts Label

- **Application Security is NOT just about the security of the application itself:**
  - It is a layered perspective (hosted environment, TTPs, etc.).
  - As one goes lower in an application architecture, the potential for harm increases.
- **An Authority to Operate (ATO) is a risk-based determination and includes many factors:**
  - The technology employed, the execution processes, the hosting environment, the risk tolerance, etc.
  - The ATO is a statement of the "Risk of Use," informing the consumer.

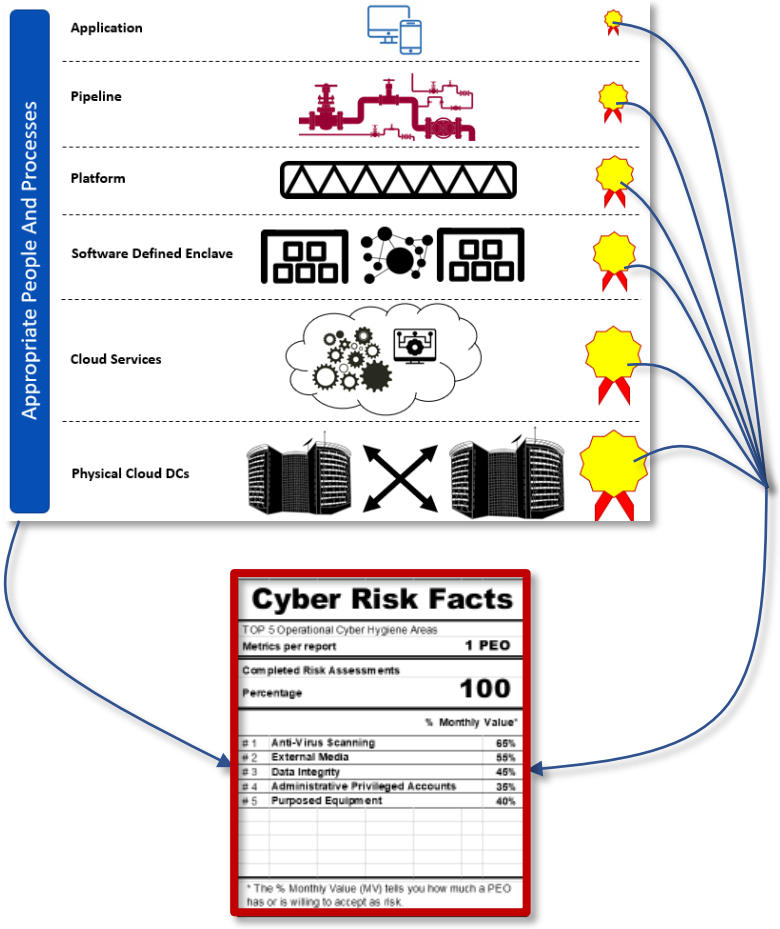


Cyber Risks Facts Label: Allowing for an Informed Consumer





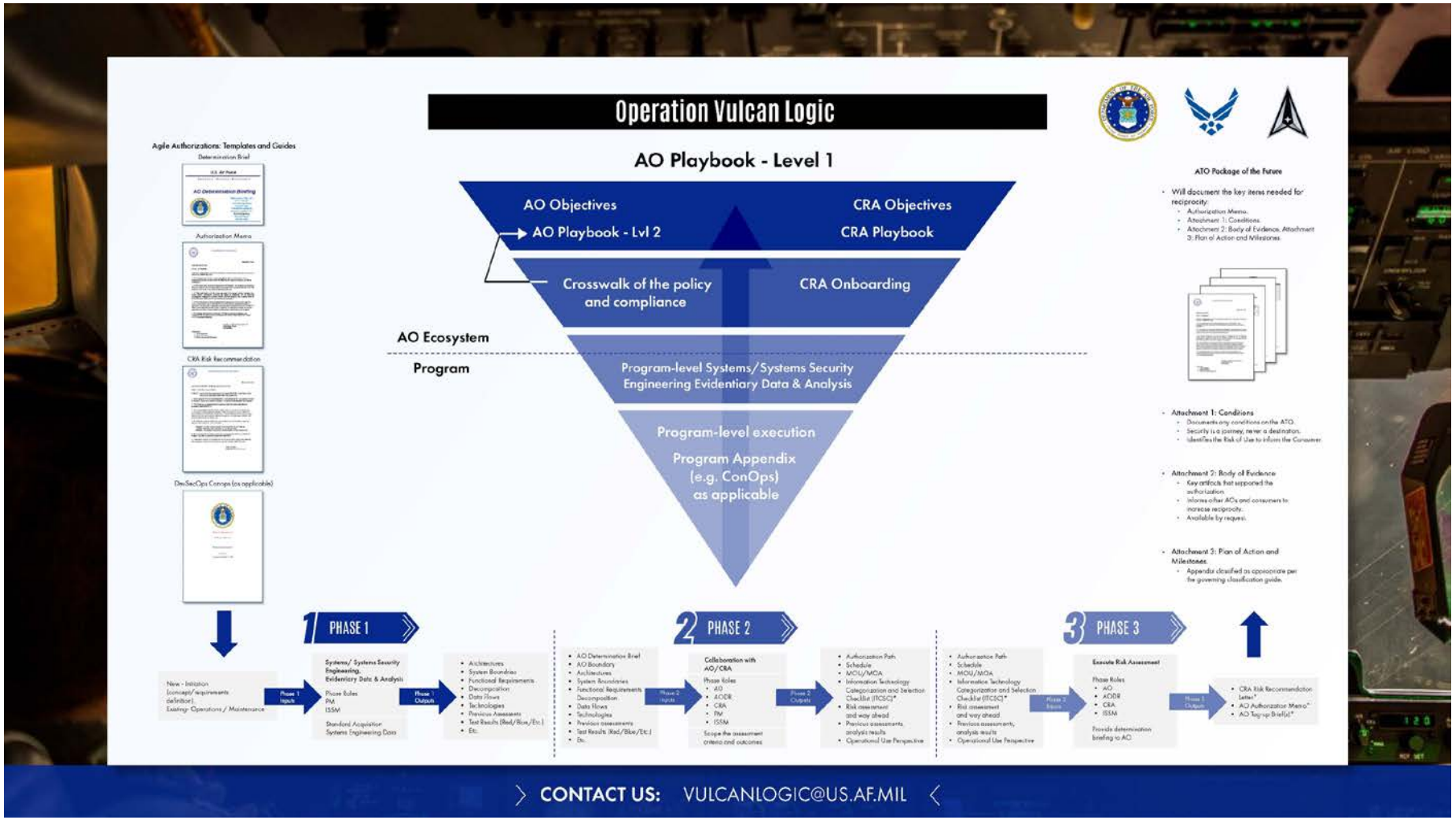
- **A Nutrition Facts label shows the consumer WHAT nutrients are in the food based on FDA guidelines.**
- **A Cyber Risk label shows the consumer what the RISK OF USE is for an application based on ATO Guidelines.**



Cyber Risk label is the foundation to an informed consumer and enables true reciprocity.

Operation Vulcan Logic Summary

VULCANLOGIC@US.AF.MIL



Summary: Keys to Success

- **Assurance:**
  - Establish Confidence:
    - We have assessed all the most significant risks.
    - Authorizations are not the finish line.
    - Continuous Monitoring is a key enabler.
- **Reciprocity:**
  - Establish Trust:
    - We will be transparent.
    - Risk tolerance variance is expected.
- **Partnership:**
  - Collaborative Risk Assessments:
    - Early coordination with stakeholders key to success.
    - Includes PEOs, SML/ML/PM, other AOs, other stakeholders (ATEA, TSN), users, industry
    - Fast-Track ATO Methodology is a key enabler.



VULCANLOGIC@US.AF.MIL

This is a work in progress. Need to continue to collaborate.

Questions and Discussion



VULCANLOGIC@US.AF.MIL

AFRMFKS Published AO Boundary Document Descriptions

- **AO Determination Brief Template:**
  - Brief to assist program personnel in understanding what the Authorizing Official is expecting to see to make an informed risk determination.
- **AO Determination Brief Guide:**
  - An AO determination brief guide has also been created to provide guidance on the completion of the above AO determination brief.
- **AO-Defined Roles and Responsibilities Chart:**
  - Roles and responsibilities for key stakeholders the AO or AO staff will interact with.
- **AO Playbook:**
  - A high-level guide on the AO objectives with Criteria, Observables, and Behavior (COB) expectations and templates used when interacting with the Authorizing Official for authorization determinations.
- **AO Tag-up Brief Template:**
  - Used to provide regular updates on system status to allow the Authorizing Official or Designated Representative to make continuous and on-going, risk-based determinations based on guidance from the Authorizing Official.
- **AODR/CRA Appointment Letter Template:**
  - Used to ensure personnel are directly appointed, in writing, to the roles of an AODR or CRA.
- **Authorization Memo Template:**
  - Leveraged to articulate the authorization determination to stakeholders. After the determination of risk from the operation or use of the information system has been made, this letter is used to inform the System Owner and other stakeholders of the authorization determination along with terms and conditions for the authorization.

AFRMFKS Published AO Boundary Document Descriptions

- **CRA Objectives:**
  - Provides an overall CRA goals and basic introduction to the Fast-Track Agile Authorization process (key steps/documents).
- **CRA Onboarding:**
  - Introduces/defines the tools (documents), websites, roles and responsibilities, engineering phases/outputs, documentation workflow, etc. (what the CRA needs to be successful in meeting the objectives/goals).
- **CRA Playbook:**
  - Outlines the Agile Authorization process, objectives, and step-by-step approach along with the templates used when interacting with the AO for authorization decisions.
- **CRA Risk Recommendation Letter:**
  - Articulates for the CRA the risk recommendation once the risk assessment is complete.
- **DSOP CONOPS:**
  - Addresses the process flows of developed code and software and the people that perform duties within that process flow, covering the hardware/software and the people operating the infrastructure.
- **Information Technology Categorization and Selection Checklist (ITCSC):**
  - Documents the security categorization of the system, including the information processed by the system and represented by the identified information types.
- **No Security Impact (NSI):**
  - Describes the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information for an information system.

Trusted Systems and Networks and Anti-Tamper in the Adaptive Acquisition Policy Framework

Randy Woods
Director, Systems Security Engineering and Anti-Tamper
Office of the Secretary of Defense for Research and Engineering

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

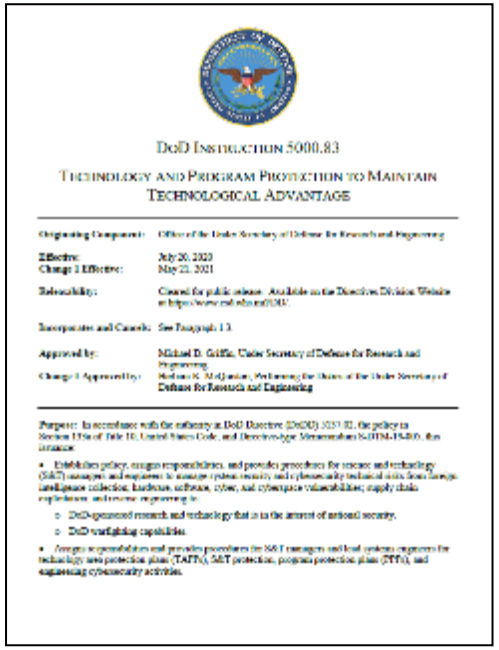
Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Briefing Overview

- DoD Instruction (DoDI) 5000.83 Role in the Adaptive Acquisition Framework
  - Hardware Assurance / Software Assurance
  - Supply Chain Risk Management (SCRM)
  - Anti-Tamper (AT)
- Adaptive Acquisition Framework (AAF)
  - Designates “Functional Areas” such as cyber and program protection to provide high level responsibilities and procedures supporting the DoD Directive (DoDD) 5000.01
- Trusted Systems and Networks (TSN) and Information and Communications Technology (ICT) Responsibilities in DoDI 5200.44
- Anti-Tamper and Exportability Responsibilities and the Establishment of the Anti-Tamper Executive Agent (ATEA) in DoDD 5200.47E
- Relationship between Program Protection and Anti-Tamper

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Program Protection and Anti-Tamper in the Adaptive Acquisition Framework



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component: Office of the Under Secretary of Defense for Research and Engineering

Effective: July 20, 2020
Change 1 Effective: May 21, 2021

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

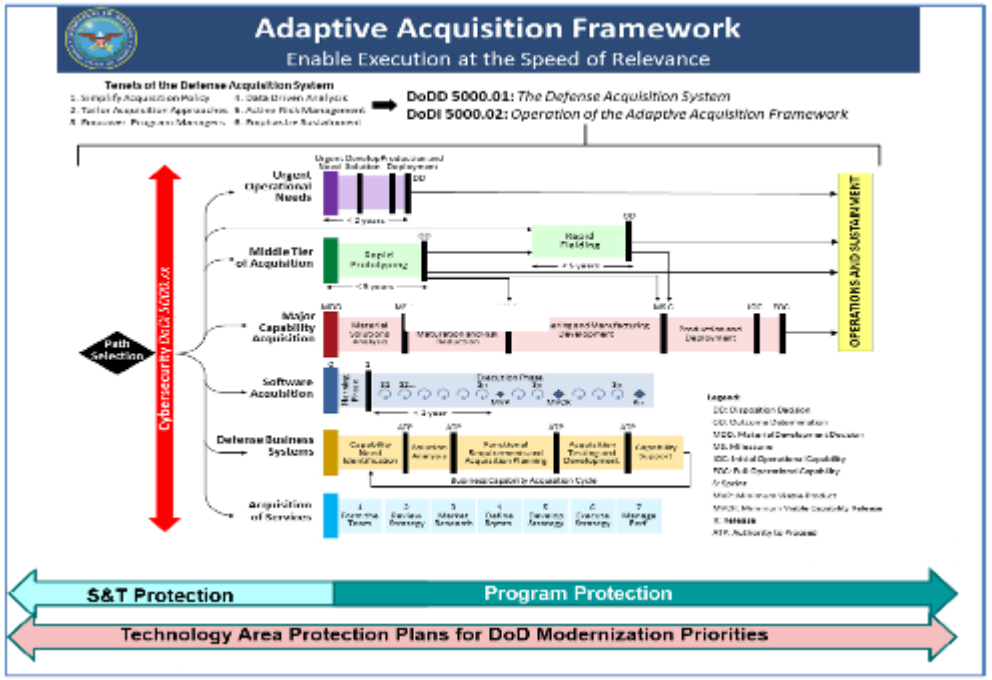
Incorporates and Cancels: See Paragraph 1.3

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Change 1 Approved by: Matthew P. Donovan, Performing the Duties of the Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Deputy's Management Action Group (DMAG) memorandum, this instruction:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering by:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

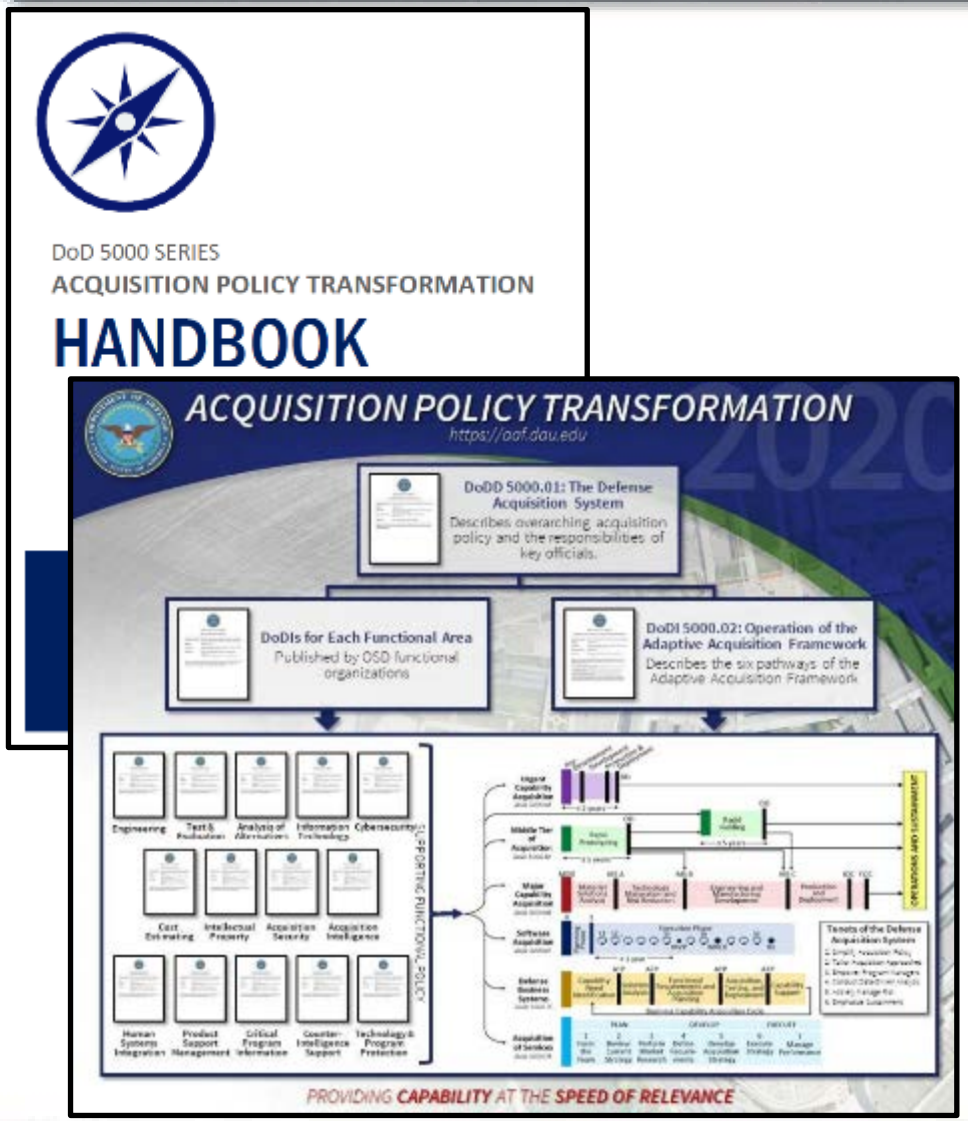


- DoDI 5000.83 establishes policy, assigns responsibilities, and provides procedures for **science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks** from: foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering.

- DoDI 5000.83 tailors program protection activities for selected Acquisition Pathways and Science and Technology:
  - DoDI 5000.85: Major Defense Programs
  - DoDI 5000.81: Urgent Capabilities
  - DoDI 5000.80: Middle Tier
  - DoDI 5000.87: Software

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Adaptive Acquisition Framework



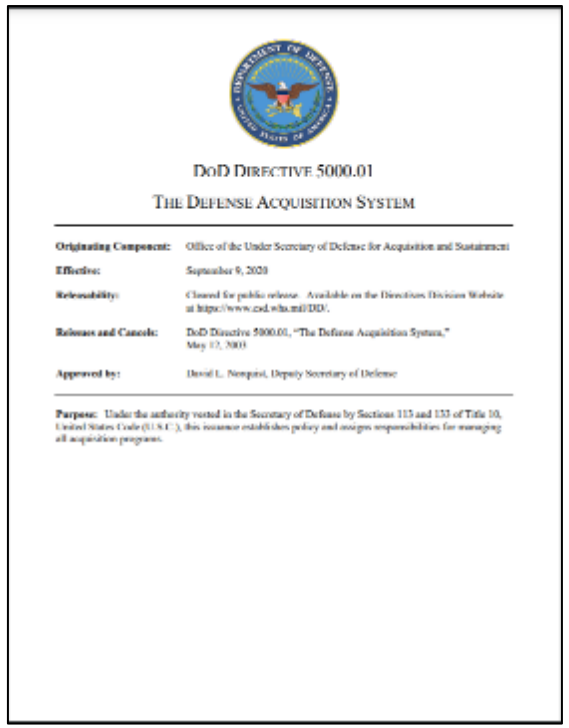
- DoDD 5000.01 *"The Defense Acquisition System"* instantiates 25 overarching policy statements supporting the National Defense Strategy (NDS)
- DoDI 5000.02 *"Operation of the Adaptive Acquisition Framework"* assigns responsibilities for employing the AAF to:
  - OUSD and DoD component heads
  - Specific program management responsibilities and authorities:
    - Milestone Decision Authority (MDA)
    - Program Executive Officer (PEO)
    - Program Manager (PM)
  - Procedures for utilizing the AAF Pathways

"MULTIPLE PATHWAYS FOR TAILORED SOLUTIONS"

HTTPS://WWW.DAU.EDU/AAF/

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

DoD Directive 5000.01
"The Defense Acquisition System"



DoD Directive 5000.01

The Defense Acquisition System

Originating Component: Office of the Under Secretary of Defense for Acquisition and Sustainment

Effective: September 9, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Reissues and Cancels: DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003

Approved by: David L. Norquist, Deputy Secretary of Defense

Purpose: Under the authority vested in the Secretary of Defense by Sections 113 and 133 of Title 10, United States Code (U.S.C.), this issuance establishes policy and assigns responsibilities for managing all acquisition programs.

d. Develop and Deliver Secure Capabilities.

Security, cybersecurity, and protection of critical technologies at all phases of acquisition are the foundation for uncompromised delivery and sustainment of warfighting capability. Acquisition managers, in coordination with security and counterintelligence (CI) professionals, will implement initiatives and processes for the identification, integration and continual evaluation of security and CI requirements throughout the life cycle of a system, service, or critical technology.

q. Deploy Interoperable Systems.

Joint concepts, standardization, and integrated architectures will be used to the maximum extent possible to characterize the exchange of data, information, materiel, and services to and from systems, units, and platforms to assure all systems effectively and securely interoperate with other U.S. forces and coalition partner systems.

t. Plan for Coalition Partners.

To enable allies and partners to enhance U.S. military capability, collaboration opportunities, potential partnerships, and international acquisition and exportability features and limitations will be considered in the early design and development phase of acquisition programs.

These three policy statements anchor program protection and anti-tamper into the Defense Acquisition System in support of the National Defense Strategy

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

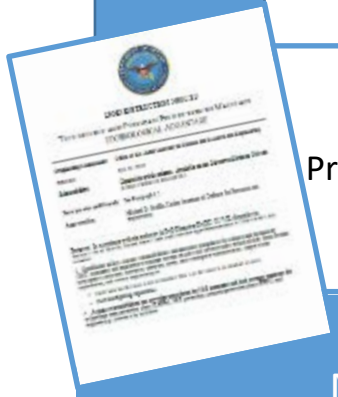
DoD Instruction 5000.83 Responsibilities: System Security Engineering and Anti-Tamper

USD(R&E) – Establish and maintain S&T and program protection policy, guidance, education and training to manage technical risk

1. Anti-Tamper/Exportability Features
2. Hardware and Software Assurance
3. Supply Chain Risk Management
4. System Assurance
5. Engineering Secure Cyber Resilient Systems

5200.47E

5200.44



DoDI 5000.83
Technology and Program Protection (T&PP) to Maintain Technology Advantage
OPR: USD(R&E)/STPE/RS

Direction to S&T Managers and Engineers

Chairman Joint Chief of Staff (CJCS) – SCRM, Export Control and AT Requirements to achieve T&PP

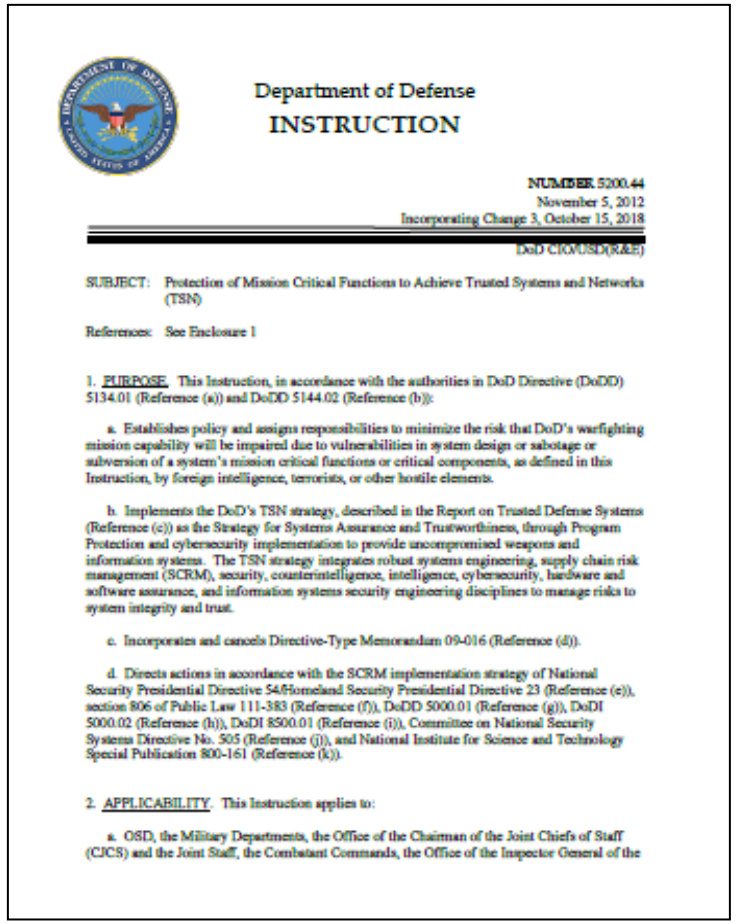
1. Included in Capability Requirement in Joint Capabilities Integration Development System (JCIDS)
2. Addressed during Capability Development

USD(A&S) - Include Technology Area Protection Plans and Program Protection Planning in:

1. The Defense Acquisition System (DAS) to inform programs and sustainment risk decisions
2. When developing and implanting international acquisition and exportability
3. In DAU education and training

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

DoD Instruction 5200.44 (Oct. 2018 Version) Protection of Mission Critical Functions to Achieve Trusted Systems and Networks



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 3, October 15, 2018
DoD CIO/USD(R&E)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoDD 5000.01 (Reference (g)), DoDI 5000.02 (Reference (h)), DoDI 8500.01 (Reference (i)), Committee on National Security Systems Directive No. 505 (Reference (j)), and National Institute for Science and Technology Special Publication 800-161 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the

- **Implements the DoD's TSN Strategy**
- **Manage risk of mission critical function and component compromise throughout lifecycle of key systems by utilizing:**
  - Criticality Analysis (based on mission's criticality) as the systems engineering process for risk identification
  - Countermeasures: SCRM, software assurance, hardware assurance, and secure design procedures
  - Intelligence and counterintelligence analysis to inform program management
  - Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document planning and accomplishments in program protection and cybersecurity activities**

Resilient Systems has close partnership with Office of DoD Chief Information Officer (CIO) and is currently working to update DoDI 5200.44

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Trusted Systems and Networks Approach to Technology and Program Protection

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

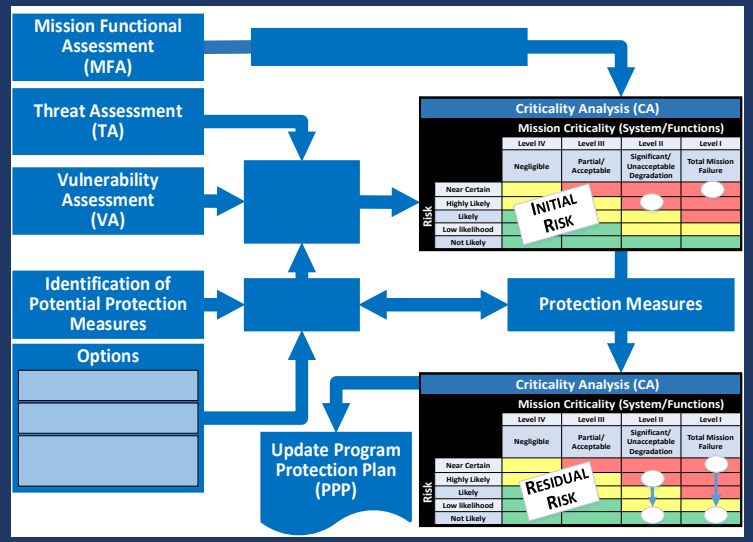
Manage Risk

TSN Strategy

Applicable Systems

- National Security Systems (NSS) as defined by Section 3552 U.S.C 44
- DoDI 8510.01: Risk Management Framework (RMF) high impact for Confidentiality/Integrity/Availability (C/I/A)
- Other DoD systems that the DoD Component Acquisition Executive (CAE) or Chief Information Officer (CIO) determines are critical

Process

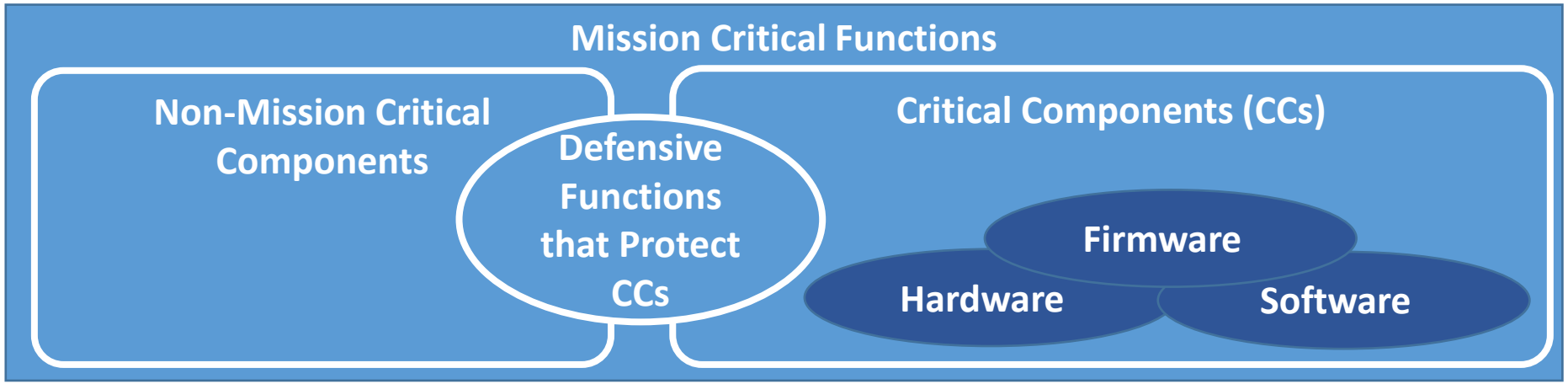


- Conduct Criticality Analysis
- Conduct Threat/ Vulnerability Analysis
- Identify/Assign Risks and Mitigations
- Track Residual Risks and Protection Measures

Technology and program protection activities occur throughout the lifecycle of the system

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

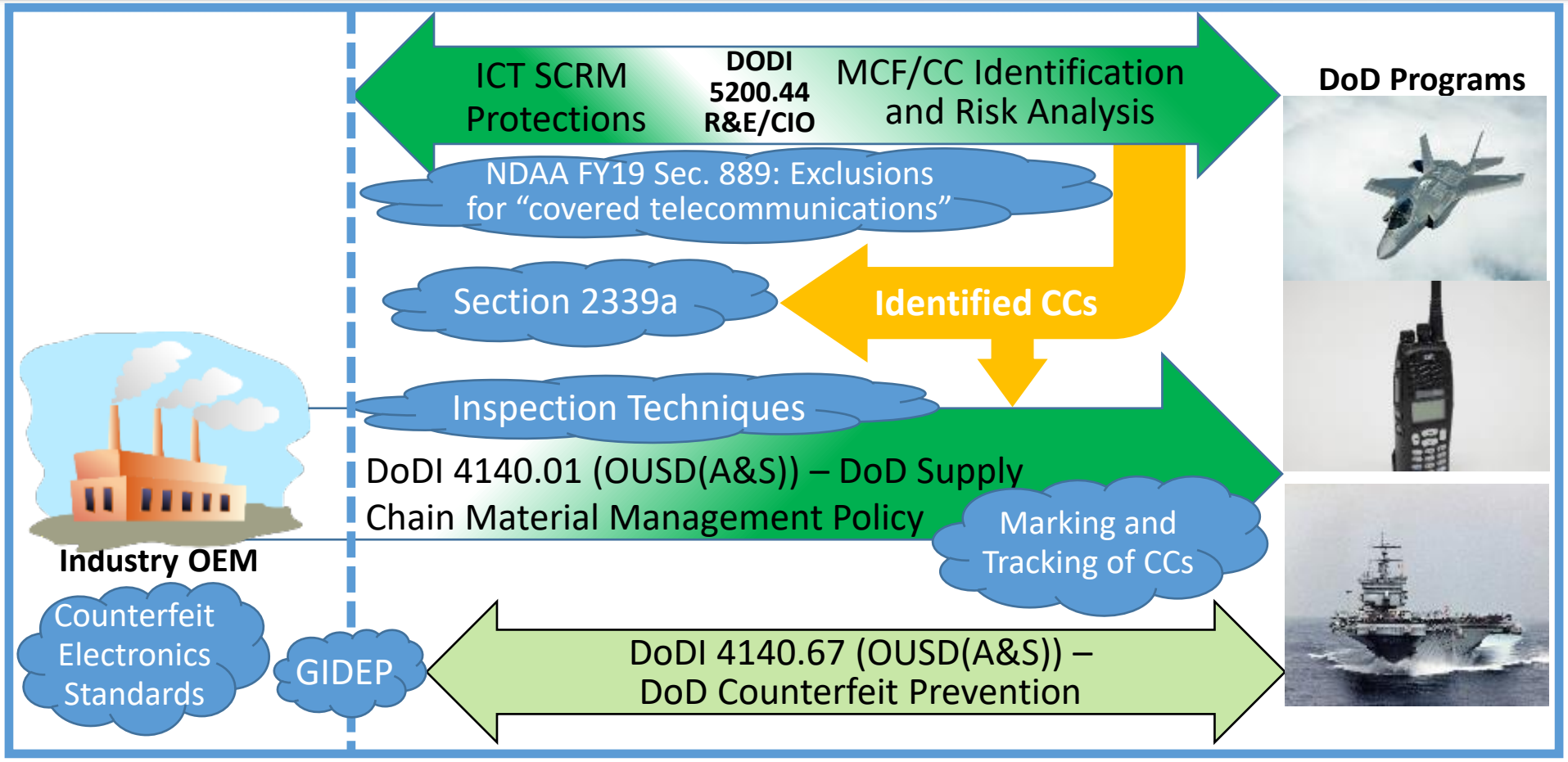
DoD Instruction 5200.44
Mission Critical Functions and Components



- **Mission Critical Functions (MCFs):**
  - Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed (Source: DoDI 5200.44)
- **Critical Components (CCs):**
  - **A component which is or contains information and communications technology (ICT)** including **hardware, software, and firmware**, whether custom, commercial, or otherwise developed and **delivers or protects** mission critical functionality of a system or which, because of the system's design, **may introduce vulnerability** to the mission critical functions of an applicable system (Source: DoDI 5200.44, 4140.01, and 4140.67)

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

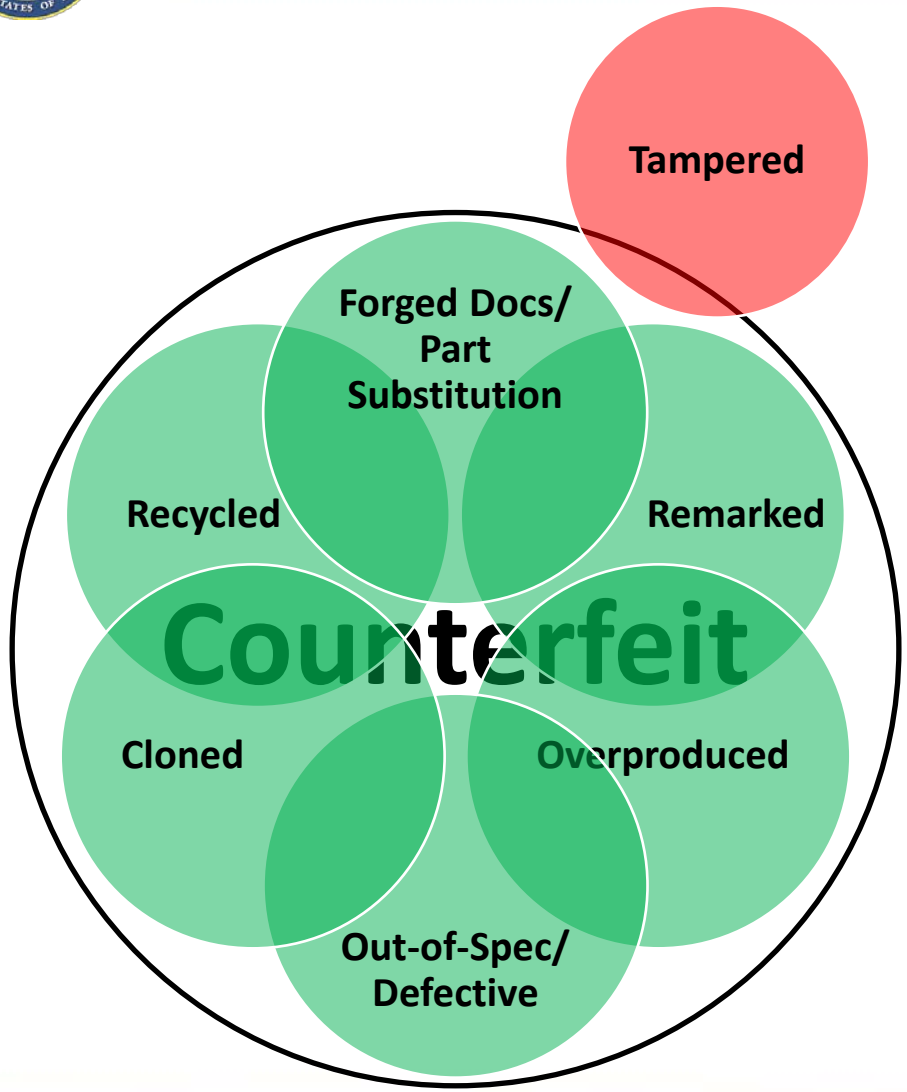
Criticality Analysis and Supply Chain Risk Management (SCRM) in Policy



SCRM: A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (Source: DoDI 5200.44)

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

DoD Instruction 5200.44
Counterfeit and Tampered Devices



- **Counterfeit electronic part:**
  - An unlawful or unauthorized reproduction **(cloned/overproduced)**, substitution **(part substitution)**, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer **(forged docs)**, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new **(recycled/remarked)**, or the false identification of grade, serial number, lot number, date code, or performance characteristics **(out-of-spec/defective).**
- DFARS 252.246-7007 or SAE AS6171 definition are not designated for the detection of tampered devices.
- DoDI 5200.44 SCRM Practices are tailored to **identify and exclude** potential suppliers who present an unacceptably high risk to procurement for DoD.

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

DoD Instruction 5000.83 Procedures: Activities to Mitigate Adversary Threats to Technology and Programs

Foreign Military Sales







Section 3.3.c.(6).a – Apply Horizontal Protection Guidance (HPG) to determine requirements for designing and implementing exportability features when outside U.S. control

Section 3.3.c.(6) - Identification and Protection of the warfighters' technical advantage

Combat Losses





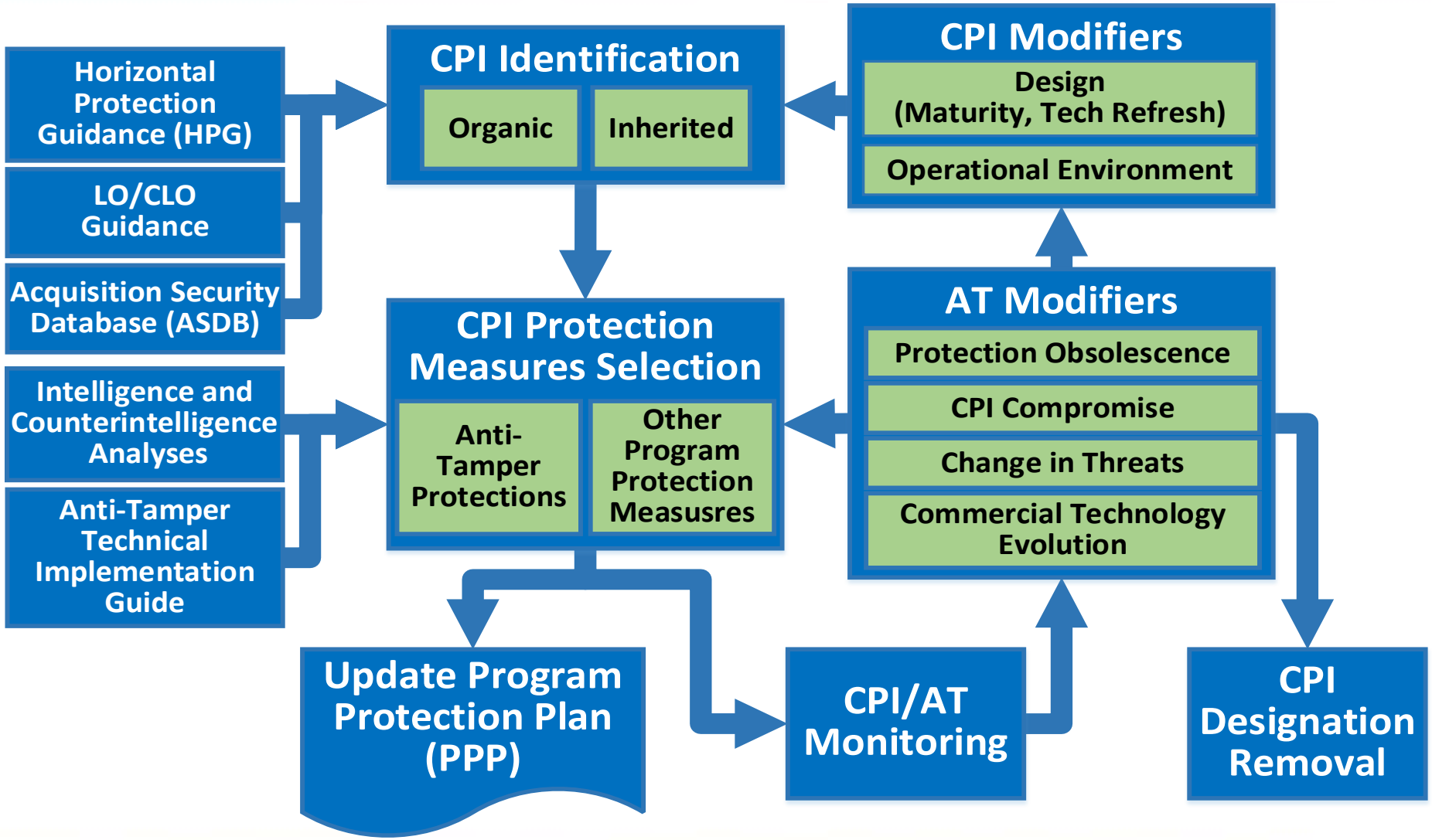




Section 3.3.c.(6).b – Coordinate with applicable DoD component's Office of Primary Responsibility (OPR) for DoD AT to mitigate reverse engineering opportunities.

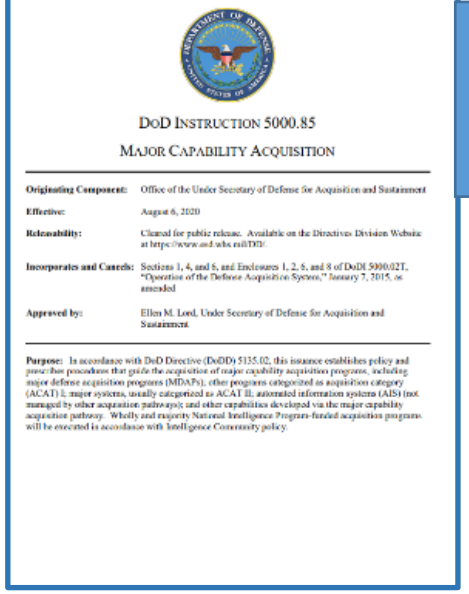
Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Critical Program Information (CPI) Identification Methodology



Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

DoD Instruction 5000.85 "Major Capability Acquisition" Relationship to Foreign Military Sales and Anti-Tamper



DoD INSTRUCTION 5000.85

MAJOR CAPABILITY ACQUISITION

Originating Component: Office of the Under Secretary of Defense for Acquisition and Sustainment

Effective: August 6, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: Sections 1, 4, and 6, and Enclosures 1, 2, 6, and 8 of DoDI 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

Approved by: Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with DoD Directive (DoDD) 5135.02, this issuance establishes policy and prescribes procedures that guide the acquisition of major capability acquisition programs, including major defense acquisition programs (MDAPs), other programs categorized as acquisition category (ACAT) I, major systems, usually categorized as ACAT II, automated information systems (AIS) not managed by other acquisition pathways and other capabilities developed via the major capability acquisition pathway. Wholly and majority National Intelligence Program-funded acquisition programs will be executed in accordance with Intelligence Community policy.

(3) Pursue cooperative opportunities and international involvement throughout the acquisition lifecycle to enhance international cooperation and improve interoperability in accordance with DoDI 2010.06.

Responsibilities:

3. DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY (DSCA)

   a. Serve as the focal point for all requests and as the approval authority for foreign military sales (FMS).

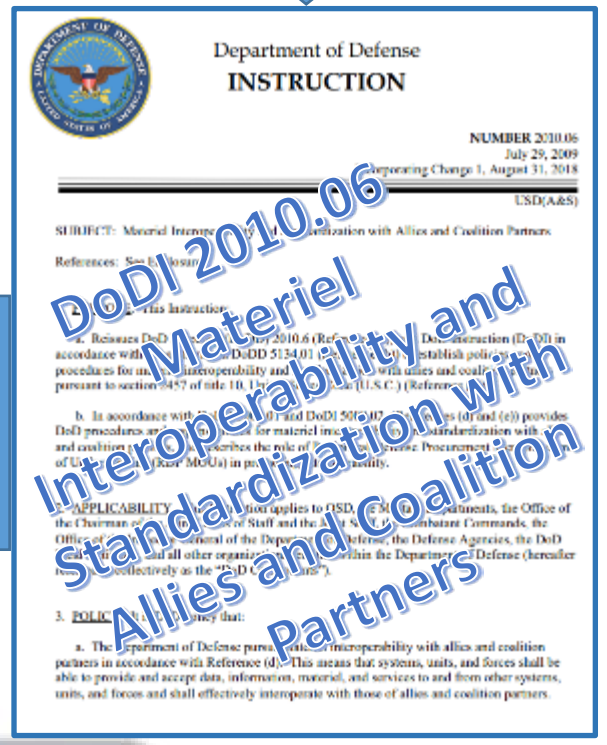
5. SECRETARIES OF THE MILITARY DEPARTMENTS AND DIRECTORS OF THE DEFENSE AGENCIES

   b. Ensure that weapon system design takes into account potential future transfers to allied nations, **incorporates needed anti-tamper features**, and accommodates modifications that make export possible and affordable.

Procedures:

c. During the production and deployment phase of systems acquisition through

   (2) FMS of military systems or equipment and support involving the use of FMS procedures and commercial licenses to transfer to a foreign nation, under DoD Manual 5105.38-M, the ability to produce U.S. defense articles developed and fielded by the Department of Defense. **Anti-tamper measures during the acquisition process need to be considered** to provide allies with U.S. origin defense articles developed and fielded by the Department of Defense.



Department of Defense

INSTRUCTION

NUMBER 2010.06

July 29, 2009

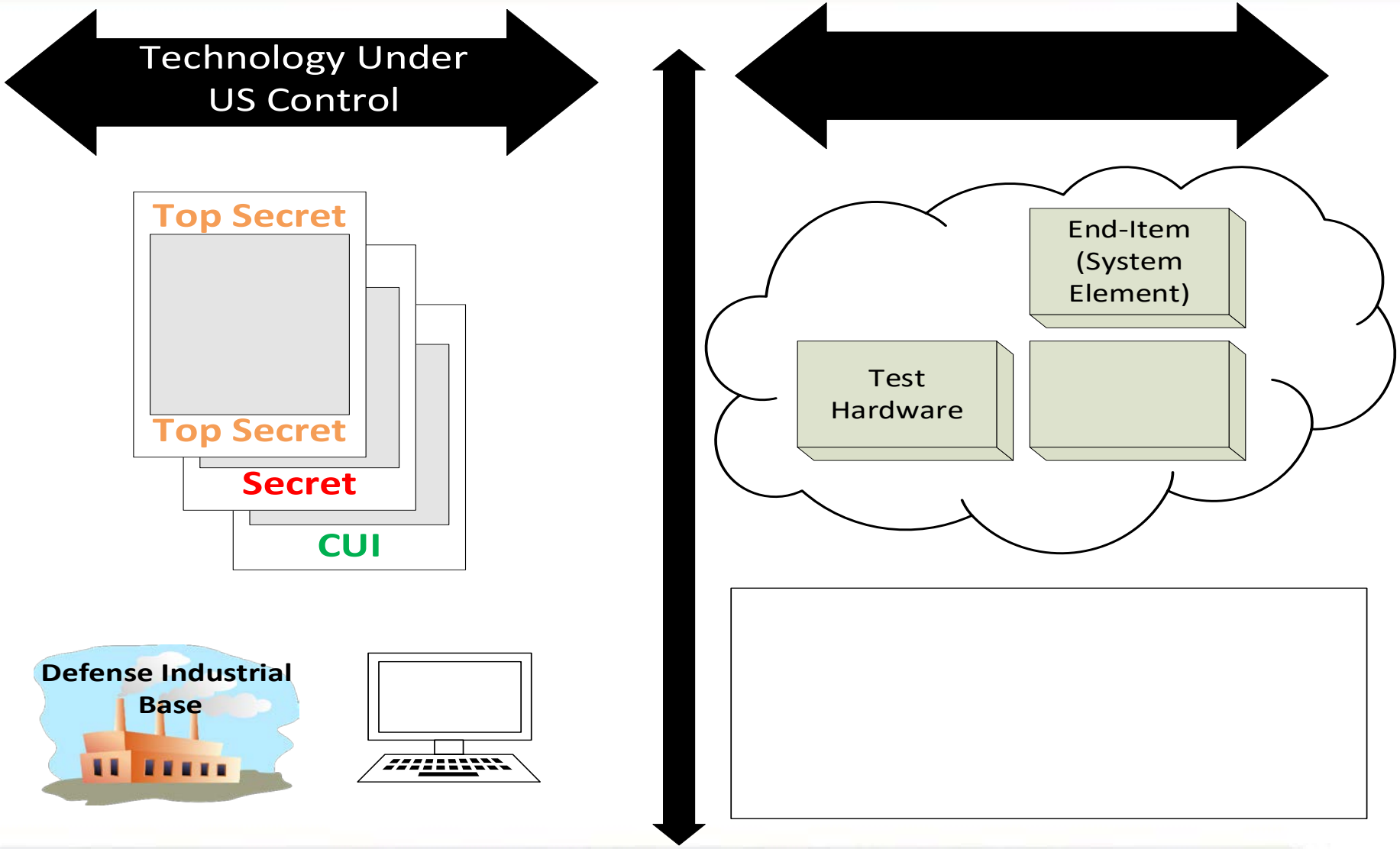
Incorporating Change 1, August 31, 2018

USD(A&S)

SUBJECT: Materiel Interoperability and Standardization with Allies and Coalition Partners

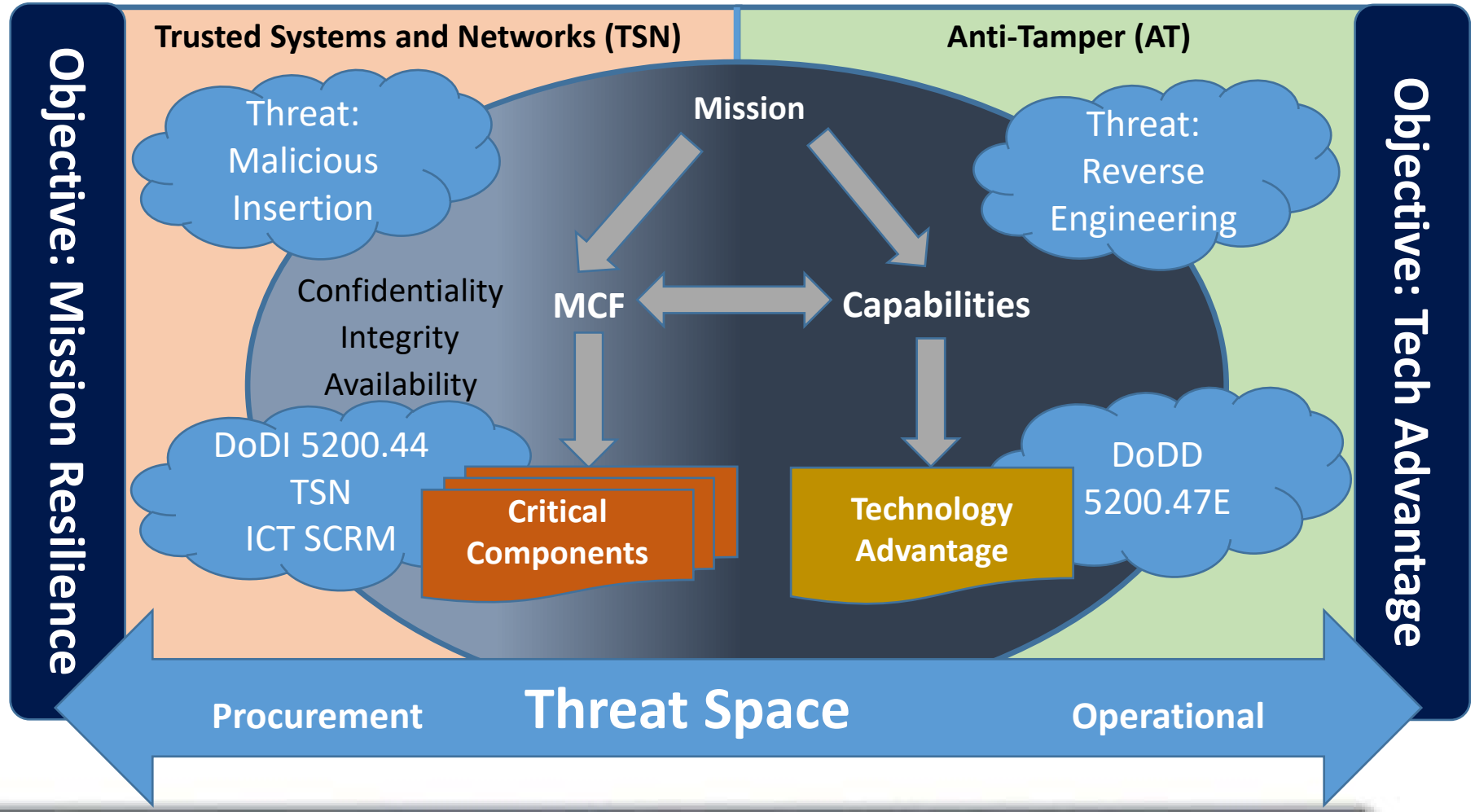
DoDI 2010.06 Materiel Interoperability and Standardization with Allies and Coalition Partners

Concepts for Technology Advantage Elements (TAE)



TSN and AT Summary

TSN and AT support the AAF across the program lifecycle to secure and maintain the warfighters' technology advantage



Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.

Questions

Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.



Distribution Statement A: Approved for public release. DOPSR case #22-S-0343 applies. Distribution is unlimited.



Raytheon Technologies

NDIA Systems & Mission Engineering Conference 2021

Cyber Supply Chain Risk Management (SCRM) Engineer, a Security Specialty within System Security Engineering

Abstract #23774

Holly Dunlap, Holly.Dunlap@Raytheon.com
Raytheon Missiles & Defense, System Security Engineering
Cyber SCRM Engineering SME

December 2021

Distribution Statement A- Approved for public release; distribution is unlimited.

© 2021 Raytheon Technologies Corporation.
All rights reserved.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Agenda

- What is Cyber SCRM?
- Adversary
- Global Supply Chain Risks
- Customer Requirements
- Standards
- Future State Vision
- Integrating Cyber SCRM into RTX – It's a journey.
- Raytheon Cyber SCRM Role & Responsibility
- Customer Program Perspective Example
- Key Takeaways

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.

Key Definitions

- **Supply Chain Risk.** The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
  - DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

- ***Cyber Supply Chain Risk Management*** **(C-SCRM)** is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. It covers the entire lifecycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an ICT product or service at any stage of the lifecycle. Department Homeland Security (DHS)

- ***Cyber Supply Chain Risk Management (C-SCRM)*** is a systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.
  - *DRAFT* NIST 800-161 Rev 1, Cyber Supply Chain Risk Management Practices for Systems and Organizations

* ICT – Information Communication Technology

Distribution Statement A- Approved for public release; distribution is unlimited.

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.

The Threat is Real…

The Adversary has moved from attacking our systems directly to attacking our supply chain.



Battlefield Losses: Yugoslav Museum of Aviation

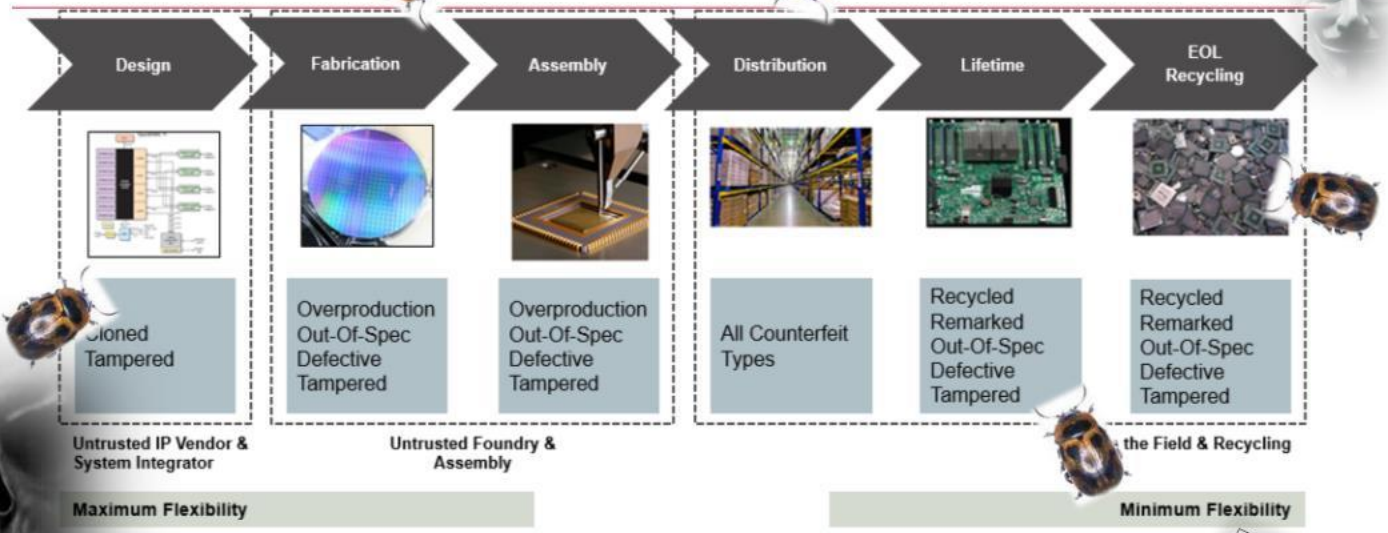


These are *Not* Cooperative R&D Efforts

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.

Cyber Supply Chain Risk Management

The Global Supply Chain presents the greatest attack surface to our national security systems.



Microelectronics is DOD's new No. 1 technology priority,
bumping hypersonics to No. 3 – Inside Defense June 29, 2020





We are responsible the authenticity & integrity of the components integrated into our systems.

Raytheon Technologies

Distribution Statement A- Approved for public release; distribution is unlimited.

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.

Key Protection Activities to Improve Cyber Resiliency

Cyber SCRM Requirements are derived from DoDI 5200.44

Program Protection & Cybersecurity

DoDI 5000.02, Enclosure 3 & 14

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

DoDI 5200.39 | DoDI 5200.44 | DoDI 5230.24 | DoDI 8510.01

Technology

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

Key Protection Activity:

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

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Activity:

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

Goal: Protect key mission components from malicious activity

Information

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

Key Protection Activity:

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

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

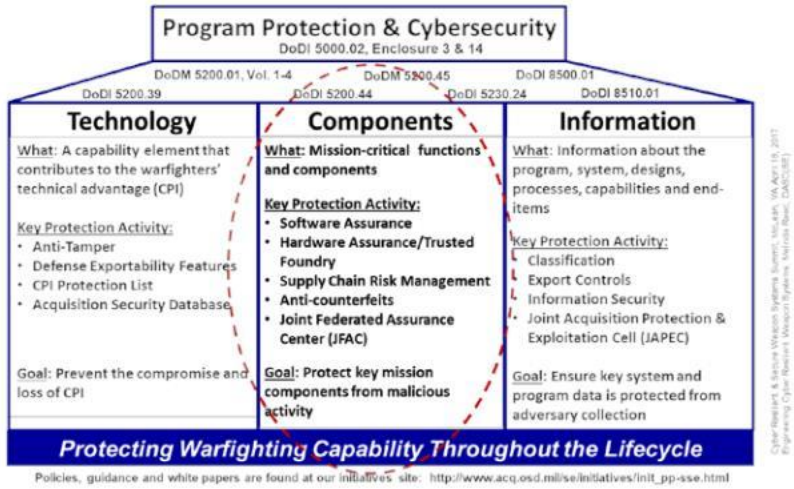
Protecting Warfighting Capability Throughout the Lifecycle

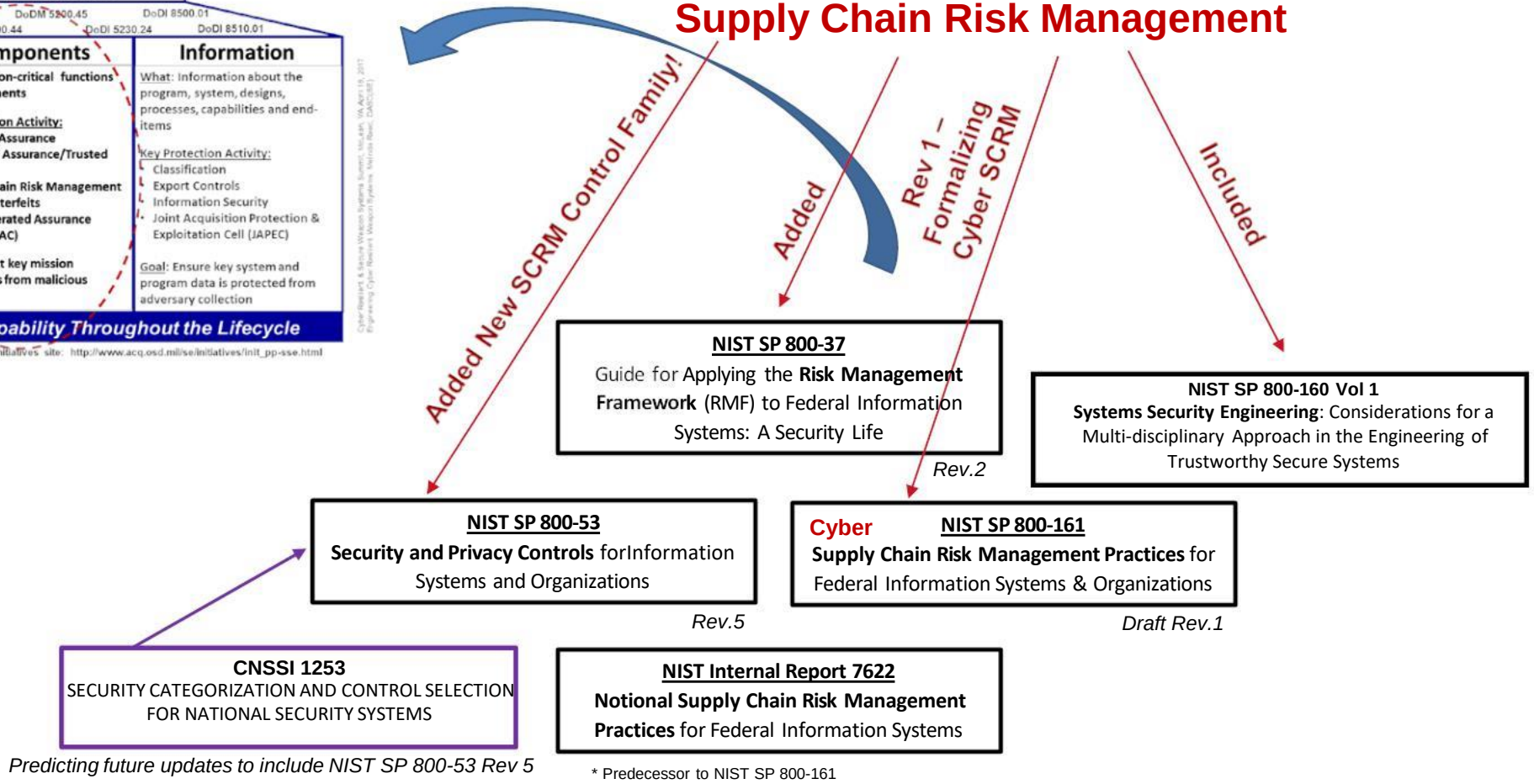
Cyber Resilient & Secure Weapon Systems Summit, McLean, VA April 18, 2017
Engineering Cyber Resilient Weapon Systems, Melinda Reed, DASD(SE)

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

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.

Relationship of DoD Acquisition Policies and Industry Best Practices often referred to as Standards





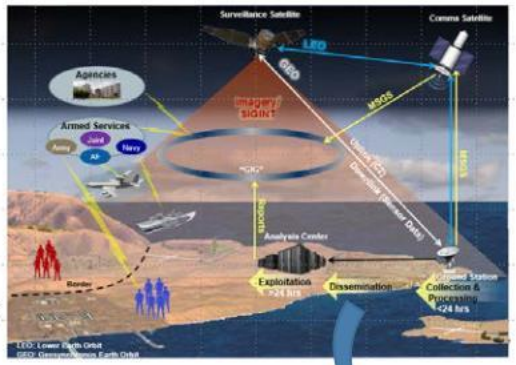
Distribution Statement A- Approved for public release; distribution is unlimited.

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.

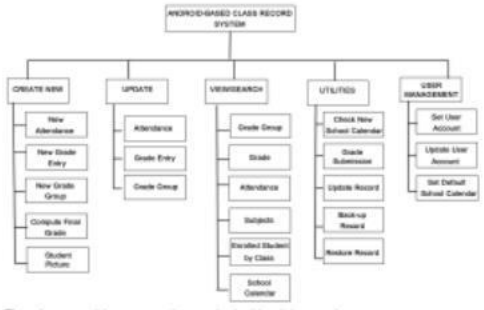
Raytheon Future State
Cyber Supply Chain Risk Management

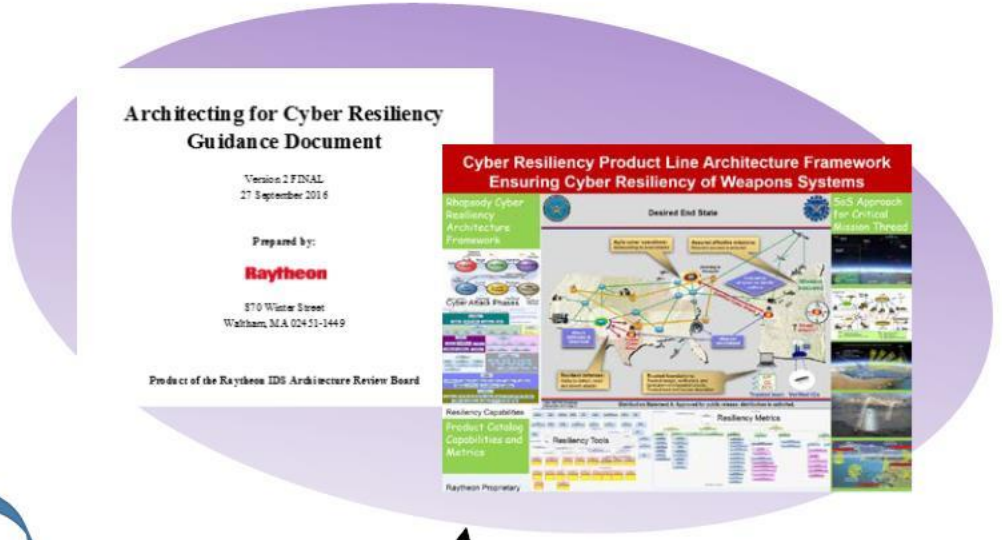
Operational Systems of Systems

Mission Thread Analysis to Critical Component Identification & Categorization Enabler



System Functional Decomposition





SwA Raytheon Vulnerability Assessment Process (Guide & Enabler)

Internal Test Capability Catalog & Guide

Capability 1,2,3,4,5….
- Applicable Type of Component
- Level of Risk Mitigation

Statistical Test Optimization

Software / Firmware (?)

Hardware / Firmware

Test

Critical Components Identification & Categorization (Hardware, Software, Firmware)

Architecture Design Testing

Internal

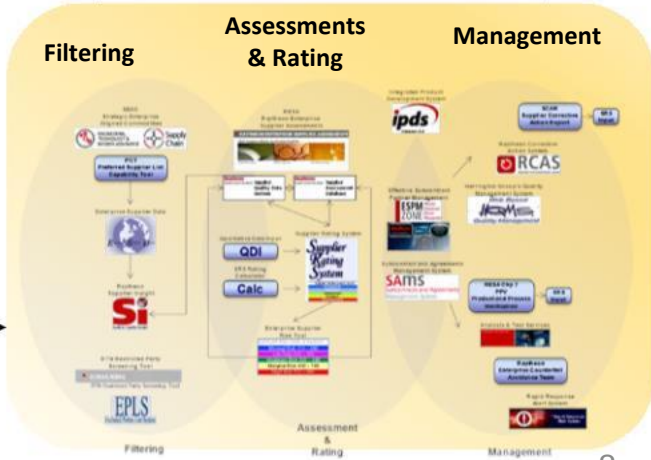
Internal Or External

External

Internal Risk Mitigation Product Catalog

Supply Chain Trade Space Options

Filtering | Assessments & Rating | Management



Raytheon Technologies

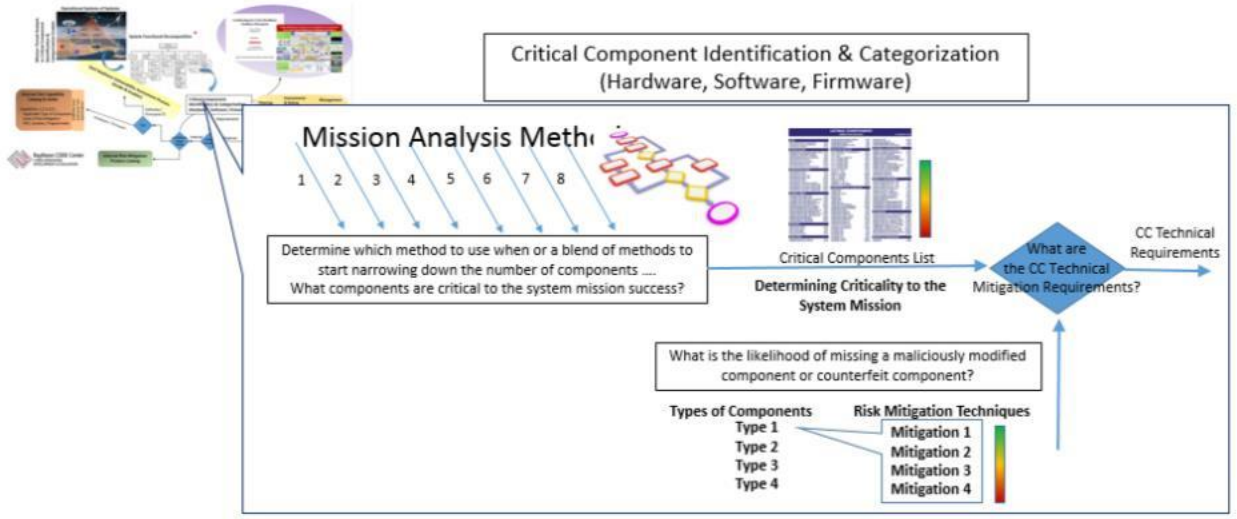
Distribution Statement A- Approved for public release; distribution is unlimited.

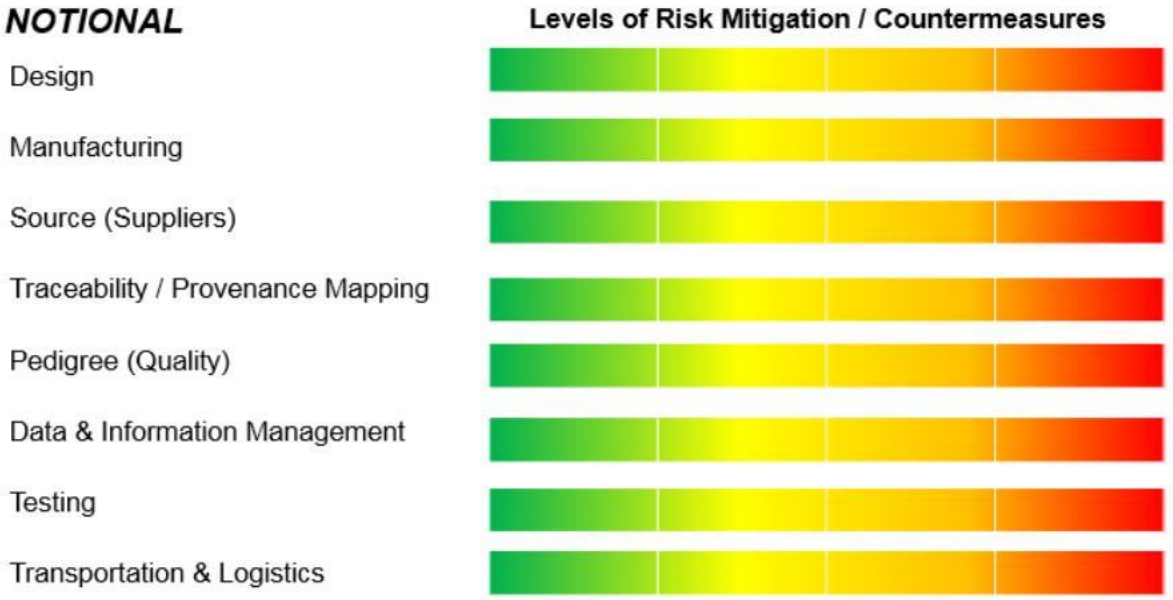
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Catalog Trade Based Cyber SCRM Options

Programs need a ***range of risk mitigations*** to address supply chain risks for our System Mission Critical Components.

- Tiered Component Design Features
- Tiered Criteria and Audits for Levels of Security in Manufacturing
- Tiered Criteria and Evaluation of Suppliers
- Tiered Criteria for Critical Component Pedigree
- Tiered Requirements to Flow to Suppliers for How to Manage Data & Information
- Tiered Criteria and Options for Test Requirements and Evidence by the Type of Component
- Tiered Criteria and Options for Transportation & Logistics Mitigations.





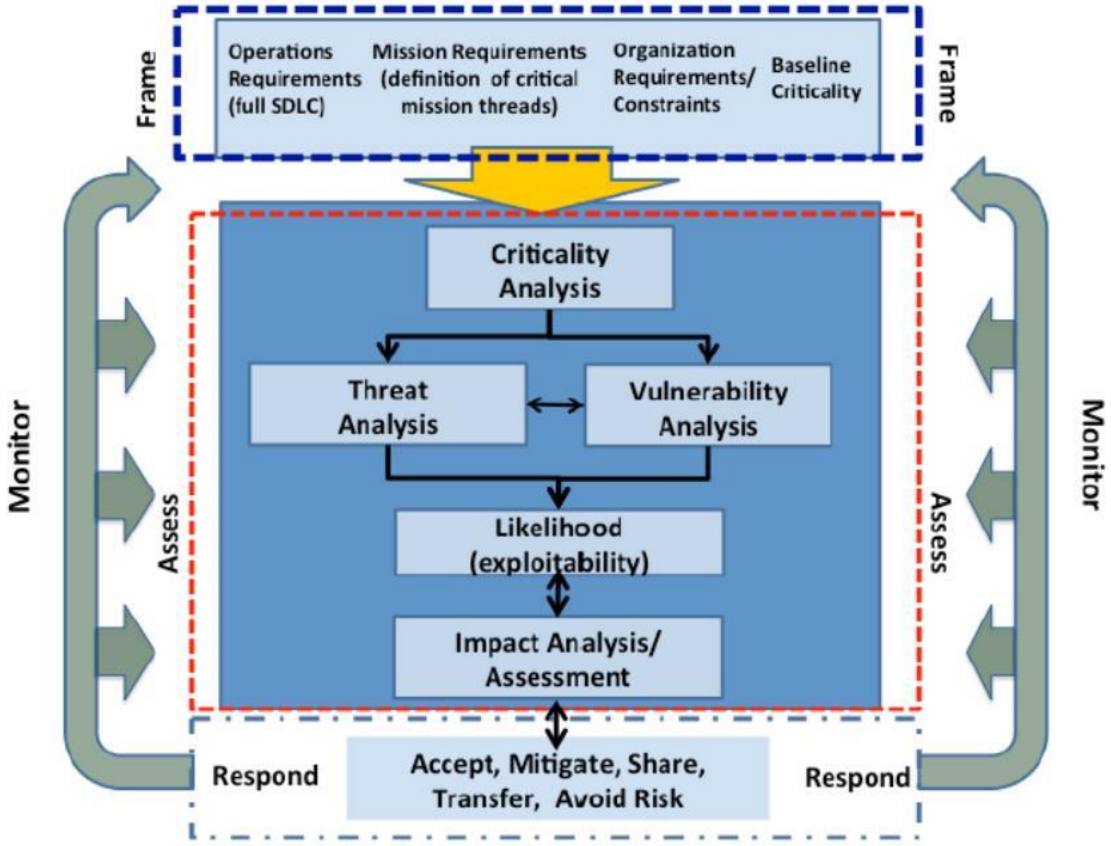
Raytheon Technologies

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.

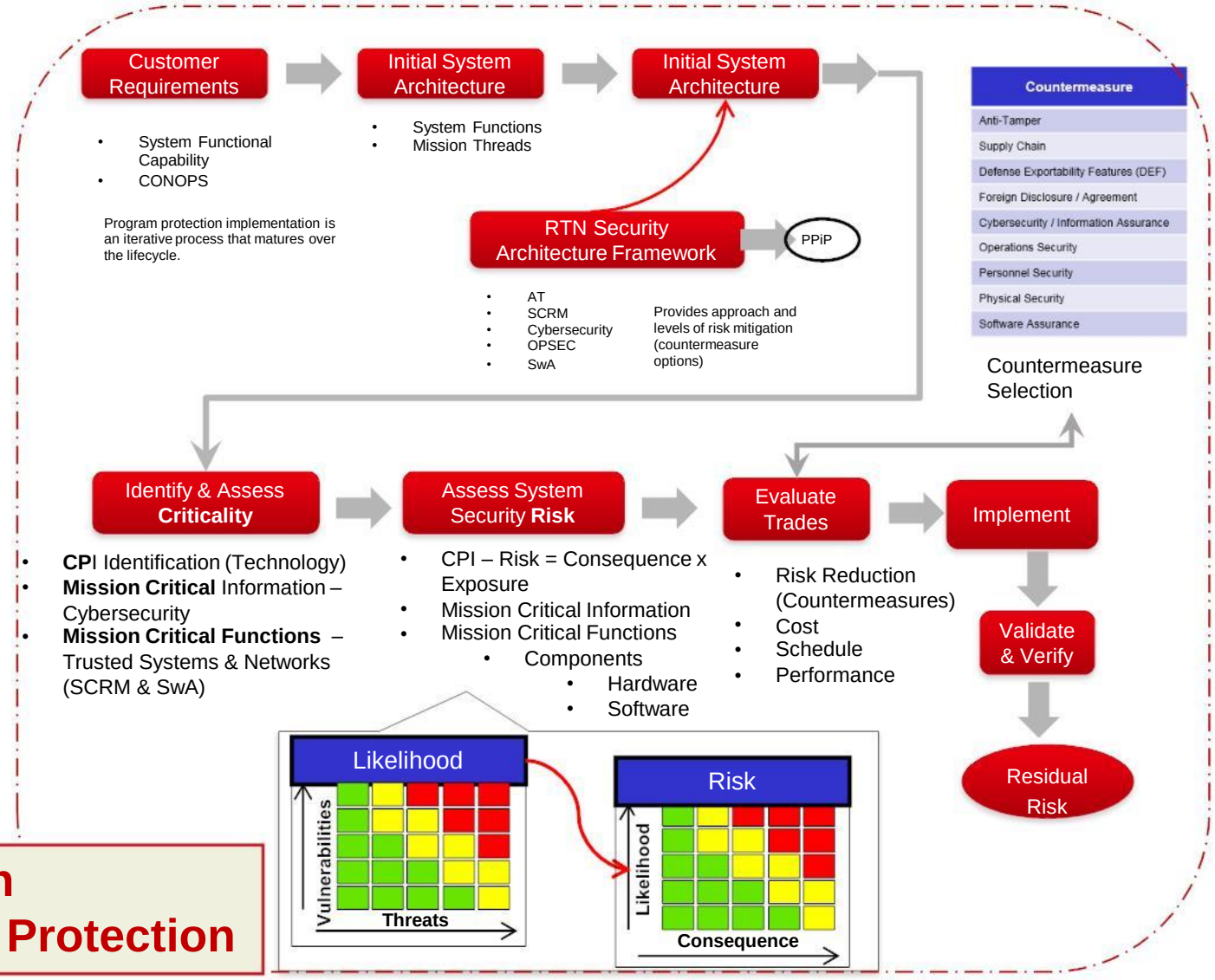
Cyber Supply Chain Risk Management

NIST SP 800-161

Supply Chain Risk Management Practices for Federal Information Systems & Organizations



https://csrc.nist.gov/publications/detail/sp/800-161/final

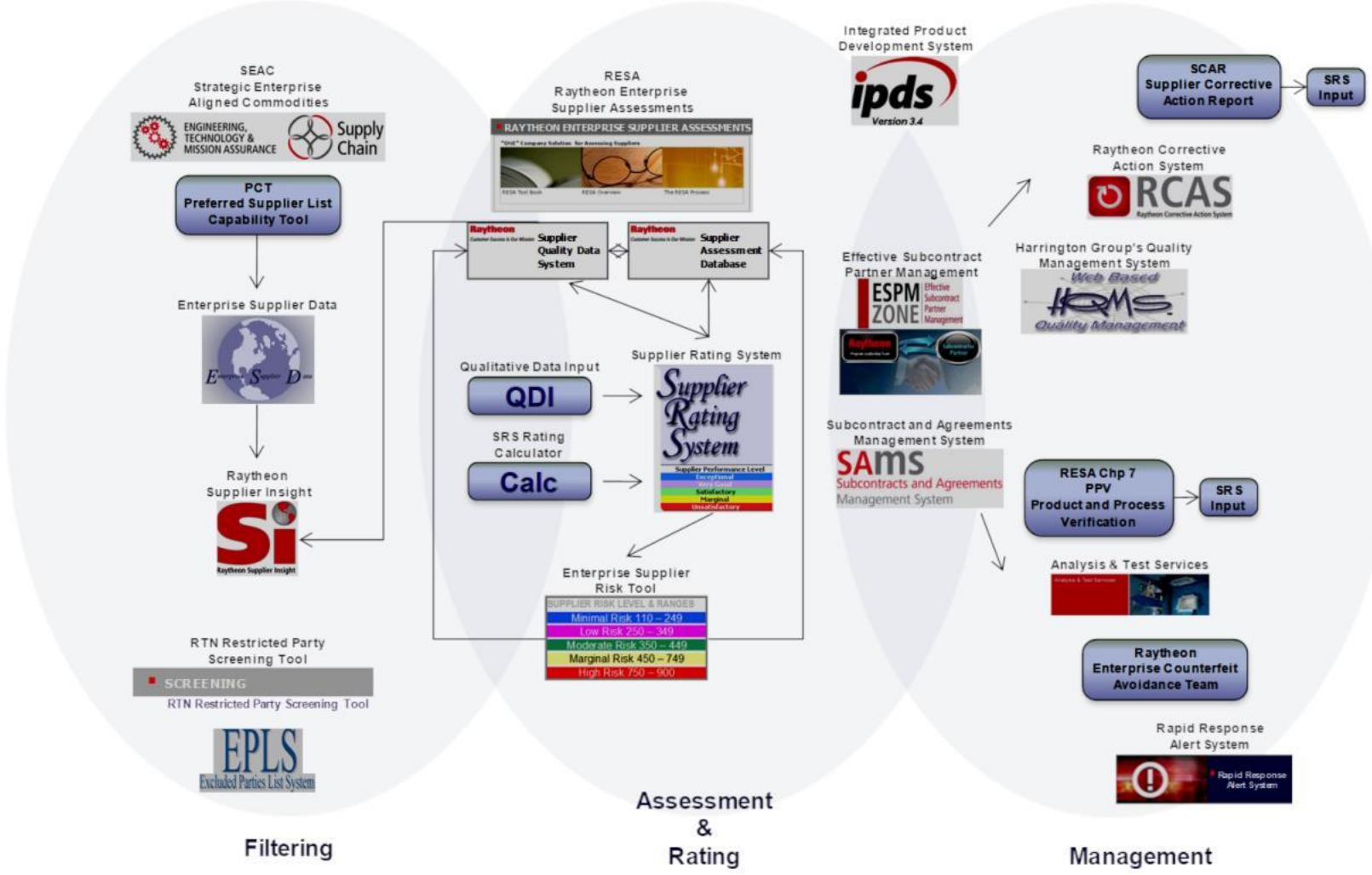


Raytheon Program Protection

Raytheon Technologies

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.

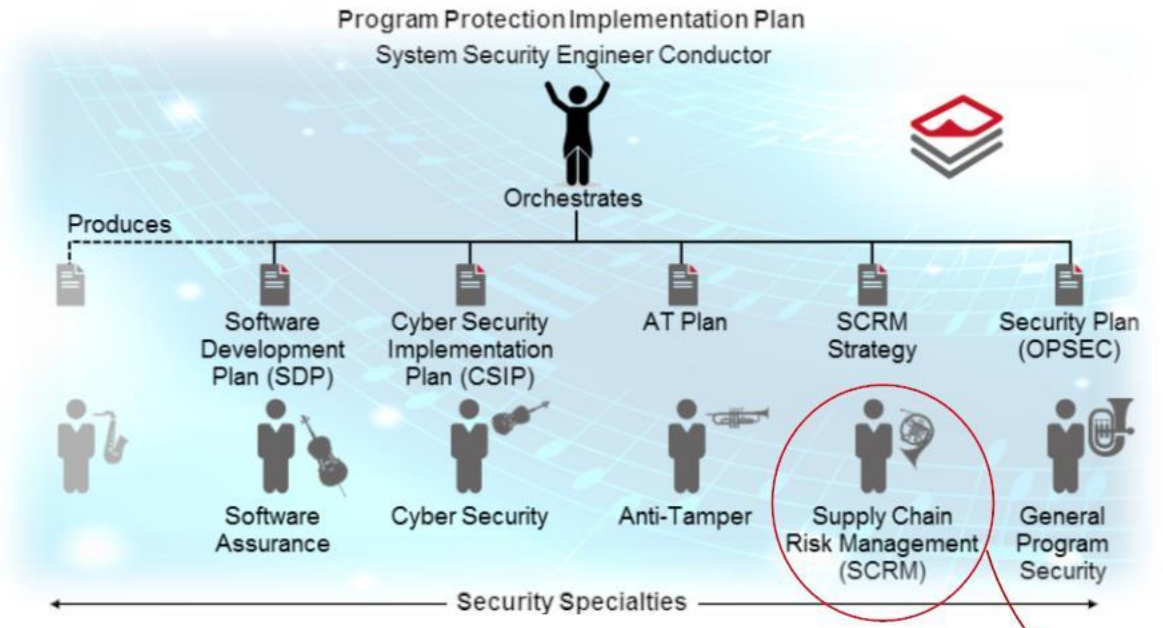
Raytheon's Integrated Supply Chain Construct

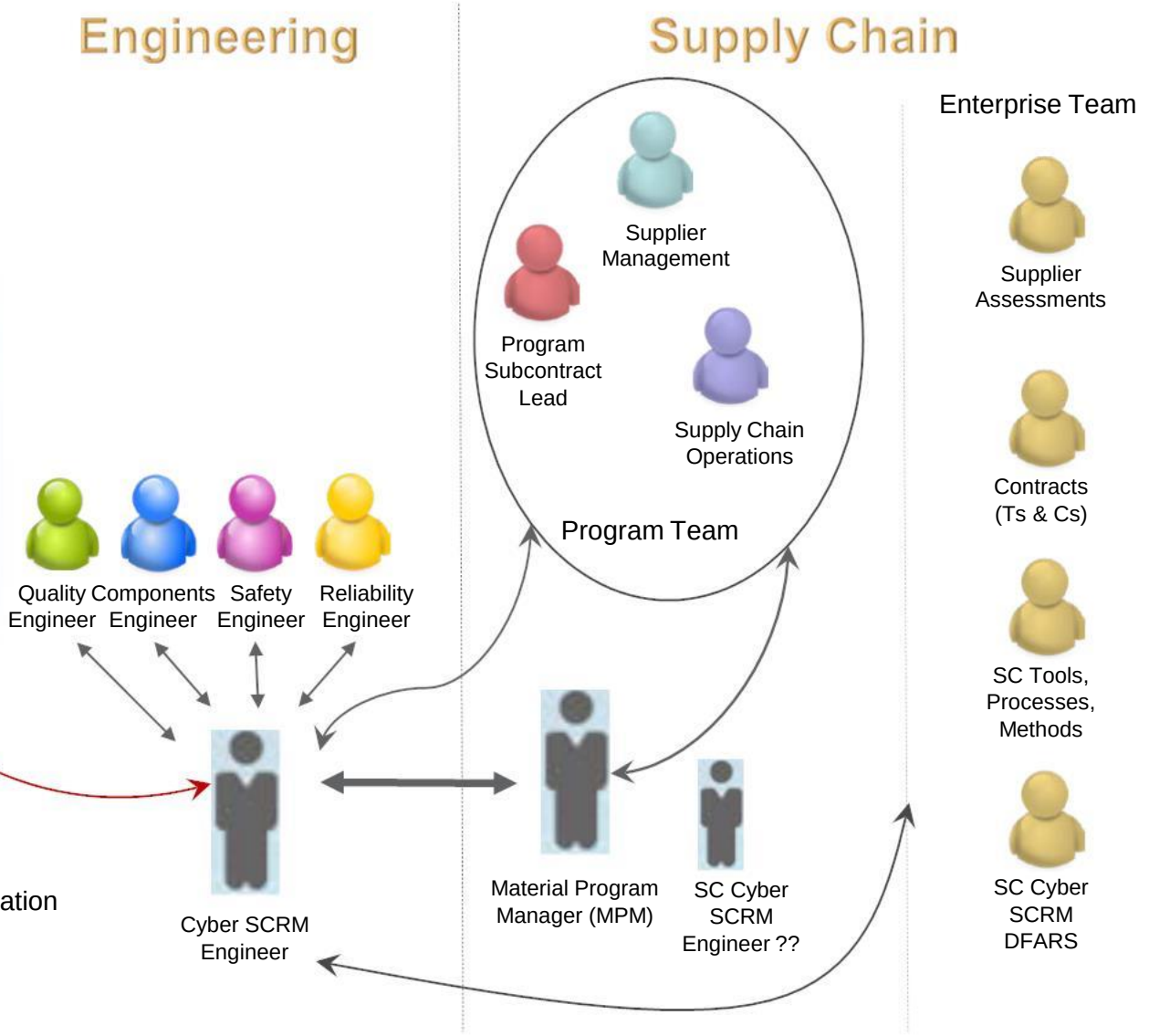


Integrate Cyber SCRM Considerations into Existing Raytheon Supply Chain Methods and Tools

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.

Raytheon's Cyber SCRM Role OV-1





The Cyber SCRM Engineering Lead is responsible for the program strategy and technical subsystem and component procurement and subcontracting requirements to address global supply chain risks.

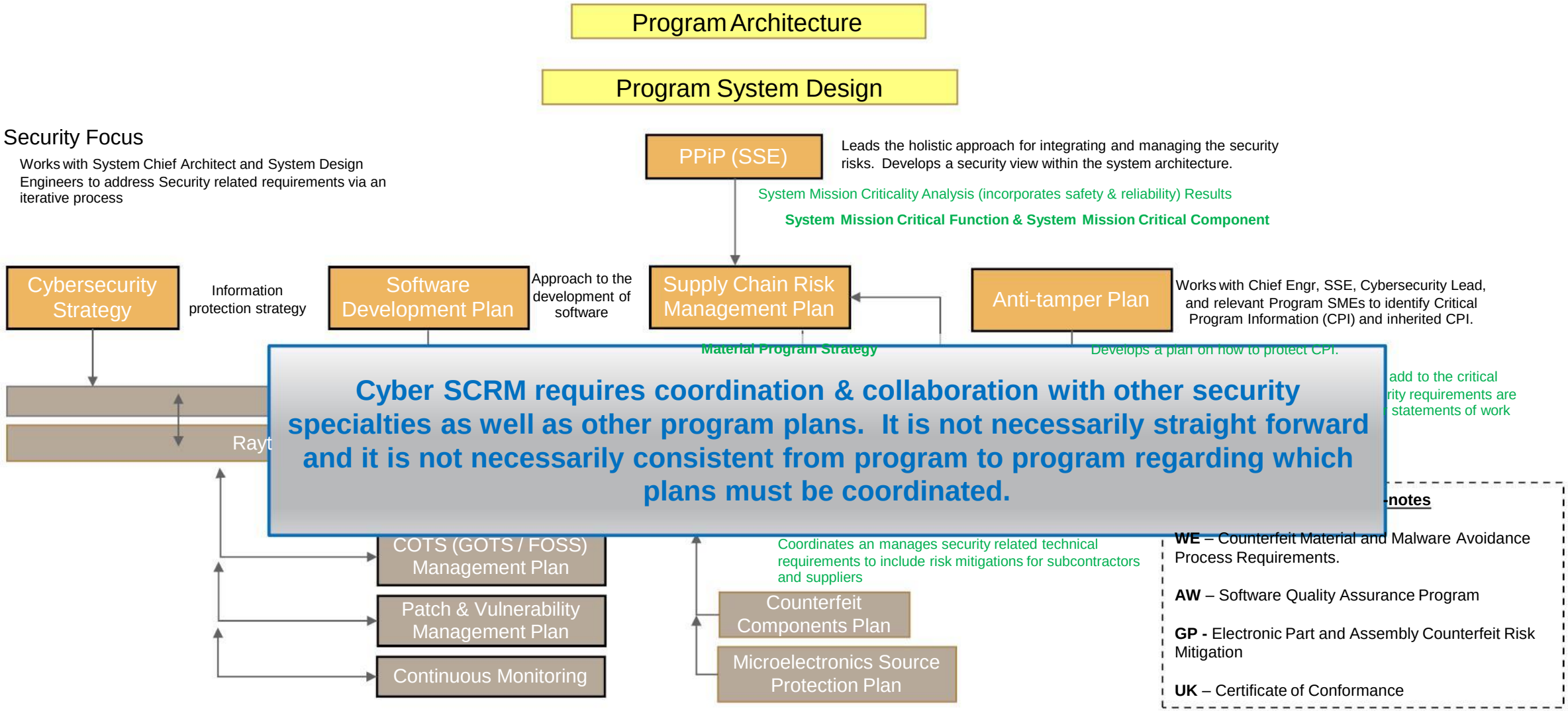
- Cyber SCRM Strategy
- System Mission Criticality Analysis for Logic Bearing Critical Component Identification
- Bill of Materials Decomposition
- Mitigation Evaluation for Procured and Subcontracted Material and Software.
- Supplier / Sub Selection Criteria for Cyber SCRM Considerations
- Cyber SCRM Asset Management Considerations

Cyber SCRM Engineer Addresses Global Supply Chain Risks to Program Procurements

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.

Example Raytheon Program Cyber SCRM Perspective

Holly Dunlap



Raytheon's Cyber Supply Chain Risk Management Program Plan Relational Mapping

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.

Cyber Supply Chain Risk Management
Key Takeaways

- Adversaries are moving from directly attacking our systems to attacking our more vulnerable supply chains.
- Cyber SCRM is a new and developing security specialty discipline within System Security Engineering and Systems Engineering
- A partnership between Engineering, Mission Assurance, and Supply Chain organizations is an imperative.
- Cyber SCRM contributes to a holistic approach to program protection and a Program Protection implementation Plan (PPiP).

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.

References:

- DoDI 5200.44
  - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903
- NIST SP 800-53 Rev 5
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST SP 800-160
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf
- NIST SP 800-161
  - https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft
- Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War
  - https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf

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.

Questions?

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.

Holly Dunlap Bio

- BS Electrical Engineering & MBA
- 10 years Nuclear Weapons, National Nuclear Security Administration (NNSA) Kansas City Plant, M&O Honeywell
  - 3 Year Rotational Leadership Development Program (10 years experience in 3 years)
    - Program Manager of B83
    - Supply Chain 18 months (Rotated every 3 months)
    - Intelligence Community (Reverse Engineering, Rapid Fielding, Analysis)
  - Certified 6 Sigma Black Belt – Microelectronics
- OSD DDR&E Technical Intelligence, Pentagon +4 years
  - Emerging & Disruptive Technology. Investment strategy to ensure US technical capability advantage. Work intimately with Anti-tamper Executive Agent, National & Defense Intelligence Community, and Defense System Developers. Strategic 15 – 20 Year Planning.
- Ktech Later Acquired by RTN RMS
  - USD(I) Contract Supply Chain & Logistics Layered Analysis; Data & Information Exploitation. 18 month effort.
- RMS – IDS – RMD (+15 years)
  - NDIA System Engineering Division Elected Chair (+13 Committees, +500 members; government, industry, academia, FFRDC)
  - NDIA System Security Engineering Committee Chair, +9 years
  - Raytheon Systems Engineering Council – Cyber Resiliency & System Security Project Lead
  - Cyber Enterprise Campaign
  - Cyber Operations Development & Evaluation (CODE) Center
  - PI Security & Trustworthy Foundations for Electronics Resurgence (STryFER) IDIQ Contracted Research & Development (CRAD) Proposal

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.

Thank you.

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.

Mission Engineering, Capability Evaluation & Digital Engineering Informing DoD Technology, Prototyping and Acquisition Decisions

Mr. Christopher Collins
Director, Developmental Test Evaluation & Assessment
Office of the Deputy Director for Engineering
Office of the Under Secretary of Defense for Research and Engineering

Dr. Suzanne Beers
Department Manager, Defense Systems Engineering & DTE&A IDSK/EF Initiative Champion
The MITRE Corporation

National Defense Industrial Association Systems and Mission Engineering Conference
December 2021

Approved for public release. DOPSR Case # 22-S-0242.

Purpose & Concept Overview

Purpose: **Apply Integrated Decision Support Key - Evaluation Framework (IDSK-EF) post Mission Engineering (ME) to evaluate capabilities and inform concept, S&T, P&E, PoR, CPM, and operational fielding decision-making**

Concept: **Mission Engineering study identifies/validates mission capability gaps and proposed technology solutions. IDSK-EF frames capability evaluation to inform decision-making throughout the concept-to-fielding continuum:**

- **Science & Technology (S&T) develops technical solutions**
  - **IDSK-EF evaluates technical capabilities; informs investment and maturity decisions**
- **Prototyping & Experimentation (P&E) operationalizes technical solutions**
  - **IDSK-EF evaluates prototype performance; informs transition decisions**
- **Acquisition Programs of Record (PoR) develop, acquire operational capability**
  - **IDSK-EF evaluates technical and operational capabilities; informs acquisition decisions**
- **Capability Portfolio Management (CPM) manages fielding of capability portfolios**
  - **IDSK-EF evaluates SoS performance; inform capability portfolio management decisions**

Approved for public release. DOPSR Case # 22-S-0242.

Mission Engineering and Continuous Evaluation Inform S&T-P&E-POR-CPM Decisions



ME: Study validates operational capability gaps; evaluates efficacy; proposes technology solutions

IDSK-EF: Tailors capability evaluation for decision-support throughout the S&T – P&E – POR – CPM continuum

- S&T: develops technology solutions
  - S&T-focused IDSK/EF informs tech investment and maturation decisions
- P&E: operationalizes advanced concepts and technologies
  - P&E-focused IDSK/EF informs transition from S&T to PoR
- PoR and CPM: deliver integrated capabilities meeting Warfighter requirements at speed of need
  - PoR or CPM IDSK/EF informs program or portfolio decisions

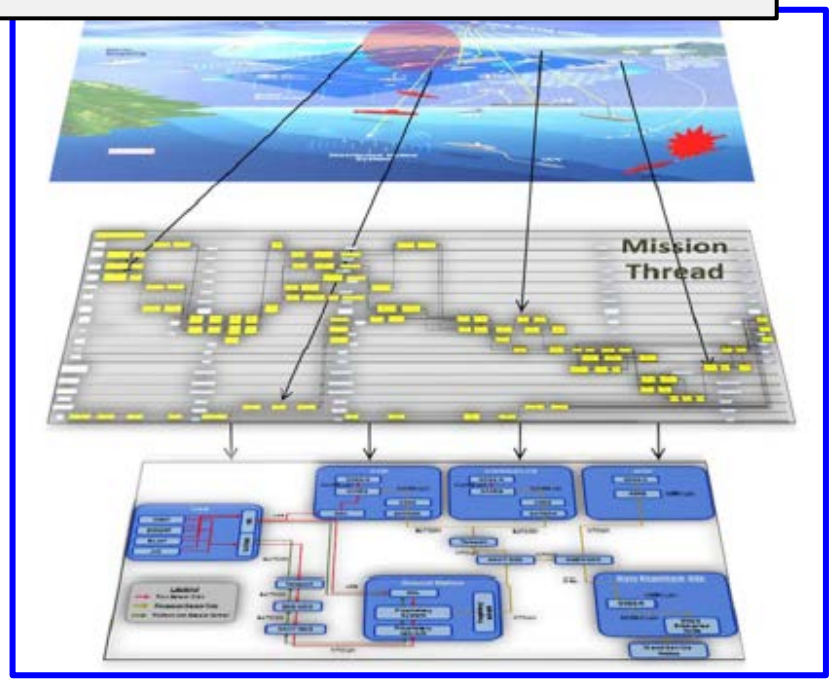
IDSK: Integrated Decision Support Key
EF: Evaluation Framework
S&T: Science and Technology

Approved for public release. DOPSR Case # 22-S-0242

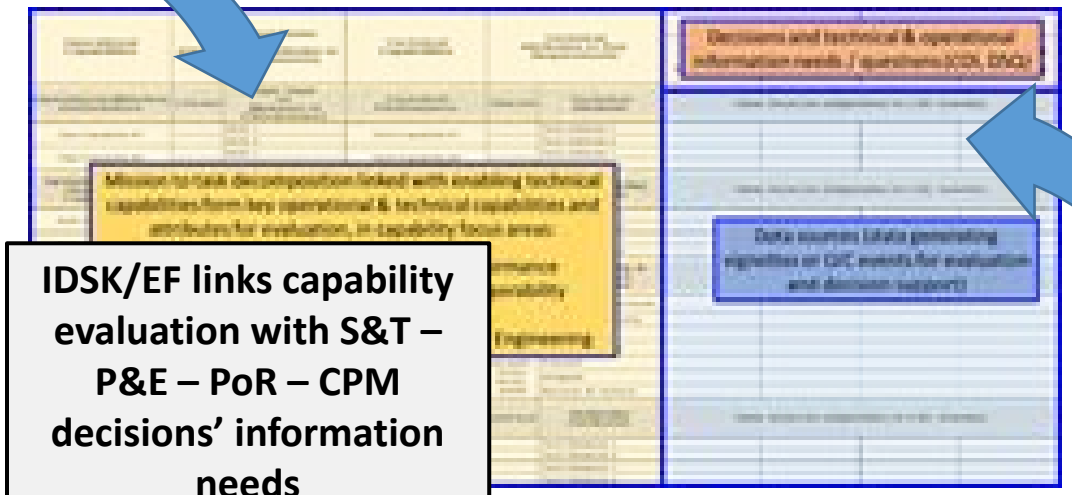
P&E: Prototyping & Experimentation
PoR: Program of Record
CPM: Capability Portfolio Management

Mission Engineering – IDSK-EF – Digital Engineering Vision

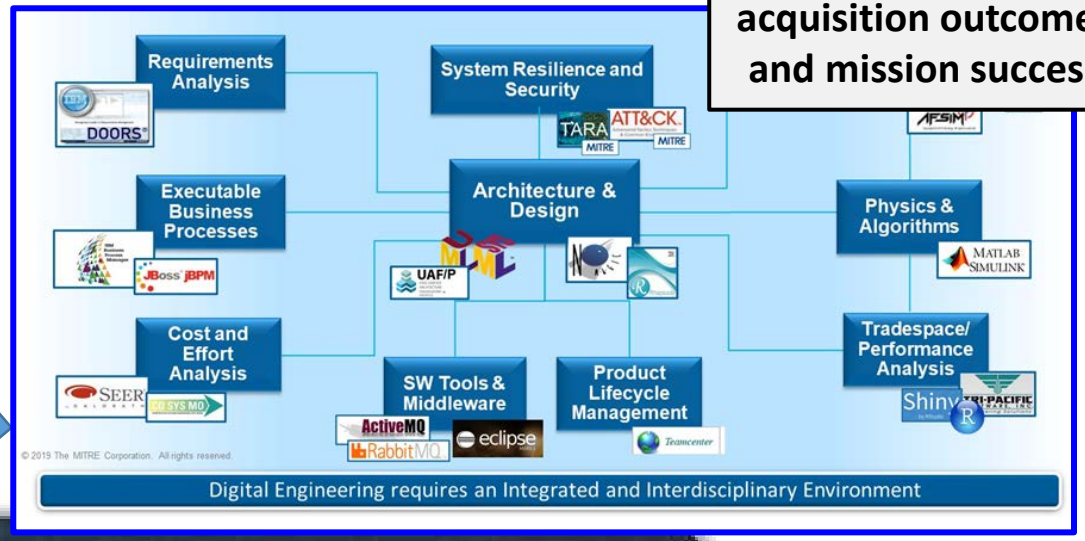
ME study defines operational architecture to mission thread (MT) to mission engineering thread (MET) – validates warfighter-identified operational capability gaps, proposes optimal technical solutions, identifies evaluation measures of effectiveness



IDSK/EF links capability evaluation with S&T – P&E – PoR – CPM decisions' information needs



DE manages data complexity and relationships; provides the analytical evaluation engine; feeds back evaluation results to inform decisions, improving mission-focused technology development, acquisition outcomes and mission success



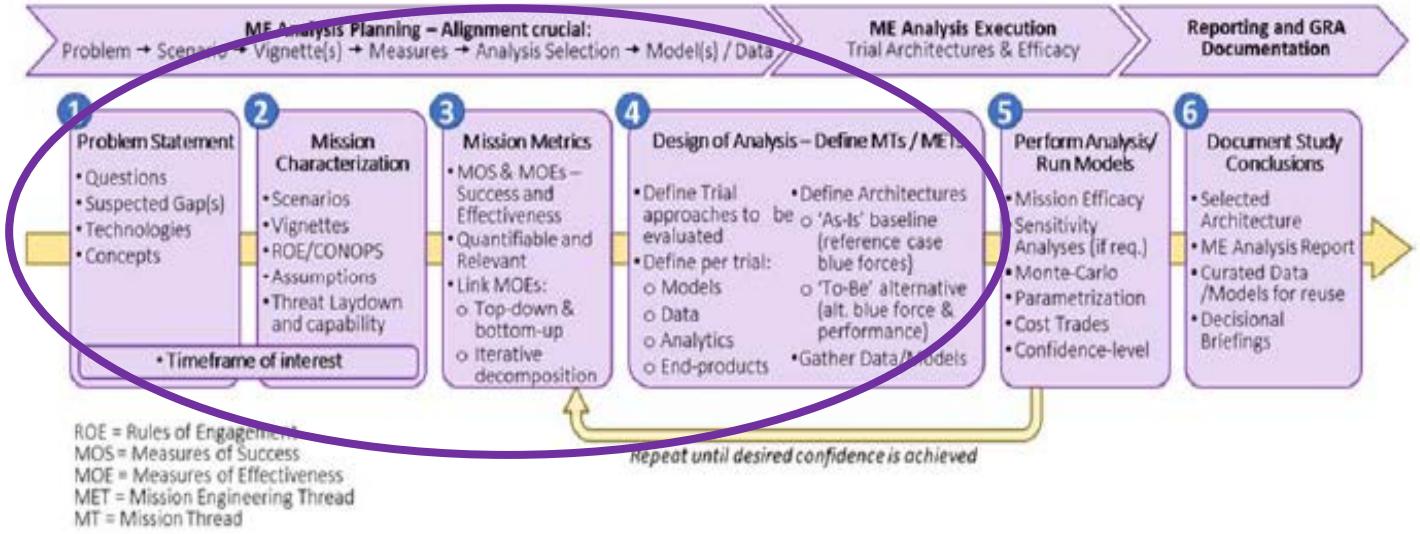
MT: Mission Thread
MET: Mission Engineering Thread

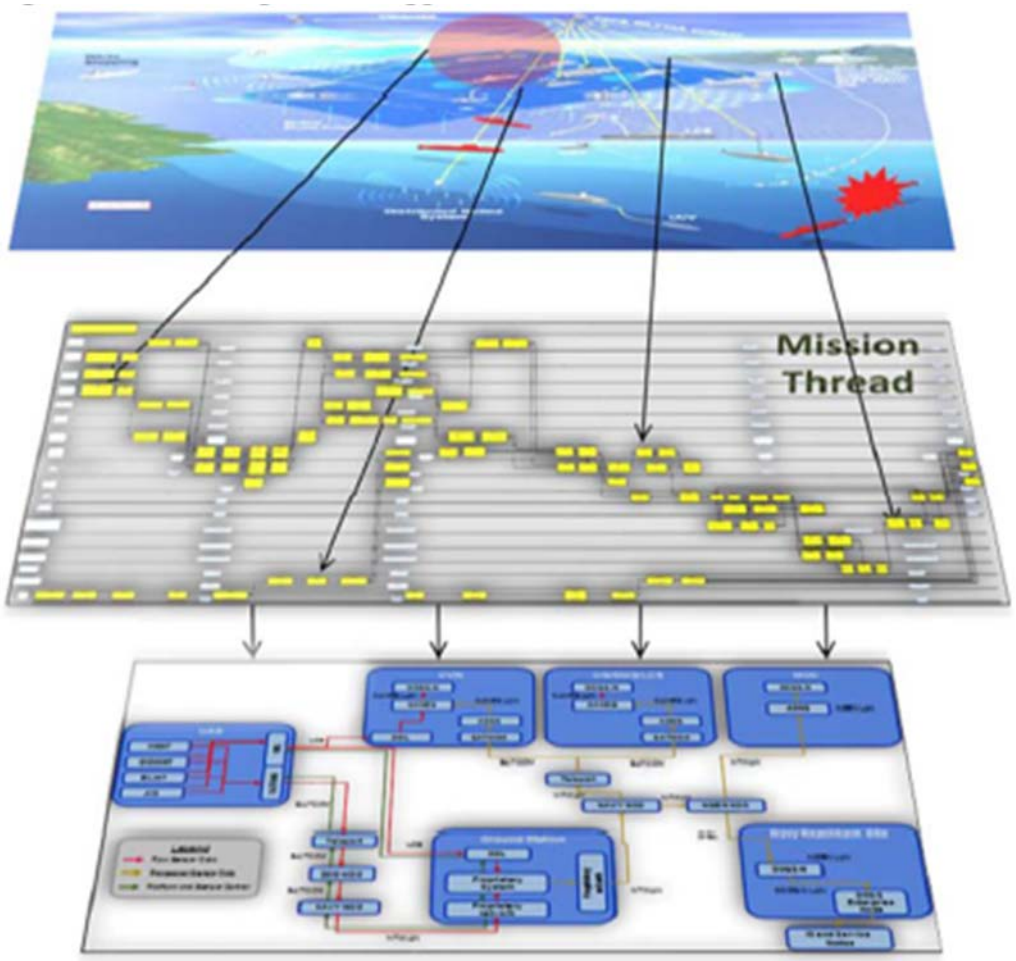
Approved for public release. DOPSR Case # 22-S-0242.

IDSK: Integrated Decision Support Key
EF: Evaluation Framework

Mission Engineering Links Mission Gaps with Technical Solutions

ME process defines problem statement, characterizes mission, defines operational and engineering metrics



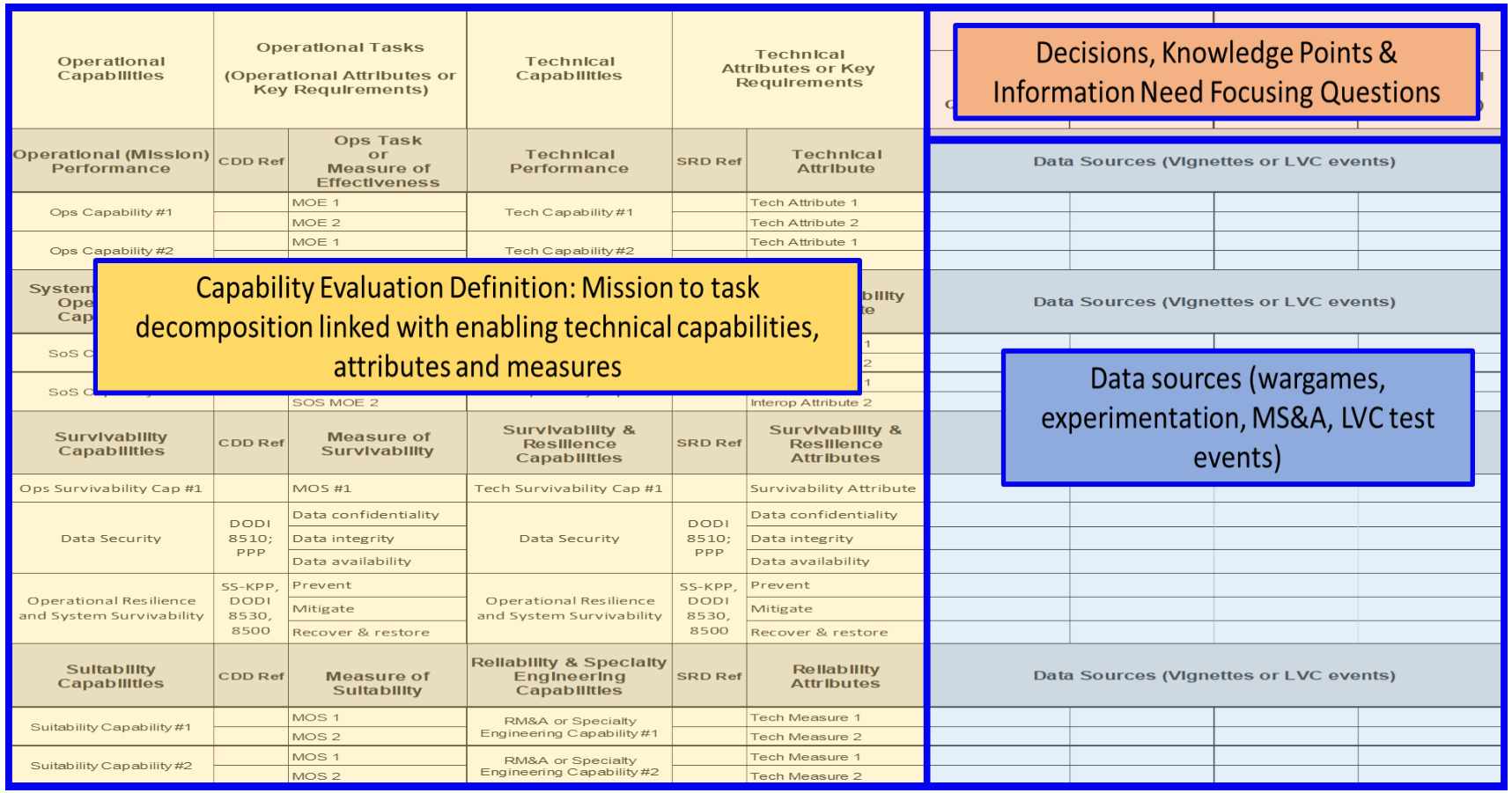


- ***Mission architecture defines the operations, systems, and data flow within the constraints of the scenario***
- ***"As-Is" mission approach represents current mission execution, provides a reference for analysis and evaluation***
- ***Variable changes (i.e., technologies, systems, performance, tactics, etc.) lead to alternate technical solutions and mission approaches – the "To-Be" for evaluation***

Reference: OSD(R&E) Mission Engineering Guide, Figure 2.1, pg 5; Figure 2.8, pg 18

Approved for public release. DOPSR Case # 22-S-0242.

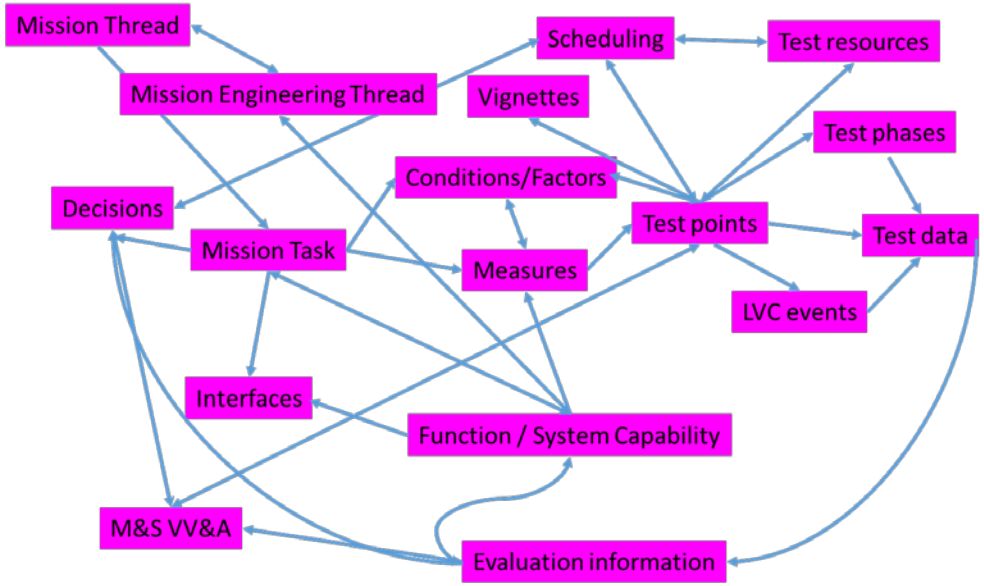
Integrated Decision Support Key – Evaluation Framework (IDSK-EF) guides Capability Evaluation for Decision-Support



- Holistic, flexible evaluation framework tailorable for decision-support throughout S&T – P&E – PoR – CPM lifecycle
- Decisions, knowledge points and information needs guide evaluation planning
- Evaluation focused to inform decisions across technology, design, development and mission continuum
- Evaluation plan guides wargaming, experimentation, MS&A, test design providing evaluation's data

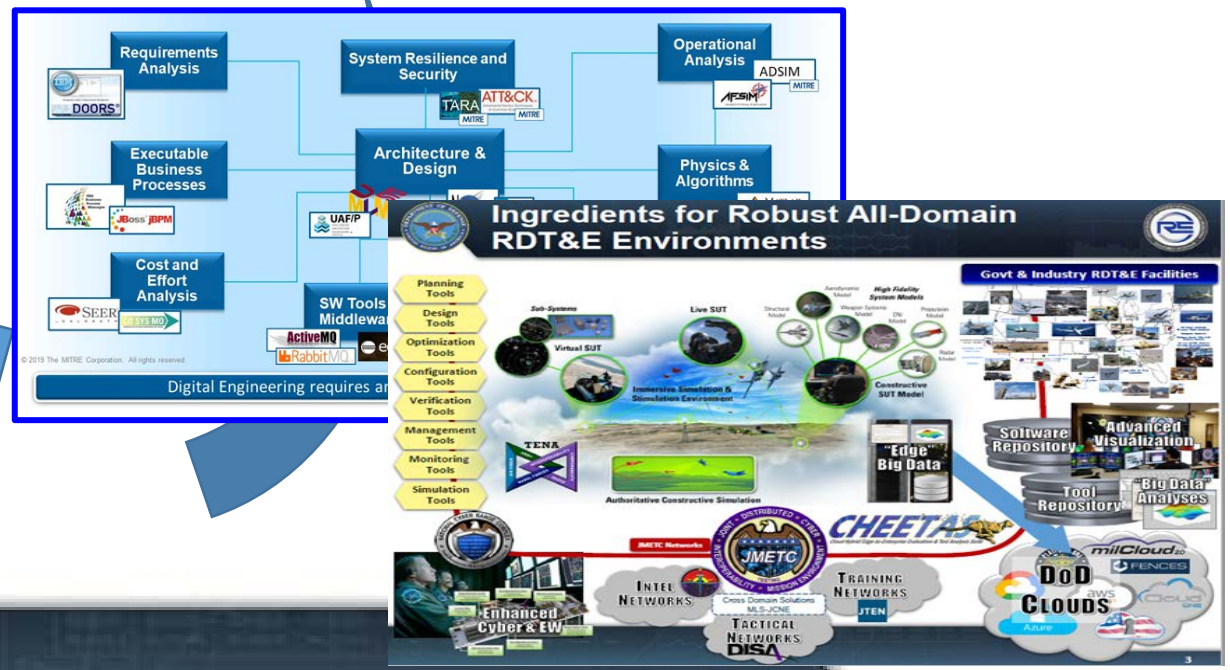
Approved for public release. DOPSR Case # 22-S-0242.

Digital Engineering Manages Data Complexity & Provides Evaluation's Analytical Rigor



DE model houses detailed data and interfaces, generates views for decision-support, evaluation planning and test design

DEE is evaluation's analytical engine; informs decisions with capability evaluation results, improves mission-focused technology development, acquisition outcomes, and mission success

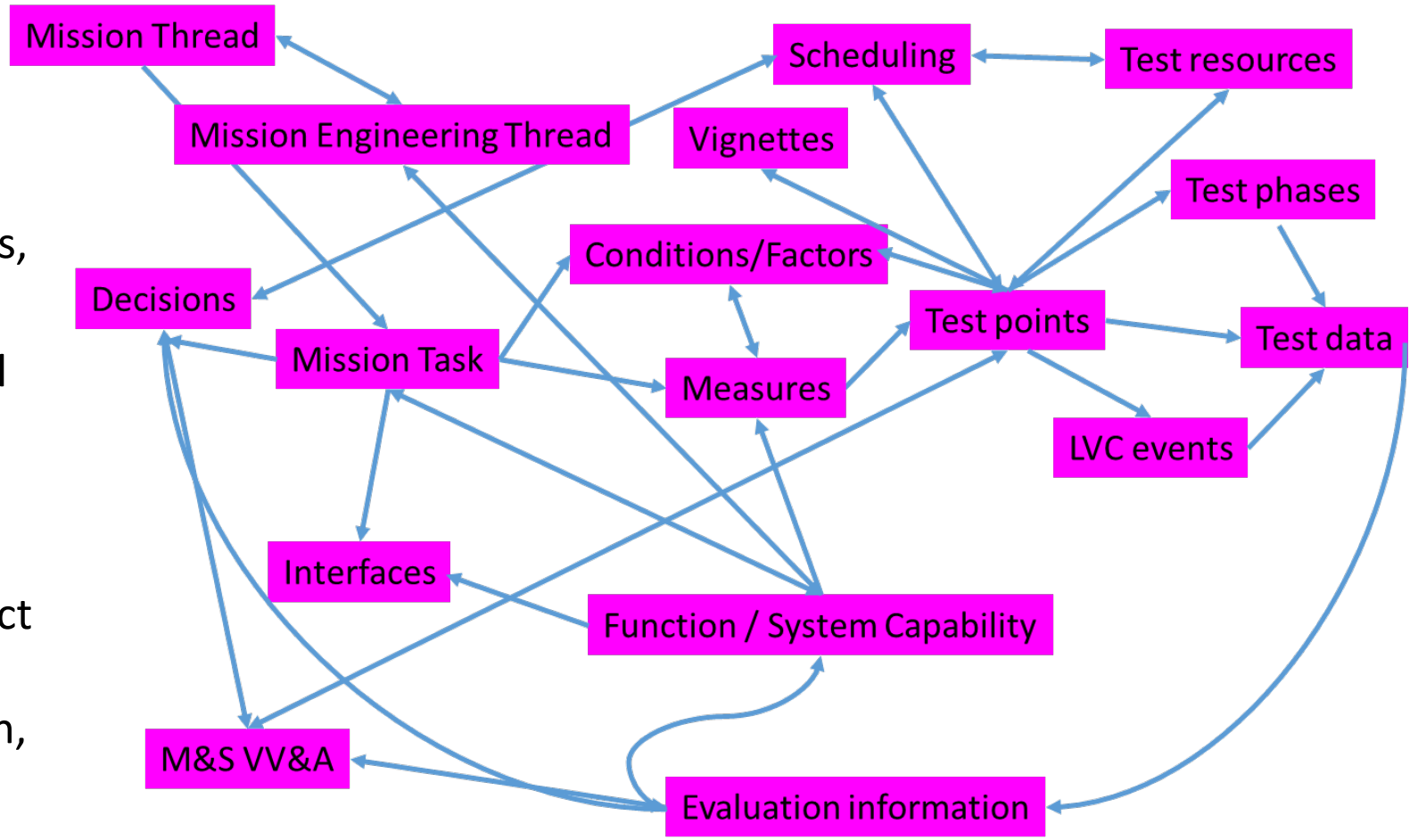


DE: Digital Engineering
DEE: Digital Engineering Environment

Approved for public release. DOPSR Case # 22-S-0242.

Digital Engineering Accelerates Capability Delivery to the Warfighter

- MBSE tools use object-oriented methods and an underlying relational database to define and maintain reusable, digital representations of multi-dimensional elements: mission threads, SoS configurations, capabilities, measures, test design, etc.
- Queries and manipulation of the digital model generate IDSK-EF views based upon stakeholder information and documentation needs
- Power of DE in ME-IDSK/EF-DE construct informs decision-making to accelerate mission-focused technology maturation, operationalization, and capability delivery to the warfighter at the speed of need



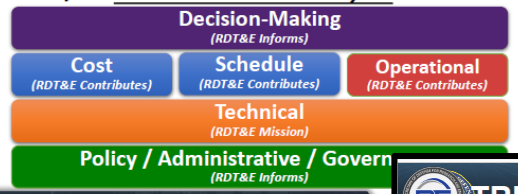
Approved for public release. DOPSR Case # 22-S-0242.

Partnering with TRMC Knowledge Management Investment Portfolio

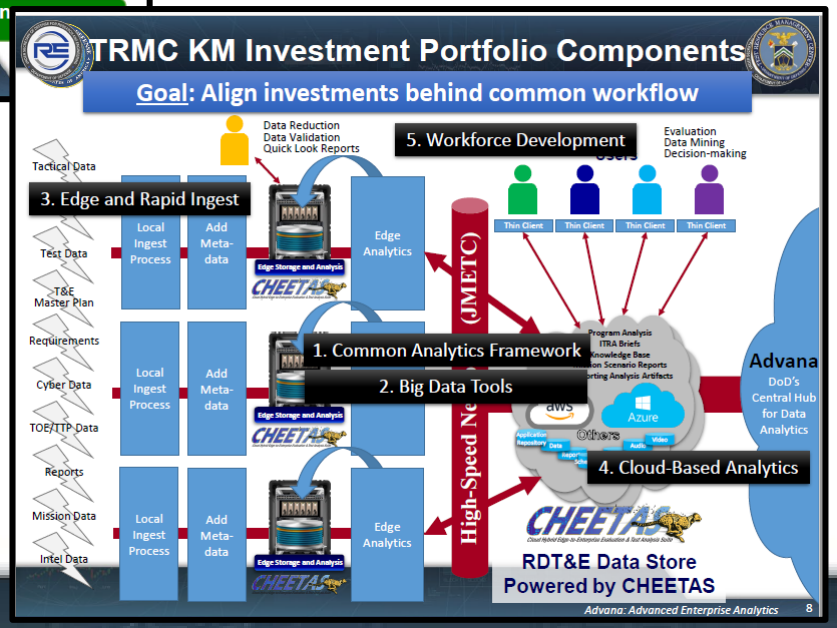
Why is RDT&E Data Different?

- **The product of RDT&E is technical data & knowledge, not applications**
  - Example: A single F-35 mission generates 0.4TB-1.0TB+ of technical data
- **Goal: Inform decision-making with system capabilities & limitations**
  - Operational data: how we use a system
  - Technical data: "truth" of what a system can do
- **Key RDT&E Tenets:**
  - Enable analysts to spend more time analyzing data – and less time gathering data
  - Maximize collaboration between government and industry
  - Accept & Federate our communities' distributed data repositories
  - Start small and grow aggressively
- **Challenge: How much data do we share?**

Notional DoD Data Layers



Discoverable, Accessible, & Understandable technical data is critical to operational & acquisition decision-making



- TRMC developing CHEETAS - integrating RDT&E infrastructure into cohesive knowledge management enterprise
- Modernize RDT&E practices & processes to leverage big data analytics techniques
- Apply big data analytics tools & techniques to the RDT&E mission space
- Enables existing analysts to become data scientists
- Emphasizes user time spent on analysis rather than data gathering
- Provides consistent access regardless of data location and/or amount
- Promotes sharing & reuse of tools & techniques across the community
- Implements the DoD Data Strategy for RDT&E

Approved for public release. DOPSR Case # 22-S-0242.

Summary – Good Decision-Making Delivers Exquisite Solutions to Warfighter Needs

ME – IDSK-EF – DE provides mission focused, capability evaluation-based decision support across S&T – P&E – PoR – CPM continuum

Evaluation-informed decision-making accelerates delivery of solutions to close Warfighter mission gaps at the speed of need

- IDSK/EF focuses the continuum of T&E activities on evaluating operational and technical capabilities to inform decision-making
- ME puts analytical rigor into operational – technical capabilities linkage; provides mission context to technical and acquisition decision-making
- DE underpinning provides thorough, consistent and rapid evaluation of complex operational and technical solutions

Approved for public release. DOPSR Case # 22-S-0242.

Contact

For more information, please contact:

Mr. Christopher Collins,
Director, Developmental Test, Evaluation & Assessment
christopher.c.collins4.civ@mail.mil

Dr. Suzanne Beers
sbeers@mitre.org
719-418-1047

https://ac.cto.mil/dte/
https://ac.cto.mil/engineering

Approved for public release. DOPSR Case # 22-S-0242.

EPSILON® Systems Solutions, Inc.

C5I

A 100% Employee-Owned Company



Abstract #23816

The Automation Framework (TAF)

Mr. Kevin Visalli
kvisalli@epsilonsystems.com
Director of Software Products, Epsilon C5I

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

Epsilon C5I, Inc.

Where our innovations become your solutions

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Agenda

- Introductions
- What is The Automation Framework (TAF)?
- How does TAF work?
- Why would I use TAF?
- What information does TAF provide?
- Demo
- TAF within a DevSecOps Pipeline
- What is TAF's Return on Investment (ROI)?
- Summary

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

BLUF

- TAF provides test and task automation as a service (TAaaS) in DevSecOps platforms and beyond
- ROI: Test Automation delivers cost and schedule savings while increasing performance
  - Schedule: 94% time savings across test environments
  - Cost: 30% reduction in man hours
  - Performance: 80% increase in defects found

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

About the Presenter



Mr. Kevin Visalli
Director of Software Products, Epsilon C5I
kvisalli@epsilonsystems.com

Mr. Kevin Visalli is the Director of Software Products at Epsilon C5I, Inc. and is the TAF Chief Architect. He holds a B.S. in Software Engineering from Rochester Institute of Technology and has over 15 years of experience designing, developing, integrating, testing and delivering software for U.S. Navy SBIRs, BAAs, and PoRs. This experience focuses on simulation, stimulation and training of C4ISR systems, and test and task automation, accelerating DevOps Pipelines for DoD programs.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Epsilon Systems – A Trusted Partner

- A Professional and Technical Services Company Founded and Headquartered in San Diego, CA
- 100% Employee-Owned Business
- Non-Traditional Defense Contractor
- Workforce of 1000+ in Support of:
  - Software and Systems Engineering
  - C5ISR & Combat Systems
  - Digital Media and Training Solutions
  - Environmental Management Services
  - Fleet Sustainment, Repair and Modernization
  - Product Engineering, Design and Manufacturing
  - Life-Cycle Engineering



Skilled Workforce

- 100% Cleared
- 60% TS/SCI
- 89% Bachelors
- 28% Masters
- 2% PhDs

ISO 9001:2015

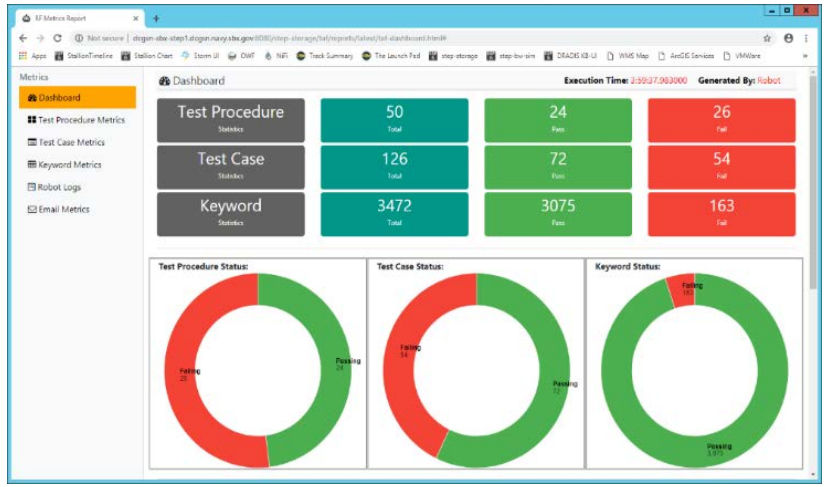
CMMI DEV/3 SM
Exp. 2021-08-31 / Appraisal #31279

SUBSAFE

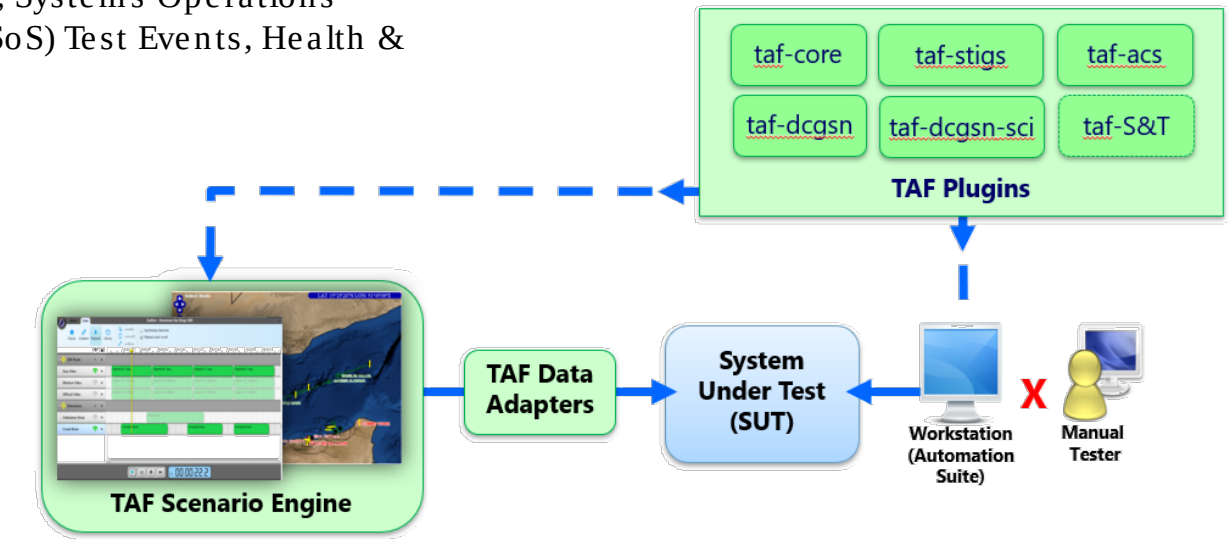
NAVSEA Note 5000

The Automation Framework (TAF)

DevSecOps Pipeline-Agnostic Test & Task Automation

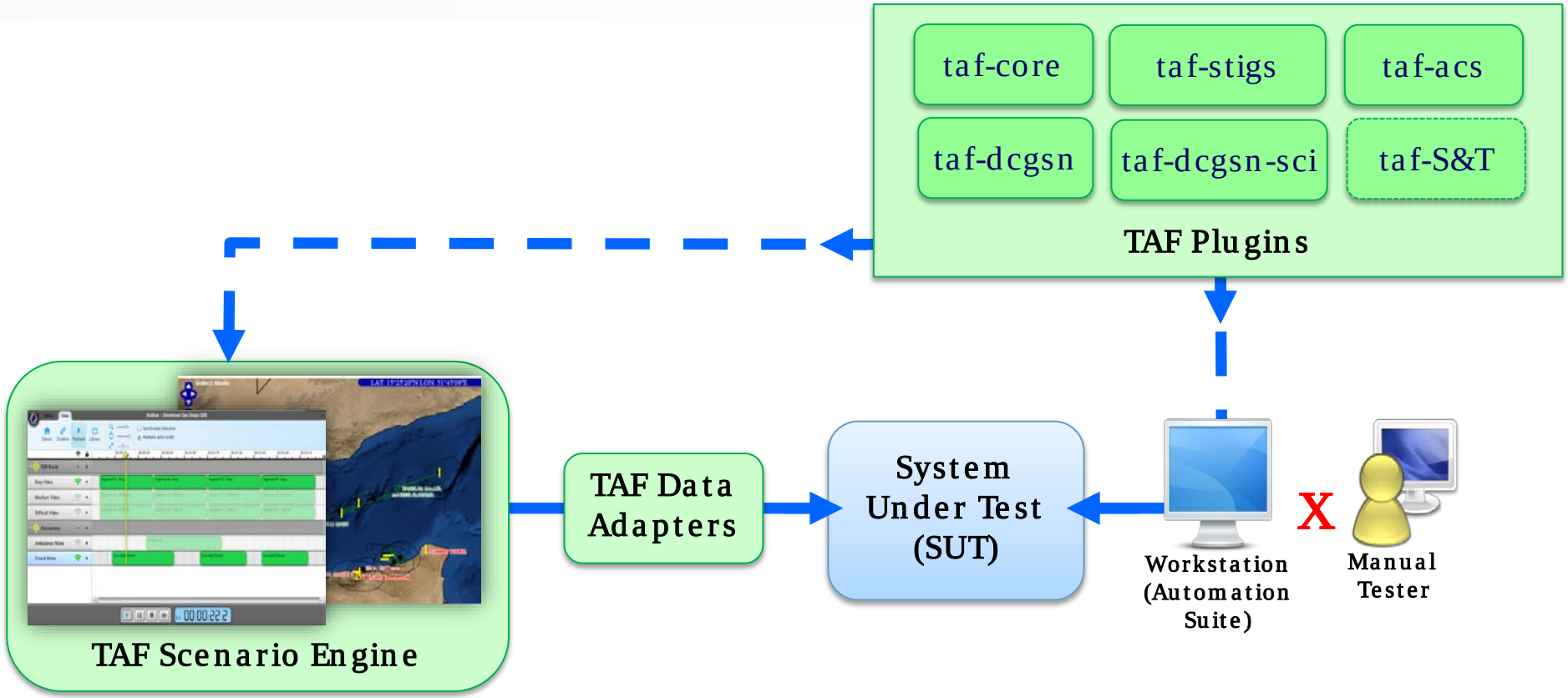


- **Intuitive Versatile Application Suite used to drive Continuous Test and Test Driven Development**
- **Programs/Projects:** Distributed Common Ground System Navy Inc 2 (DCGS-N Inc. 2); Ship's Signal Exploitation Equipment (SSEE Inc. F); Agile Core Services (ACS), Consolidated Afloat Networks and Enterprise Services Application Integration (CANES AI), CANES MARKSMEN, Automated Digital Network System (ADNS), Maritime Tactical Command and Control (MTC2), Tactical Shore Platform (TSP), Overmatch Software Amory (OSA) and many others
- **Use Cases:** Developmental Testing, Integration Testing, Regression Testing, Validation and Verification, Functional, Performance, Interoperability, Cybersecurity, Systems Operations Verification Test (SOVT), Family of System (FoS) / System of System (SoS) Test Events, Health & Status, System Monitoring, Interactive Installs & Configuration
- **Results:**
  - ***Test Execution***: 61.5 hours to 3.5 hours (94% time savings)
  - ***Bug Identification***: 80% improvement in defects found/number
  - ***Test Efficiency:***
    - Integration testing – went from 1x every 4 weeks to nightly
    - Regression testing – near real-time identification; faster delivery



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

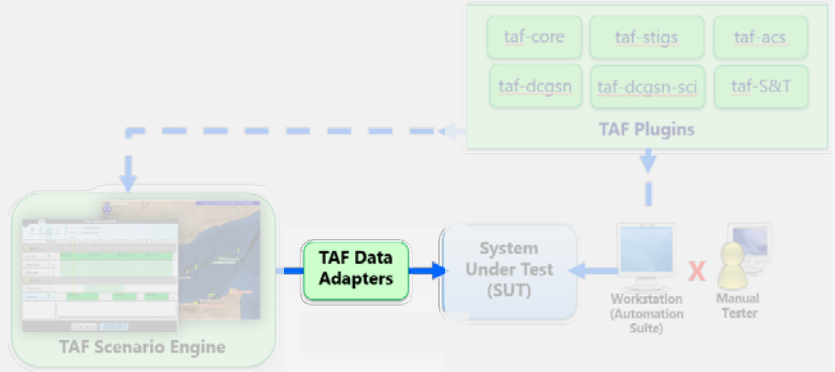
TAF: How TAF Works



TAF incorporates technologies that simulate and stimulate DOD-centric data sources in a repeatable and consistent manner

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Existing TAF Sim/Stim Adapters



Supported Intel Types (Formats)
- Audio (32f, 16T, wav, IQ)
- AIS (OILSTOCK, TMS, OTH-GOLD/XCTC, CMF-X, CMF-B)
- ELINT (TMS, OTH-GOLD/XCTC, CMF-X/B)
- FMV (H264)
- KL
- M3
- P-Data (OILSTOCK), Para-126
- S2A (Tx-logs, VOI List)
- TACREP
- Theater Ballistic Missiles (TAB37)
- Thresher

Simulators/Mock Services
- AMS (White Shipping)
- FOM
- MEPED
- MIDB
- LDAP

Simulators
- BORESIGHT/BE3
- Platform location and DF
- Sensor & Equipment (radar, AIS transponder, NAVSSI, etc.)
- Signal processing, signal generation
- Signal propagation and off-tuning
- Synthetic video generation

Data Input Adapters
- Audio streams from JSAF/JBUS/MARS
- HTTPS/SOAP for SIGINT/IO system tasking and receiver tuning
- HTTPS/SOAP registrations from other system so they can receive Stallion XML events
- Stallion XML events from JSAF/JBUS

Data Output Adaptors
- DCGS Inc. 1 DIB V4.0 web service
- Email
- ICSF TMS
- ICSF UCP
- Real-time Streaming Protocol (RTSP)
- SIGINT/IO system (simulated signals/audio, intercepts, LOBs, etc.)
- Stallion XML events via HTTPS/SOAP to registered systems
- TCP/IP socket – simulates IBS-N
- Video Scout

Systems
- SSEE Increment F, SSEE Increment E 5.0 + ICSF, Red Falcon, Graywing, HITS, SSC-S
- DCGS FoS
- DI2E Environments, GCCS (demonstration)

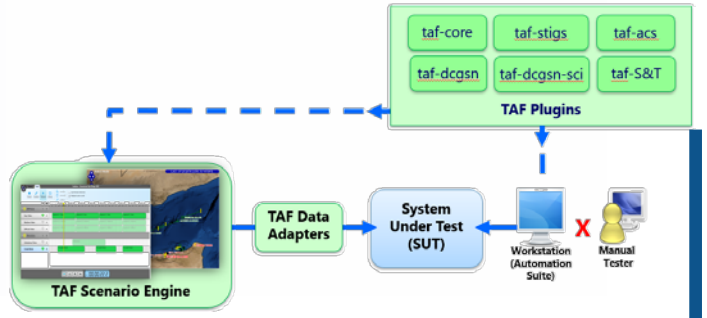
Why TAF?

- Test & Task Automation Solution for DevSecOps
- Many test automation tools exist, but what makes TAF better?
  - Framework incorporates various OSS tools for different use cases
  - Intuitive SDK with Installers for both Windows and Linux Servers/Workstations
  - A "keyword-based" plugin framework allowing for re-use across projects
    - e.g. Keywords for SSH, REST, Files, Services, JBoss, etc.
  - Dashboard & Trend Analysis visualizations for understanding test results
  - Adoption by Programs of Record, ONR, and DARPA

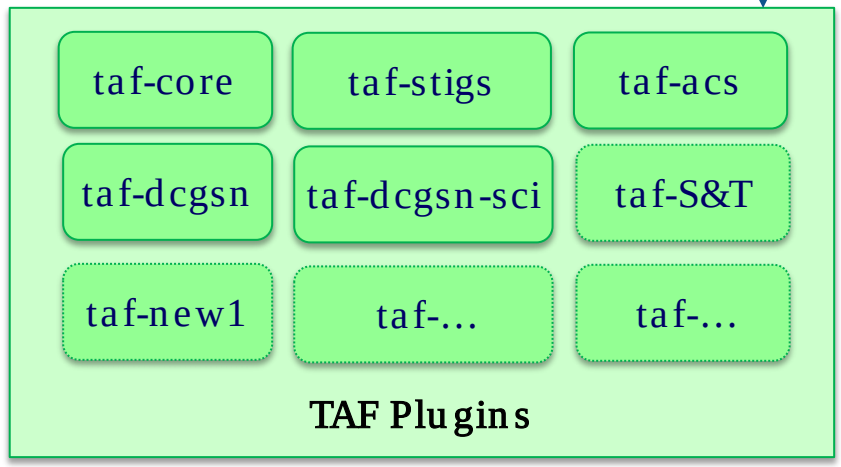
TAF provides a rich test and task automation ecosystem, tailored for the use cases and requirements of the DoD

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

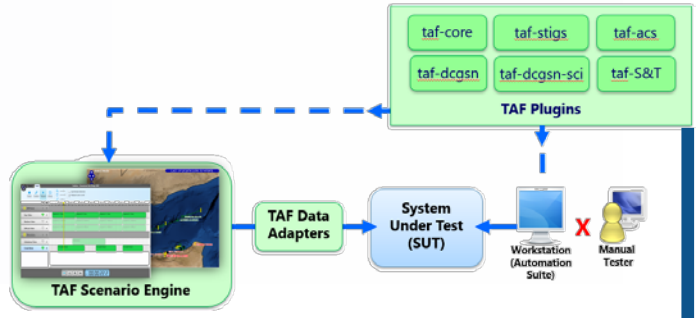
TAF: Plugin Codebase



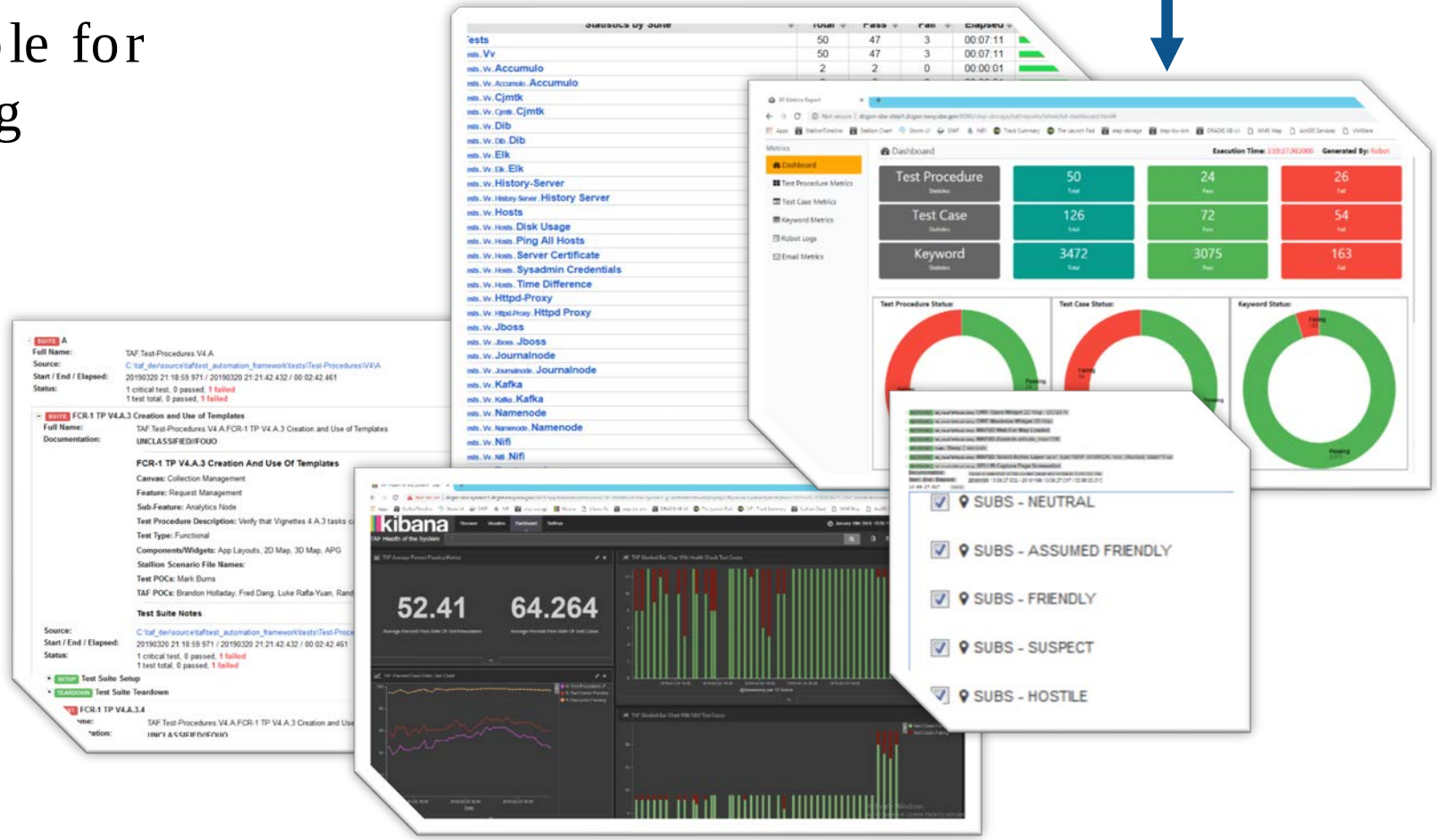
- TAF Plugins contain reusable keywords (e.g. actionable phrases)
- TAF leverages plugin code base to accomplish
  - Reusability
  - Extensibility
  - Resolve classification issues



What Information Does TAF Provide?



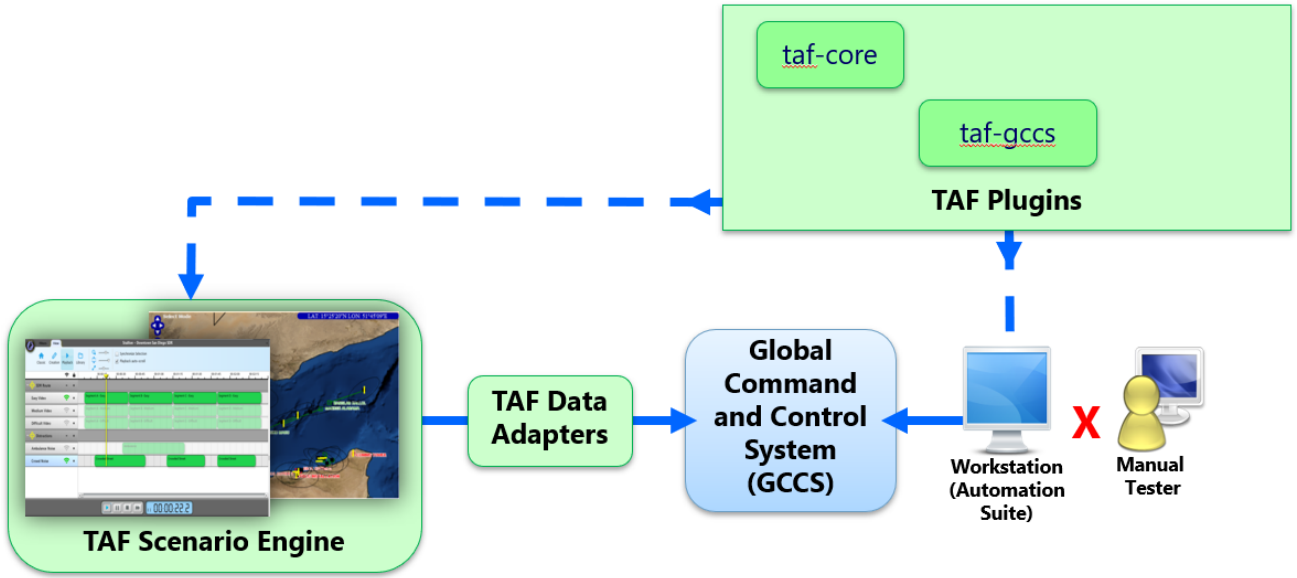
- TAF automatically generates Test Artifacts - suitable for submission to testing authorities
  - Logs
  - Screenshots
  - Test Reports
  - Trend Analysis
  - Metrics



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

TAF Demo

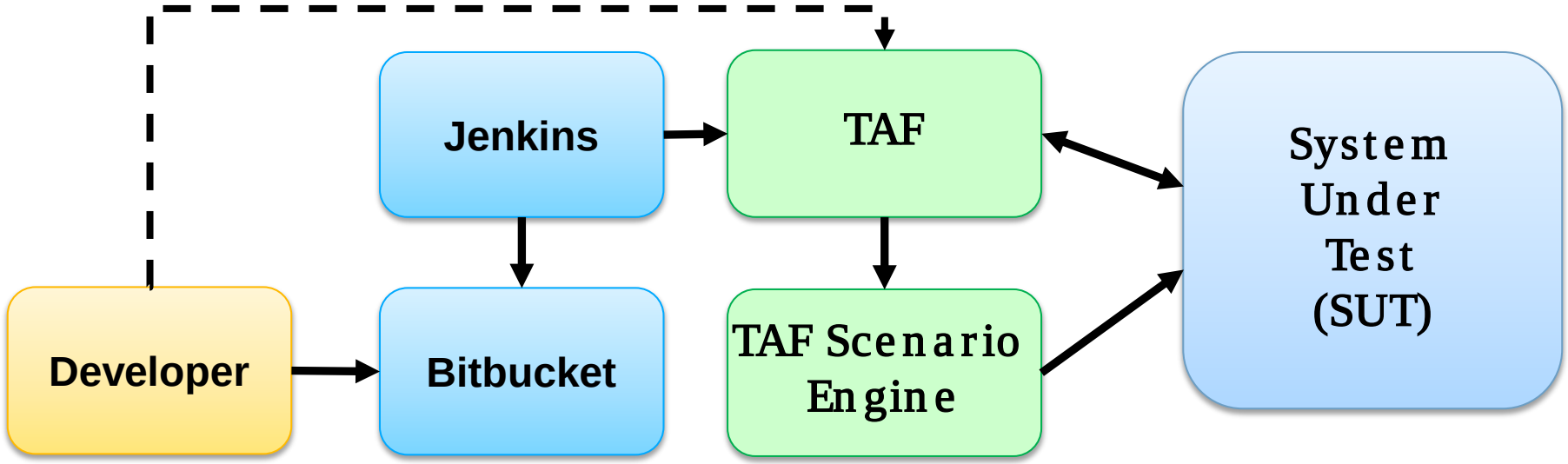
Demo w/ GCCS as SUT



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

How Does TAF work within a DevSecOps Pipeline?

1. Automated tests developed on workstations against SUT
2. Automated tests and resources stored in GIT
3. Continuous Integration Server kicks off automated TAF tests
4. All software stakeholders given consistent understanding of system state



Significantly increases confidence of deliveries within a DevSecOps CI/CD Pipeline

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Emphasizing Security using TAF

- **Rule of thumb**: Push security 'left' (e.g. build on-top of pre-locked down servers and applications)
- Task Automation
- But how do you verify?
  - Continual ACAS Scans
  - Continual DISA STIG checks
  - Continual Penetration Testing
  - Continual execution of V&V, API, health checks and functional tests against both non-locked down and locked down instances of system

TAF verifies security lockdown and enables monitoring and reporting of DevSecOps

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

TAF: Return on Investment (ROI)

Metrics Provided by Government Stakeholders

Test Coverage Performance

- 30% increase coverage of requirements
- 50% increase in new test capabilities
- 70% Reusability improvement

Test Efficiency Performance

- 50% increase in Failures found
- 80% increase in defects found
- 20% improvement in defect-free testing

Costs

Man-hour reduction:

- Manual: .5 HRS/test case
- ✓ Automated: 36 Seconds/test case

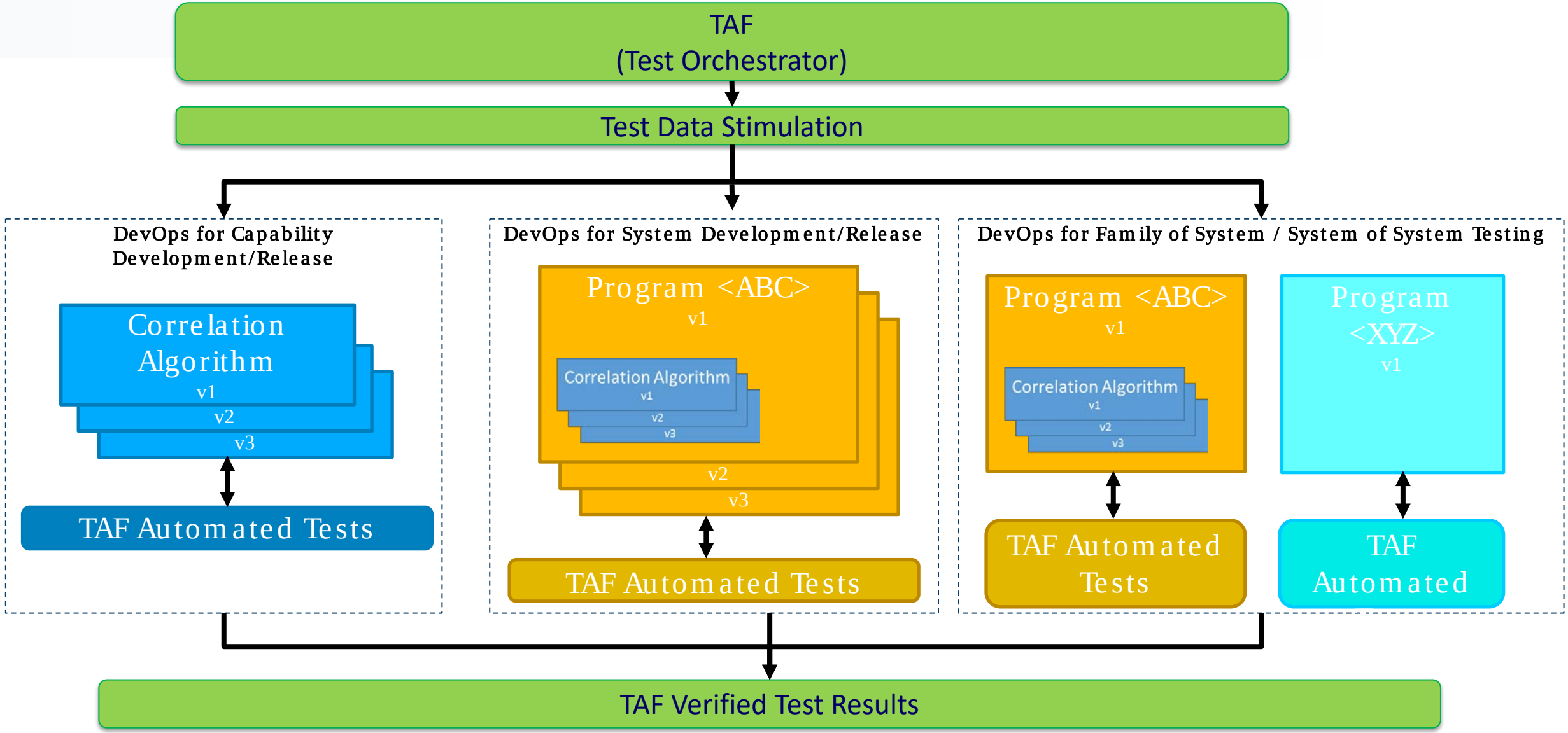
- Manual: 61.5 Hours/program
- ✓ Automated: 3.4 hours/program

Schedule

- 94% Test Execution time improvement
- 80% Test Planning/Setup time improvement
- 75% improvement in time to determine failures/defects and analyze data

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

DoD Initiative Test Automation Architecture



Summary: Test Automation as a Service (TAaaS)

- Same automated tests used across entire software lifecycle
  - Capability development
  - Integration testing
  - Regression testing
  - Formal SIT Testing
  - Formal Operational Tests
  - Family of System / System of System Test Events
  - Health and Status monitoring
- Simply scale up/down testing based on desired use case
- **Government Buy-in:** 3-year Sole Source TAF Enterprise Task Order kicked off September 2021

Reusable automation framework yields efficiencies across testing ecosystem

TAF: Questions?



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

EPSILON® Systems Solutions, Inc.



BACKUP SLIDES

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

TAF Relation to DoD Initiatives

- Deliver reliable new/updated capabilities to the warfighter faster
- Perform consistent and repeatable automated testing at all levels
  - Automated Component/Capability testing
  - Automated System testing
  - Automated System-of-System Testing
  - Automated Integration Testing At the Edge
  - Operational Health & Status Monitoring
- Enable test environments to replicate deployed environments

Bring capabilities to Warfighter Faster (e.g. JADC2, Overmatch, ABMS, etc.)

TAF: Core Test Tools

- Robot Framework
  - Framework that allows a user to orchestrate acceptance testing in an automated fashion using keywords
- Selenium
  - DOM-Based test automation tool to develop and generate test cases/scripts
  - Easy-to-use Firefox plug-in to record test scripts
- Lackey
  - Tool to automate test cases, uses image recognition to identify and control GUI components.
  - Allows user to automate both desktop or web applications
- Stallion
  - Used to Sim/Stim Data using scenarios generated & played back using Stallion
- Open Source Plugins to meet unique automation needs: UIAutomationCore, Java, SquishTest

TAF: Capabilities

- V&V Test
  - Tools: TAF: Robot and Python
  - Validate Deployment of Products
  - Validate Configurations
- Contract/API Test
  - Tools: TAF::Robot and Python
  - Validate user stories that don't have existing user Interface
  - Validate API calls
  - Validate Data against schemas
- Functional Test
  - Tools: TAF::Robot, Python, and Stallion
  - Validate user stories with existing user interface (end-to-end)
- Performance/Load Test
  - Tools: TAF::JMeter, Robot, Stallion
  - Used to Sim/Stim Data using generated scenarios from Stallion

Acronym List

Acronym	Definition
ACS	Agile Core Services
AIS	Automated Identification System
AMS	Automated Manifest System
API	Application Programming Interfaces
AWS	Amazon Web Services
C4I	Command, Control, Communications, Computers, and Intelligence
CM	Configuration Management
DARPA	Defense Advanced Research Projects Agency
DCGS	Distributed Common Ground System
DCGS-N	Distributed Common Ground System Navy Inc 2
DF	Direction Finding
DI2E	Defense Intelligence Information Enterprise
DIB	Distributed Common Ground System Integrated Backbone
DoD	Department of Defense
ELINT	Electronic Intelligence
FAT	Factory Acceptance Test
FMV	Full Motion Video
FOM	Federated Order of Battle Management
FoS	Family of System
GALE	Global Autonomous Language Exploitation
GCCS	Global Command and Control System
GOTS	Government Off The Shelf
HITS	Hostile Force Integrated Targeting System
HTTPS	Hyper Text Transfer Protocol with Secure Sockets Layer (SSL)

Acronym	Definition
IBS	Integrated Broadcast Service
ICSF	Integrated C4I System Framework
JAIC	Joint Artificial Intelligence Center
JBUS	Joint Simulation Bus
JCF	Joint Common Foundation
JSAF	Joint Semi-Automated Forces
KL	Klieglight
LDAP	Lightweight Directory Access Protocol
M3	Multimedia Message Manager
MEPED	Military Equipment Parametrics and Engineering Database
MIDB	Modernized Integrated Database
NAVSSI	Navigation Sensor System Interface
NLP	Natural Language Processing
ONR	Office of Naval Research
OSINT	Office of Naval Research
ROI	Return on Investment
RTSP	Real-time Streaming Protocol
S2A	Sealink Advanced Analysis
SDK	Software Development Kit
SIGINT/IO	Signals Intelligence/Information Operations
SIT	System Integration Test
SME	Subject Matter Expert
SOAP	Simple Object Access Protocol
SOT	System Operations Test

Acronym	Definition
SOVT	Systems Operations Verification Test
SSEE	Ship's Signal Exploitation Equipment
SSH	Secure Shell
SoS	System of System
TAF	Test Automation Framework
TACREP	Tactical Report
TCP/IP	Transmission Control Protocol Internet Protocol
TMS	Track Management System
UCP	Universal Communication Processor
V&V	Validation and Verification
VOI	Vessels of Interest
XML	Extensible Markup Language