UPDATED 10.31.22

NDIA

25TH ANNUAL
SYSTEMS & MISSION ENGINEERING CONFERENCE

November 1 – 3, 2022 | Orlando, FL | NDIA.org/SME

MONDAY, OCTOBER 31

1:00 – 5:00 PM

REGISTRATION
PENINSULA FOYER

TUESDAY, NOVEMBER 1

8:00 AM – 5:00 PM

REGISTRATION
PENINSULA FOYER

8:00 – 8:10 AM

OPENING REMARKS
PENINSULA 1-7

Holly Dunlap
Principal System Security Engineer, Cyber Supply Chain Risk Management, The MITRE Corporation
NDIA Systems Engineering Division Chair

The Hon. David L. Norquist
President and CEO, National Defense Industrial Association

8:10 – 8:40 am

KEYNOTE: SYSTEMS & MISSION ENGINEERING CAPABILITES
PENINSULA 1-7

Elmer Roman, SES
Director, Mission Integration, Mission Capabilities Office of the Under Secretary of Defense for Research and Engineering

8:40 – 9:10 am

NETWORKING BREAK
PENINSULA FOYER

9:10 – 9:40 am

LAY OF THE LAND & STRATEGIC INITIATIVE
PENINSULA 1-7

Chris Collins, SES
Executive Director, Developmental Test, Evaluation, and Assessments (ED, DTE&A), OUSD(R&E)

Dr. Sandra Hobson, SES
Deputy Director, Strategic Initiatives, Policy and Emerging Technologies Director, Operational Test and Evaluation Office of the Secretary of Defense

9:40 – 10:55 am

DIGITAL TRANSFORMATION IN SUPPORT OF TEST & EVALUALTION PANEL

PENINSULA 1-7

Dr. Laura Freeman
Deputy Director, Virginia Tech National Security Institute, Assistant Dean for Research, College of Science
Moderator

Chris Collins, SES
Executive Director, Developmental Test, Evaluation, and Assessments (ED, DTE&A), OUSD(R&E)

Dr. Sandra Hobson, SES
Deputy Director, Strategic Initiatives, Policy and Emerging Technologies Director,
Operational Test and Evaluation Office of the Secretary of Defense

Mark Kassan
Technical Director, Engineering and Technical Management Directorate, Air Force Nuclear Weapon Center
Tentative

Policarpio Sorbanis
Engineering Manager, Aeronautics Sector

David Harrison
Associate Fellow, Space, Lockheed Martin

Chris Carhart
Senior Engineer, Boeing Company

10:55 – 11:25 am

AWARD CERMONY

PENINSULA 1-7

Holly Dunlap
NDIA Systems Engineering Division Chair
Award Presenter

BOB RASSA EXCEPTIONAL SERVICE AWARD

Bob Rassa
Awardee

Robert Scheurer
Systems Engineering / Technical Fellow Boeing Defense, Space, & Security - St. Louis
Awardee

LT GEN THOMAS R. FERGUSON AWARD

Rolf Siegers
Engineering Fellow, RTX Corporate Architecture Board
Individual Award Winner

Object Management Group Space Domain Task Force &
INCOSE Space Systems Working Group CubeSat Systems Reference Model Team
Group Award Winner

TESTER OF THE YEAR AWARDS

Jeff Bilco
Senior Manager, Boeing Test & Evaluation, Engineering Strategy, Technology & Initiatives
Chair Test & Evaluation Division, NDIA
Award Presenter

Chris Collins
Executive Director, Developmental Test, Evaluation, and Assessments (ED, DTE&A), (OUSD(R&E))
Award Presenter

THE WALTER W. HOLLIS AWARD

Jeff Bilco
Chair Test & Evaluation Division, NDIA
Award Presenter

Mike Rabens
Chair Industrial Committee on Operational Test & Evaluation, NDIA
Award Presenter

Hon Bob Behler
Awardee

11:25 am - 12:25 pm

LUNCH BREAK

PENINSULA 1-7

12:25 – 1:10 pm

FEATURED SPEAKER

PENINSULA 4

Dr. Tim Grayson
Special Assistant to the Secretary of the Air Force

1:10 – 1:55 pm

CHINA AEROSPACE STUDIES INSTITUTE UPDATES

PENINSULA 4

Dr. Brendan Mulvaney
Director, China Aerospace Studies Institute

1:55 – 2:55 pm

SYSTEMS ENGINEERING TRANSFORMATION IN THE DIGITAL WORLD

PENINSULA 4

Holly Dunlap
Principal System Security Engineer, Cyber Supply Chain Risk Management, The MITRE Corporation
Moderator

Chris Schreiber
Chief Engineer, Information Technology & Digital Enablement, LM Space Systems Company

Dr. Katrina Mansfield
S&T Deputy Director, Acting, Acquisitions and Systems, Army Futures Command

Christopher Garrett
Technical Advisor for Architectures, AFLCMC/EN-EZ

Allan Dianic
Director, Software Engineering, SE&A OUSD (R&E)

Chris DeLuca
Director, Specialty Engineering, SE&A, OUSD (R&E)

2:55 – 3:10 pm

NETWORKING BREAK

PENINSULA FOYER

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.

CONCURRENT BREAKOUT SESSIONS

TRACK NAME	1A1 – Digital Engineering	1A2 – Architecture / MOSA	1A3 – Mission Engineering / System of Systems	1A4 – System Security Engineering	1A5 – Test & Evaluation
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber	Bob Scheurer & Rebecca Hicks	Dr. Judith Dahmann	Cory Ocker	Jeff Bilco & Mike Rabens
3:10 – 3:40 pm	DE-24798 Digital Engineering Strategy for DHS **Yonas Nebiyeloul-Kifle** Senior Advisor Department of Homeland Security **Kerry Wilson** Deputy Director Department of Homeland Security, Under Secretary of Science and Technology, Office of Science & Engineering	Arch/MOSA-24810 Implementing an ARINC 661 CDS with MOSA **John Macauley** Manager, Application Engineering Ansys	ME/SOS-24789 Mission Engineering – Panel **Dr. Judith Dahmann** Technical Fellow, The MITRE Corporation *Moderator* **Elmer Roman** Director, Mission Integration Office of the Under Secretary of Defense for Research and Engineering **Nicole Hutchison** Principal Investigator Systems Engineering Research Center **Tom McDermott** Research Director Stevens Institute of Technology **John Daly** Chief Engineer Booz Allen Hamilton **Dr. Peter Korfiatis** Department Manager, Systems Engineering Innovation Center MITRE Corporation	SSE-24774 System Security Committee & Track Welcome **Cory Ocker** System Security Engineer Raytheon Technologies	Test & Evaluation -ICOTE Invitation Only
3:40 – 4:10 pm	DE-24571 Digital Engineering Trade Study Example: NASA Ranger Program **Mark Payton** Digital Engineer SAIC	Arch/MOSA-24660 A Model-Based Approach to Evaluating Architecture Specifications for MOSA Compliance **Dr. Awele Anyanhun** Senior Research Systems Engineer Georgia Tech Research Institute		SSE–24760 Program Protection and Secure Cyber Resilient Engineering Initiatives **Melinda Reed** Systems Security Director OUSD (R&E)	
4:10 – 4:40 pm	DE – 24612 Lessons Learned on Data, Systems, and Organization modeling in UAF **Charles Stirk** Senior Research Engineer GTRI			SSE-24594 Joint Federated Assurance Center Modernization 2022 **Brian Nowotny** JFAC Director OUSD(R&E) **Dr. Mark Winstead** Systems Security Engineering Department, Chief Engineering MITRE	
4:40 – 5:10 pm	DE-35000 Digital Engineering the Next Chapter **Daniel Hettema** Director, Digital Engineering Modeling & Simulation OUSD (R&E)				

5:10 pm	**RECEPTION**

WEDNESDAY, NOVEMBER 2

CONCURRENT BREAKOUT SESSIONS

TRACK NAME	2A1 – Digital Engineering	2A2 – Architecture/MOSA	2A3 – Mission Engineering / System of Systems	2A4 – System Security Engineering	2A5 – Test & Evaluation / Program Management
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber	Ed Moshinsky & Mike Franco	Dr. Judith Dahmann	Cory Ocker	Jeff Bilco
8:00 – 8:30 am	Agile-24812 Challenges and Success Patterns to Delivering Capabilities Faster **Dr. Suzette Johnson** NG Fellow, Lean Agile Northrop Grumman **Robin Yeman** Chief Technical Officer Catalyst Campus for Technology & Innovation	Arch/MOSA-24764 Preview of an Enterprise Product Architecture (EPA) to Support a Modular Open Systems Approach (MOSA) **Dr. Thomas DuBois** CTO JHNA	ME/SOS-24791 NDIA Systems Engineering Division Mission Engineering Initiative **Dr. Judith Dahmann** Technical Fellow The MITRE Corporation	SSE-24589 Office of the Under Secretary of Defense for Research and Engineering Software Assurance Roadmap **Steven Grice** Software Assurance Technical Director OUSD (R&E)	T&E-24509 Automation of Test Case Generation and Software System Modelling **Dr. Michael Lingg** Principal Computer Engineer Array Of Engineers
8:30 – 9:00 am	DE-24510 Collaborative Modeling - Agile Model-Based Systems Engineering **Ken Kubo** Director, Engineering Technologists Northrop Grumman Space Systems	Arch/MOSA-24597 An Update to the Comprehensive Architecture Strategy (CAS) and its Supporting Architecture Body of Knowledge **Scott Wigginton** Experimental Developer U.S. Army DEVCOM AvMC	ME/SOS-24795 Mission Engineering and Complexity **Dave Chesebrough** Vice President Government, Defined Business Solutions	SSE–24595 A Comprehensive Look at Software Assurance Through DevSecOps **Bradley Lanford** Systems Security Contract Support OUSD(R&E)	T&E-24512 Advancing M&S in Acquisition Test and Evaluation **Dr. Jason Daly** Department Chief Engineer, Defense Systems Engineering MITRE
9:00 – 9:30 am	DE-24657 Leveraging Model-Based Systems Engineering Tools and Techniques to Build Enterprise Knowledge Models **Patrick Bains** Lead Systems Engineer Booz Allen Hamilton	Arch/MOSA-24609 A MOSA for Directed Energy Weapon Systems **Walter Roscello** Lead Scientist U.S. Navy	ME/SOS-24797 Relationship of Mission Engineering to Systems of Systems Engineering **Dr. Judith Dahmann** Technical Fellow The MITRE Corporation	SSE-24593 Secure Cyber Resilient Engineering (SCRE) Design Code **Melinda Reed** Systems Security Director OUSD (R&E)	SSE-24518 Summary of the Ongoing OUSD DT&E Cyber Analytics Landscape Task **Sarah Standard** Cybersec/Interop Tech Dir D DTE&A OUSD (R&E)

9:30 – 10:00 am	**BREAK**				
TRACK NAME	**2B1 – Digital Engineering**	**2B2 – Architecture/MOSA**	**2B3 – Mission Engineering / System of Systems**	**2B4 – System Security Engineering**	**2B5 – Test & Evaluation / Program Management**
ROOM	Peninsula 1-3	Peninsula 4	Peninsula 5-7	Biscayne 1-2	Canaveral 2-3
MODERATOR	John Daly & Chris Schreiber	Ed Moshinsky & Mike Franco	Dr. Judith Dahmann	Cory Ocker	
10:00 – 10:30 am	DE-24524 Accelerating Digital Transformation of Engineering: Progress by the NDIA / INCOSE DEIX Working Group (DEIXWG) **Sean McGervey** Director, Model-Based Enterprise Dassault Systems	Arch/MOSA-24770 Achieving MOSA Benefits: "A Decision Framework for Choosing MOSA Metrics" **Steve Henry** Professor DAU	ME/SOS-24653 Context is Everything! **Matthew Hause** Principal System Strategy, Inc.	SSE-24471 Accelerating Modernization of Software Systems Engineering with a Special Emphasis on the New Version of IEEE SWEBOK (v.4.0) and the New Software Security Knowledge Area **Dr. Kenneth Nidiffer** Professor George Mason University	T&E-24631 Technical Debt as a Potential Leading Indicator for Test and Evaluation **Zakaria Ouzzif** Chief Engineer Raytheon Technologies
10:30 – 11:00 am	DE-24604 Digital Engineering Standardization - Current Landscape and Future Development **Celia Tseng** Sr Manager A&D Industry Dassault Systems	Arch/MOSA-24517 Digital Engineering Tool Selection Criteria **Frank Salvatore** Senior Systems Engineer OUSD (R&E)	ME/SOS-24538 The Israel Air Force take on System of Systems Engineering for International Platform Integration **Maj Tzvika Kaminsky** Chief System Engineer Israel Air Force	SSE-24540 Using Product Cybersecurity to Implement Software Assurance **Randall Brooks** Principal Engineering Fellow Raytheon Technologies	T&E – 24637 The Evolution of Systems Verification and Validation in Vehicle Simulation Modeling at ERDC **Dr. Jessica Lyons** Research Social Scientist Engineer Research Development Center
11:00 – 11:30 am	DE-24763 How to "Digital Viewpoint Model (DVM) **Ken Zhang** MBSE Chief Engineer for the Space and Airborne Systems Sector L3Harris	Arch/MOSA-24568 Don't Play the Telephone Game: Ensuring Architectural Fidelity **Michael Vinarcik** Director SAIC	ME/SOS – 24535 Applied Digital Engineering – A Case Study in Using Space System Architectures to Understand Program and Mission Risks **Lauren Hale** Sr. Engineering Specialist System of Systems Engineering Office The Aerospace Corporation	SSE-24759 Application of Marking and Distribution Statements on Controlled Technical Information **Melinda Reed** Systems Security Director OUSD (R&E)	PM – 24784 Systems Engineering Planning and Architecture Challenges In an Agile Culture **Gordon Kranz** Chief Engineer Enlightened IPM

11:30 am – 12:00 pm	DE-24483 Adventures in Building a Digital Engineering Ecosystem **Julie DeMeester** Engineering Fellow Raytheon Technologies	Arch/MOSA-24519 Agile/MOSA/Microservice Architectures – Stronger Together **Kurt Mohr** Engineering Fellow Raytheon	ME/SOS-24794 Applying Mission Engineering to the U.S. Department of Defense Rapid Defense Experimentation Reserve **Dr. Judith Dahmann** Technical Fellow The MITRE Corporation	SSE - 24678 Risk and Issue Revisited in Systems Security Engineering **Dr. Mark Winstead** Chief Engineer, System Security The MITRE Corporation	PM – 24674 A Retrospective on Model-based Systems Engineering in Undergraduate Engineering Education **LT Col Jeff Newcamp, USAF** Director United States Air Force Academy's Systems Engineering Program
12:00 – 1:00 pm	**LUNCH BREAK**				
TRACK NAME	**2C1 – Digital Engineering**	**2C2 – Architecture/MOSA**	**2C3 – Mission Engineering / System of Systems**	**2C4 – System Security Engineering**	**2C5 – Program Management**
ROOM	**PENINSULA 1-3**	**PENINSULA 4**	**PENINSULA 5-7**	**BISCAYNE 1-2**	**CANAVERAL 2-3**
MODERATOR	John Daly & Chris Schreiber	Laura Hart & Tamara Hambrick	Dr. Judith Dahmann	Cory Ocker	
1:00 – 1:30 pm	DE-24792 Improved Data Fusion in Digital Twins: A Requirements Analysts **Laura Hugill** Analyst Department of Defense	Arch/MOSA-24548 DoD MOSA Implementation Guidance **Nadine Geier** Director Systems Engineering OUSD (R&E)	ME/SOS-24435 Model-Based Capability Planning and Enterprise Portfolio Management **Dr. James Martin** Aerospace Corporation, UAF Revision Task Force with OMG	SSE – 24761 Addressing Critical Program Information Challenges **Randy Woods** SSE & Anti-Tamper Director OUSD(R&E)	PM-24515 A Rocket Scientist's Approach to Continuous Innovation and Improvement **Andy Inkeles** Risk and Innovation Lead USSF National Security Space Launch Program
1:30 – 2:00 pm	DE-24677 Application of the Digital Thread Through the Digital Engineering Framework for Integration and Interoperability **Daniel Dunbar** Research Assistant Stevens Institute of Technology	Arch/MOSA-24572 Architecting Deep Learning Models to Enable AI Capability to Complex Adaptive Systems Architectures **Richard Threlkeld** PhD Student University of Missouri, Science and Technology	ME/SOS-24646 An Enterprise Portfolio Management Framework for Mission Planning, Engineering, and Acquisition **Dr. Warren Vaneman** Professor of Practice Naval Postgraduate School	SSE-24591 Secure Cyber Resilient Engineering (SCRE) Practice **Melinda Reed** Systems Security Director OUSD (R&E)	PM-24619 From Lessons Learned to Lessons Applied: A Digital Paradigm Shift **Paul Wach** Senior Engineer Virginia Tech

2:00 – 2:30 pm	DE-24776 Digital Twin to Detect Nuclear Proliferation: A Case Study **Christopher Ritter** Director, DICE/Dept Manager, Digital Eng. Idaho National Laboratory	Arch/MOSA-24816 Long Term Trends in Security Threats and an Approach for Integrating Them into System Architecture and Design **Larri Rosser** Engineering Fellow Raytheon Intelligence and Space	ME/SOS-24667 Mission Engineering-based Portfolio Management **Dan DeLaurentis** Professor Purdue, University's School of Aeronautics and Astronautics	SSE-24676 Where to Step – A Guide to Minefield of Modeling Complex Security Systems **Mitchell Brooks** Cyber Systems Engineer System Security, Inc.	PM-24641 Can Systems Engineering Enhance Policy Development? **Dr. Steven Dam** President and COO SPEC Innovations
2:30 – 3:00 pm	**BREAK**				

TRACK NAME	2D1 – Digital Engineering	2D2 – Architecture / MOSA	2D3 – Mission Engineering / System of Systems	2D4 – System Security Engineering	2D5 - Physics Based Model Simulation
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR		Laura Hart & Tamara Hambrick Scheurer	Dr. Judith Dahmann	Cory Ocker	David Allsop
3:00 – 3:30 pm	DEIXWG Workshop **Sean McGervey** Director, Model-Based Enterprise Dassault Systems **Risa Gorospe** Solutions Consultant, CATIA No Magic, Dassault Systems Technical Lead, INCOSE Digital Engineering Information Exchange Working Group (DEIXWG) **Ken Zhang** MBSE Chief Engineer for the Space and Airborne Systems Sector L3Harris **Celia Tseng** Sr Manager A&D Industry Dassault Systems	Arch/MOSA-24552 SE Modernization Across the Program Lifecycle **Nadine Geier** Director Systems Engineering, OUSD (R&E)	ME/SOS-24778 Mission Engineering Applied to System of Systems Architecture Analysis **Dr. Peter Korfiatis** Department Manager The MITRE Corporation	SSE–24526 Cyber Supply Chain Risk Management (C-SCRM) a System Security Engineering Role in the Future of Systems Engineering **Holly Dunlap** Principal System Security Engineer Cyber Supply Chain Risk Management The MITRE	PBMS-24613 Machine Learning-Based Surrogate Modeling of Human Vehicular Vibrational Injuries **Will Kirkpatrick** Graduate Research Assistant Mississippi State University
3:30 – 4:00 pm		Arch/MOSA-24516 Architecting for the Cloud: A SysML-Based Profile for Cloud Deployments **Jonathan Backhaus** Engineering Fellow ManTech International Corporation	ME/SOS–24606 Digital Threads: Benefits, Challenges, And Practices **Eran Gery** Solutions Architect IBM	SSE-24607 Building Hardware Assurance with Trusted Suppliers: Creating Multi-layered Security **Dave Chesebrough** Vice President Government Defined Business Solutions	PBMS– 24785 Incorporating Technical Measures of Performance into Project Metrics **Nick Pisano** President and CEO SNA Software, LLC
4:00 – 4:30 pm		Arch/MOSA-24504 Eight Components of an Autonomous, Self-Healing System **Matthew Kehret** CTO, Senior Director Technology, Integratison & Accel Raytheon Missiles and Defense, Digital Technology	ME/SOS-24611 Method for Developing SoS Architectures using SysML Model Federation **Chris Swickline** Digital Engineer SAIC	SSE–24490 Criticality of Software Supply Chain Security **Alan Hohn** Director, Software Strategy Lockheed Martin	
4:30 – 5:00 pm		Arch/MOSA-24544 Modeling a Space Launch System Using the Unified Architecture Framework (UAF) **Logan Mitchell** Junior Systems Engineer Quantum Research International	ME/SOS-24582 Operationally Responsive Mission Engineering (ORME) **Ray Etter** President/Chief Engineer TerraConcepts, LLC	SSE – 24815 Capability-Based Security Engineering for Strategy Formulation and Stakeholder Alignment **Rick Dove** Independent Strategist	

THURSDAY, NOVEMBER 3

CONCURRENT BREAKOUT SESSIONS

TRACK NAME	3A1 – System Security Engineering / Digital Engineering	3A2 – Architecture/MOSA	3A3 – Specialty Engineering / Safety & Environmental Engineering	3A4 –Agile	3A5 – Physics Based Model Simulation
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber	Ed Moshinsky & Karl Shephard	Tim Sheehan & Diane Dray	Ken Kubo	David Allsop
8:00 – 8:30 am	SSE-24777 Implementing Software Bill of Materials (SBOM) in DoD Acquisition **Bradley Lanford** Systems Security Contract Support OUSD(R&E)	Arch/MOSA-24817 Standardization of Model Based Acquisition (MBAcq) **Laura Hart** Engineering Research Engineer Lockheed Martin	SE/SEE-24586 DoD Sustainability Program and the DoD Sustainable Technology Evaluation and Demonstration (STED) Program **David Asiello** Director of Sustainability & Acquisition OASD EI&E	Agile–24491 Starting the Transition From DevOps to DevSecOps **Allan Matthews** Senior Principal Software Engineer Raytheon Technologies	PBMS-24698 Progress Towards Improving the Models in Model Based Systems Engineering with High Fidelity Physics **Dr. Scott Morton** Associate Director for CREATE DoD HPCMP
8:30 – 9:00 am	SSE-24771 Missing In Action: Mission Impact Assessment **Teresa Merklin** Cyber Fellow Lockheed Martin Aeronautics	Arch/MOSA-24638 Can Data-Driven Systems Engineering Meet the Goals of SE Modernization? **Dr. Steven Dam** President & COO SPEC Innovations	SE/SEE-24511 Data Centricity: Multi-Directional Flow of Specialty Engineering Data Throughout the Life Cycle **Chris DeLuca** Director for Specialty Engineering OUSD (R&E)		E&T-24610 Competency-Based Online Education Using AFIT's Avolve Application **Richard Sugarman** Department Head Air Force Institute of Technology
9:00 – 9:30 am	DE-24657 Leveraging Model-Based Systems Engineering Tools and Techniques to Build Enterprise Knowledge Models **Patrick Bains** Lead Systems Engineer Booz Allen Hamilton	Arch/MOSA-24679 Standardized Analytic Viewpoint Overlays (AVOs) **Laura Hart** Engineering Research Engineer	SE/SEE-24649 Regulatory and Sustainability Challenges for the Automotive Industry **Drew Rak** Program Manager Toyota Motor North America	Agile-24514 Software Science & Technology Strategic Vision, Goals, and Focus Areas **Allan Dianic** Director, Software Engineering & Prototyping, OUSD (R&E)	E&T – 24545 Systems Engineering Modernization (SE MOD) Key Enablers for System Development on DoD Programs **Dr. Robert Raygan** Prof. of Engineering Mgmt., DAU CNE Defense Acquisition University
9:30– 10:00 am	**BREAK**				

TRACK NAME	3B1 – Digital Engineering	3B2 – Architecture/MOSA	3B3 – Specialty Engineering / Safety & Environmental Engineering	3B4 – Agile	3B5 – Education & Training
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber	Ed Moshinsky & Karl Shephard	Tim Sheehan & Diane Dray	Ken Kubo	Dr. Robert Raygan
10:00 – 10:30 am	DE-24658 Transforming Systems Engineering Reviews **Toni Nolder** Space Architecture Department Aerospace Corporation	Arch/MOSA-24672 Dynamic Capability Investment for Emerging Missions **Mike Franco** Chief Architect, Processes & Tools Chief Architect Boeing Defense, Space & Security	SE/SEE-24622 Implementation Guide: Model-Based Systems Engineering (MBSE) for System Safety **Trung Hoang** Safety Engineer Naval Ordnance Safety & Security Activity (NOSSA)	Agile-24525 Defining a Measurement Framework for Digital Engineering **Tom McDermott** Research Director Stevens Institute of Technology	E&T-24636 Implementing SysML 2.0 – Part 2 **Michael Campbell** Senior Systems Engineer, Manager of Innovation SPEC Innovation
10:30 – 11:00 am	DE-24551 Analyzing Digital Engineering Data: Transforming the Way We Think About Model Reviews **Heidi Jugovic** Digital Engineer Chief SAIC	Arch/MOSA-24808 Model For a Purpose: Scoping an Architecture Model Using the ASDP Digital Transformation Contract Language **Brad Kukurza** Systems Engineering Manager The Boeing Company	SE/SEE-24675 Sustainability Analysis in the Adaptive Acquisition Framework **Michael Bruckner** Principal Engineer Manager Noblis	Agile-24559 Agile and DevSecOps in the DoD Space Acquisition Environment **Dr. Michael Orosz** Research Associate Professor and Research Director USC Information Sciences Institute	E&T-24584 When Worlds Collide: Leveraging MBSE/SysML for DoDAF Architectures in Programs and Formal Requirements **Maj Brandon Froberg, USAF** Chief Integration & Interoperability Branch Air Force Special Operations Command

11:00 – 11:30 am	DE-24663 Solution Debt in the Age of Digital Engineering **Dr. Heidi Davidz** Intelligent Systems Engineering SME **ManTech International Corporation**	Arch/MOSA-24651 Modeling System Configurations Over Time **Matthew Hause** Principal System Strategy, Inc.	SE/SEE-24521 Strategic Alternate Sourcing Program Office (SASPO): Alternate Sourcing and Diminishing Manufacturing Sources and Material Shortages **Jerry Zamora** Chief, Strategic Alternate Program Office 448th Supply Chain Management Wing	Agile-24684 Digital Transformation in NSSL Quality Engineering: Establishing the Digital Data Chain Framework through the Provenance Chain Transparency Platform **Maj Juan Mayssonet** NSSL Quality Engineering Branch Launch Enterprise	SEMOD Panel **Dr. Robert Raygan** Prof. of Engineering Mgmt., DAU CNE Defense Acquisition University
11:30 am – 12:00 pm	DE-24750 Modeling Information to Support Systems Engineering Technical Reviews Based on DOD Data Item Descriptions (DIDs) **Robert Wojcik** Senior Member of the Technical Staff CMU/SEI	Arch/MOSA-24639 What is Systems Engineering? **Dr. Steven Dam** President & COO SPEC Innovations	SE/SEE 24696 Using Model Based System Engineering to Identify Safety Critical Functions in Airworthiness Certifications **Capt Jeff King, USAF** Instructor of Systems Engineering Air Force Institute of Technology	Agile-24693 Integrating Elements of Digital Engineering into Agile Software Acquisition Training **Curtis Jefferson** Software Tech Expert HA AFMC DoE Systems Engineering Division	
12:00– 1:00 PM	**LUNCH ON OWN**				

TRACK NAME	3C1 – Digital Engineering	3C2 – Architecture / MOSA / Program Management	3C3 – Specialty Engineering / Safety & Environmental Engineering	3C4 – Agile	3C5 - Education & Training
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber	Bob Scheurer & Rebecca Hicks	Tim Sheehan & Diane Dray	Ken Kubo	Dr. Robert Raygan
1:00 – 1:30 pm	DE-24577 Architecting the Digital Thread Enabling the Digital Transformation (DTx) of Raytheon Missiles and Defense **Tara Trumbull** Senior Principal Systems Architect **Deborah Thomas** Senior Principal Systems Engineer Raytheon Missiles and Defense	Arch/MOSA-24799 An Acquisition System Meta Model **Chris Garrett** Senior Leader U.S. Air Force	SE/SEE-24755 Poly-fluorinated Alkyl Substances Primer and Update **Col Tim Sheehan, BRANCH (Ret)** Engineering Fellow Raytheon Technologies	Agile-24605 Exploring the Enablers of Post-Production Change for Flexible System Design **Aditya Singh** NSF Research Traineeship Fellow The George Washington University	E&T-24775 2022 SSE Workforce Development Sampling and Feedback Analysis **Matthew Lee** System Security Engineer Raytheon Technologies
1:30 – 2:00 pm	DE-24685 Ready One: Delivering Digital Engineering and the Digital Thread **David Ewing, Jr.** Director Digital Engineering Digital Thread & Tool Federation Leader Engineering Innovation Factory SAIC	Arch/MOSA-24804 The Intellectual Property (IP) Thread in Digital Engineering and Acquisition implementation in the Department of Defense (DoD) **John Daly** Chief Engineer Booz Allen Hamilton	SE/SEE-24682 Regulation Impacts and Management Steps of Hydrofluorocarbons (HFCs) Drawdown for the U.S. Department of Defense (DoD) and Defense Industrial Base (DIB) **Dr. Kari Meier** Greenhouse Gases & Sustainable Chemistry (ODASD (E&ER))	Agile-24520 Codemmandos: Empowering Agile/ DevSecOps Citizen Developers with No-code & Scripting **Maj Brandon Froberg, USAF** Chief Integration & Interoperability Branch Air Force Special Operations Command	
2:00 – 2:30 pm	DE-24506 Creating a Digital Foundation Through the Development of a Digital Thread **Cathrin McCaghren** Systems Engineer Raytheon Missile Defense		SE/SEE-24627 Impacts to the U.S. Department of Defense and Defense Industrial Base from the Toxic Substances Control Act **Dr. Patricia Underwood** Director, Chemical & Material Risk Management ODASD (EI&E)	Agile-24522 System Test Verification: The Digital Thread Lynchpin Between Systems Engineering Requirements Development and Software Deployment **Yvonne Green** Senior Manager Software Engineering Raytheon Technologies	E&T-24596 Cross Domain Solutions Tutorial **Burhan Adam** Policy Guidance & Standards Director OUSD (R&E)
2:30 – 3:00 PM	**BREAK**				

TRACK NAME	3D1 – Digital Engineering	3D2 – Project Management / Mission Engineering / System of Systems	3D3 – Specialty Engineering / Safety & Environmental Engineering	3D4 – Agile	3D5 – Education & Training
ROOM	PENINSULA 1-3	PENINSULA 4	PENINSULA 5-7	BISCAYNE 1-2	CANAVERAL 2-3
MODERATOR	John Daly & Chris Schreiber		Tim Sheehan & Diane Dray	Ken Kubo	Dr. Robert Raygan
3:00 – 3:30 pm	DE-24528 Converging MBSE Methodology **Ryan Noguchi** Senior Engineer Specialist, Space Architecture Department The Aerospace Corporation		SE/SEE-24680 Joint System Safety Standards Working Group MIL-STD-882E Initiative **Lori Hales** Senior Acquisition ESOH Analyst Booz Allen Hamilton		E&T-24541 A Digital Twin Simulation Equivalence Principle **Richard Boyd** CEO Ultisim, Inc.
3:30 – 4:00 pm	DE-24556 Utilizing Automation and Ontologies to Design, Deploy, and Sustain an Effective Model Governance Program **Dr. Heidi Davidz** Intelligent Systems Engineering SME ManTech International Corporation		SE/SEE-24474 How to Use Physics-based Digital Human Models Early In Systems Design and During Test and Evaluation **Travis Klofenstein** Executive Director for Programs University of Iowa Technology Institute		E&T-24617 Simulation Training Environment for Digital Engineering **Paul Wach** Senior Engineer Virginia Tech
4:00 – 4:30 pm	DE-24575 MBSE Model Management Pain Points – Wait, this looks familiar! **Barry Papke** Industry Process Success Team, Senior Manager Dassault Systems – CATIA/No Magic		SE/SEE-24647 Hybrid Digital Twin Technology for Predictive Maintenance **Reni Raju** Director, Business Development – FA&D Ansys		
4:30 – 5:00 pm	DE-24642 A Common Ontology: The Rosetta Stone for Exchanging Data between Different Digital Engineering Tools, Languages, and Frameworks **Dr. Warren Vaneman** Professor of Practice Naval Postgraduate School				

National Defense Industrial Association Systems and Mission Engineering Conference

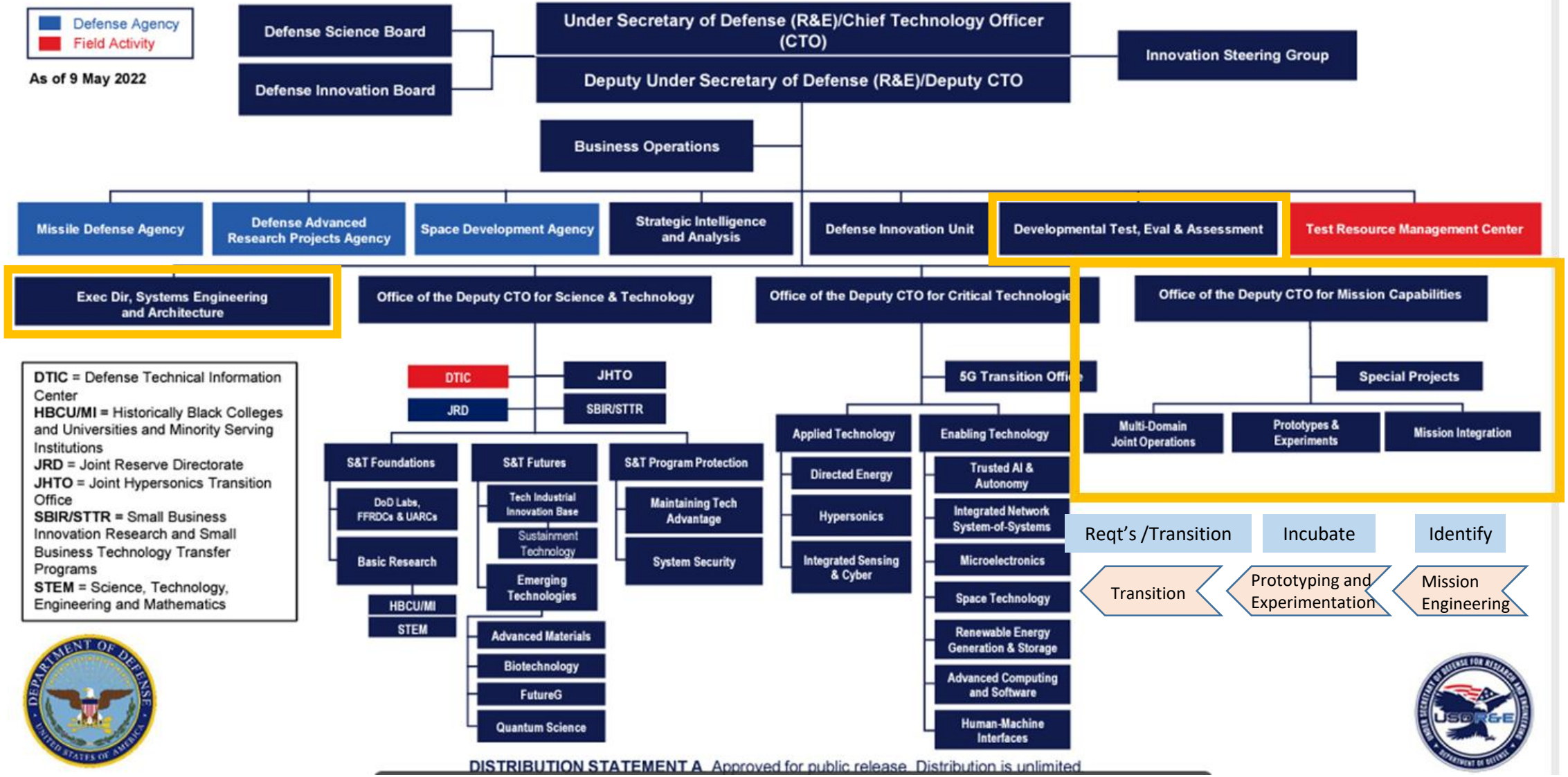
November 2022

OUSD(R&E) Technology Transition and Engineering Initiatives

Mr. Elmer L. Roman, SES
Director, Mission Integration
OUSD (R&E), Mission Capabilities

Distribution Statement A. Approved for public release. Distribution is unlimited. (Case 23-S-0257)

OUSD(R&E) Organizational Structure



DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Rapid Defense Experimentation Reserve (RDER)

The Secretary of Defense established RDER to:

- Focus multi-Component experimentation in a structured, multi-year campaign of learning.
- Proposed experiments based on alignment to Joint missions and potential to yield demonstrable warfighting utility in the near-term.
- Demonstrations and experiments will be conducted at key exercise venues (INDOPACOM Focused).
- Successful demonstrations and experiments can be quickly transitioned to the Components for fielding as new systems or approaches.

"RDER will drive efforts to compete with peer and near-peer adversaries through the development of capabilities that support the Joint Warfighting Concept (JWC) including, but not limited to, fires, command and control, logistics, and capabilities that will drive information advantage." – Deputy Secretary of Defense Dr. Kathleen Hicks

RDER will bring five benefits to DoD:

1. Accelerate Joint Warfighting Capability
2. Expand International Partnerships and Multi-lateral engagement
3. Focus Service experimentation to enable the JWC
4. Quickly demonstrate and assess innovative ideas
5. Provide feedback to future Warfighting concept development

Scope of Mission Engineering

Mission Engineering (ME) – An interdisciplinary approach and process encompassing the entire technical effort to analyze, design, and integrate current and emerging operational needs and capabilities to achieve desired mission outcomes.
(from the draft ME Guide 2.0)

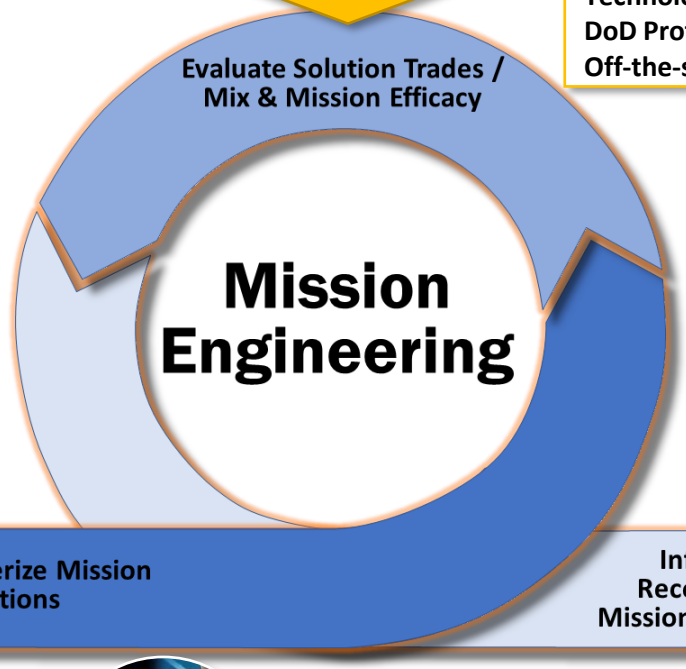
Capability Gaps

- Joint Warfighting Concept (JWC)
- Capability Gap Assessments (CGA)
- Joint Emergent & Urgent Operational Needs
- Emergent & Urgent Operational Needs
- Previous Studies, Analyses, and Experimentation Events

Capability Gaps Define Analysis Focus

Technologies to Close Gaps

- R&E Technology Roadmaps
- RDER Concepts
- Technology Demonstrations
- DoD Prototypes
- Off-the-shelf items

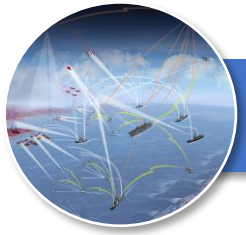


Inform & Recommend

- Requirements
- Architecture implications
- Mission maturation roadmaps

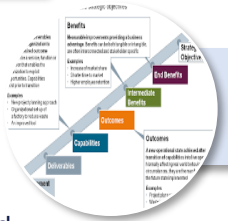
- Capability Integration
- Concept development & Maturation

- Technology roadmaps
- Prototype decisions
- Investment decisions



Characterize Mission & Operations

Evaluate Solution Trades / Mix & Mission Efficacy



Inform & Recommend Mission Solution(s)

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

Mr. Elmer L. Roman, SES
Director, Mission Integration
OUSD R&E/Mission Capabilities
Phone: 703-693-0398
Email: elmer.l.roman.civ@mail.mil

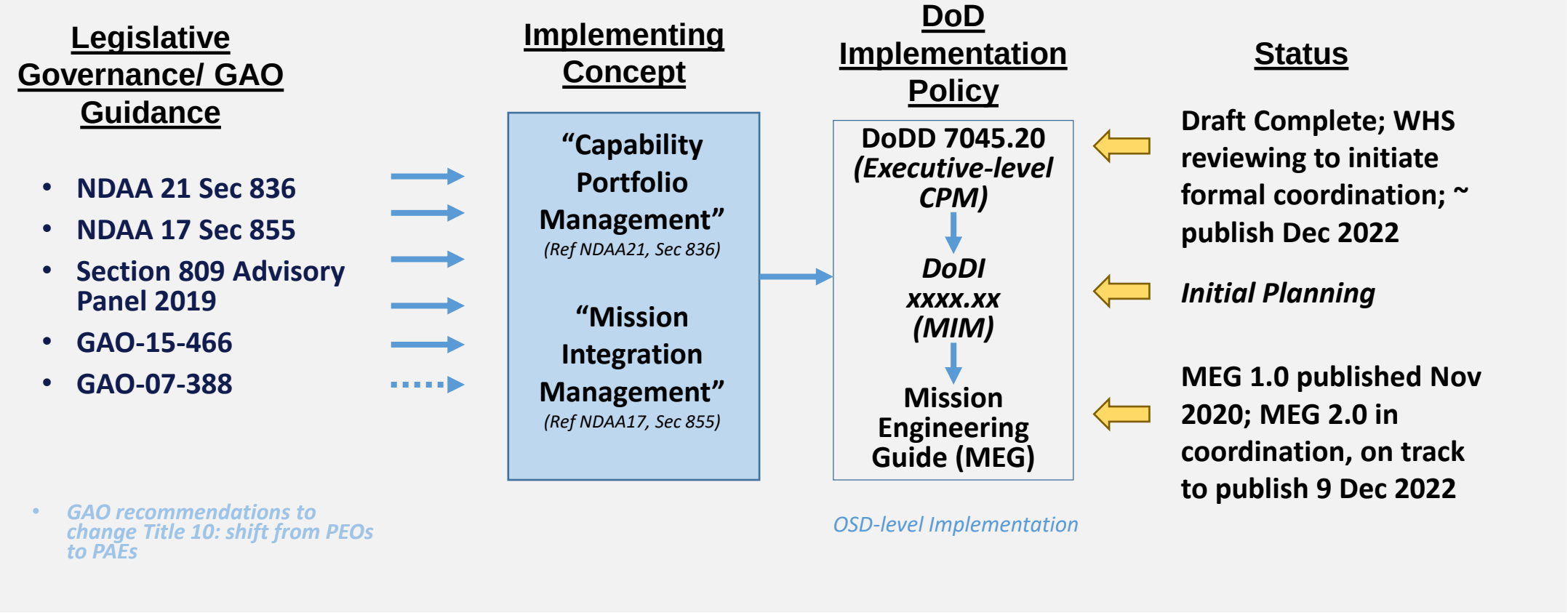
Distribution Statement A. Approved for public release. Distribution is unlimited.

BACKUP

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

Policy Changes for Portfolio Management

Legislative direction is driving changes to the acquisition, requirements, and budgeting processes to focus on delivering *integrated mission capability*, not just individual programs.



Department of the Air Force

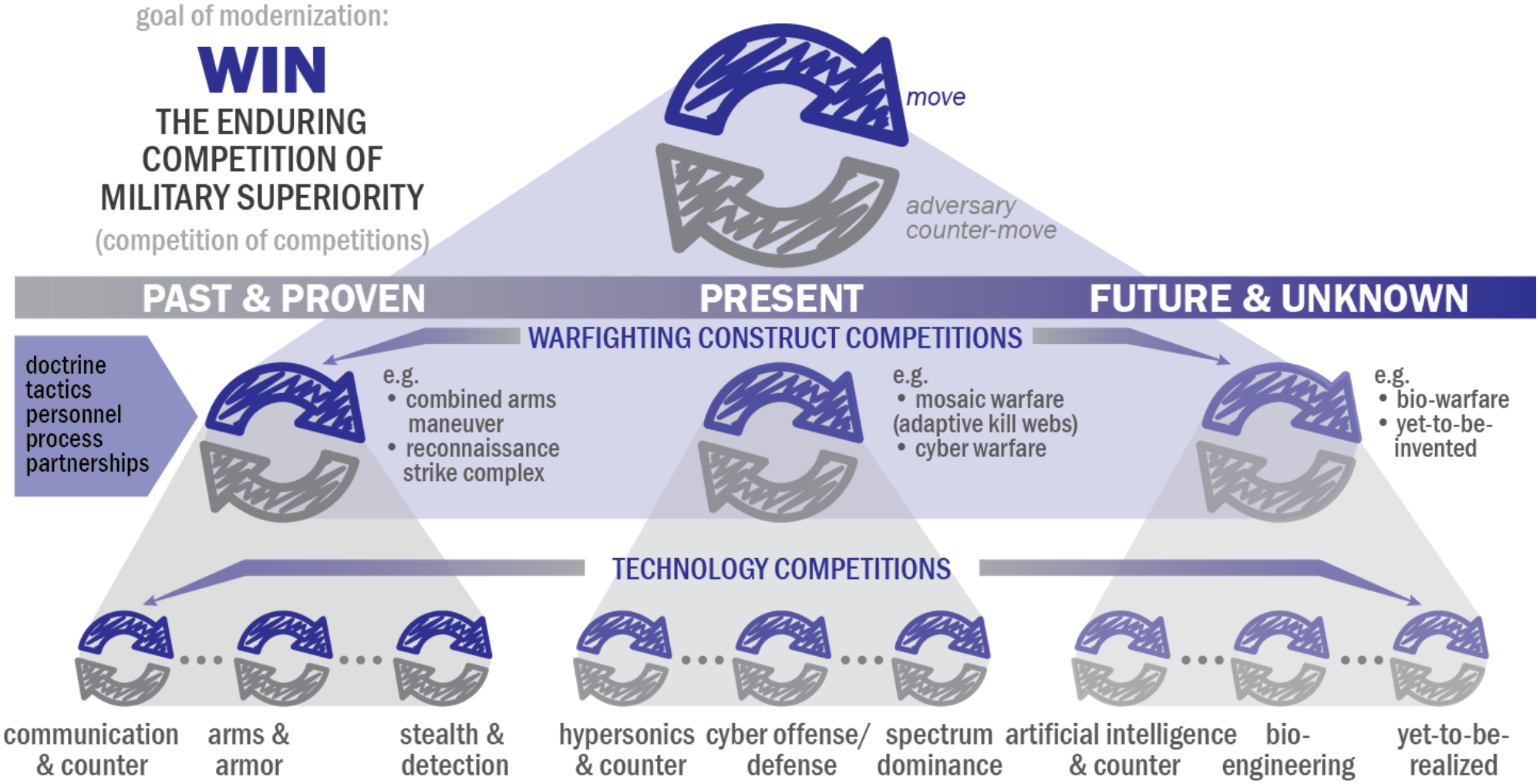
Integrity - Service - Excellence

Mission Engineering and the DAF Operational Imperatives

Dr. Timothy Grayson
Special Assistant to the Secretary of the Air Force
1 November 2022

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Development of new military concepts must take a mission-centric approach



DAF Operational Imperatives

- Defining Resilient Space Order of Battle and Architectures.
- Achieving Operationally-Optimized Advanced Battle Management System (ABMS) / Air Force Joint All Domain Command and Control.
- Achieving Moving Target Indication and Tracking at Scale.
- Defining the Next Generation Air Dominance Family of Systems.
- Defining Optimized Resilient Basing, Sustainment, and Communications in a Contested Environment.
- Defining the B-21 Long Range Strike Family of Systems.
- Ensure the Ability of the DAF to Transition to a Wartime Posture Against a Peer Competitor.

Adaptive System of Systems drive the need for Mission Engineering

DARPA

System of Systems (SoS) delivers lethality by busting the use of only monolithic platforms and networks

STO

Implementing Scales of Integration

Govt (buyer) as Integrator

Approach

- One or more program offices acquire individual elements of a SoS as a collection of stand-alone programs
- In-house engineers attempt to integrate based upon common standards

Outcome

- Reference architecture limiting and burdensome
- Results in interoperability challenges and loose integration at best

Implementing Scales of Integration

Large System Integrator — **Govt (buyer) as Integrator**

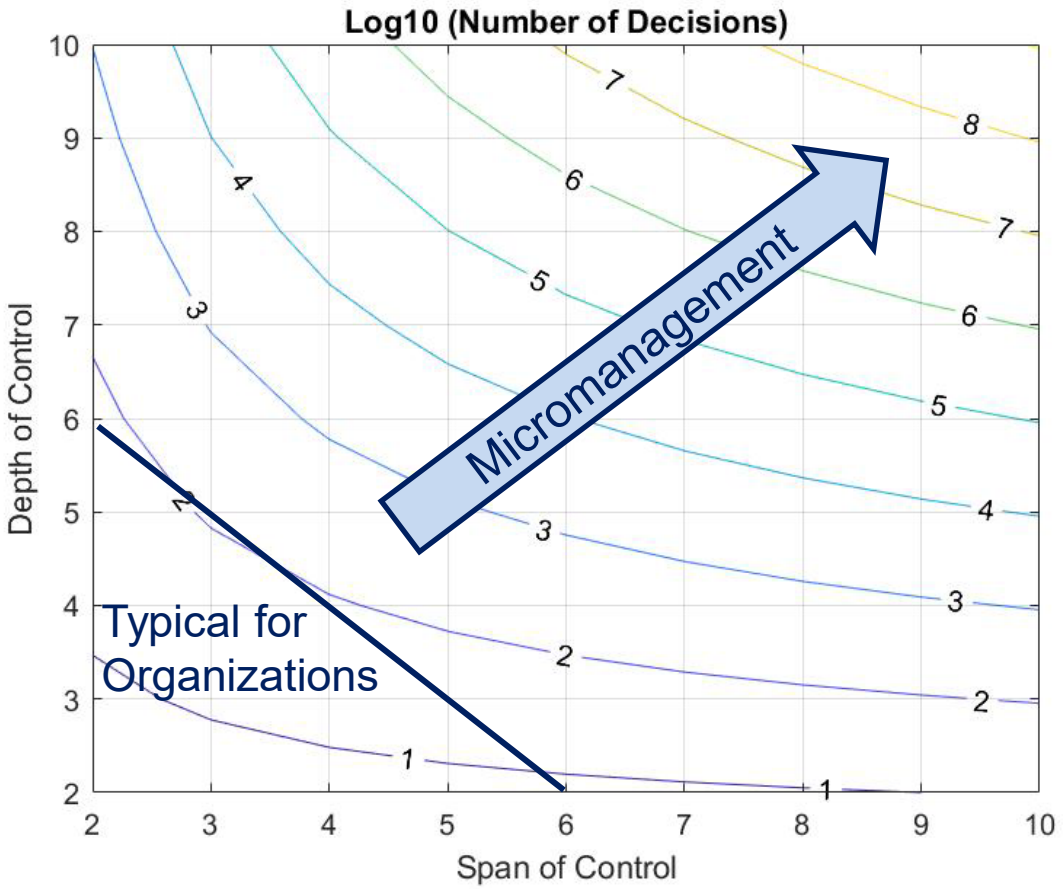
Approach
- Large RFP for highly specified full system of systems
- Single award (usually to large prime) to implement as a major platform program

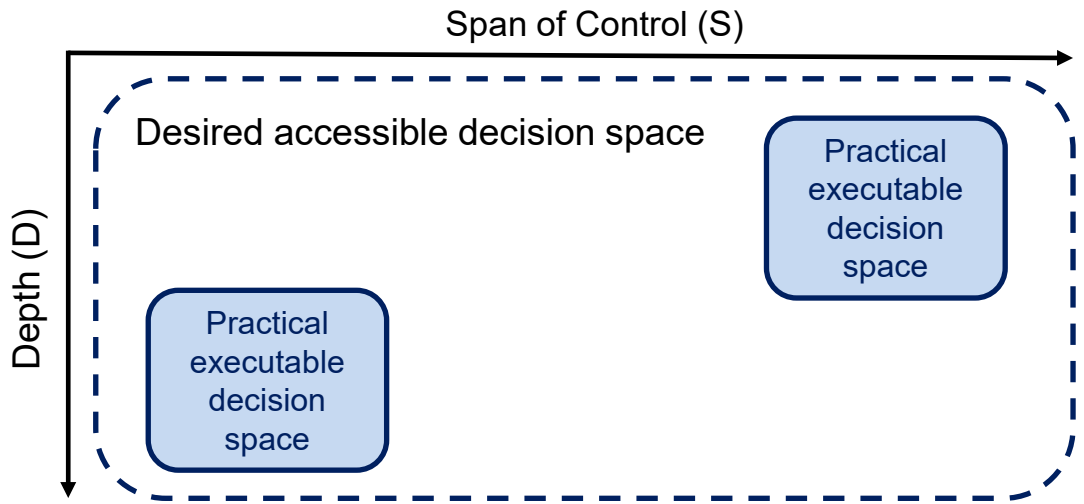
Outcome
- Not aware of any successful examples
- SoS is too complex to system engineer in detail
- Loses flexibility to adapt to mission need
- Unnecessary overhead for little added value

Approach
- One or more program offices acquire individual elements of a SoS as a collection of stand-alone programs
- In-house engineers attempt to integrate based upon common standards

Outcome
- Reference architecture limiting and burdensome
- Results in interoperability challenges and loose integration at best

Maximizing options while minimizing complexity



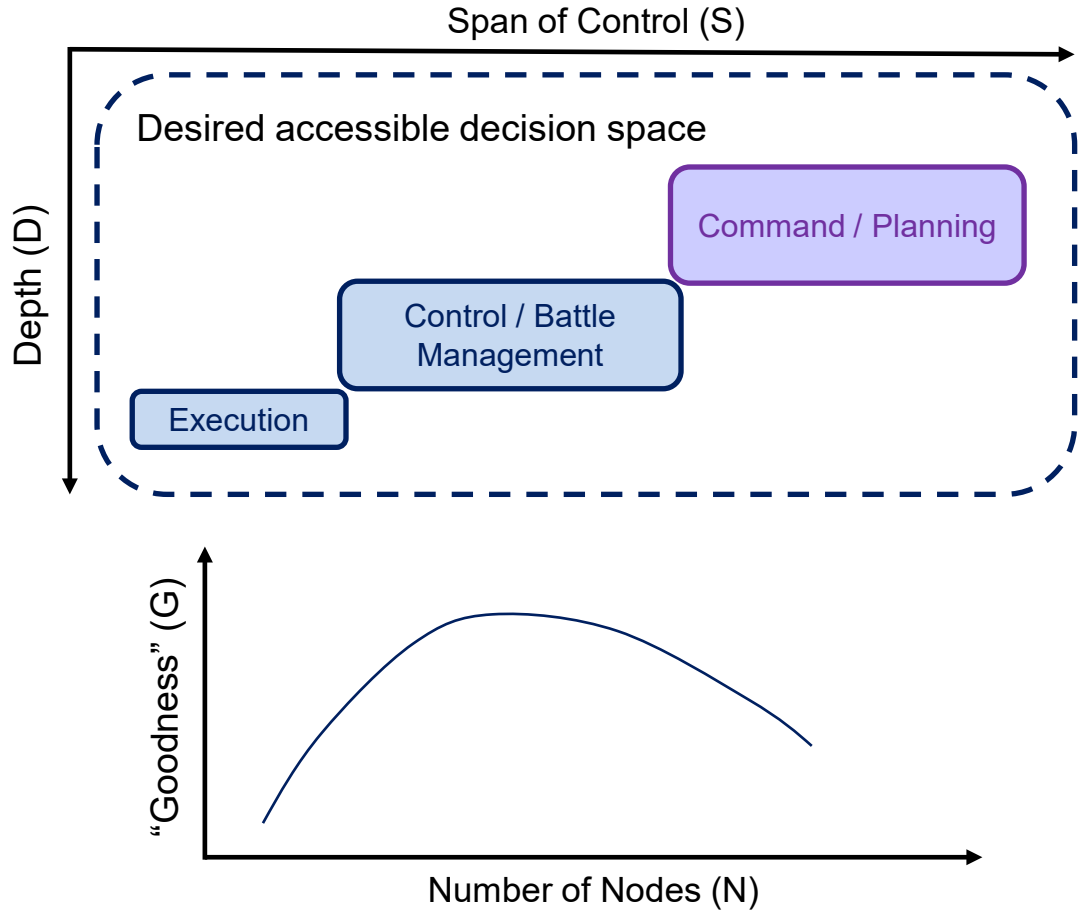


Challenge: ***How to provide the greatest range of options while managing complexity of decision making (for humans and AI)?***

DAF Operational Imperatives #2: Operationally-Optimized Advanced Battle Management System (ABMS) / Air Force Joint All Domain Command and Control (JADC2)

Approach: ***Create Separability of Command from Control, Distributed Battle Management***

- **Objectives:**
  - *Speed* – Must manage complexity
  - *Agility* – Must maintain interoperability
  - *Resilience* – Must maintain redundancy
- **Can start Mission-specific in order to build up to large-scale jointness**



Implementing Scales of Integration

Approach
- Large RFP for highly specified full system of systems
- Single award (usually to large prime) to implement as a major platform program

Outcome
- Not aware of any successful examples
- SoS is too complex to system engineer in detail
- Loses flexibility to adapt to mission need
- Unnecessary overhead for little added value

Approach
- General requirement to engineering services contractor to build platform, integrate tools, and scale
- My bring mix of own and external IP

Outcome
- Commercial-like model
- Taps industry expertise to develop platform and workflow for efficiency
- Risk of vendor lock

Approach
- Technically empowered program office builds platform, buys individual tools, and integrates
- Govt reference architecture, in-house contractors, tool consortia

Outcome
- Agility in selecting tools and adapting/scaling platform
- Can tailor to current mission and operator need (DevOps)
- Avoids vendor lock, but also potentially limited in marketplace and tool sophistication

Approach
- One or more program offices acquire individual elements of a SoS as a collection of stand-alone programs
- In-house engineers attempt to integrate based upon common standards

Outcome
- Reference architecture limiting and burdensome
- Results in interoperability challenges and loose integration at best

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

AFC Digital Engineering Transformation

ARMY FUTURES COMMAND

Dr. Katrina Mansfield

Systems Engineering Branch Chief

November 1, 2022

Approved for Public Release

TOMORROW IS WORTH PROTECTING®

AFC Digital Engineering Transformation

- **Objective:** Establish a collaborative, interoperable digital environment that provides enhanced speed and availability to authoritative data and digital artifacts throughout the system lifecycle to effectively support program milestones, Systems of Systems (SoS) integration, Modeling and Simulation (M&S), test events, exercises, experimentations, and drive senior leadership decision making.

- Strategic (*Drive change across the DoD*) : (1) Supports and aligns to the DoD Digital Engineering Strategy and allows for better synchronization of technology across the DoD; (2) Supports mission thread and capability analysis for Joint operations and exercises

- Operational (*Drive change in the Army*): (2) Establishes the Army Digital Thread and traceable digital artifacts to support system development, integration, analysis, and sustainment across the system development life cycle, (2) Expedites seamless controlled transfer of authoritative technical data, software, information and knowledge between external stakeholders and system owners (e.g. ASA(ALT), AMC, etc.) for continued system development and integration efforts expanding beyond Milestone B

- Tactical (*Drive Change in AFC*): (1) Provides a modernized and adaptable systems engineering environment, changes within a system and system of systems (SoS) can be rapidly evaluated for benefits of cost, schedule, performance and technical risk reduction throughout a system's life cycle; (2) Enhanced rigor and speed of information availability and reuse, analysis, and development of systems and capabilities to Milestone B, (3) Provides verification and validation for interfaces between systems and SOS integration prior to experimentation and exercise events allowing for enhanced learning

DoD Digital Engineering Strategy & AFC

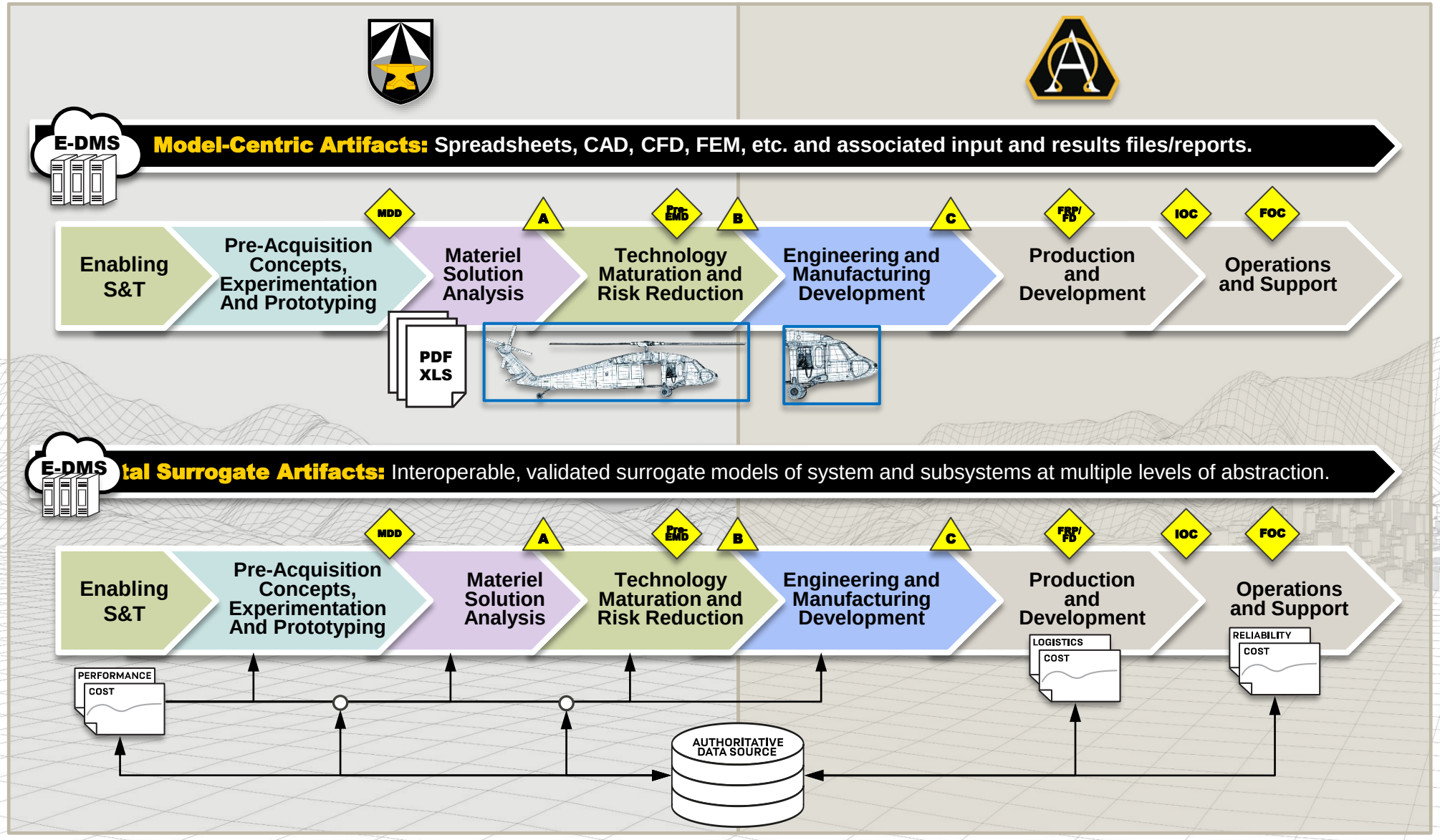
June 2018: The Deputy Assistant Secretary of Defense for Systems Engineering implemented a Digital Engineering Strategy with five goals.

1	**Formalize Development Integration and Use of Models** | There is current collaboration across the CFTs with the RSI Division for the implementation and increased use of MagicDraw for MBSE artifacts. This approach requires the Teamwork Cloud environment for MagicDraw to achieve maximal effectiveness. This is not intended to be prescriptive
2	**Provide an Authoritative Source of Truth** | The ArCADIE repository is described as the architectural source of truth for the Army. However, improved linkage between the system models and the AFC managed AME Baseline model is needed.
3	**Incorporate Technological Innovation** | AFC will increase digital engineering capabilities to enhance decision-making, through automation by the integration of digital engineering tools and data already used within AFC.
4	**Establish Infrastructure and Environments** | Deploying the AME cloud environment will create the necessary infrastructure for data storage and collaboration across the AME. Full understanding and usage of the capabilities will be the responsibility of AFC HQ to ensure all parts of the AME are collaborating and the cloud environment is properly informed.
5	**Transform Culture and Workforce** | This strategy will alleviate the issues of complex culture change using a collaborative approach to the implementation of digital engineering. Create a DE Transformation whitepaper from the RSI Division to serve as the communication of the digital engineering vision and strategy for AFC.

Digital Engineering and the Acquisition Lifecycle

Needs to span the lifecycle from concept to disposal.

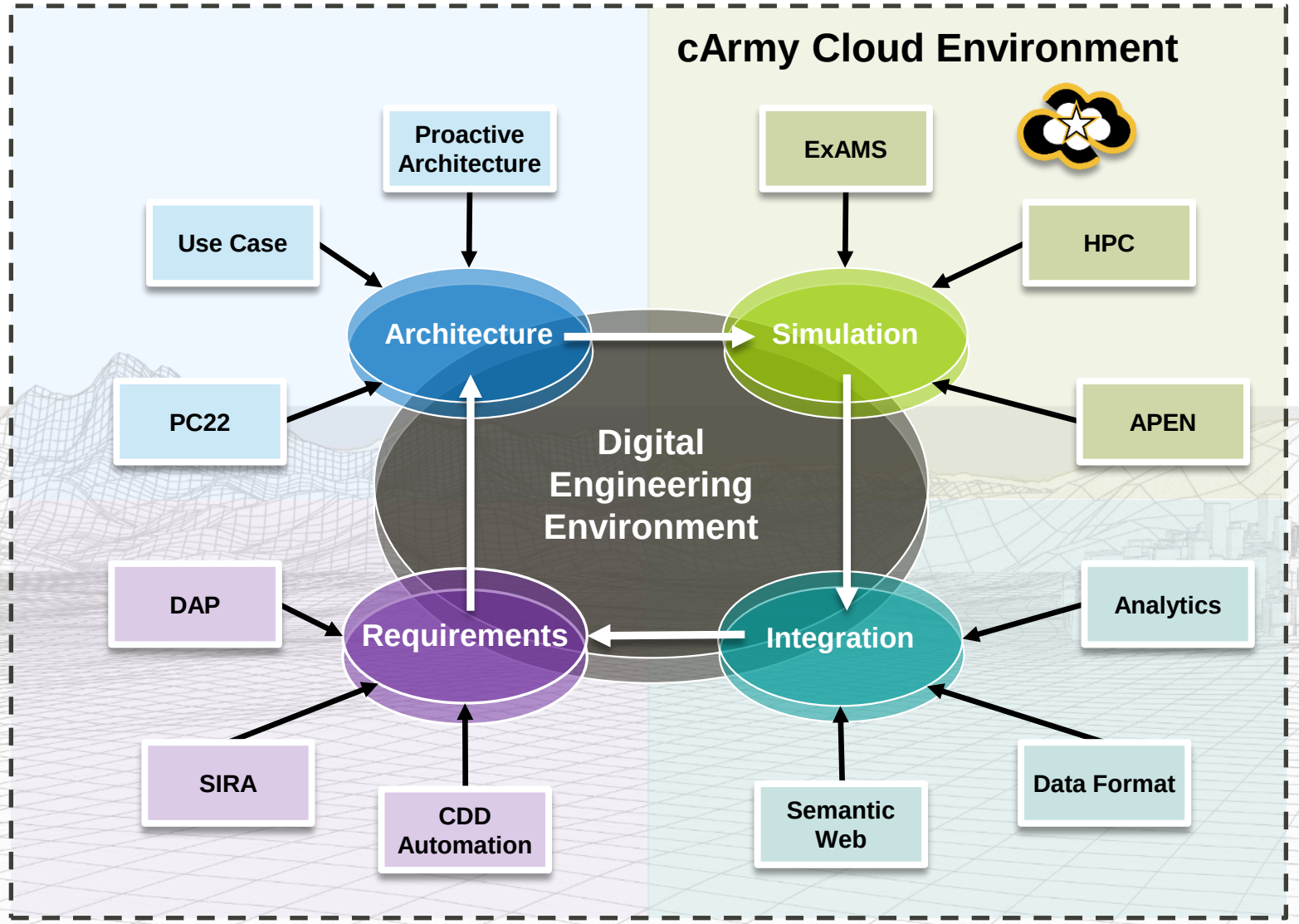
AFC is focused on defining the digital thread from Pre-Milestone A to Milestone B and ensuring a smooth transition to ASA(ALT)



Digital Ecosystem

System Engineering Transformation utilizing DE

- Utilize DE to drive, mature and support evolving requirements
- Drive better interoperability and System of System integration
- Model operational capabilities with authoritative data to drive better decision making
- Full digital traceability of requirements, design, test, and information; available from one source of truth
- Model Operational capabilities with authoritative data to drive better decision making
- Risks are identified and risk mitigations are executed via DE enterprise processes
- Reduced deliverable defects, deliverables acceptance rate



UNCLASSIFIED

Points of Contact

Dr. Katrina Mansfield
- System Engineer Branch Chief
- katrina.m.mansfield.civ@army.mil

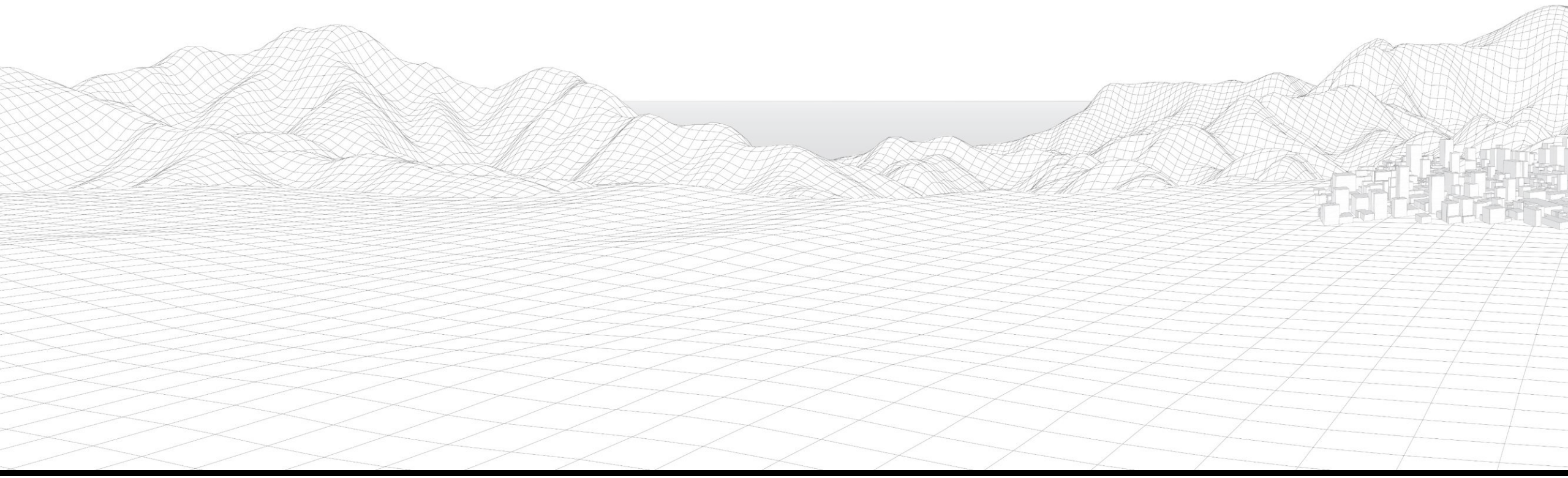
Michael Tucker
- Systems Engineer
- michael.p.tucker38.civ@army.mil

Adeola Olabisi
- Systems Integrator
- adeola.olabisi.civ@army.mil

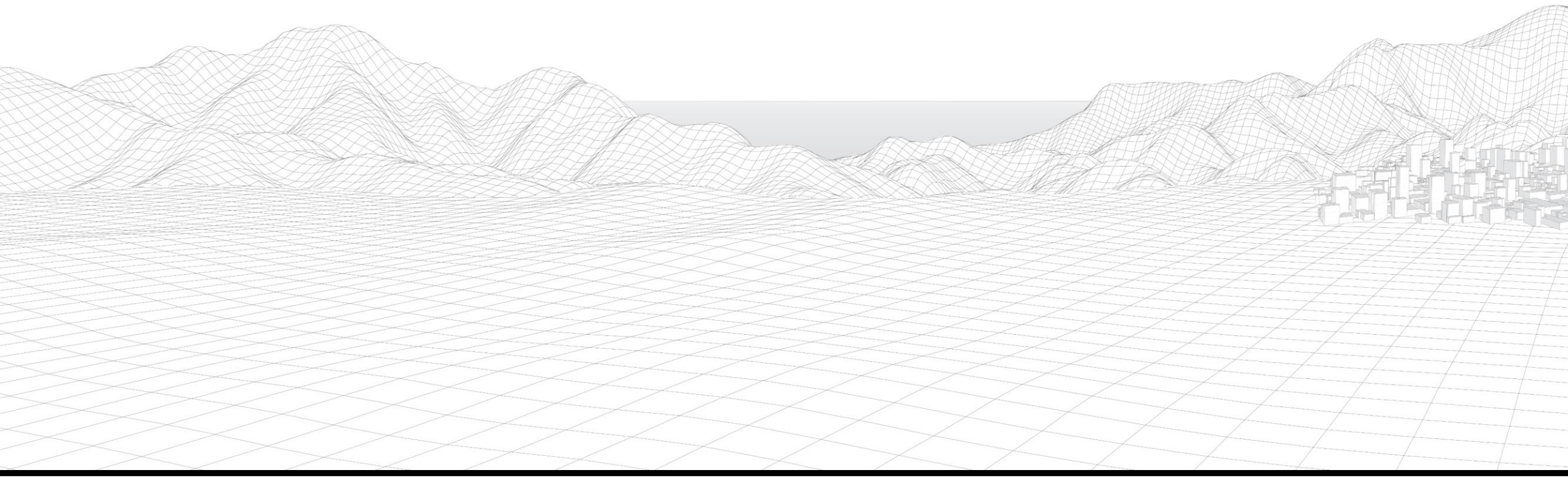
Dr. Joshua Davis
- Data Engineer Sr.
- joshua.t.davis89.ctr@army.mil

Dr. Arthur Brooks
- Systems Engineer Sr. Principal
- arthur.h.brooks.ctr@army.mil

Questions?

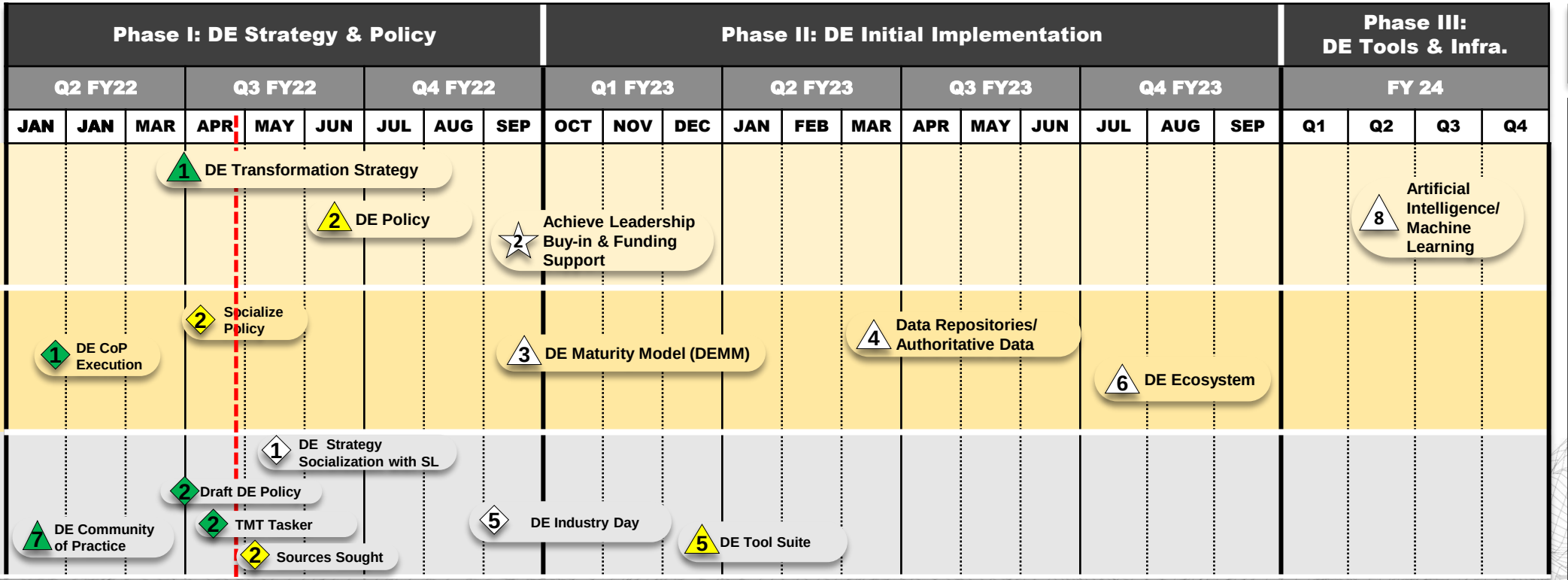


Back-up



ARMY FUTURES COMMAND

LOE 2, OBJ D: Transform Digital Engineering



Desired Future State

S: Supports JADC2 mission thread and capability analysis
O: Establishes the Army Digital Thread and traceable digital artifacts to support system development & integration
T: (1) Provides a modernized and adaptable systems engineering environment, (2) Systems and system of systems (SoS) can be rapidly evaluated for benefits of cost, schedule, performance and technical risk reduction throughout a system's life cycle; (3) Provides enhanced rigor and speed of information availability and reuse, analysis, and development of systems and capabilities

Assessment

Phase I: DE Strategy and Policy

Create a community of practice within the organization to provide DE guidance, expertise, and other resources

Indicators:
- DE Strategy and Policy are being executed
- Define and implement a systematic change approach to implement DE
- Messaging, awareness of DE, participation in reviews, performance management incentives, succession planning

Phase II: DE Initial Implementation

Demonstrate commitment and general support for DE implementation

Indicators:
- Better communication/info sharing
- Collaboration
- Leadership support
- Change management processes
- Availability of tools, investment in tools, experience with tools, stability of tools
- Appropriately trained & experienced workforce, customer
- better access to information

Phase III: DE Tools and Infrastructure

Develop a workforce having the knowledge and competencies to support DE adoption.

Indicators:
- Provide a foundation to integrate models.
- Risks are identified and risk mitigations are executed via DE enterprise processes.
- Existing data repositories are linked and interoperable
- Full digital traceability of requirements, design, test, and information; available from one source of truth
- Reduced deliverable defects, deliverables acceptance rate

End State

Design outcomes show improvement over similar programs, the design process is more effective compared to similar programs

Indicators:
- Integrated data repositories, with access and availability to authoritative data
- Readily accessible system data to feed M&S capabilities to support key decision making.
- Automated versus manual activities
- cArmy unclassified and classified domains are fully operable

Legend:

- ☆ Decision Point
- 1 Primary Task
- 1 Supporting Task
- Task Complete
- Task Incomplete

Enterprise DE Tool Suite Requirements

How an Enterprise Tool Suite and License will reduce overall costs to the command.

- **Reduce** the costs of licenses and sustainment
- **Maintain** interoperability of tools
- **Standardize** product formats for reuse and sharing
- **Standardize** business practices

Enterprise DE Tool Suite Requirements

- **Architecture** (Cameo / MagicDraw)
- **Requirements** (may need light version of DOORS NextGen for occasional pulls from DEVCOM)
- **M&S** (licenses to see/ingest products developed; verify integration requirements met and feed SoS analysis / ExAMS)
- **PLM** (CM/traceability and integration of potential ePDM stovepipes, Aras Innovator)
- **PDM (**ePDM**)**
- **Analysis/Visualization** (R, Python, MATLAB, Spark, SAS, Tableau, PowerBI)
- **Risk/Schedule** (Sword ARM, Project Cloud, Resolver)
- **DDSD Support** (database mining/integration scripts)

MBSE Model Management

Full Lifecycle Configuration Management of MBSE Models

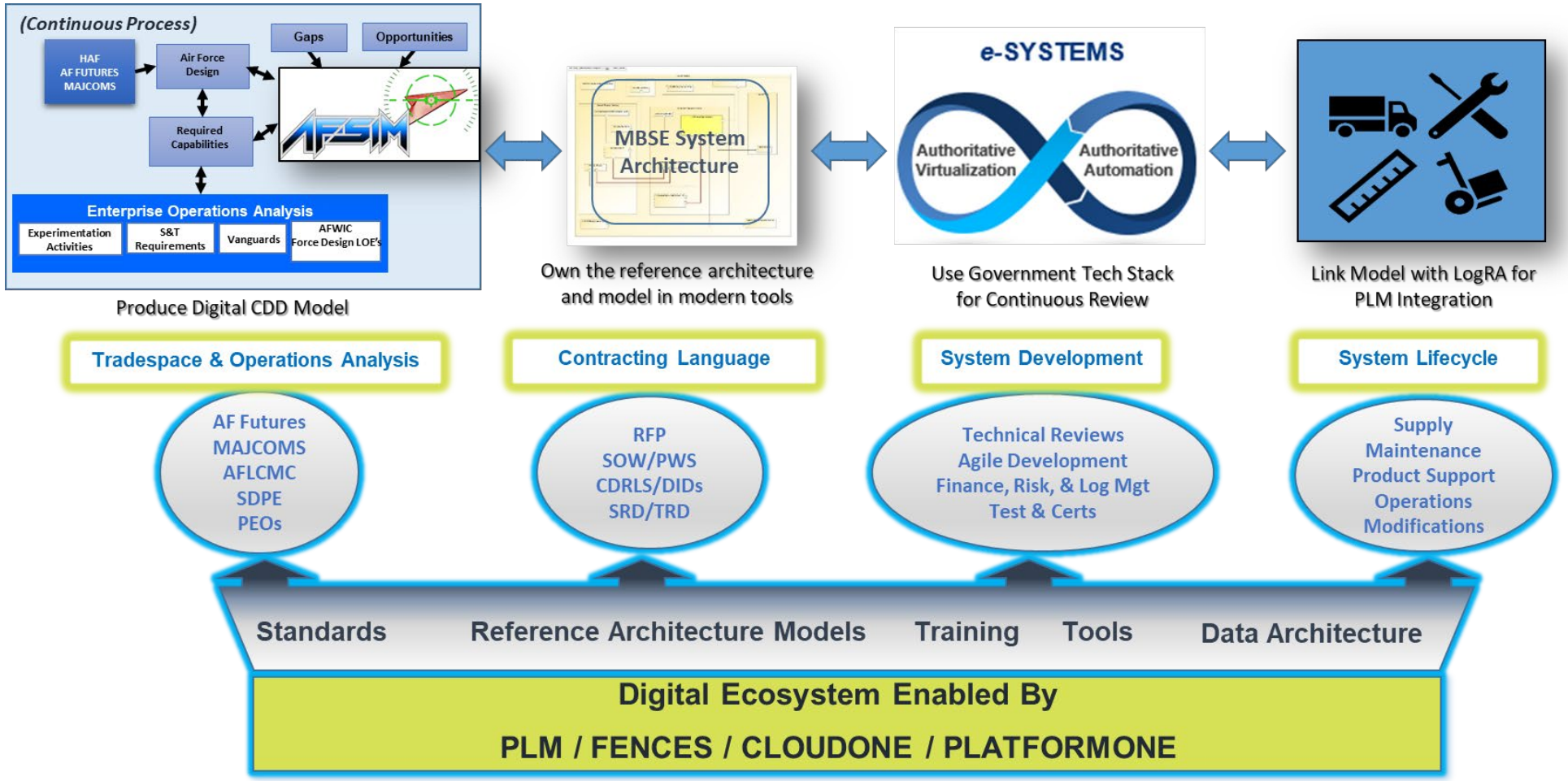
Chris Garrett, SL
Systems Engineering

DISTRIBUTION STATEMENT A. Approved for public release: AFLCMC-2022-0256. Distribution is unlimited.

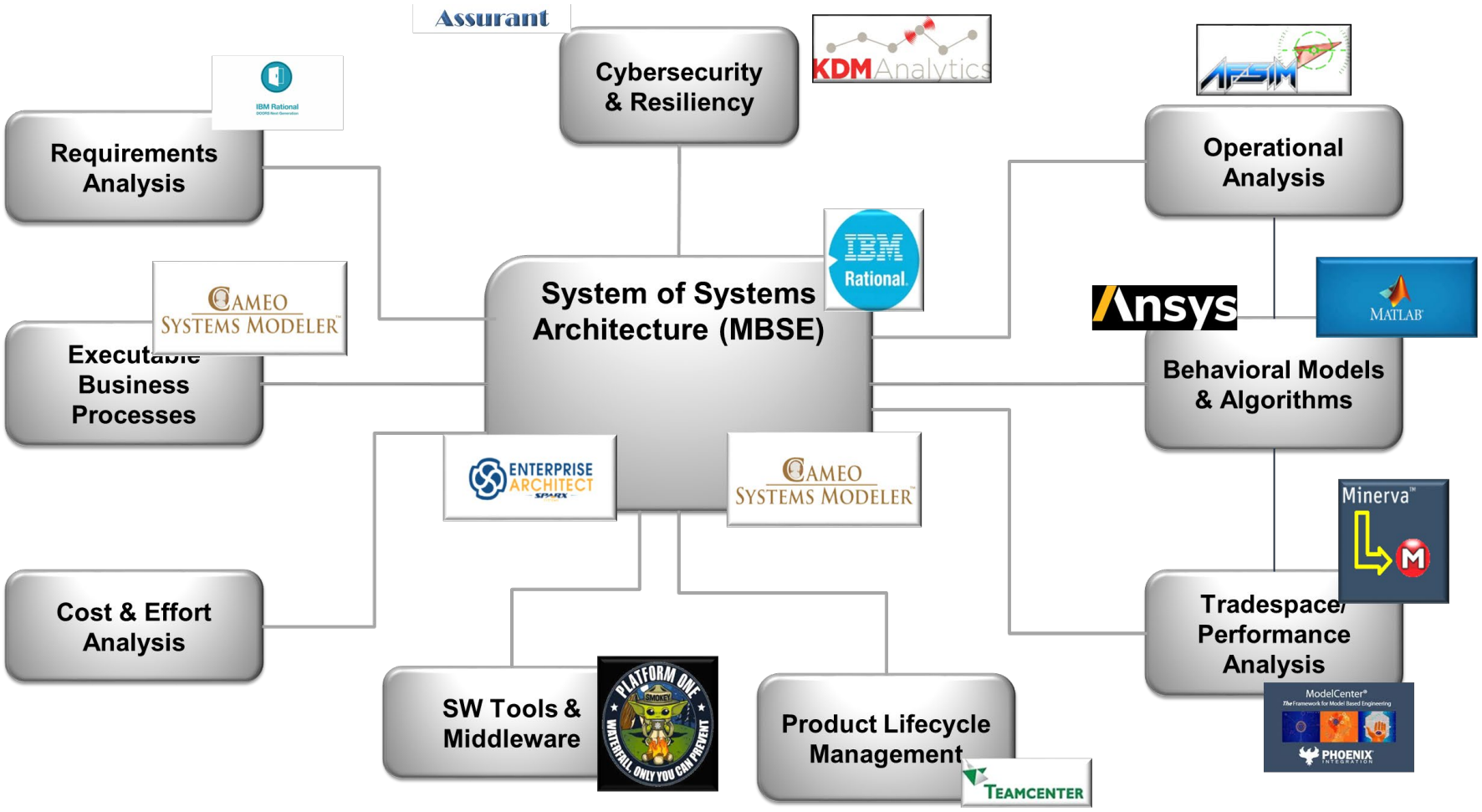
Overview

- BLUF:
  - System Model Configuration and Release Management is basically like Software Configuration and Release Management
- Key point is that Software Configuration Management (SCM) tools allow us to manage multiple configuration baselines

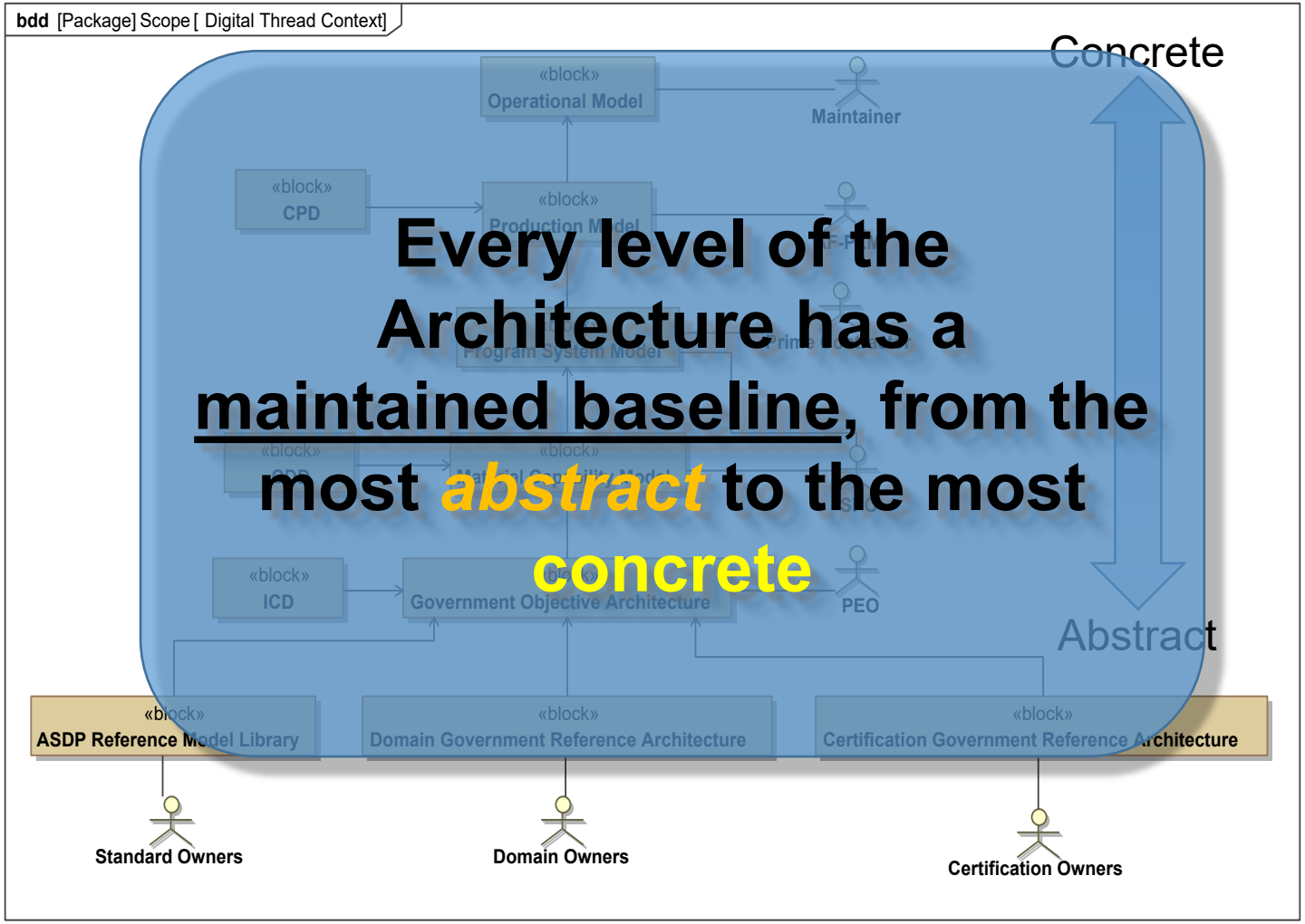
Digital Ecosystem



Architecture in Action!



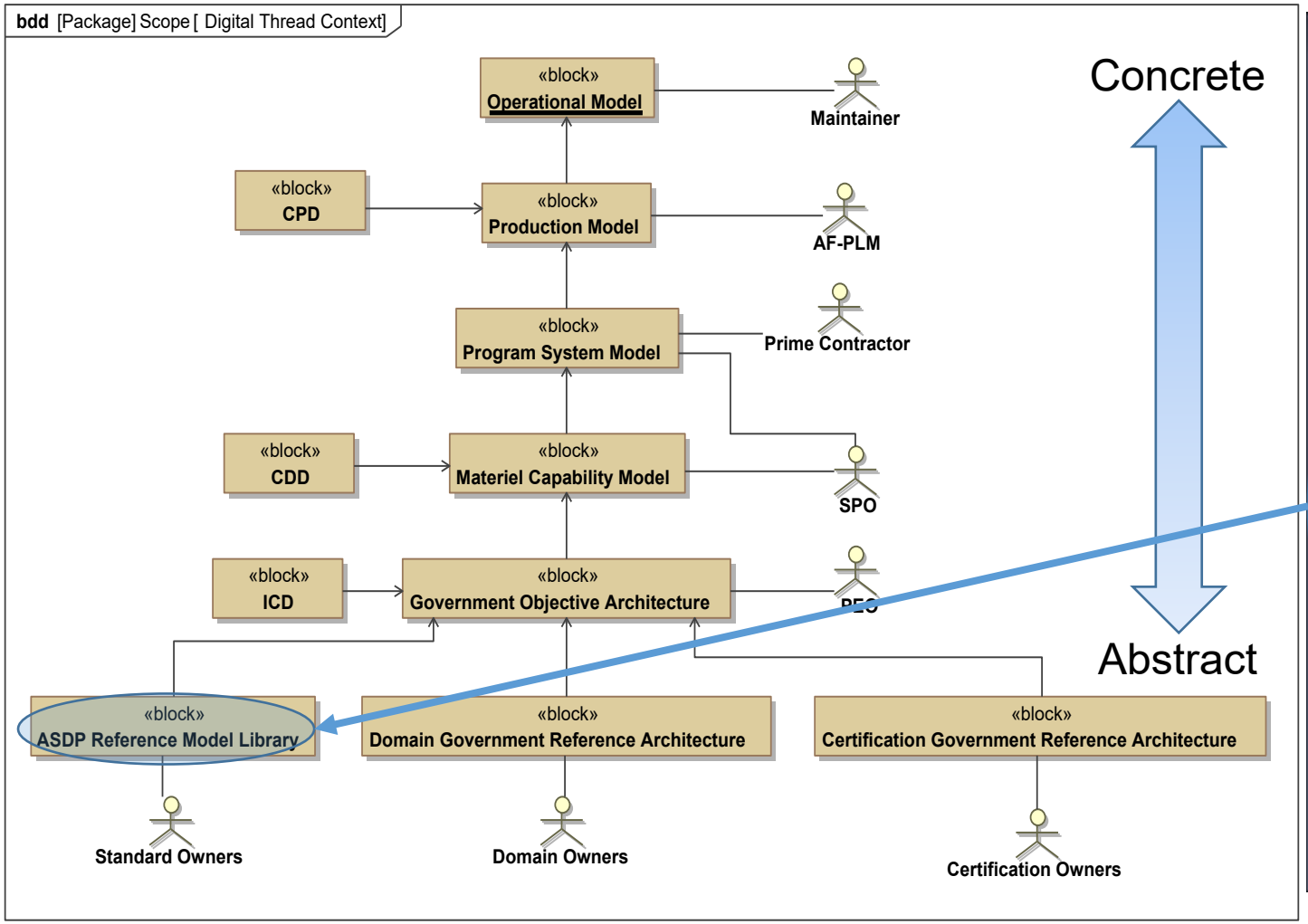
ASDP Future in the Digital Thread

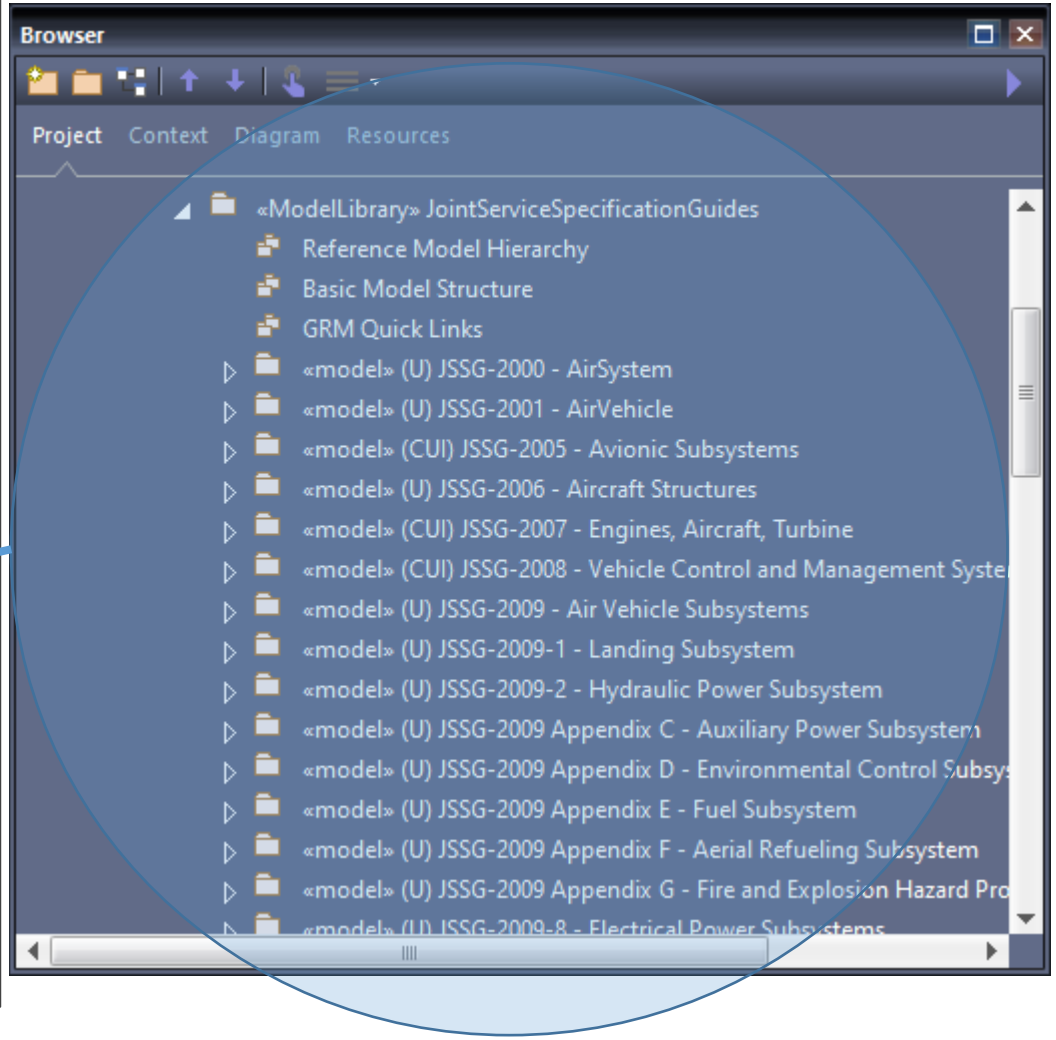


Baseline Configuration Considerations

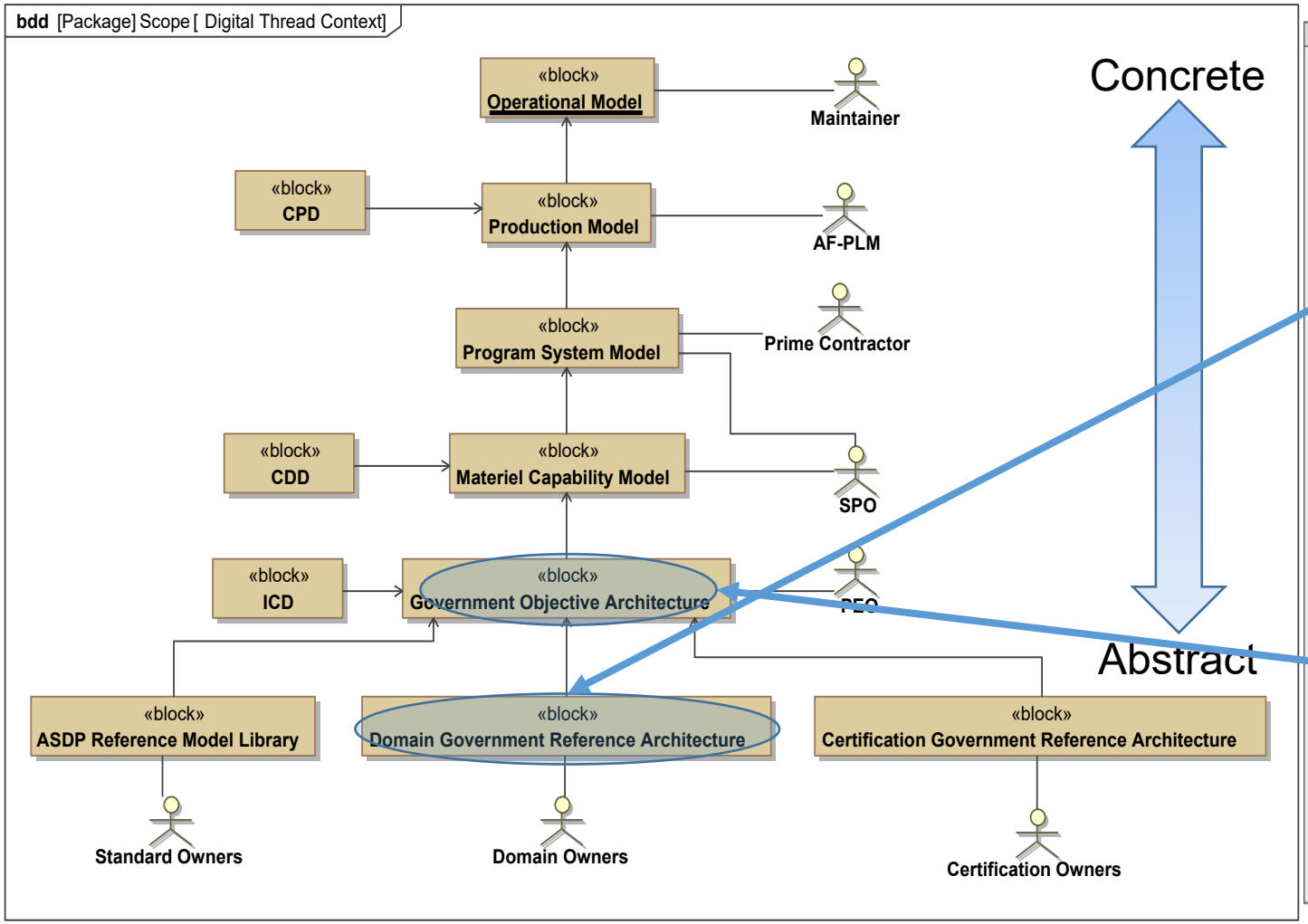
- Software attempts to merge to a single trunk release
  - Not always possible
  - Different targets need different feature sets from the trunk
    - Sometimes with modifications of the trunk that are never merged back
  - Results in multiple edition releases
- Theoretically, the only common aircraft baseline will be the abstract Air Vehicle model
  - Each level of the architecture has a release branch of its own
  - Each branch is managed separately as its own “trunk”
  - Changes to the more abstract trunk may drive changes to more concrete
- Every Air Vehicle will consist of library-based common system / subsystem elements (from the JSSGs), but pulls “Legos” from the library to define the whole
- Model libraries are separate baselines

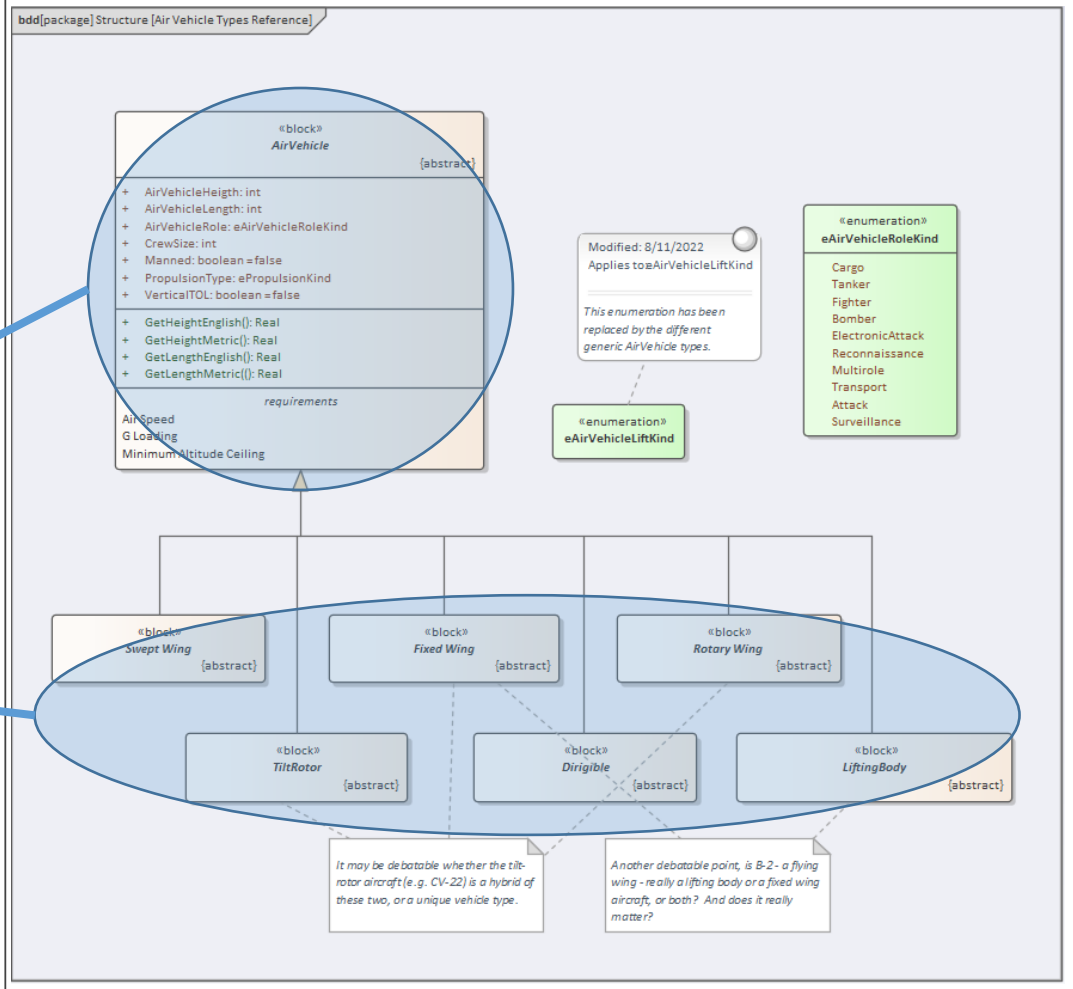
Abstract Models Managed per Level



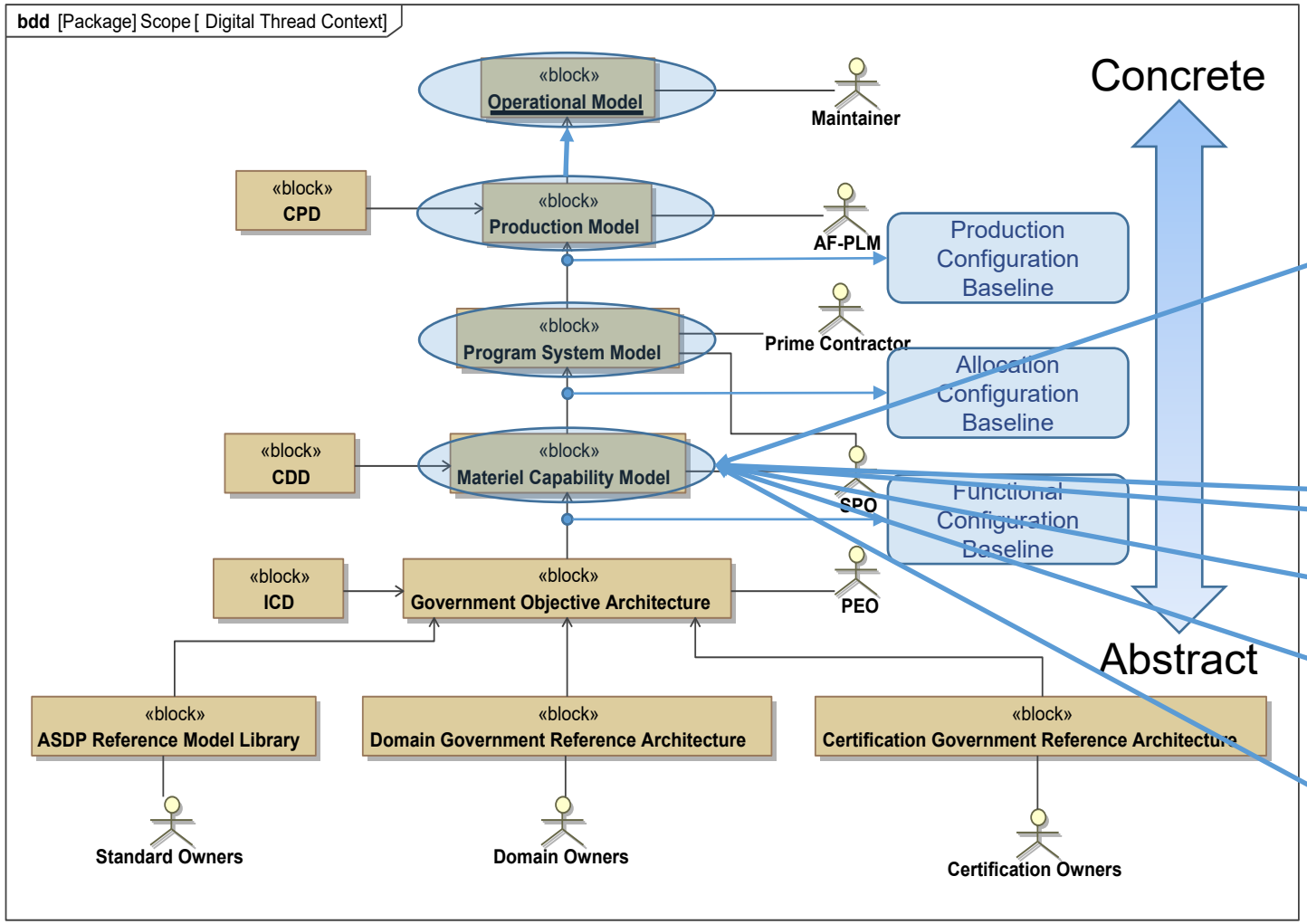


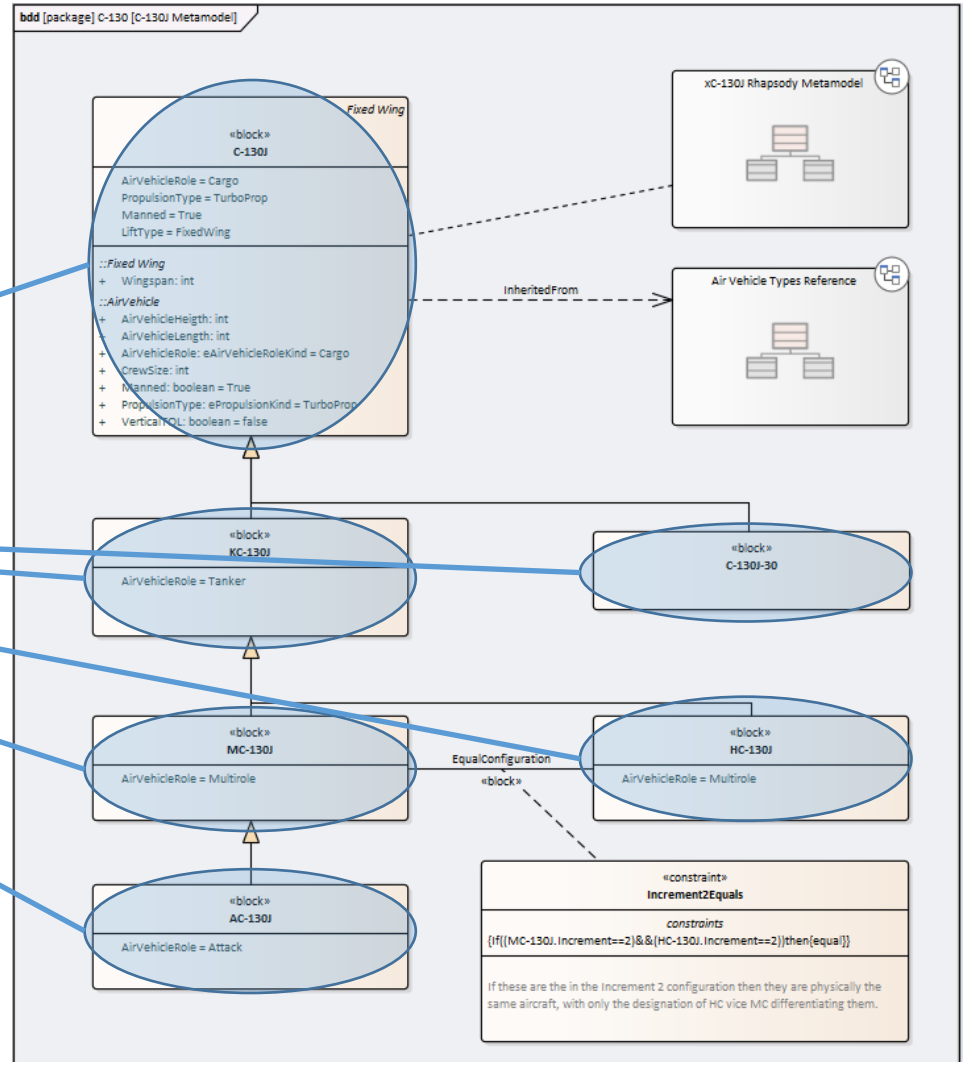
Abstract Models Managed per Level





Abstract Models Managed per Level





Summary

- **CM of MBSE Models basically equivalent to Software CM**
  - **Will be even more so with SysML v2.0**
- **Multiple levels of architecture CM is needed**
  - **Each level needs its own repository**
  - **Repositories need to be able to exchange model data**

Questions

AFLCMC… Providing the Warfighter's Edge

Changes in the Near-term Future

- SysML v2.0 is in review (with updates) for formal release
  - Target date may have slid into 2023/24
  - Based on a new language standard (not a UML profile)
    - Kernel Modeling Language (KerML)
    - KerML v1.0 is also in review for formal release
- SysML (and KerML) is text-based
  - Still has a graphical representation
  - Tools are expected to add text editing with graphical editing
- Model CM will be virtually identical to SCM
  - Both managed at the textual content level

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Systems Engineering Transformation in a Digital World

Mr. Allan Dianic

Director Software Engineering

Office of the Executive Director, Systems Engineering and Architecture

Office of the Under Secretary of Defense for Research and Engineering

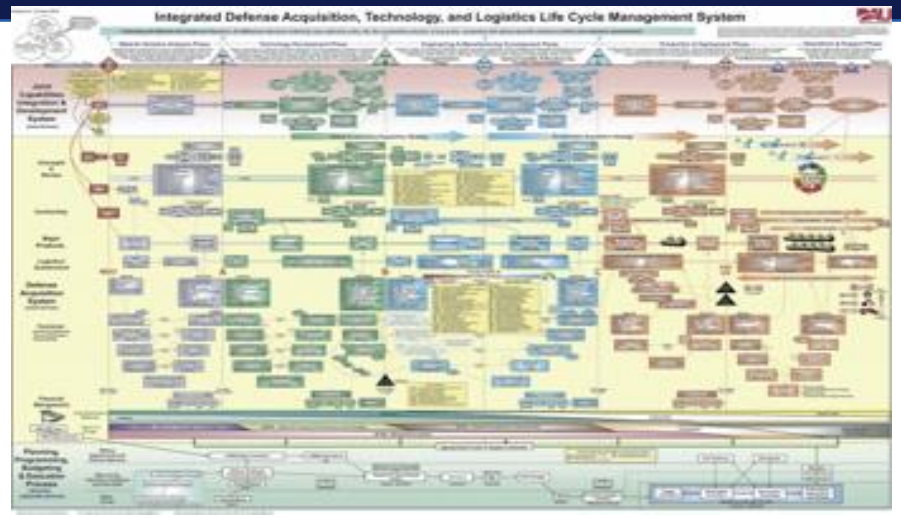
Distribution Statement A. Approved for public release. Distribution is unlimited.

As we strive to deliver capability faster …

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

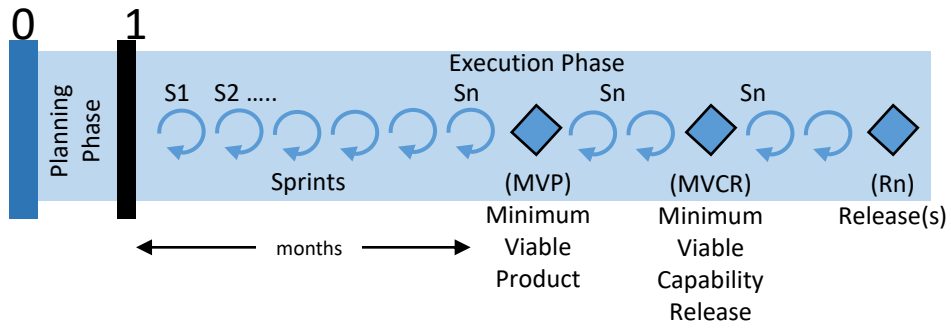
Software Engineering Is Changing

DoDI 5000.02 milestones, models, and documentation did not provide the proper structure for managing software development.



"Going forward, DoD should shift away from its traditional linear system development process and adopt a nimbler approach to iteratively design, test, and fix systems. ,"
-The Honorable Heidi Shyu, USD, R&E

The new way facilitates rapid and iterative development of software – systems engineering is still essential but must be more agile



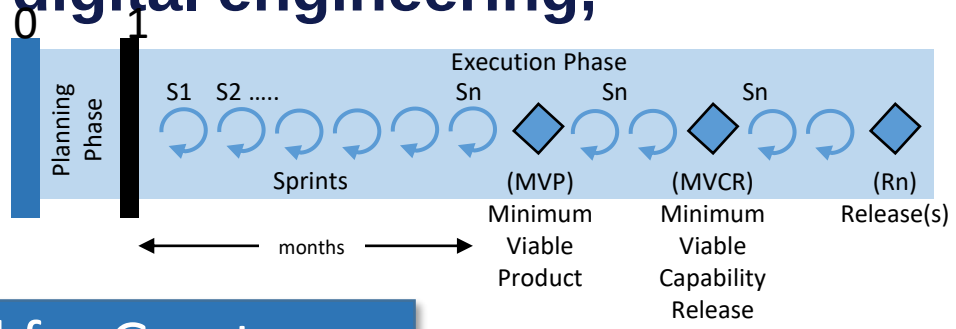
OLD WAY

NEW WAY

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

Why Rapid Iterative Approaches

- **Promise to field new capability faster**
- **Strategic guidance and directives from leadership**
- **Automated software development pipelines encourage iteration**
- **SWE technology advances** **Containerization, Micro Services, Zero Trust, Cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Continuous Integration Continuous Delivery (CI/CD)**
- **Artificial intelligence/machine learning, digital engineering, models and simulations**
- **Cybersecurity needs rapid adaptation**



Digital Engineering Needed for Greater Speed and Flexibility

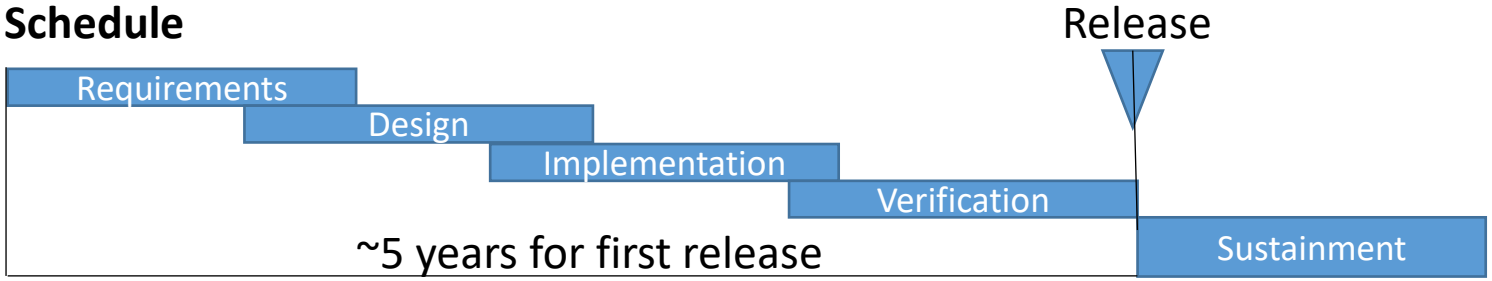
Distribution Statement A. Approved for public release. Distribution is unlimited.

Systems and Software Engineering – Legacy Approach

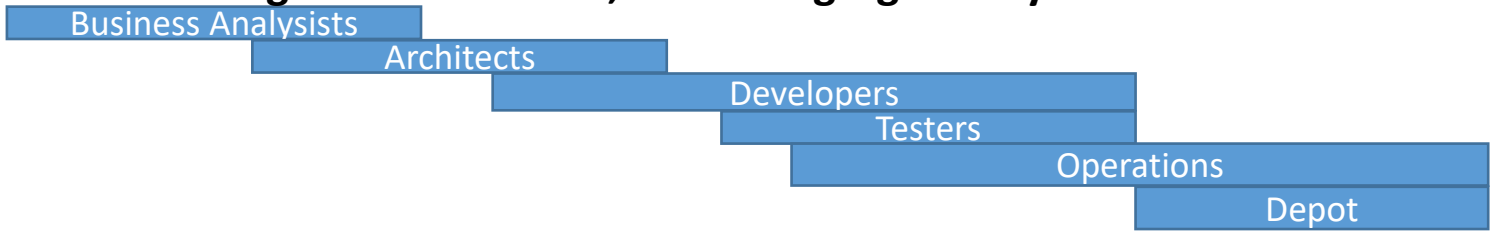
Waterfall

- **Inflexible requirements** –assumes detailed knowledge of needs 5 years in advance.
- Software processes **mimic manufacturing process**
- Schedule or funding short falls result in **technical debt.**
- Work conducted in **silos**
- **Late stage testing/security** scans
- Throw it over the wall mentality
- Delivery often doesn't meet user needs

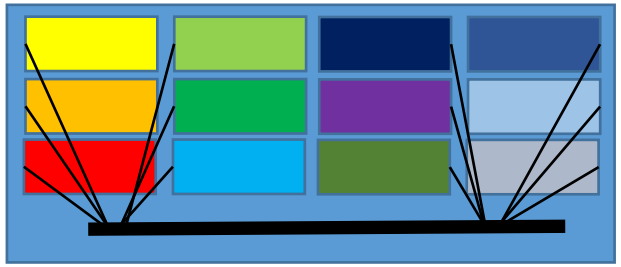
Schedule



Workforce Organization – Silos, Teams Segregated by Phase



Architectural Approach – Monolithic, Modular, n-Tier



- Highly complex
- Brittle
- Difficult to maintain

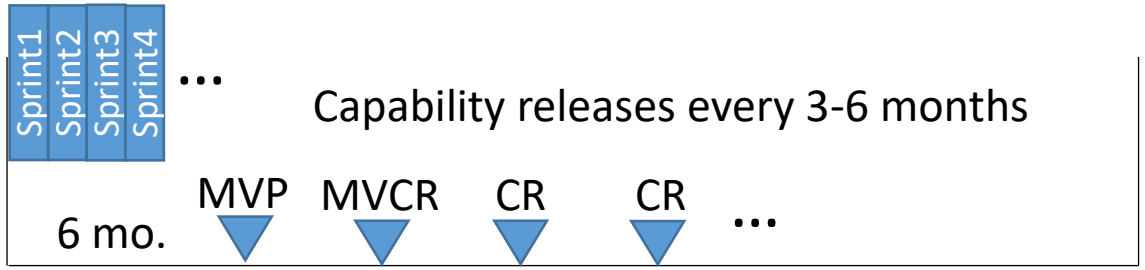
Distribution Statement A. Approved for public release. Distribution is unlimited.

Systems and Software Engineering – New Way

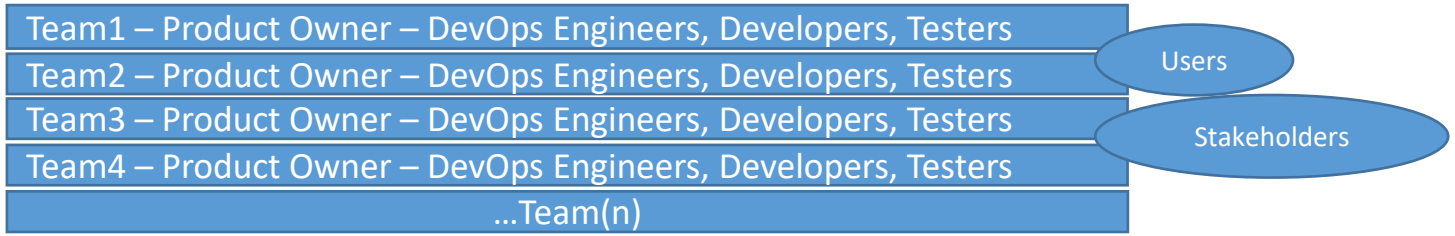
Digital Approach Supporting Agile Software

- Software is never done
- **MVP** within **6-12 months**
- **MVCR/CR** every **3-6 months**
- Cross Functional Teams
- Loose Coupling
- **Zero Trust**
- **Continuous ATO**
- **Continuous Sustainment**
- **Cloud-Native** Microservices
  - Scalability
  - Elasticity
  - Reliability
- **Evolutionary Architecture**

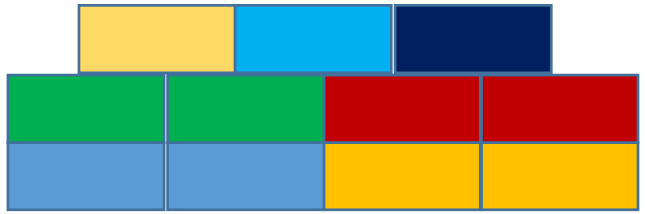
Schedule



Workforce Organization – Cross Functional Teams



Architectural Approach - Microservices



MVP = Minimum Viable Product
MVCR = Minimum Viable Capability Release
CR = Capability Release

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

Backup

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

New Realities and Digital Technology Advances Driving Change

	Old Way	Disadvantages	New Way	Advantages
Policy	Title 10 DoDI 5000.02	Regulatory Requirements Manufacturing Orientation	Adaptive Acq Framework DoDI 5000.87 SW Acq Pathway	Less Bureaucracy Capability Driven Commercial Best Practices Adopt Modern SWE Practices
Method	Document Centric Waterfall	Fixed Requirements Milestone Driven Months/Years Delivery Cycles	Curated Digital Models Continuous Delivery DevSecOps	Days/Weeks Delivery Cycles Rapid Feedback Collaborative Culture Responsive to Needs
Technology	Local Physical Servers	One offs (staff/sched/perf) Dedicated HW infrastructure Slow Tech Insertion Hard to Scale	Cloud Services Containers Microservices	Shared Infrastructure Simpler to Deploy Rapid Tech Insertion Easy to Scale
Security	Perimeter Security Static Trust	Systemic Fragility Poor support for mobile Privilege bound to location Assume secure perimeter	Zero Trust	Systemically Robust Natural Support for Mobile Privilege bound to identity Assume adversary present

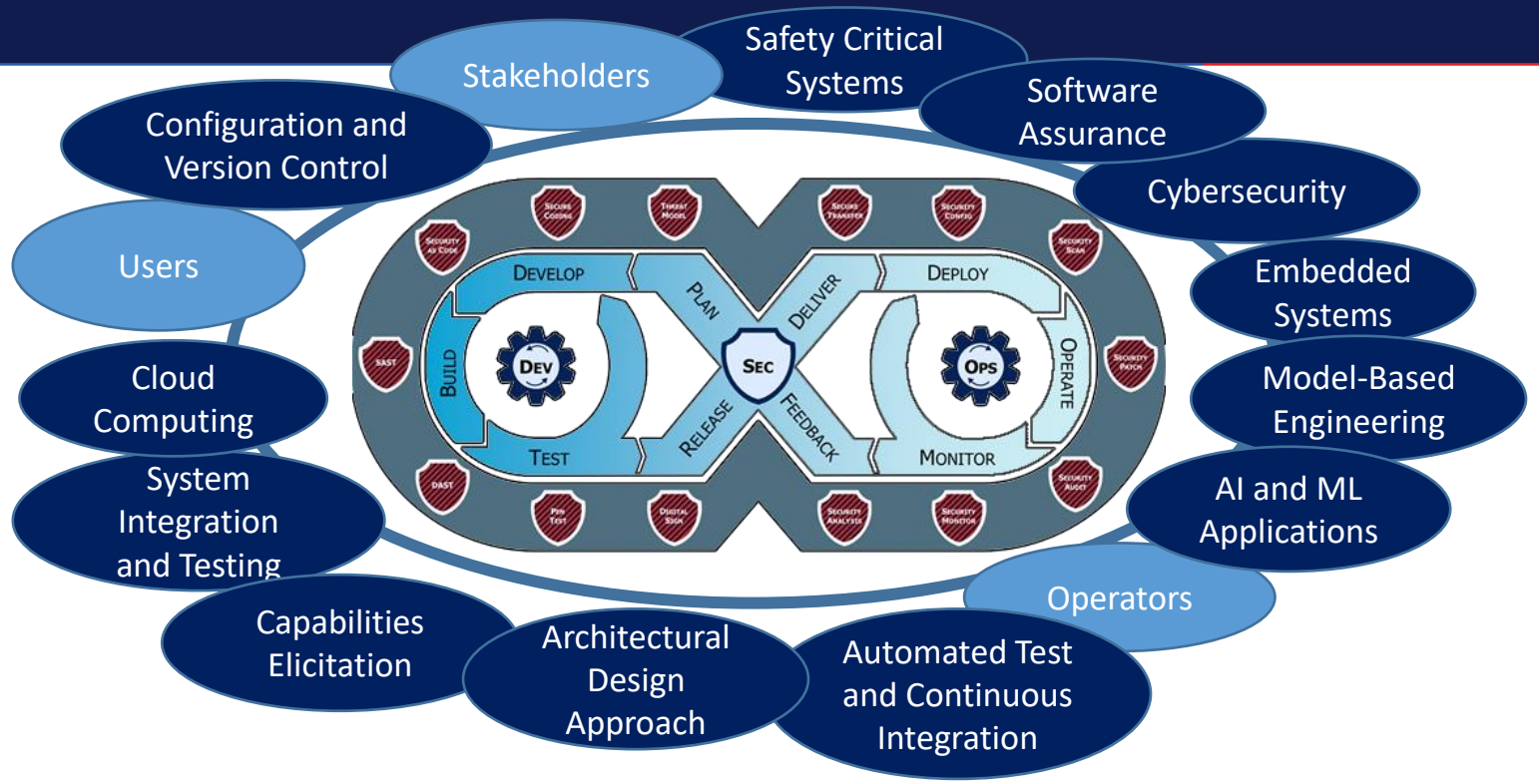
Distribution Statement A. Approved for public release. Distribution is unlimited.

DevSecOps Collaborative Culture and Shift Left Strategy Relies on Digital Engineering

People with specific competencies collaborate on the entirety of the pipeline

No competency is restricted to a single phase

Expertise captured and automated into the pipeline whenever possible



Software Competency as defined by R&E sponsored software initiative

https://www.rand.org/pubs/research_reports/RR3145.html

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

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Data Centricity: Multi-Directional Flow of Specialty Engineering Data Throughout the Life Cycle

Mr. R. Chris DeLuca

Director Specialty Engineering

Office of the Executive Director, Systems Engineering and Architecture

Office of the Under Secretary of Defense for Research and Engineering

Distribution Statement A. Approved for public release. DOPSR # 23-S-0003. Distribution is unlimited.

DoD Is a Data-Centric Organization

David L. Norquist, Deputy Secretary of Defense
2020

- **"Unleashing data to advance the National Defense Strategy"**
- **Guiding Principle #5: Enterprise-Wide Data Access and Availability "DoD data must be made available for use by all authorized individuals and non-person entities through appropriate mechanism."**
- **"Data underpins digital modernization and is increasingly the fuel of every DoD process, algorithm, and weapon system."**

"We have a very large AI challenge ahead of us but in order to do this, we have to get the data right"

Craig Martell, Pentagon CDAO, 2022 Intelligence & National Security Summit (C4ISRNET September 15)

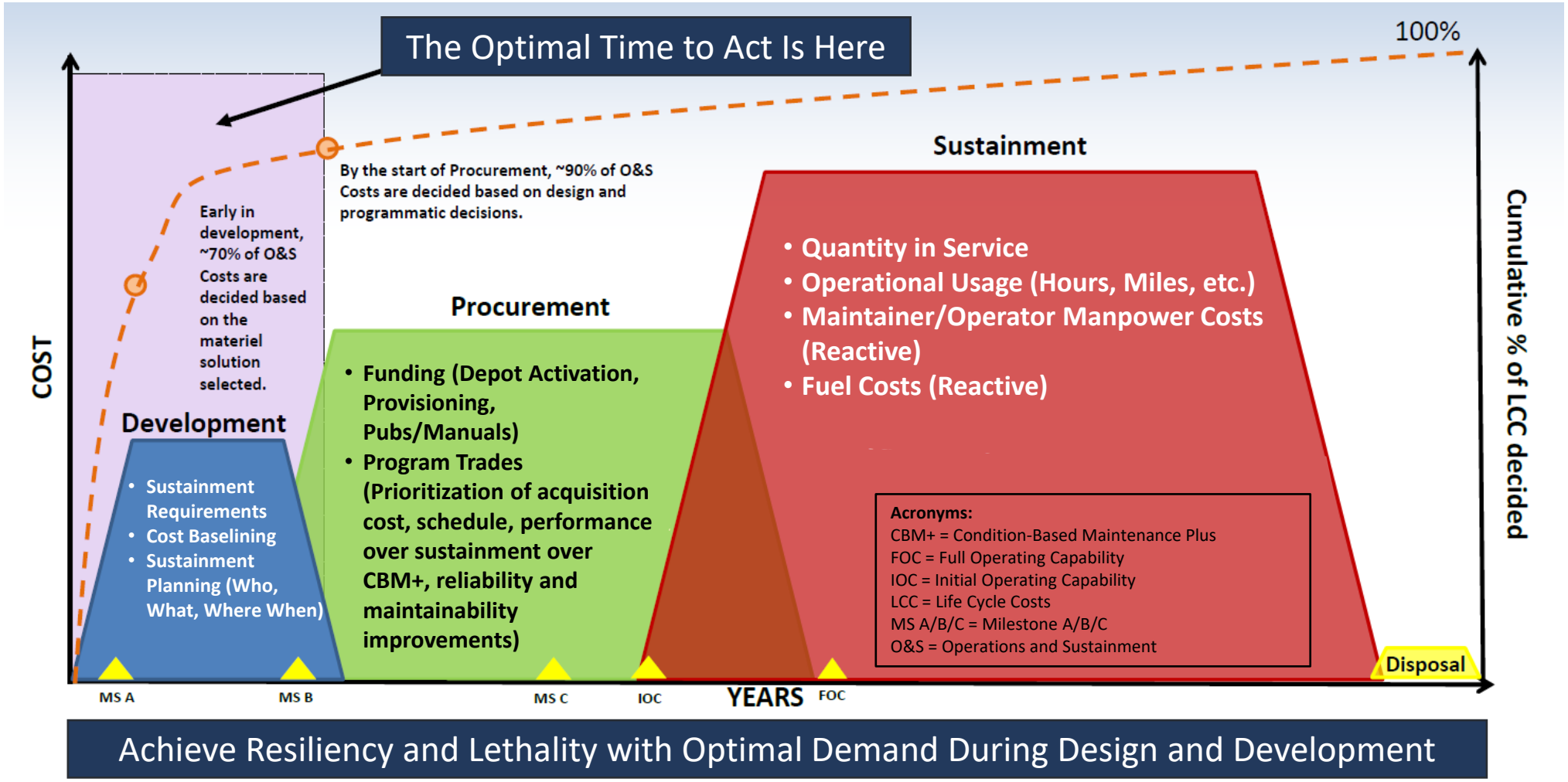
Distribution Statement A. Approved for public release. Distribution is unlimited.

Increasing Complexity and Challenges

Source: 2022 PSM Workshop, RDML Dion English, SC, USN

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

“Bake In” Data During System Design



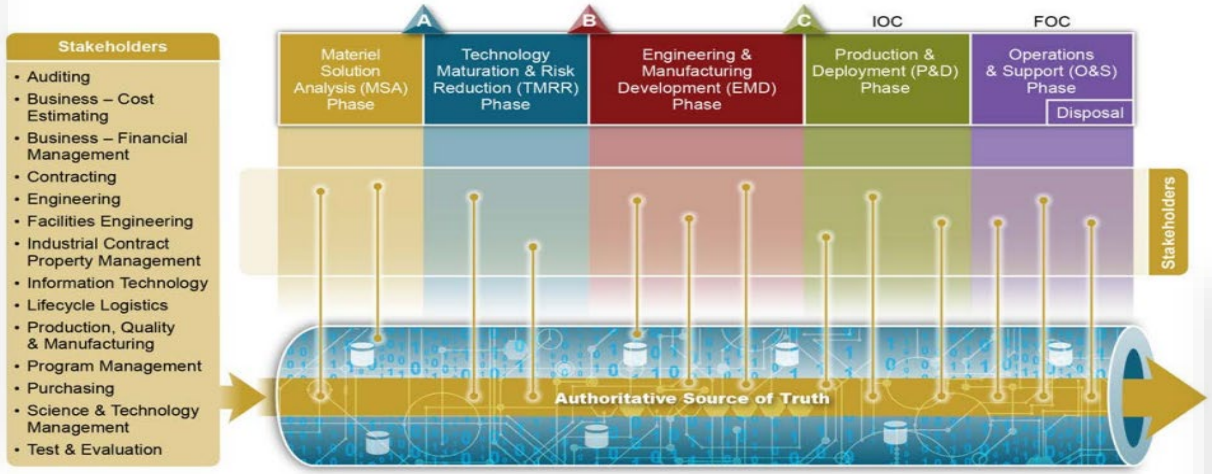
Achieve Resiliency and Lethality with Optimal Demand During Design and Development

Source: 2022 PSM Workshop, Principal Deputy Assistant Secretary of Defense (Sustainment)

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

Lesson Learned: Ecosystem Needed

U.S. Air Force photo by Jill Pickett
HIGH MACH, Vol 67, No 12



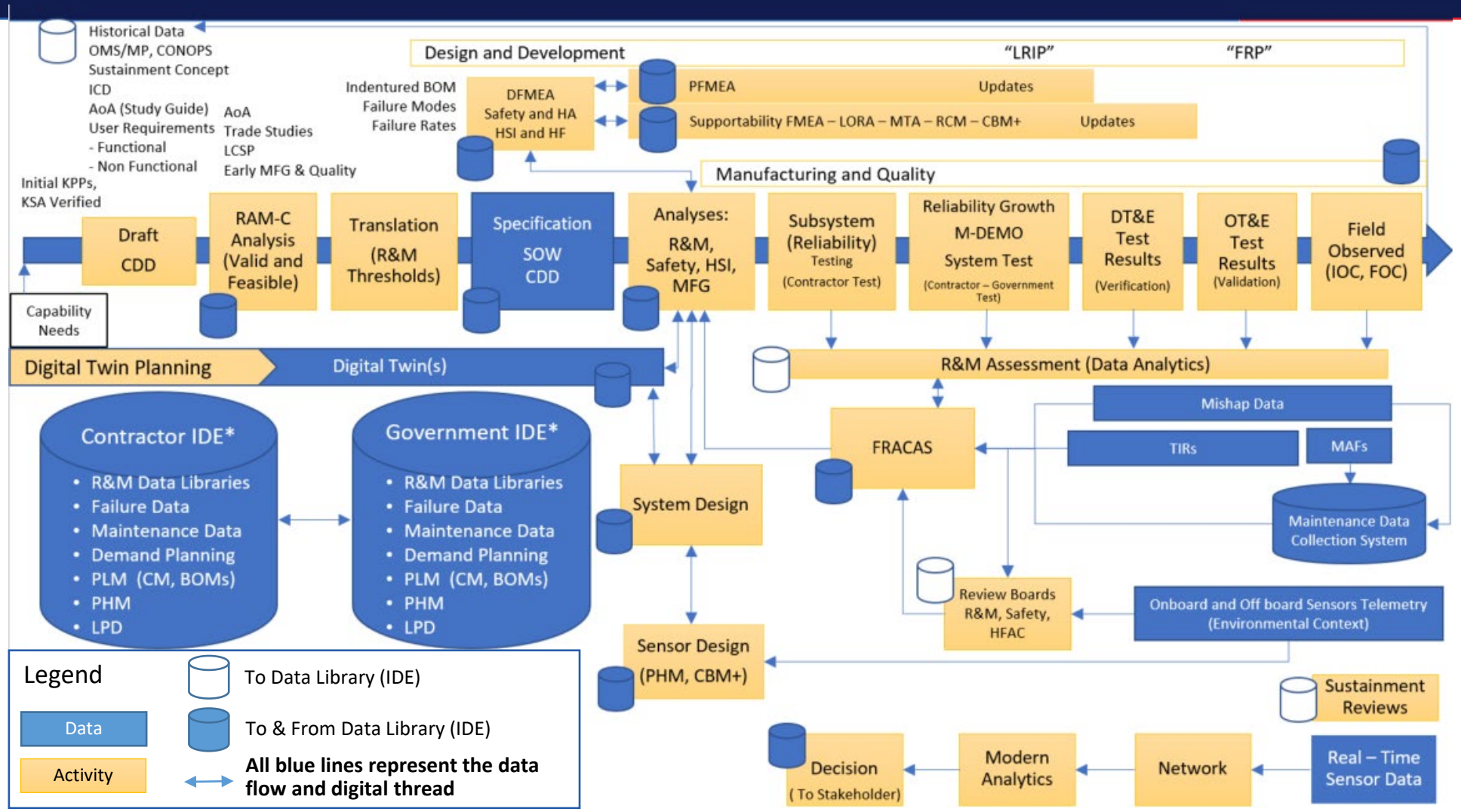
Authoritative Source of Truth, Digital Engineering Strategy

Photo By: Army Spc. Kayla Anstey, "Digital Transformation, AI Important in Keeping Battlefield Edge" June 9, 2022
960cyber.afrc.af.mil/News

"Warfighters at all echelons require tested, secure, seamless access to data across networks, supporting infrastructure, and weapon systems out to the tactical edge"
DoD Data Strategy, 2020

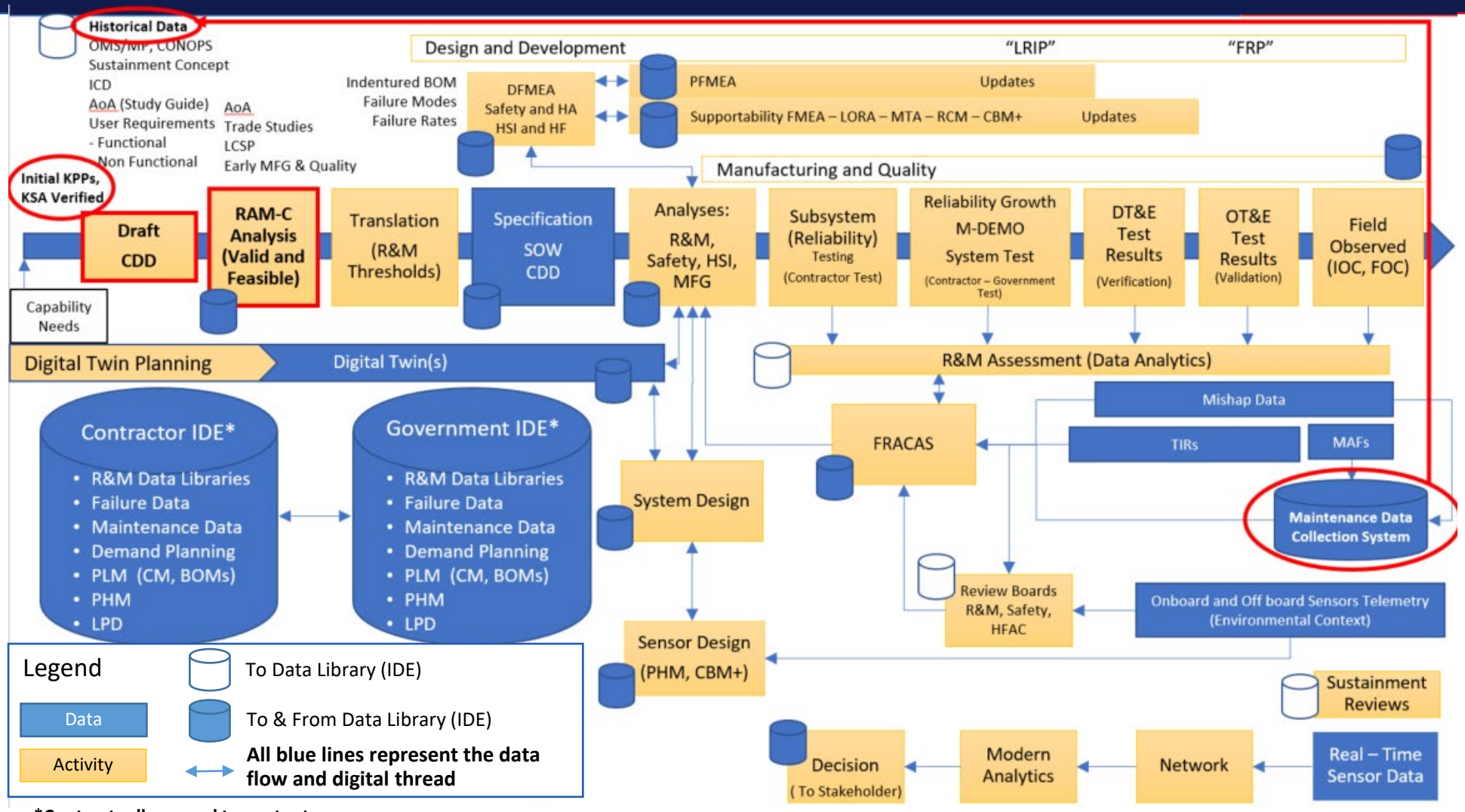
Distribution Statement A. Approved for public release. Distribution is unlimited.

Engineering Data in a DE Ecosystem



***Contractually agreed to content, views, access, and delivery of data.**

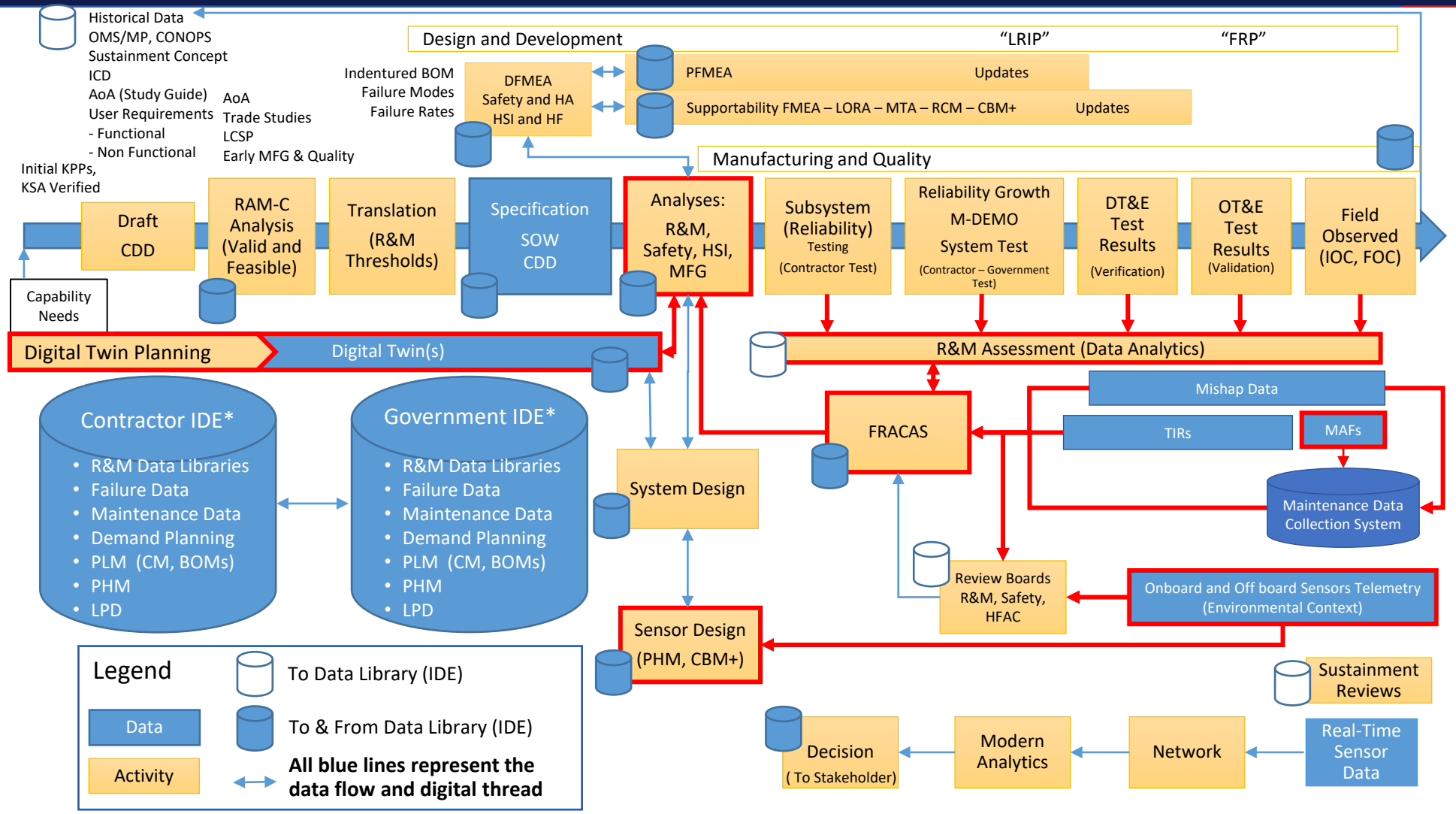
Early Application in Engineering Data



***Contractually agreed to content, views, access, and delivery of data.**

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

Failure Reporting Analysis and Corrective Action System (FRACAS) Feedback to the Digital Twin



***Contractually agreed to content, views, access, and delivery of data.**

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

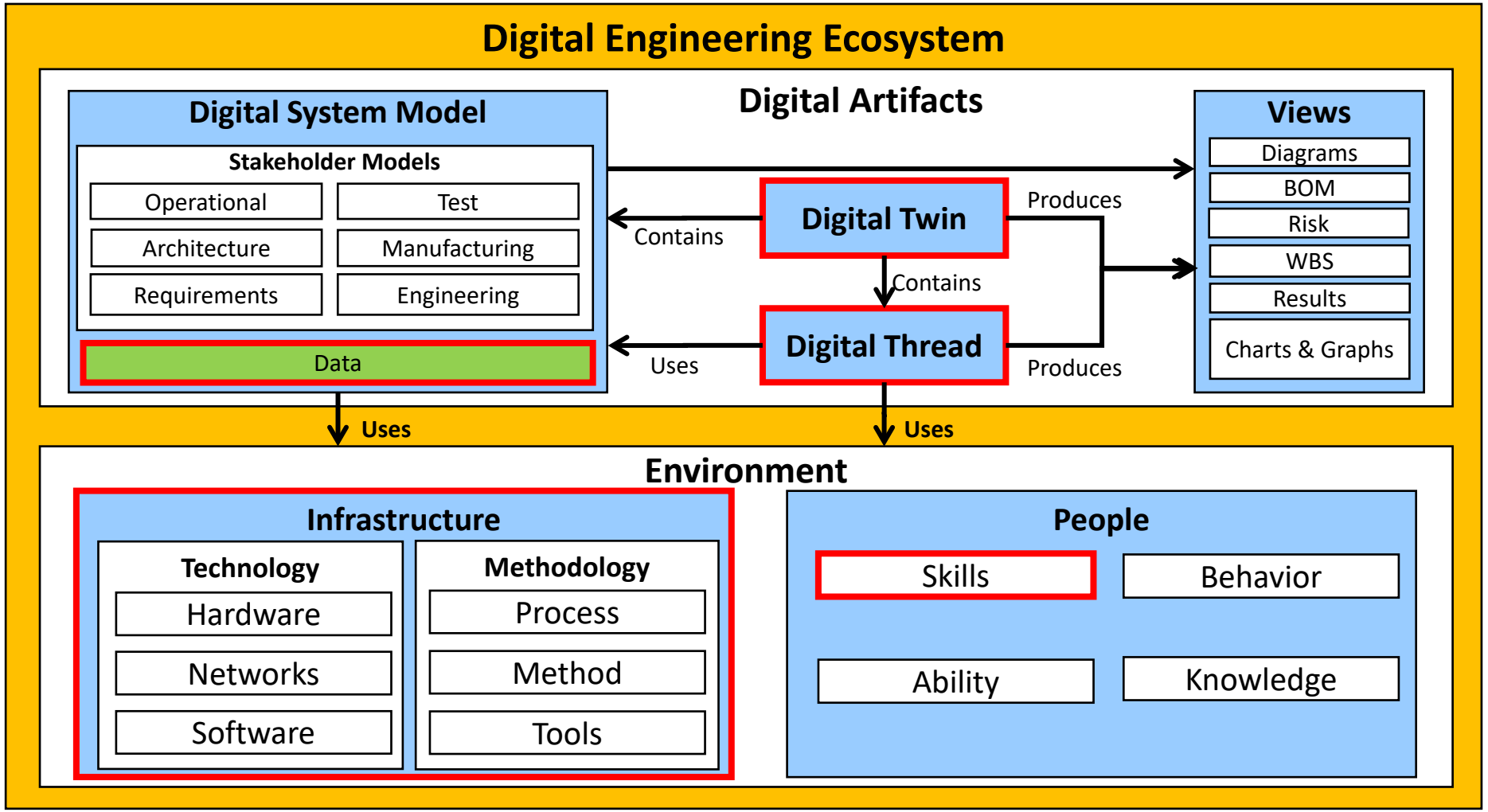
Digital Engineering Ecosystem

Infrastructure includes:

- Compute & Storage
- HVAC
- DevSecOps Tools
- AI/ML/DT Tools
- Simulation Tools
- MLS/CDS Security
- Authority to Operate
- Budget

Skill sets include:

- IT, OT, PIT
- Information Assurance
- Data Engineers & Scientists
- System Admins
- High Performance Compute
- SW Developers
- Scrum Masters
- Security ISSO
- System Engineers
- HW Designers
- Specialty Engineers
- Budget



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

Its All About the Data – Enhanced by AI

Photo By: Army Spc. Kayla Anstey, “Digital Transformation, AI Important in Keeping Battlefield Edge” June 9, 2022 960cyber.afrc.af.mil/News

… AI, Machine Learning, NLP … to be continued

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

Contact

Office of the Under Secretary of Defense for Research and Engineering
osd.r-e.comm@mail.mil | Attn: Specialty Engineering
https://www.cto.mil

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

USD(R&E)

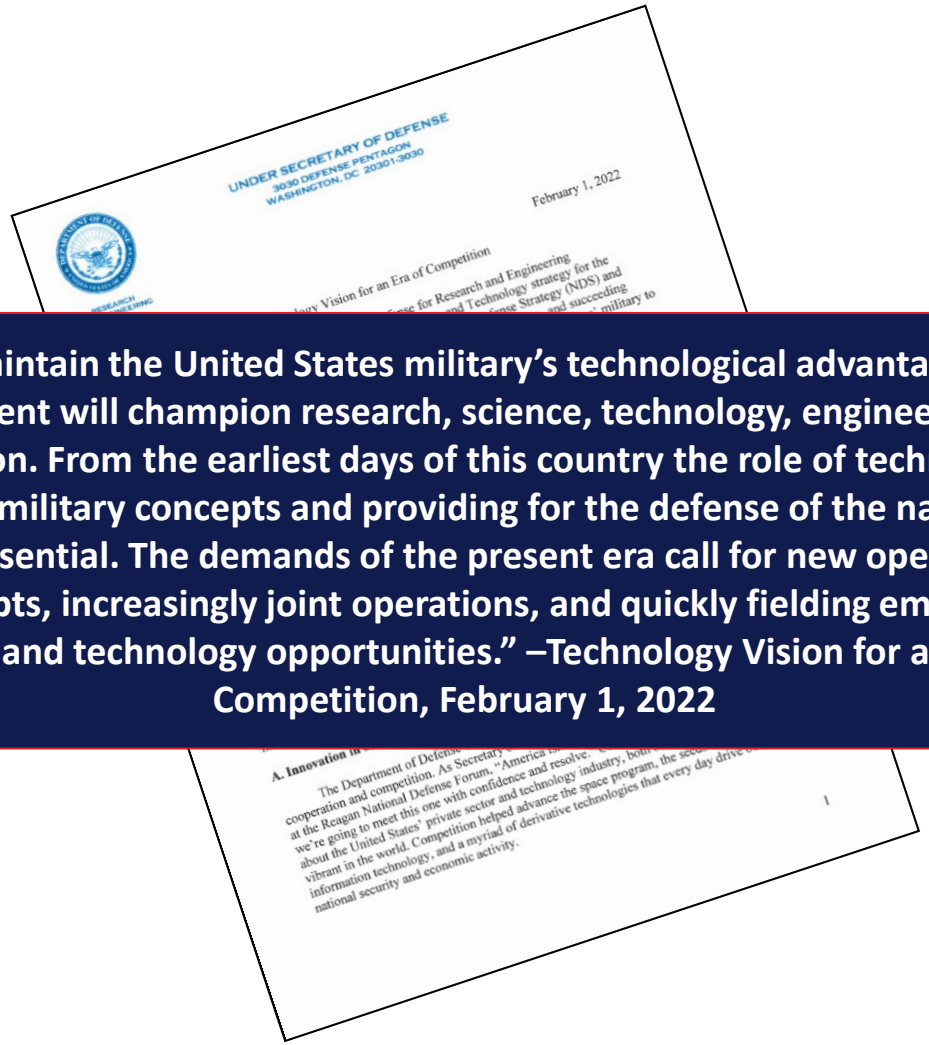
Program Protection and Secure Cyber Resilient Engineering Initiatives

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for
Research and Engineering
Science and Technology Program Protection

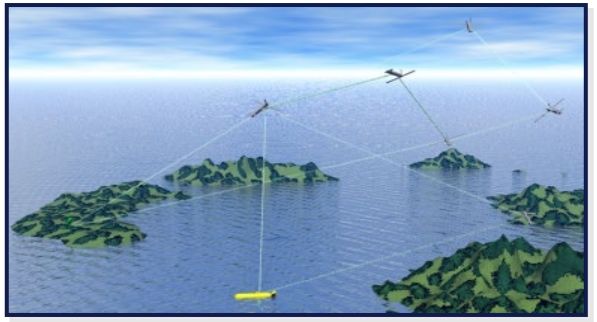
Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

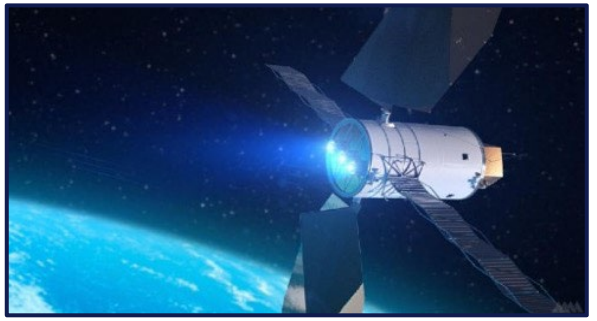
Our Mission


UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

February 1, 2022

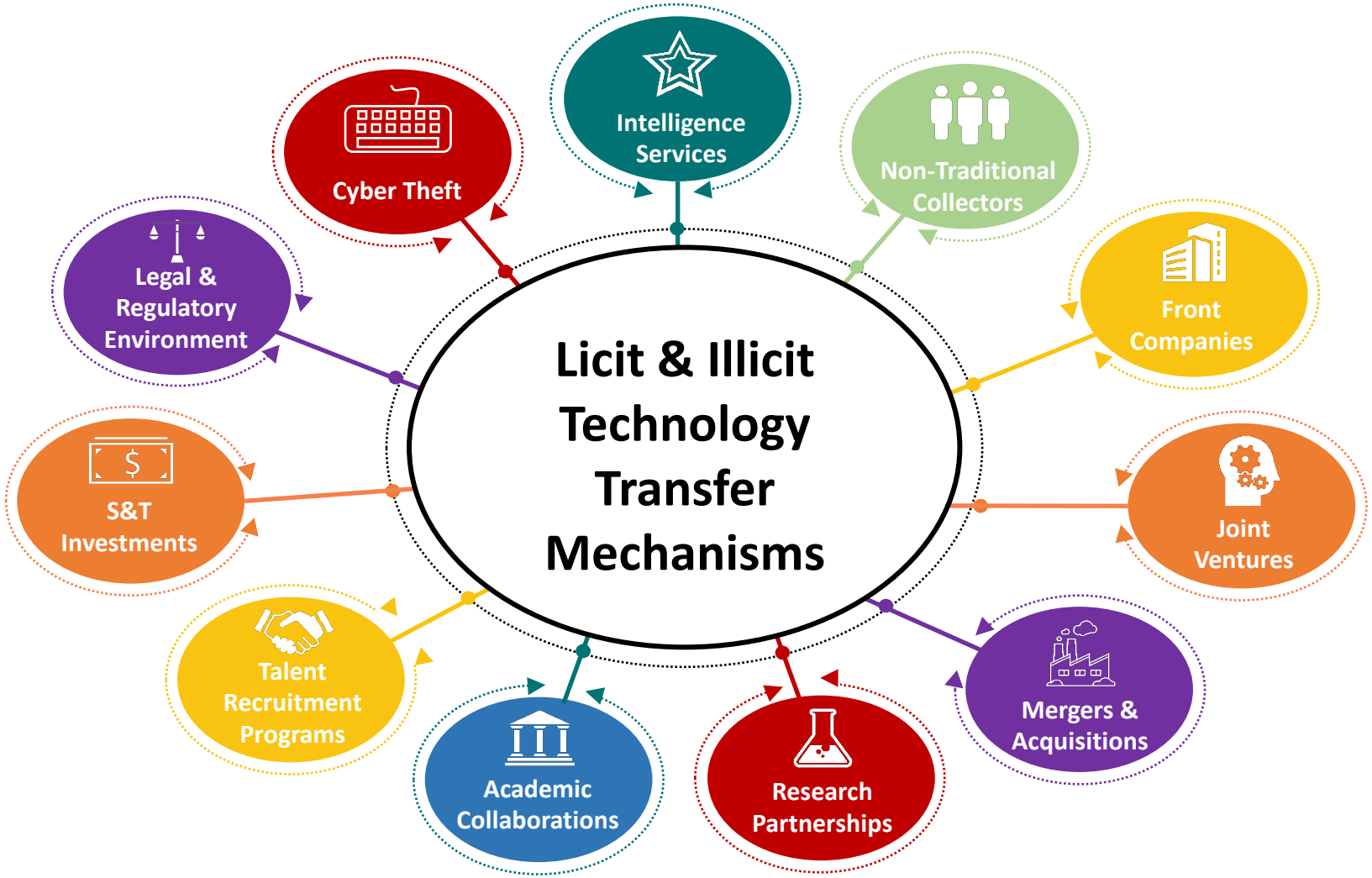
"To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities." –Technology Vision for an Era of Competition, February 1, 2022





Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Threats to Our Mission



Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Technology and Program Protection Planning Across the Lifecycle

Critical Technology Areas

- Advanced Computing and Software
- Advanced Materials
- Integrated Sensing and Cyber
- Integrated Network Systems-of-Systems
- Trusted AI and Autonomy
- Biotechnology
- Future Generation Wireless Technology (FutureG)
- Directed Energy
- Human-Machine Interfaces
- Hypersonics
- Quantum Science
- Renewable Energy Generation and Storage
- Microelectronics
- Space Technology

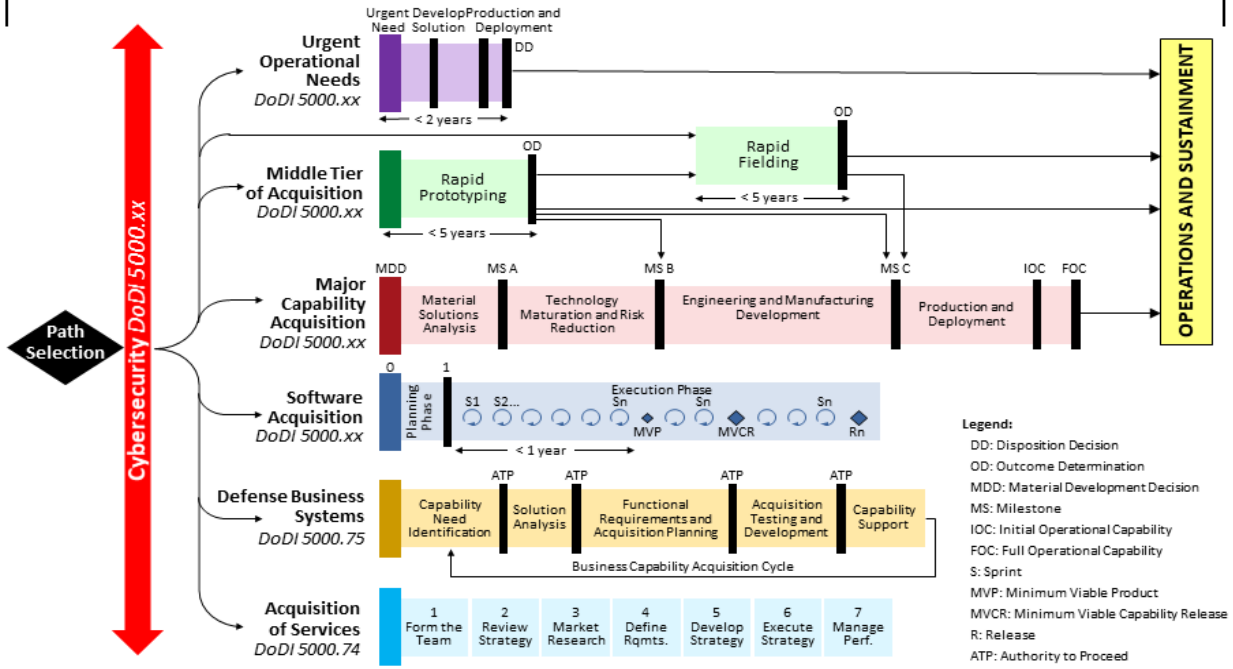
Adaptive Acquisition Framework

Enable Execution at the Speed of Relevance

Tenets of the Defense Acquisition System

1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Data Driven Analysis
5. Active Risk Management
6. Emphasize Sustainment

DoDD 5000.01: *The Defense Acquisition System*
DoDI 5000.02: *Operation of the Adaptive Acquisition Framework*



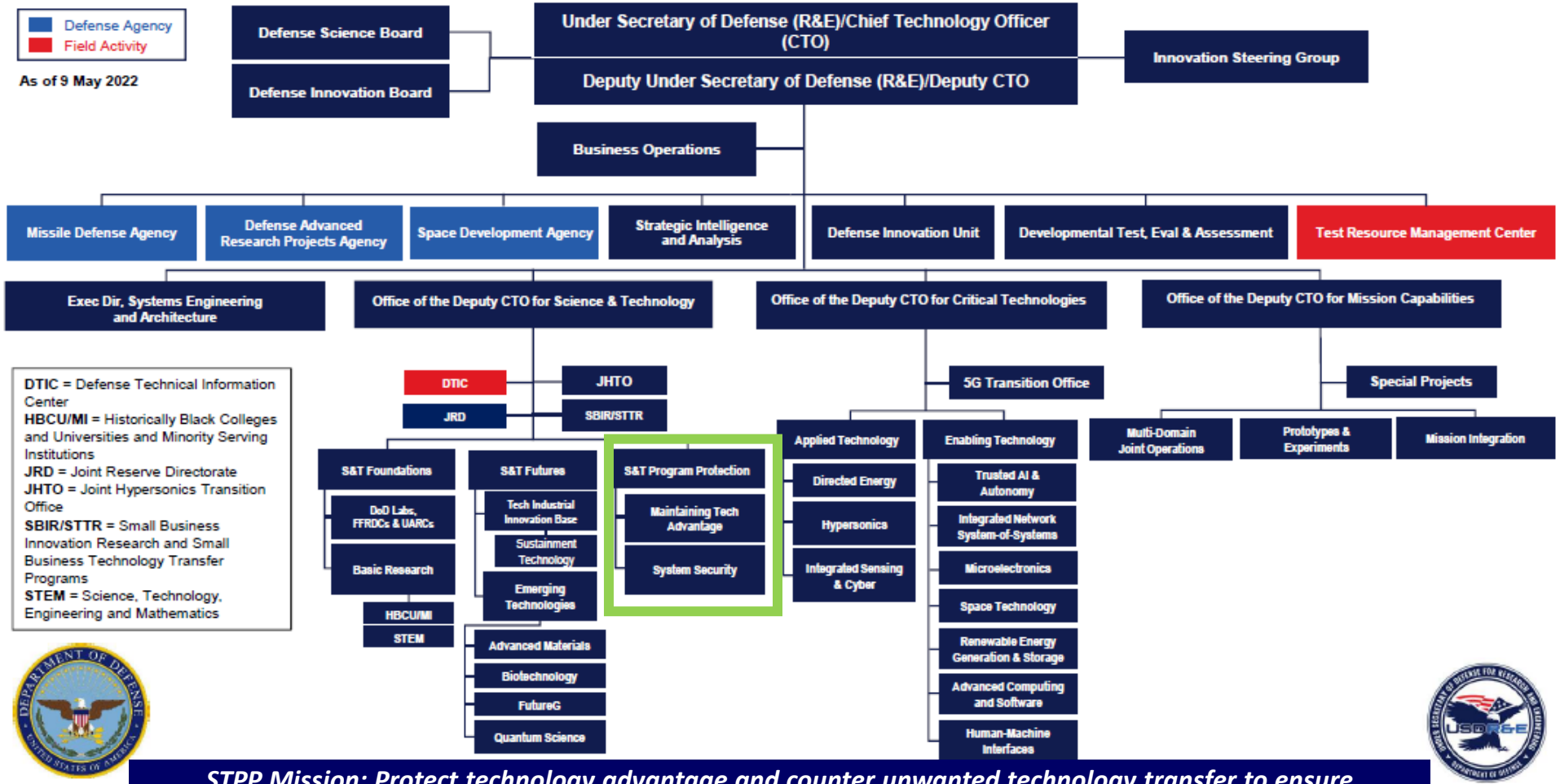
S&T Protection

Program Protection

Technology Area Protection Plans for DoD Critical Technology Areas

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Office of the Under Secretary of Defense for Research and Engineering Organization



STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through assured, secure and resilient systems and a healthy viable national security innovation base

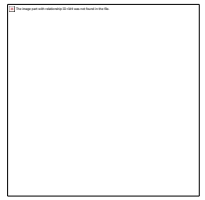
Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Systems Security Mission and Priorities

The Challenge

Problem: Adversary threats are outpacing policies and practices for engineering weapon systems; requires knowledgeable S&T and engineering workforce to provide dependably safe, secure, and resilient systems to operations at speed and scale

- **Advance policy and guidance to balance technology and program protection that enables rapid delivery of warfighter capability**
- **Strengthen System Security/Secure Cyber Resilient Engineering workforce through innovative education and training methods**
- **Advance Technology and Program Protection methods to ensure technological superiority**
- **Advance the practice of Trust and Assurance through Joint Federated Assurance Center**



Lead Policy :

- DoDI 5000.83, DoDI 5200.44, DoDD 5200.47E

Guidance:

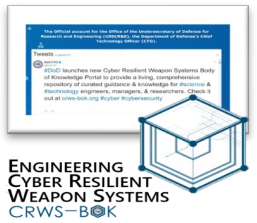
- Program Protection Planning
- Information Communications Technology Supply Chain
- Secure Software Supply Chain
- Software Assurance
- Controlled Technical Information
- Hardware Assurance
- Anti Tamper

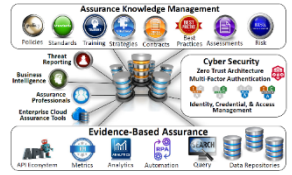
Standardization:

- Secure Cyber Resilient Engineering

Competency:

- System Security Engineering
- Secure Cyber Resilient Engineering





Joint Federated Assurance Center (JFAC)

Systems Security Mission: Foster Assured, Secure, Resilient Innovation, Missions, Systems and Components

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Systems Security Directorate

Responsibilities:

Program Protection
Secure Cyber Resilient Engineering

- DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*
- Program Protection Plan
- Program Protection/cyber technical risk assessments
- Secure Cyber Resilient Engineering (SCRE) methods, and workforce
- SCRE Standards Area

- DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting*

Systems Security Policy, Guidance and Standards

ICT SCRM
Anti Tamper
Hardware Assurance

- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*
- DoDD 5200.47E, *Anti Tamper*
- Information Communications Technology Supply Chain Risk Management
- Critical program information identification
- Hardware Assurance

- DFARS 252.239-7018 *Supply Chain Risk*

System Security Engineering/Anti Tamper

ICT SCRM
Software Assurance
Secure Software Supply Chain

- Joint Federated Assurance Center Modernization
- Provides Federated Software Assurance tools, processes and expertise
- Partners with Military service leads to transition innovative Software Assurance Tools for use across the Department

Joint Federated Assurance Center/Software Assurance

- Software Assurance Roadmap
- Innovative S&T software assurance mitigation and resilience needs
- Software Assurance mitigations
- Software Assurance mitigation approaches

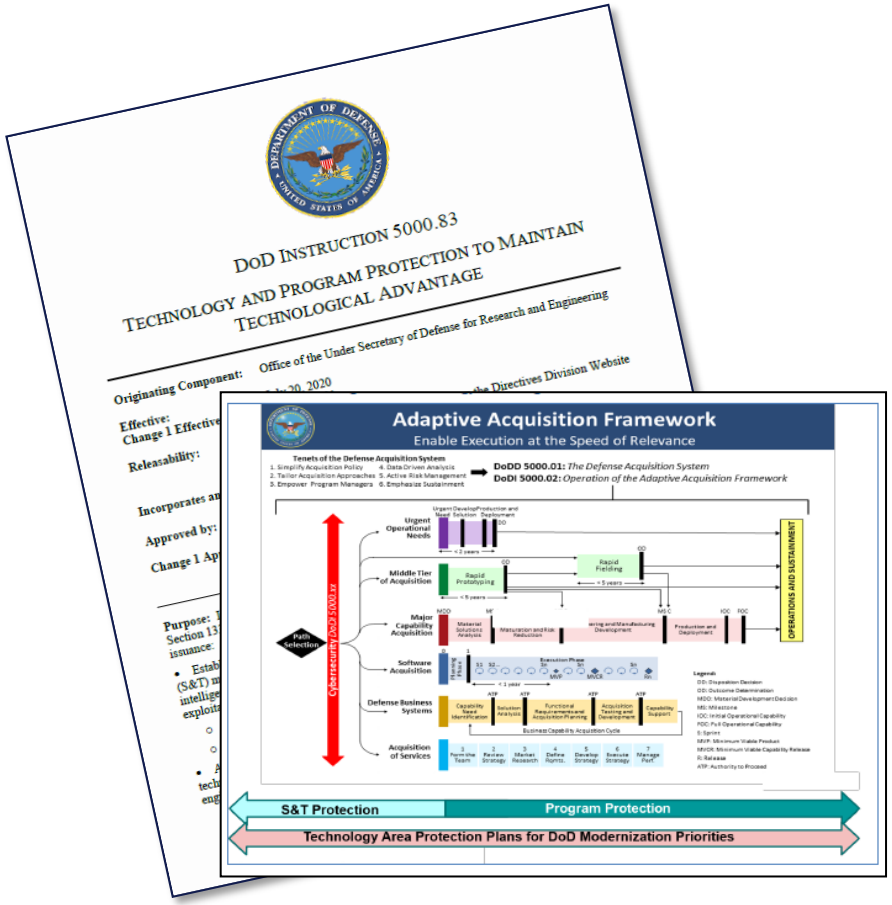
- EO 14028 Improving the Nations' Cybersecurity-Secure Software Supply Chain and Software Bill of Materials

Software Assurance Technical Lead

MISSION: Foster Assured, Secure, Resilient Missions, Systems and Components

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

DoDI 5000.83: Technology and Program Protection



- **Establishes responsibilities and procedures for *S&T managers and engineers* to manage system security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **System security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber, and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration
- **Employ systems security engineering and Secure Cyber Resilient Engineering methods**
- **Introduces S&T protection and Technology Area Protection Plans**
- **Points to Engineering and T&E issuance**
- **Aligns Program Protection Planning and Secure Cyber Resilient Engineering with acquisition pathways**

Establishes responsibilities for technology and program protection in support of the Adaptive Acquisition Framework; includes pre-acquisition protection activities

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Technology and Program Protection to Maintain Technological Advantage

1. **GENERAL ISSUANCE INFORMATION**

2. **RESPONSIBILITIES**
   USD(R&E), USD(A&S), USD(I&S), DoD CIO, USD(P), DoD Component Heads

3. **PROCEDURES**

3.1. **TECHNOLOGY AND PROGRAM PROTECTION**
   a. Adversary impact on technology and programs
   b. Technologists and lead systems engineers responsibilities

3.2. **ACTIVITIES TO MITIGATE ADVERSARY THREATS TO TECHNOLOGY AND PROGRAMS**
   a. Safeguard Information
   b. Control DoD-sponsored research
   c. Design for security and cyber resiliency
   d. Protect the system against Cyberattacks from enabling and supporting systems
   e. Protect fielded systems
   f. Enhanced protections for critical programs and technologies

3.3 TECHNOLOGY AND PROGRAM PROTECTION MANAGEMENT
   a. Technology Area Protection Plan (TAPP)
   b. S&T Protection Plan
   c. Program Protection Plan (PPP)
   d. Independent Technical Risk Assessment (ITRA)
   e. System Engineering Plan (SEP)
   f. Test and Evaluation Master Plan (TEMP)
   g. Lifecycle Sustainment Plan

3.4 TAILORED PROGRAM PROTECTION FOR SELECTED ACQUISITION PATHWAYS
   a. Major capability acquisition
   b. Urgent operational needs
   c. Operation of the middle tier of acquisition
   d. Software acquisition

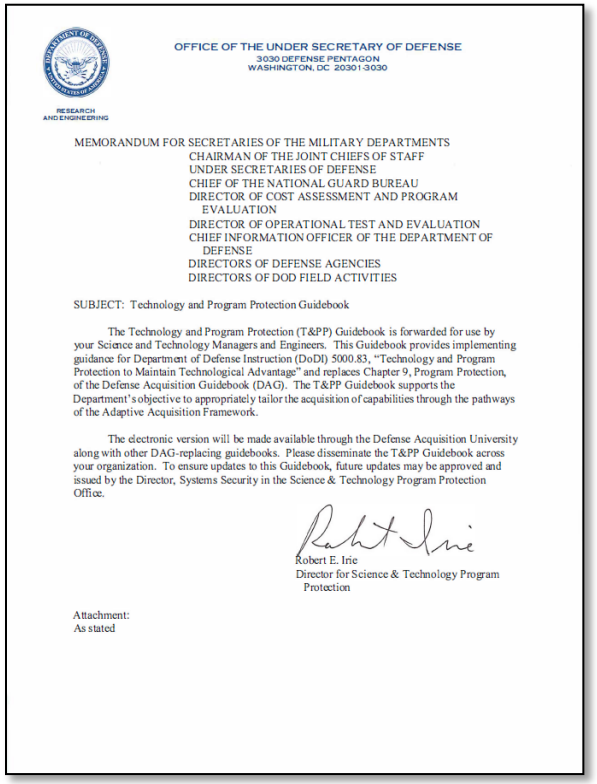
Prevent compromise or loss of critical technology transfer

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

Safeguard system and technical data from adversary collection and disruption

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Technology and Program Protection Guidebook



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH AND ENGINEERING

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Technology and Program Protection Guidebook

The Technology and Program Protection (T&PP) Guidebook is forwarded for use by your Science and Technology Managers and Engineers. This Guidebook provides implementing guidance for Department of Defense Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage" and replaces Chapter 9, Program Protection, of the Defense Acquisition Guidebook (DAG). The T&PP Guidebook supports the Department's objective to appropriately tailor the acquisition of capabilities through the pathways of the Adaptive Acquisition Framework.

The electronic version will be made available through the Defense Acquisition University along with other DAG-replacing guidebooks. Please disseminate the T&PP Guidebook across your organization. To ensure updates to this Guidebook, future updates may be approved and issued by the Director, Systems Security in the Science & Technology Program Protection Office.

Robert E. Irie
Director for Science & Technology Program Protection

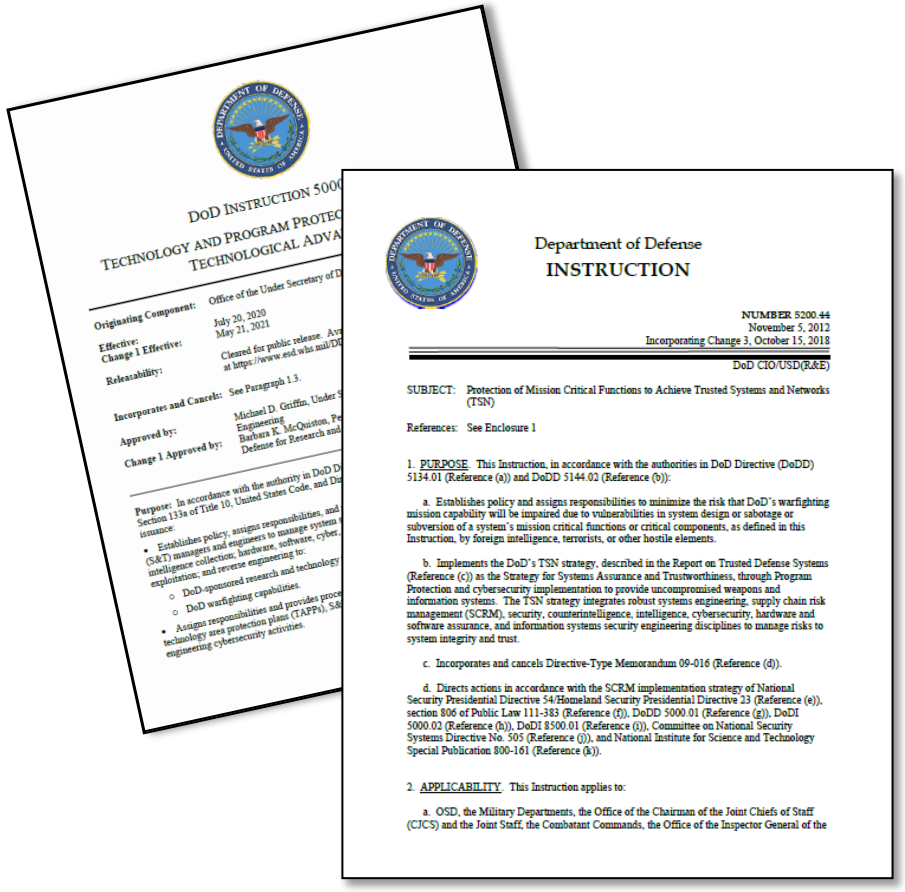
Attachment:
As stated

- **Provides implementing guidance for DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"**
  - Replaces Defense Acquisition Guidebook (DAG) Chapter 9, "Program Protection"
- **Incorporates technology protection activities for DoD-sponsored research and technology**
- **Emphasizes the S&T manager and engineering responsibilities for technology protection, program protection, and cyber**
- **Aligns S&T manager and engineering procedures with DoDI 5000.02, "Operation of the Adaptive Acquisition Framework"**

Supports the Department's objective to tailor acquisition of capabilities through the Adaptive Acquisition Framework pathways

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 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
  - Trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document Program's implementation and outcomes in Program Protection Plan and relevant cybersecurity plans, as appropriate**

Draft update incorporates procedures to implement information communication technology (ICT) exclusion authorities

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Joint Federated Assurance Center

Mission: JFAC provides a federation of software and hardware assurance capabilities across the Department of Defense (DoD), supports implementation of DoDI 5200.44

Origin: Software Assurance FY13 NDAA Sec. 933, JFAC FY14 Sec. 937, 2015 DSD JFAC Policy Memo

System Application: DoD Weapon Systems, DoD Information Systems, and National Security Systems

Goals

- Stay Ahead of the Threat Landscape
- Migrate towards Holistic Assurance across the Life Cycle
- Maximize Discovery and Utilization of Federated Assurance Resources
- Mature Assurance Technologies and Deliver Capabilities at the Speed of Mission
- Provide Affordable and Scalable Assurance Solutions

Joint

Air Force | Army | Navy | OSD

Federated

People / Organizations

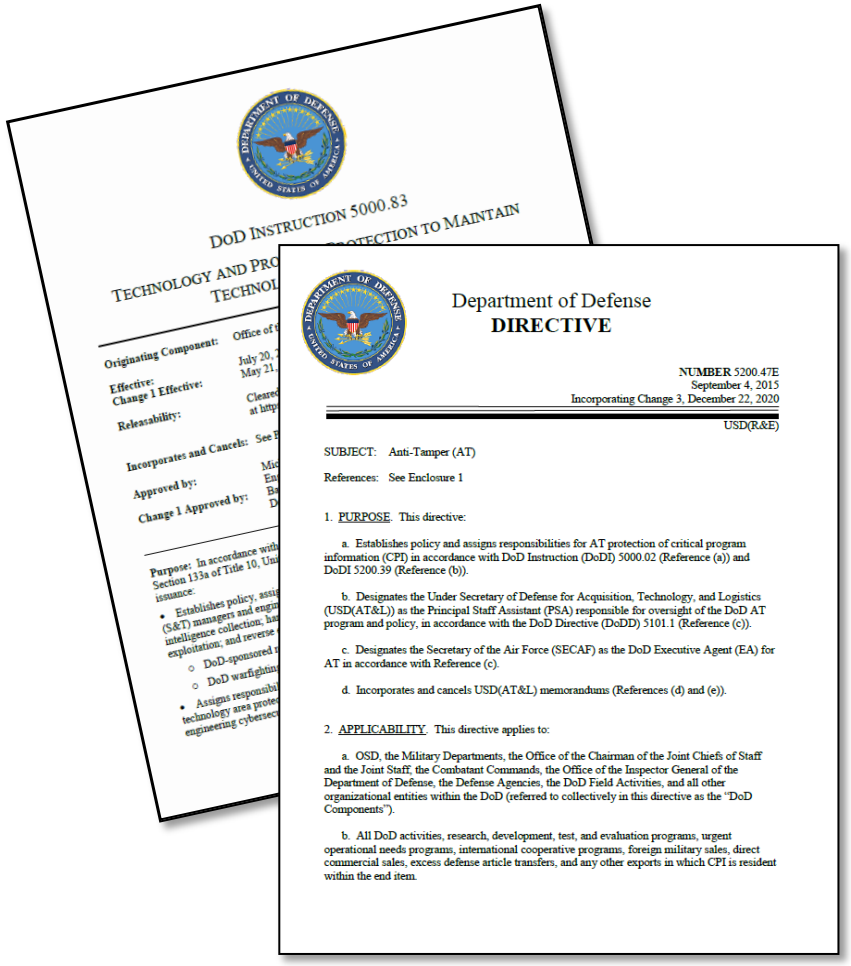
Digital Infrastructure

Roadmap

JFAC Priorities	Current	Near Term	Mid Term	Long Term
Portal	Knowledge Management	Assurance Tool Catalog	Assurance Tool Market Place	
Assurance Technology	2017 Gap Assessment	S&T Assurance Projects	Assurance Investment Roadmap	
Assurance Assessment	Experts			Users
Assurance Licenses	Distributed COTS Tools	Assurance-as-a-Service	JFAC Sponsored Licenses Available via Market Place	

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

DoDD 5200.47E: Anti-Tamper



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).

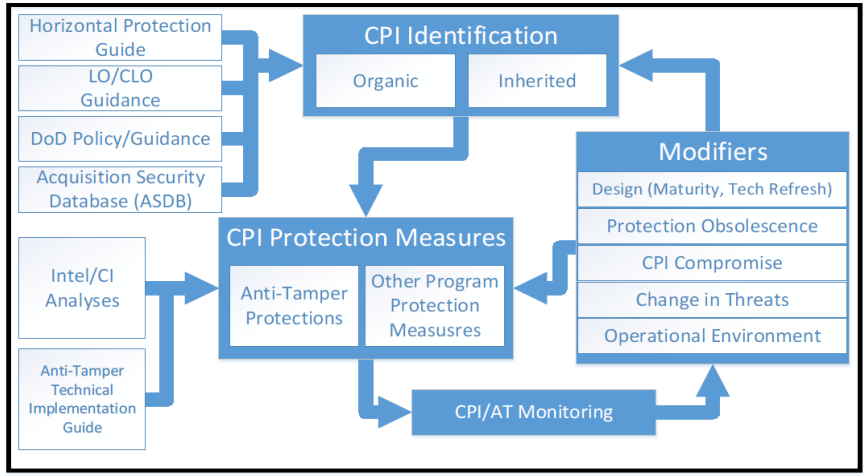
d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

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, excess defense article transfers, and any other exports in which CPI is resident within the end item.

- **Establishes DoD Anti-Tamper (AT) Executive Agent**
- **Establishes responsibility for anti-tamper planning, implementation, and evaluations in alignment with guidance from the DoD Executive Agent for AT**

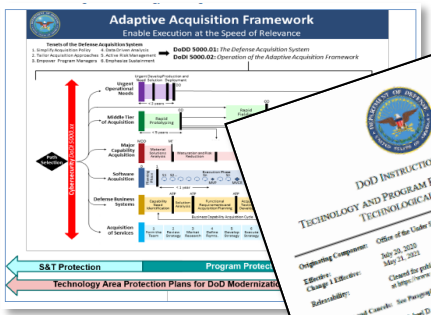


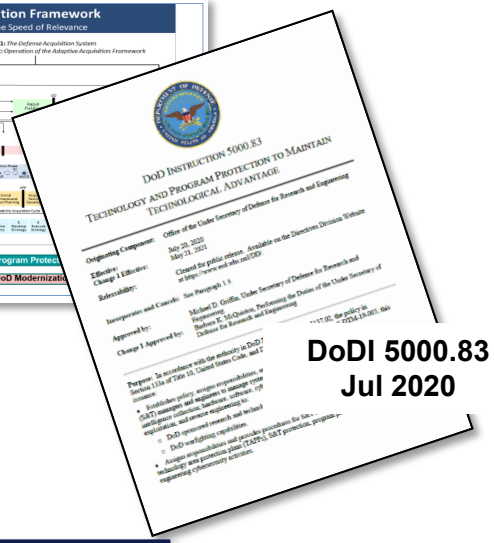
Established Critical Program Information Working Group across DoD stakeholders to identify efficiencies in the identification process

Draft update consolidates anti-tamper activities for the end item, to include identification of the end item

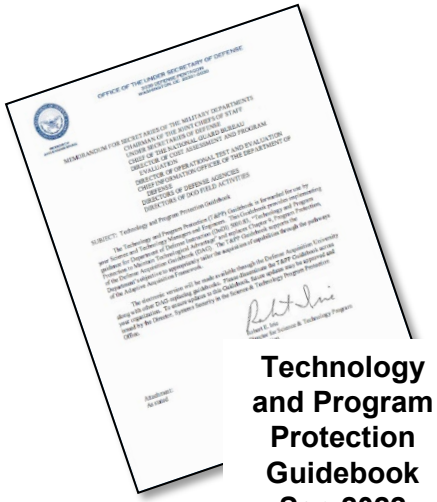
Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Alignment to the Adaptive Acquisition Framework

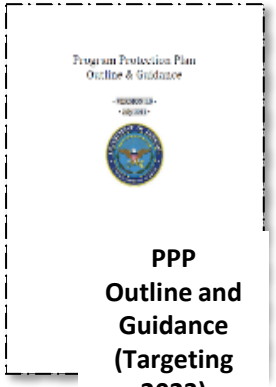




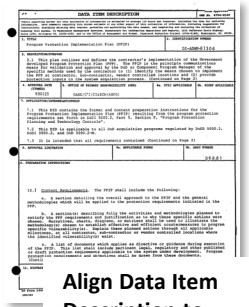
DoDI 5000.83 Jul 2020



Technology and Program Protection Guidebook Sep 2022

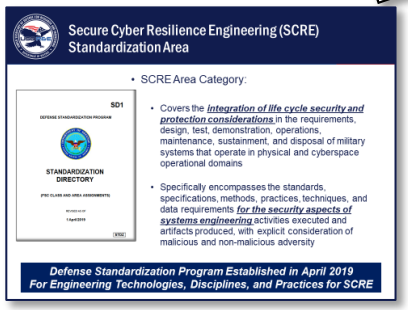


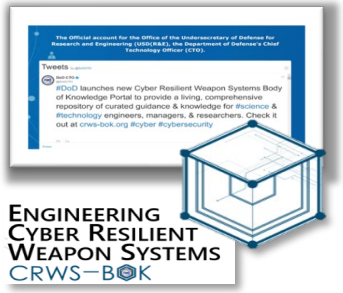
PPP Outline and Guidance (Targeting 2023)



Align Data Item Description to Updated Tables

- Fact of Life Policy Updates
- Acquisition Regulations updates
- Standardization
- Remove duplication
- Lessons Learned



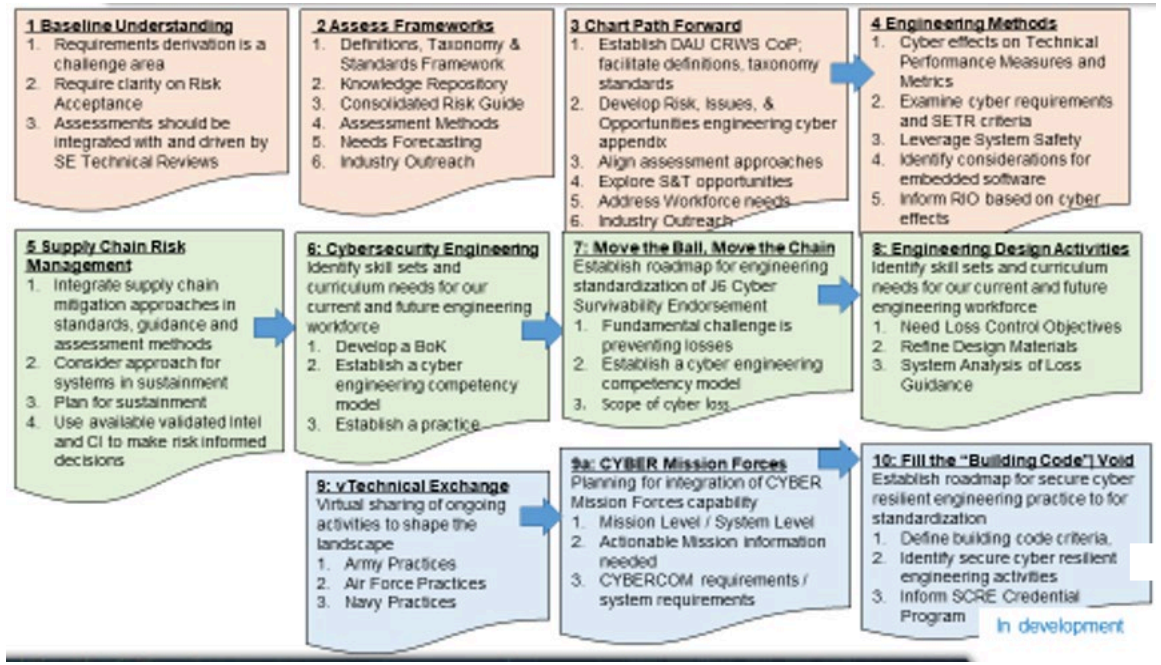


Support USD(R&E) Program Protection and Cyber Independent Technical Risk Assessments Assessments

2020 2021 2022 2023

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Engineering Cyber Resilient Weapon Systems Workshop Series

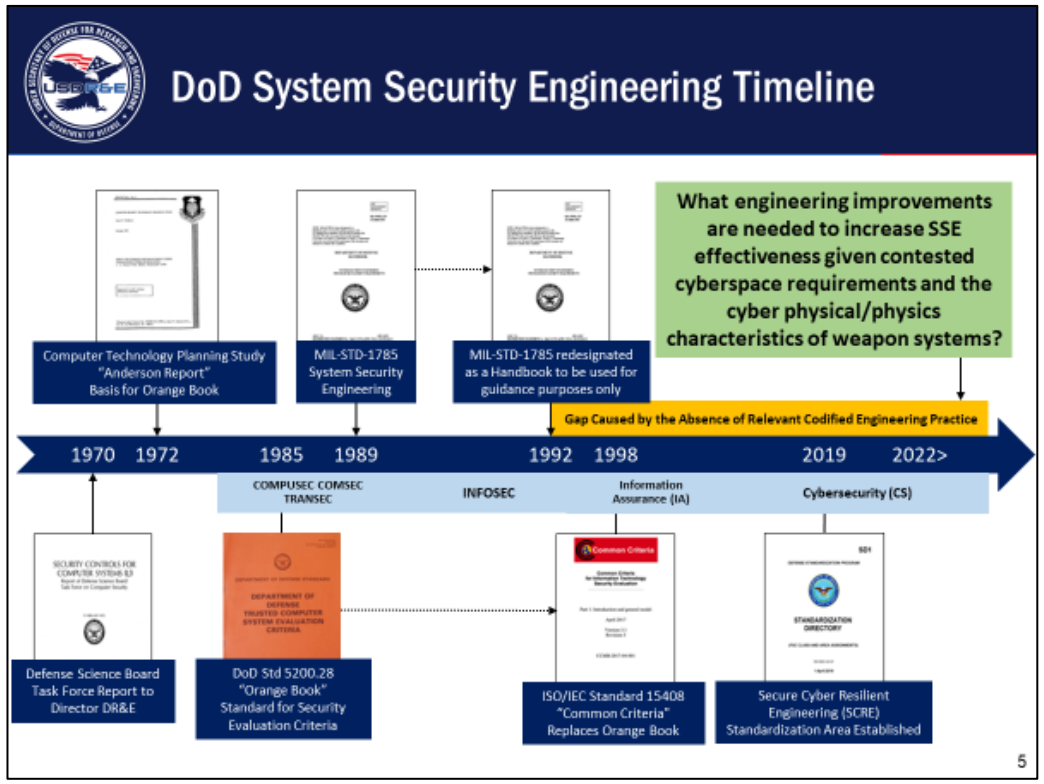


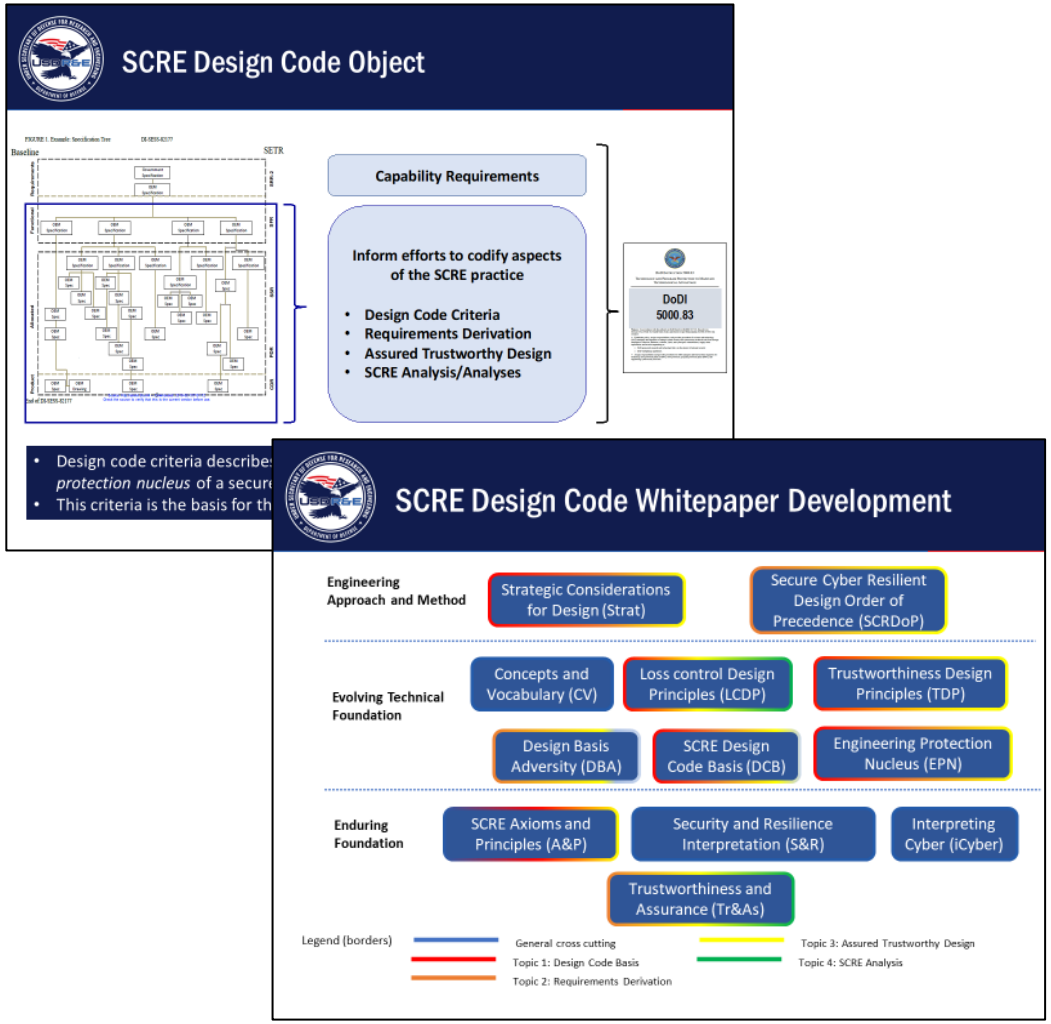
Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

- **March 2017:** Secure Cyber Resilient Engineering (SCRE) Standardization Area
  - Defense Standardization Program
- **August 2018:** CRWS Workshop Report: Preparing the Engineering Workforce for Cybersecurity Challenges
- **March 2019:** Draft SCRE Competency Model
- **November 2020:** DAU Approved to Establish the SCRE Credential Program
- **June 2021:** CRWS Book of Knowledge Deployment
- **August 2022:** 12 Secure Cyber Resilient Engineering Design Code White Papers

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Secure Cyber Resilient Engineering Design Code





Advancing the Secure Cyber Resilient Engineering Practice and Standards

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

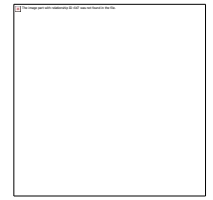
Workforce Competency

System Security Engineering

Secure Cyber Resilient Engineering

Defense Acquisition University

- Program Protection Credential Program
  - ACQ 160: Program Protection Planning Awareness
  - ENG 260: Program Protection for Practitioners
- CLE 022: Program Manager Introduction to Anti-Tamper



Defense Acquisition University

- Secure Cyber Resilient Engineering Credential Program
  - Under Development

Partnering with NDIA System Security Engineering Committee and DAU

- Controlled Technical Information Tabletop; findings and recommendations presented Feb. 2022
- Hardware Assurance Tabletop Tutorial initiative

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Summary

- **DoDI 5000.83 establishes roles and responsibilities for the S&T manager and engineering workforce**

- **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 system security engineering and secure cyber resilient engineering methods and standards**

- **Improve the communication between government, industry, and operational stakeholders**

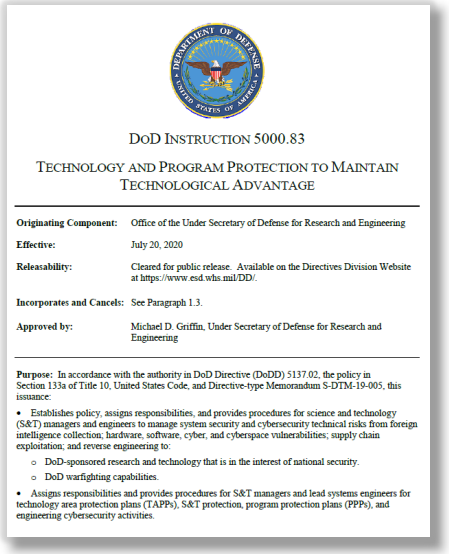
Customer-Focused: Outcome-Based

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Backup

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

DoDI 5000.83: Technology and Program Protection to Maintain Technological Advantage



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
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

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- 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 to:
  - 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.

Main Content

- **Safeguard information**
- **Control DoD Sponsored Research**
- **Design for Security and Cyber Resiliency**
- **Protect the System Against Cyber Attacks From Enabling and Supporting Systems**
- **Protect Fielded Systems**
- **Enhance Protection for Critical Programs and Technologies**

Technology Area Protection Plan (TAPP)

- OUSD(R&E) identifies broad technology elements to protect that are central to accelerating warfighter capabilities in key technology areas across the Department
- Set boundaries on what should be communicated by stakeholder groups for protection purposes

Science & Technology Protection Plans

- Management tool to guide protection activities for S&T Investments at DoD Component level
- Implement risk-based protection measures to reduce compromise or loss to competitor nations through transition to acquisition

Program Protection Plan (PPP)

- Acquisition management tool to guide the systems security engineering, to include cyber resilient engineering, activities across the life cycle
- Informed by TAPP and S&T Protection Plans

DoD S&T (Budget Activities 6.1 - 6.4)

DoD RDT&E Programs (Budget Activities 6.4+)

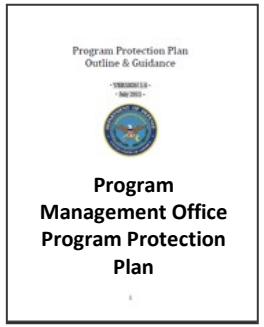
TAPP – Technology Area Protection Plan
PPP – Program Protection Plan

Manage risk of adversarial exploitation and compromise beginning with early S&T and continues through the Acquisition lifecycle

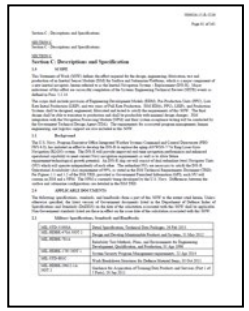
Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Delivering Assured, Secure, Resilient Systems

Government Furnished Information



Government Furnished Information

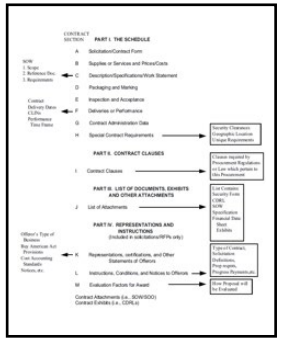


Section C Statement of Work

Contract Data Requirements List (CDRL): Contractor Program Protection Implementation Plan

Section I FAR/DFAR Contract Clauses

Consistent implementation will provide balanced and seamless protections



Solicitation/Contract

Increase consistency and repeatability of system assurance, system security, and cybersecurity methods and technologies

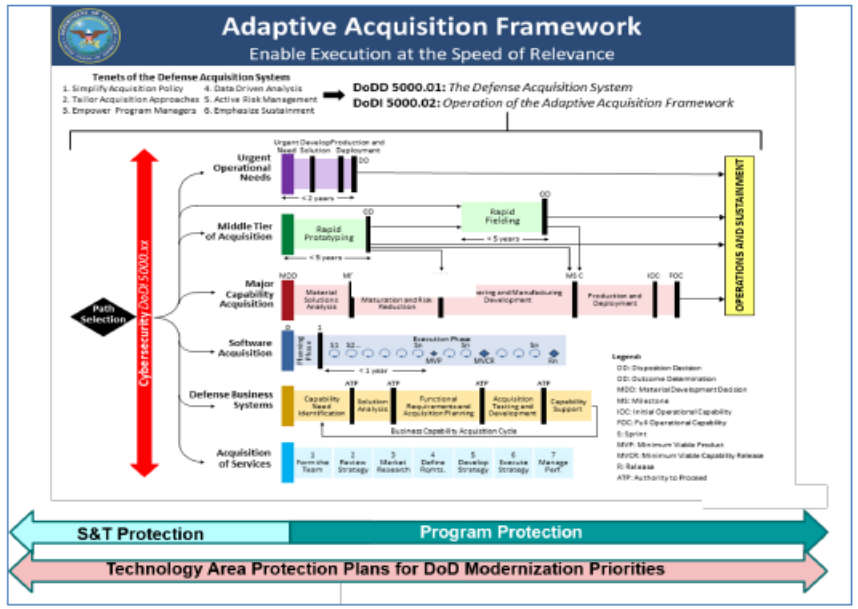
Improve expectations across Government, industry, academia and operational stakeholders

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Adaptive Acquisition Framework Pathway Considerations

All program must consider program protection, however:

- Not all programs require PPPs
  - Business Systems & Service Contracts do not require PPPs
  - Only programs where the DAE is the milestone decision authority have to submit the PPP to USD(R&E) for approval
  - DoD Components determine approval levels for other PPPs
- Tailored based on the pathway and anticipated risks the program will encounter:



- All programs must follow pathway Statutory & Regulatory Requirements
- Should use ***streamlined***
  - Program Protection Trade-off Analyses
  - Information Analysis
  - Critical Program Information (CPI) Analysis
  - Trusted Systems & Network (TSN) Analysis
- Ensure operators are informed of operational risks when the system is fielded

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

Fostering Assured, Secure, Resilient Missions, Systems, and Components

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**
- **DFARS 225.7901 Export-controlled items**

Mission Components

Key Protection Activities:

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

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**
- **NDAA FY11 Sec 806; Requirements for Information Relating to Supply Chain Risk**
- **NDAA FY18 Sec 1659. Supply Chain Risk Management of Critical Missions**
- **NDAA FY20 Sec 224, Trusted Supply Chain Standards**
- **NDAA FY17 Sec 231 DoDI Microelectronics**

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**

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

Distribution Statement A: Approved for public release. DOPSR case #23-S-0064 applies. Distribution is unlimited.

USD(R&E)

Joint Federated Assurance Center Overview

Mr. Brian Nowotny
Director, Joint Federated Assurance Center
Office of the Under Secretary of Defense for Research and Engineering
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Joint Federated Assurance Center

Director: Mr. Brian Nowotny

Mission: The Joint Federated Assurance Center (JFAC) provides a federation of software and hardware assurance capabilities across the Department of Defense (DoD).

Vision: Building Trust through Holistic Assurance

Origin: Fiscal Year (FY) 2013 National Defense Authorization Act (NDAA) Section 933 (Software Assurance), FY 2014 NDAA Section 937 (JFAC), 2015 Deputy Secretary of Defense JFAC Policy Memo

System Application: DoD weapon systems, DoD information systems, and national security systems

JFAC Strategic Goals

- Stay ahead of the threat landscape
- Migrate towards holistic assurance across the lifecycle
- Maximize discovery and utilization of federated assurance resources
- Mature assurance technologies and deliver capabilities at the speed of mission
- Provide affordable and scalable assurance solutions

Joint

Air Force | Army | Navy | OSD

Federated

People / Organizations

Digital Infrastructure

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

JFAC Strategic Goal 1: Stay Ahead of the Threat Landscape

Hardware Supply Chain

Security Clearance News & Career Advice

Chinese Magnets in F-35s Make Pentagon Hit Pause

At issue is material in the aircraft's engine that was made with ... Force was forced to temporarily ground their F-35 fleets after an issue...

Software Supply Chain

Security Intelligence

How Log4j Vulnerability Could Impact You

If you hadn't heard of Apache Log4j, chances are it's on your radar now. In fact, you may have been using it for years. Log4j is a logging...

Pirated Software

Department of Justice

CEO of Dozens of Companies and Entities Charged in ...

As alleged, the Chinese counterfeiters often added pirated Cisco software and unauthorized, low-quality, or unreliable components – including...

Counterfeit Parts

Yahoo

An F-16 pilot died when his ejection seat failed. Was it counterfeit?

While the Air Force suspected parts of the seat were counterfeit, it buried the information in a nonpublic section of its accident...

Foreign Investments

Reuters

Biden tells foreign investment panel to screen deals for data, cyber risks

U.S. President Joe Biden on Thursday directed the committee that reviews foreign investment for national security risks to sharpen its focus...

Trade Secret Theft

Bloomberg.com

Ex-Apple Engineer Pleads Guilty in Trade Secrets Theft Case

"Xpeng strictly abides by the related laws and highly values the protection of intellectual property." In January 2019, federal prosecutors...

Nation-State Actors

Washington Times

China and the theft, weaponization of intellectual property

China and the theft, weaponization of intellectual property ... Pilot National Laboratory for Marine Science and Technology in China.

Individual Threats

PC Gamer

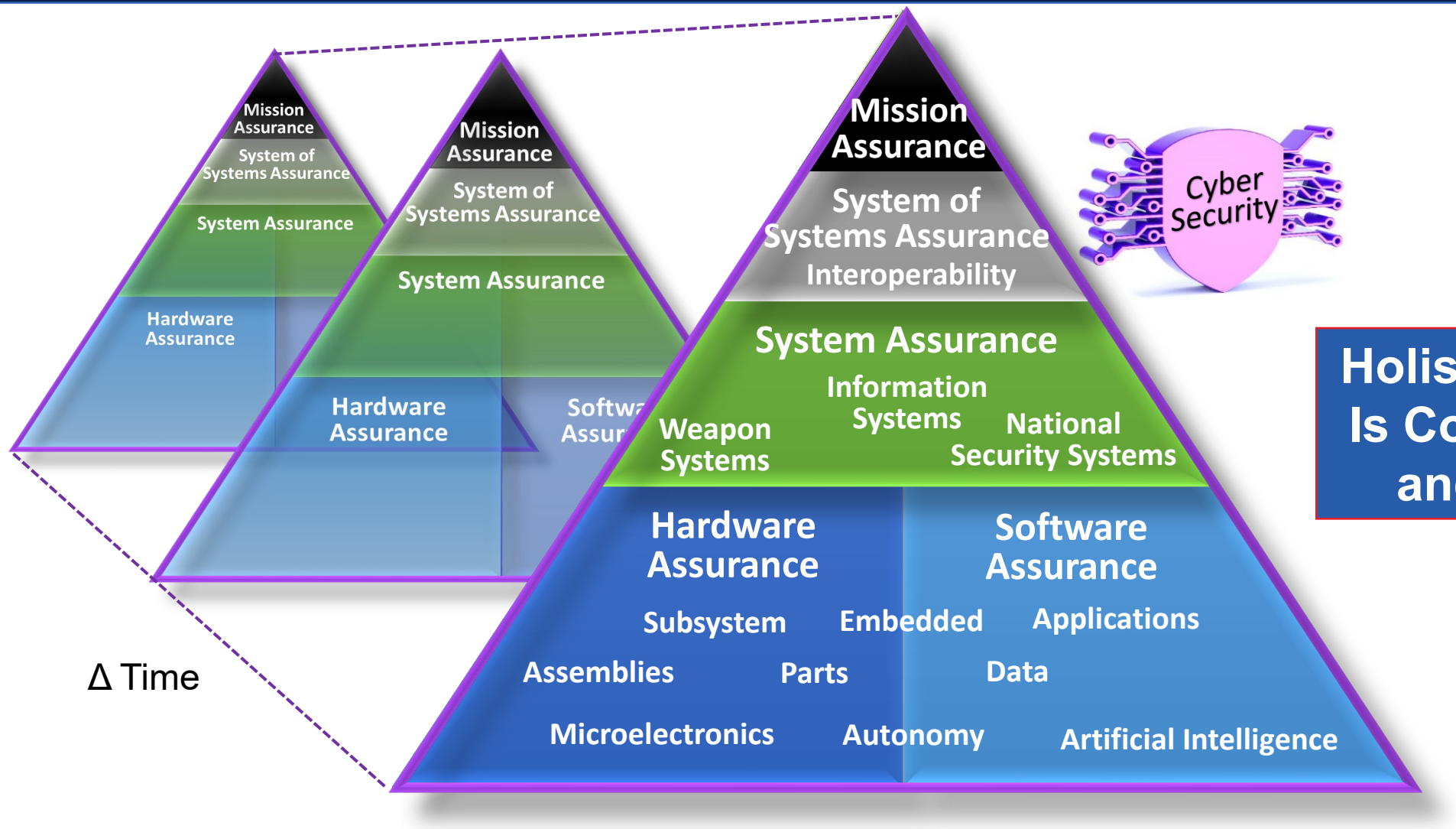
Uber's been hacked by an 18 year old, go figure

It appears Uber has been hacked by an 18-year-old. ... having spoken to the apparent hacker, who claims to be just 18 years old.

Threat landscape is complex and risks are significant

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

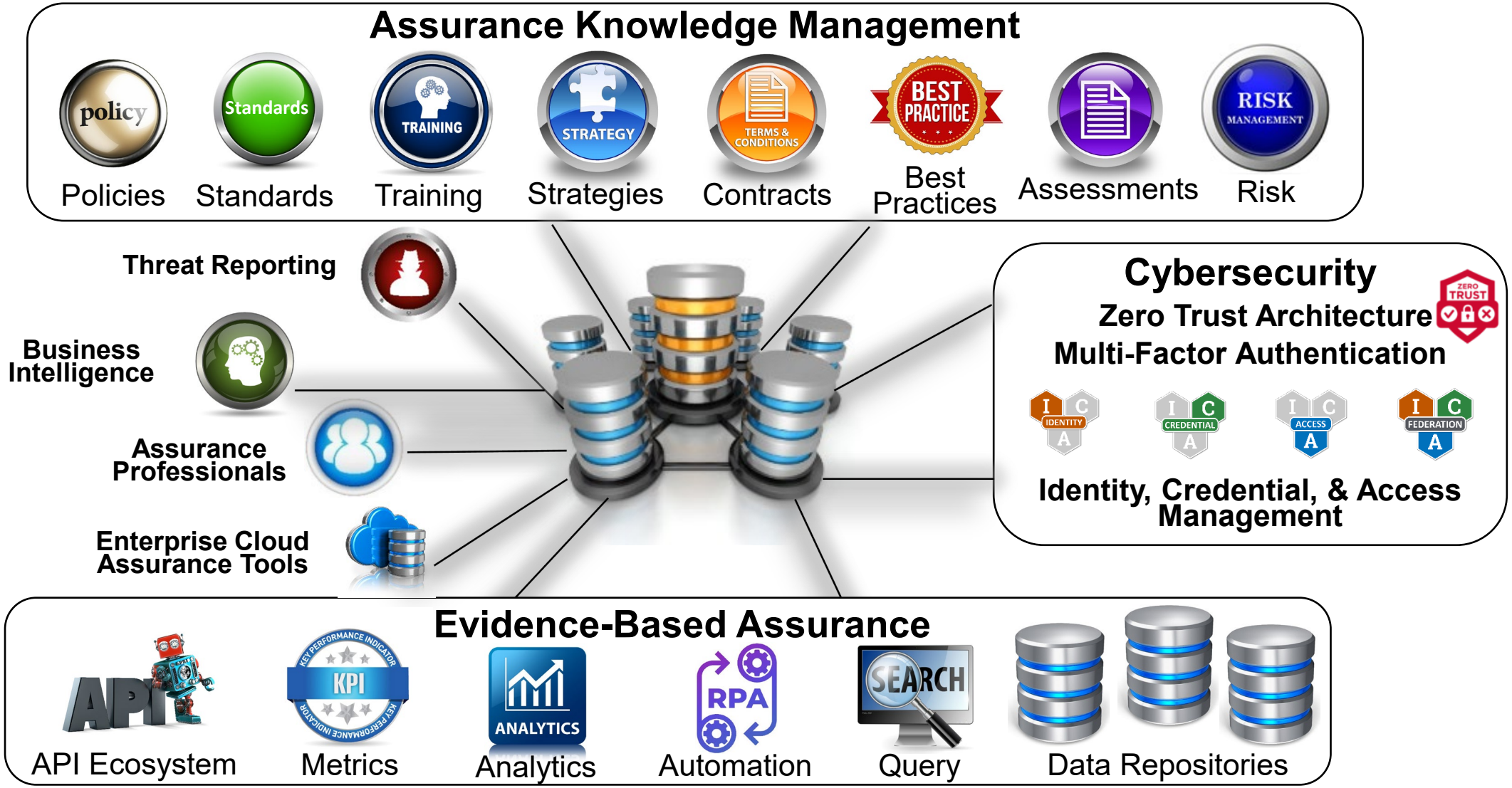
JFAC Strategic Goal 2: Holistic Assurance Across the Lifecycle



Holistic Assurance Is Comprehensive and Traceable

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

JFAC Strategic Goal 3: Maximum Discovery and Utilization of Federated Assurance Resources



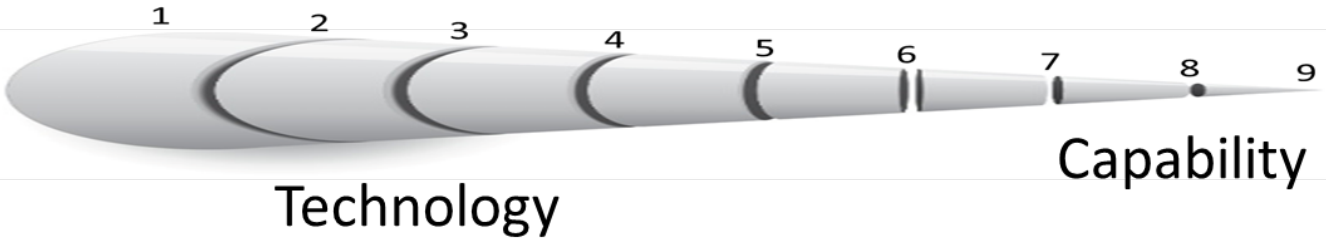
Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

JFAC Strategic Goal 4: Mature Assurance Technologies and Deliver Capabilities at the Speed of Mission

Assurance Gaps

DoD Science & Technology (S&T) | **Acquisition**

Technology Readiness Levels



- FFRDC & UARCs
- Academia
- Commercial Industry
- Open Source
- Other Government Agencies

JFAC Enterprise Assurance Repository

Mitigating Assurance Gaps, Maturing Technologies into Capabilities, & Scaling to Enterprise Discoverability

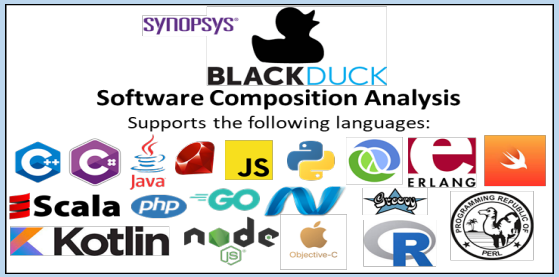
Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

JFAC Strategic Goal 5: Providing Affordable and Scalable Assurance Solutions

Affordable Assurance Solutions

1) Leverage open-source assurance tools*

2) Develop government assurance tools



3) Sponsor commercial licenses for joint enterprise

Scalable Assurance Solutions

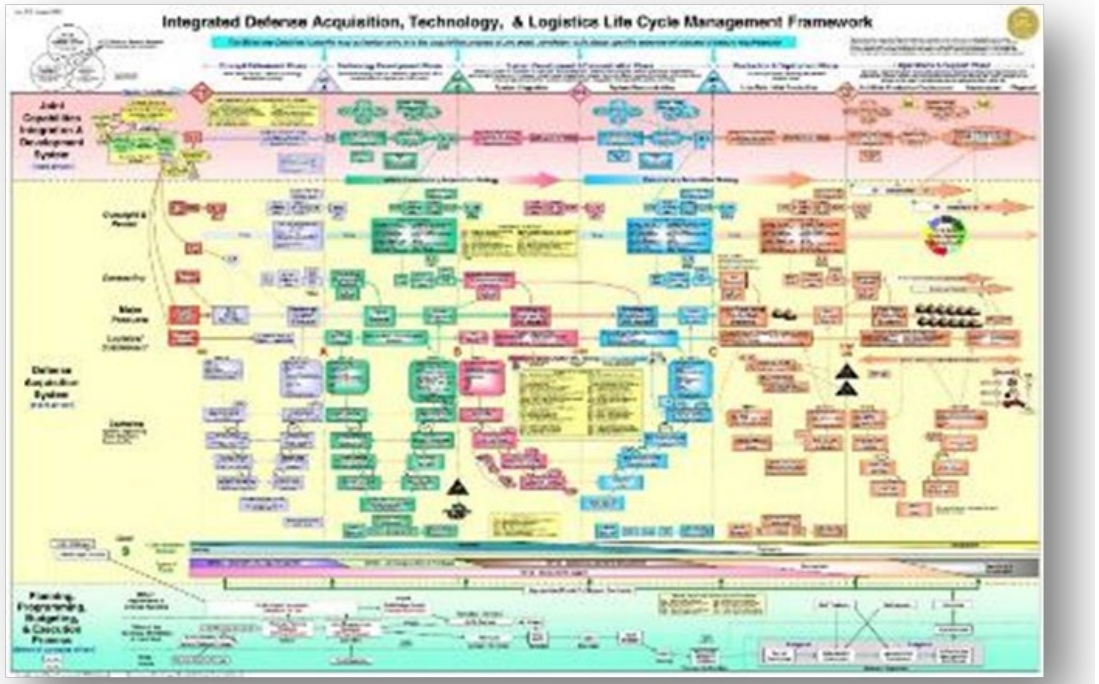
- Establish joint federated assurance marketplace
- Assurance technology development repository
- Federated enterprise assurance data discovery and exchange
- Deployment of assurance capabilities at the edge

**Restrictions based upon open-source license terms and conditions*

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Competition-Driven Transformation

Acquisition Approach



Series, Discrete, Document, and Segmented

Competition Drives Need to Reduce Concept to Fielding Time

Visionary Approach

- Continuous Mission Engineering
- Continuous SoS/Systems Engineering
- Continuous Development
- Continuous Integration
- Continuous Modeling & Simulation
- Continuous Test & Evaluation
- Continuous Manufacturing/Production
- Continuous Security/Cybersecurity
- Continuous Fielding
- Continuous Operations
- Continuous Sustainment

Parallel, Continuous, Digital, and Interconnected

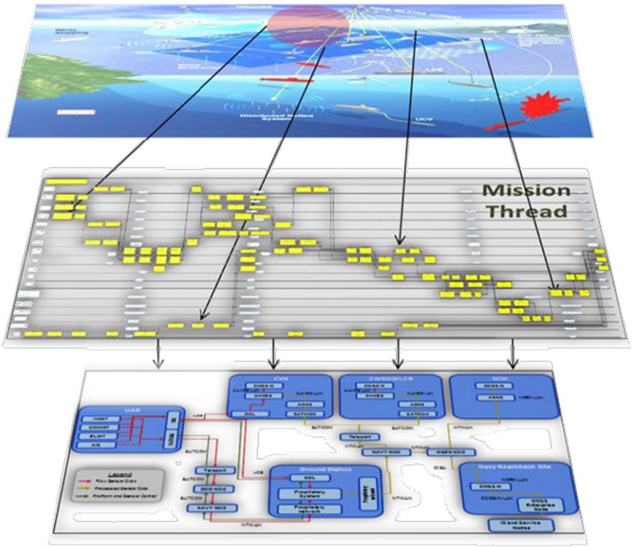
Prioritize Speed, Agility, and Resilience

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Mission and Systems Engineering

Current Digital Engineering Constructs

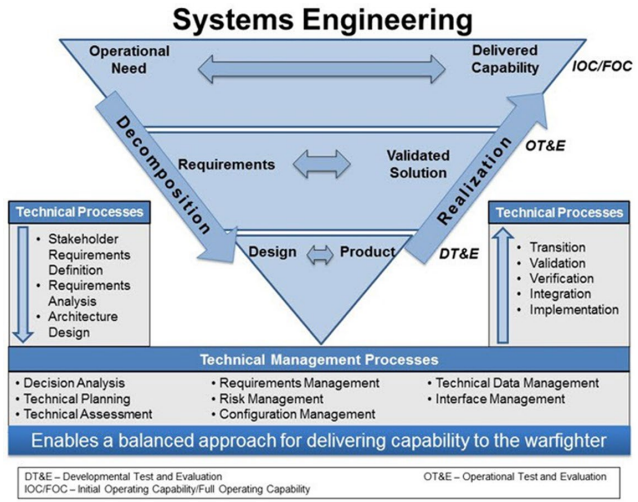
Mission Engineering (ME) Environment



ME Workflow

ME Tools | ME Data

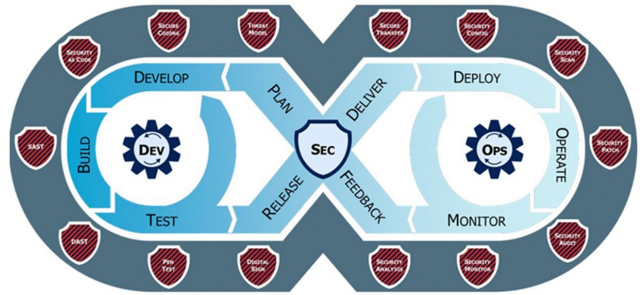
Systems Engineering (SE) Environment



SE Workflow

SE Tools | SE Data

Software Development, Security, and Operations (DevSecOps) Environment



DevSecOps Workflow

DSO Tools | DSO Data

Segregated Digital Infrastructures

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Mission and Systems Engineering

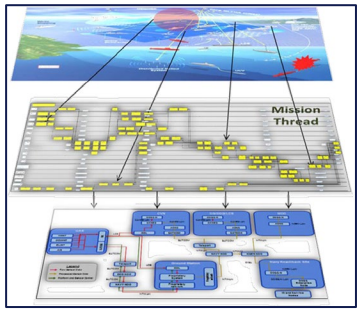
Visionary End-to-End Digital Engineering Construct

End-to-End Digital Engineering Environment (SAP/SAR)

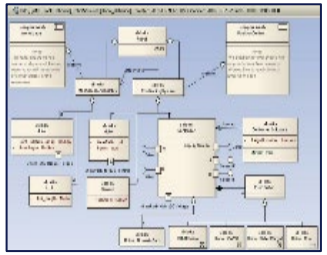
End-to-End Digital Engineering Environment (IL 7 / Top Secret / JWICS)

End-to-End Digital Engineering Environment (IL 6 / Secret / SIPR)

End-to-End Digital Engineering Environment (IL 5 / CUI / NIPR)



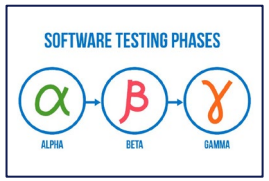
Mission Engineering



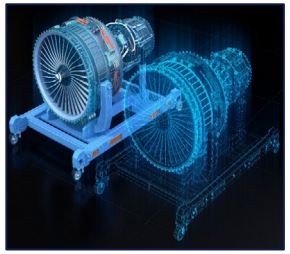
Systems Engineering

Development

Security



Testing



Simulation

Cyber-Hardened Containerized Digital Tools (CHCDT)

- CHCDT Repo 1
- CHCDT Repo 2
- CHCDT Repo 3
- CHCDT Repo 4

- Data Repo 1
- Data Repo 2
- Data Repo 3
- Data Repo 4

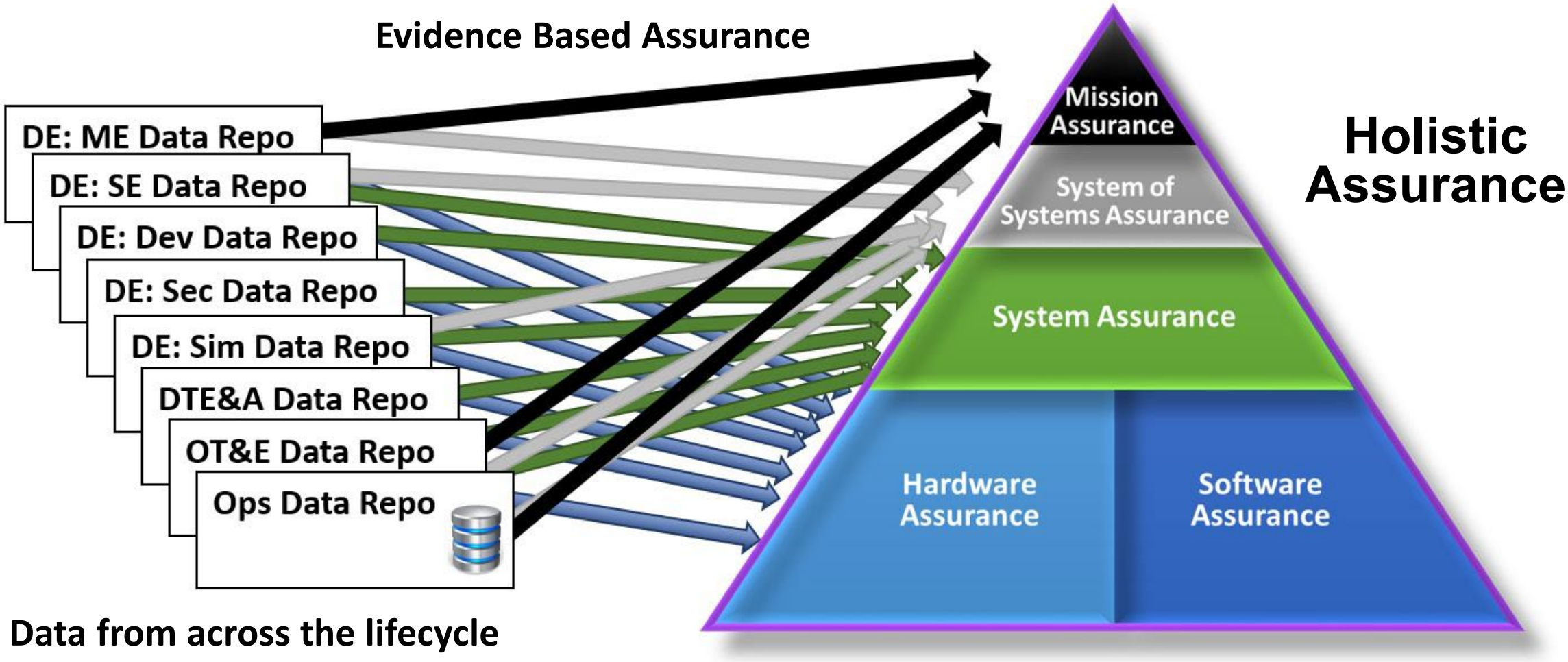
Federated Data Repositories

Accredited Infrastructures, Federated Digital Tools and Data, Streamlined Workflows

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Mission and Systems Engineering

Federated Data Enabling Holistic Assurance



Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Current JFAC Assurance Federation

Research and Engineering
Joint Federated Assurance Center, Microelectronics, Integrated Sensing and Cyber, Development Test and Evaluation, Defense Advanced Research Project Agency (DARPA), Missile Defense Agency (MDA)

Acquisition and Sustainment
Defense Logistics Agency, Defense Microelectronics Activity (DMEA)

Chief Information Officer
Cyber Security, Information Enterprise, Defense Information Systems Agency

Chief Digital and Artificial Intelligence Office

National Reconnaissance Office

Department of the Air Force

Department of the Army

Department of the Navy

Director of National Intelligence
Intelligence Advanced Research Projects Agency (IARPA)

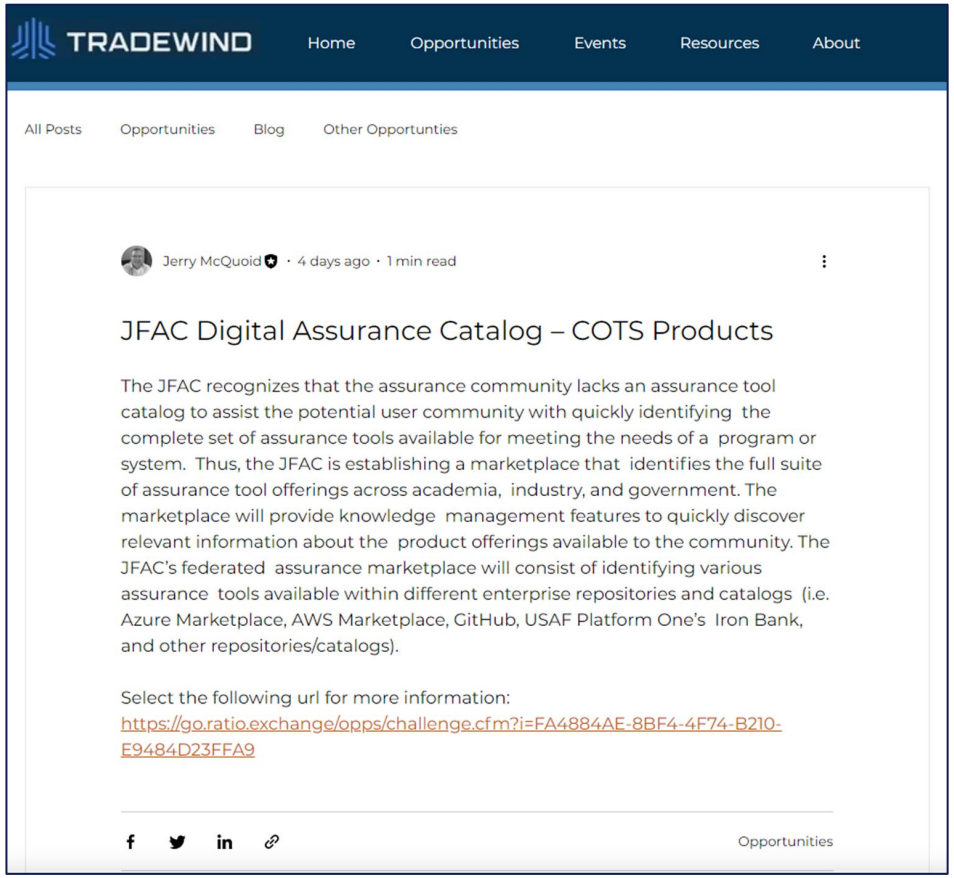
National Security Agency

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Industry Engagement Opportunities

- **Respond to the JFAC request for information to support building a JFAC digital assurance tool catalog**
  - https://www.tradewindai.com/post/jfac-digital-assurance-catalog-cots-products

- **Future FY23 announcements expected via CDAO's Tradewind**
  - https://www.tradewindai.com/opportunities



Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Q&A

Questions

Distribution Statement A: Approved for public release. DOPSR case #23-S-0009 applies. Distribution is unlimited.

Digital Engineering Information Exchange Working Group (DEIXWG)

Digital Viewpoint Model (DVM)

Tech Lead: Terri Chan: terri.w.chan@boeing.com
Tech Lead: Veejay Gorospe: veejay.gorospe@3ds.com
Tech Lead: Ken Zhang: LeqiKen.Zhang@l3harris.com

Chair: Sean McGervey: sean.mcgervey@3ds.com
Deputy-Chair: Tamara Hambrick: tamara.hambrick@boeing.com
Co-Chair: Celia Tseng: celia.tseng@3ds.com
Co-Chair: Ken Zhang: LeqiKen.Zhang@l3harris.com
Co-Chair: Frank Salvatore: Frank.Salvatore@saic.com
Co-Chair: Chris Schreiber: Chris.Schreiber@lmco.com

Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

Table of Contents

- DEIX and Digital Viewpoint Model (DVM)
- Overview of Digital Viewpoint Model (DVM)
- Example DVM Use Case Walkthrough
- Next Steps

Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

What is the DEIXWG?

- Collaboration between the International Council of Systems Engineers (INCOSE), National Defense Industrial Association (NDIA), and the Office of the Under Secretary of Defense for Research and Engineering (DoD OUSD(R&E))
- The DEIXWG supports the strategic objective of accelerating digital engineering transformation by characterizing the content and relationships involved in the exchange of digital artifacts between stakeholders of various disciplines throughout the engineering lifecycle

What is the DVM?

- The Digital Viewpoint Model (DVM) is an implementation-agnostic (platform independent), conceptual ontology developed from DEIXWG
- The DVM provides a high-level framework for describing sources of digital information in a digital engineering ecosystem (DEE)
- The DVM also conceptualizes how that information can be transferred, translated, transformed, and related for the purpose of exchanging digital information between stakeholders… who might not have the same DEE infrastructure or standards

Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DEIXWG Activities

Digital Viewpoint Model (DVM) WG

- **Manage DVM Baselines**
  - Release/Publish DVM Baselines
  - Capture proposed changes to DVM
  - Facilitate updates to DVM baseline with DEIX committee
  - Support DVM proposal to industry standards
- **Facilitate DVM Usage through Use Cases**
  - Develop supporting material for DVM usage
  - Capture use cases that involves digital exchanges
  - Host workshops on use case development and DVM usage

Standards Framework (SF) WG

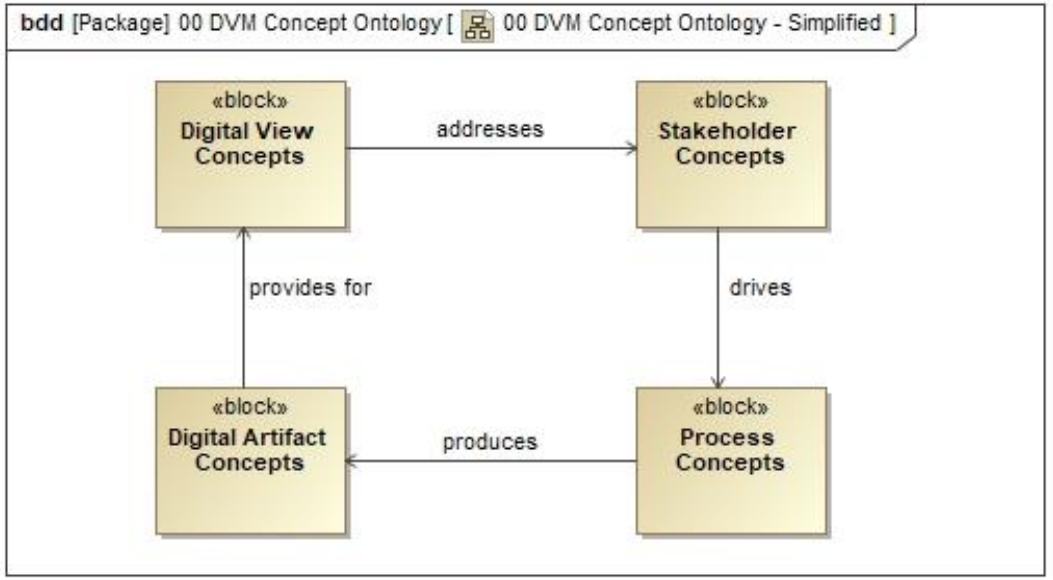
- INCOSE/ISO liaison for digital engineering standards
- Manage proposals of DEIX concepts/products to ISO standards

Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM Ontology Overview

- Defined at a high-level
- Allow stakeholders to extend them with more specialized concepts
- Can be specialized to a given domain or need
- Instead of defining a set of all-purpose views, the ontology simply provide guidance in defining views for specific exchanges
- DVM is about how to better define what needs to be exchanged, not the implementation of the exchange and associated artifacts
- The DVM is divided into four interconnected ontologies



While the DVM is modeled using SysML, the concepts are agnostic of any particular language, tool, or infrastructure

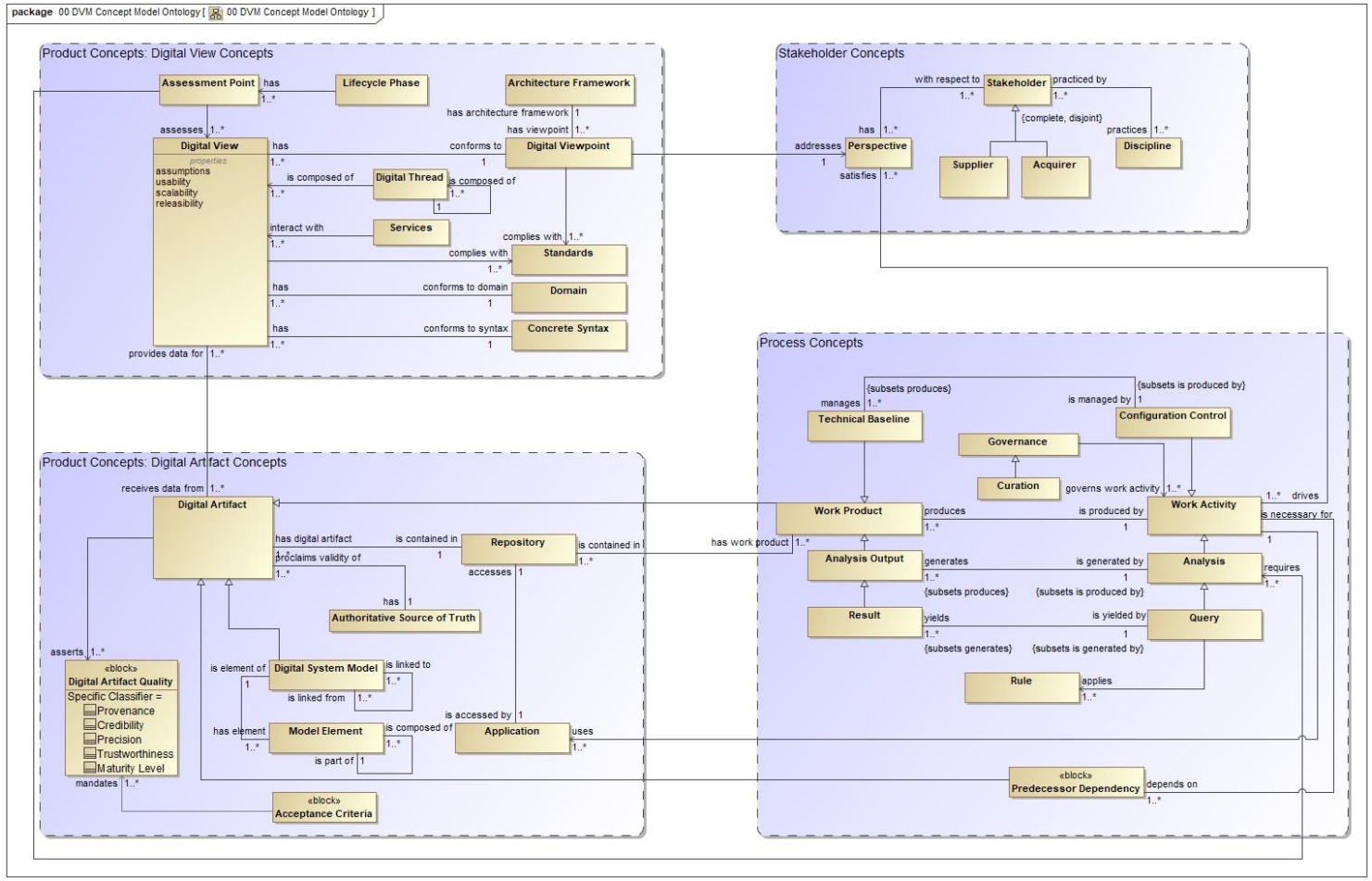
Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM: Exchanging Data Related Across Different Metamodels

Digital View Concepts

Digital Artifact Concepts



Stakeholder Concepts

Process Concepts

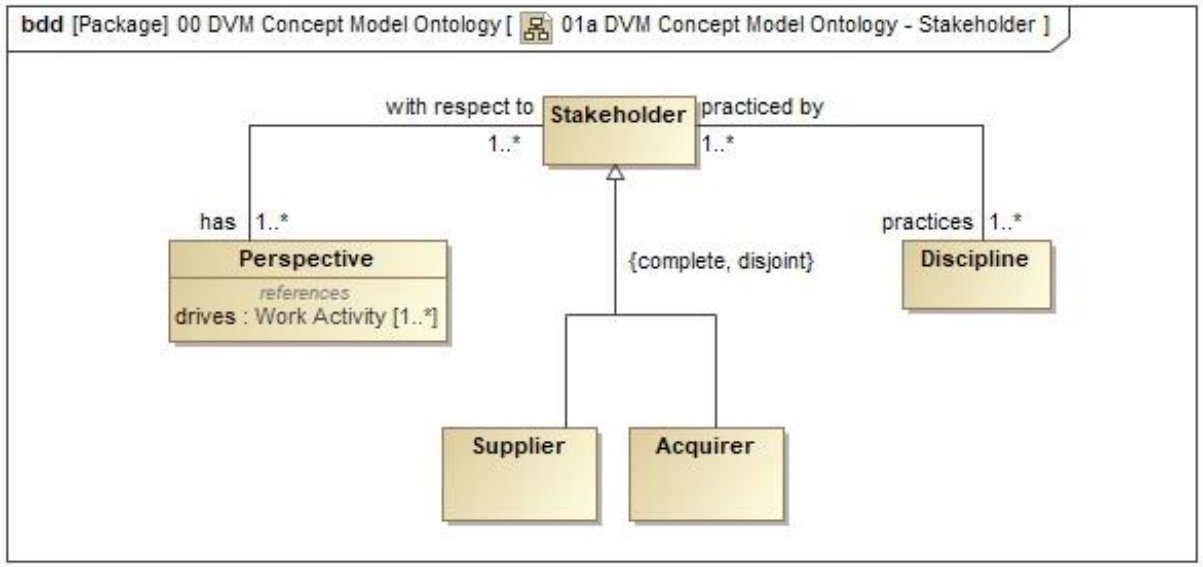
Rev A

Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM: Stakeholder Concepts Ontology

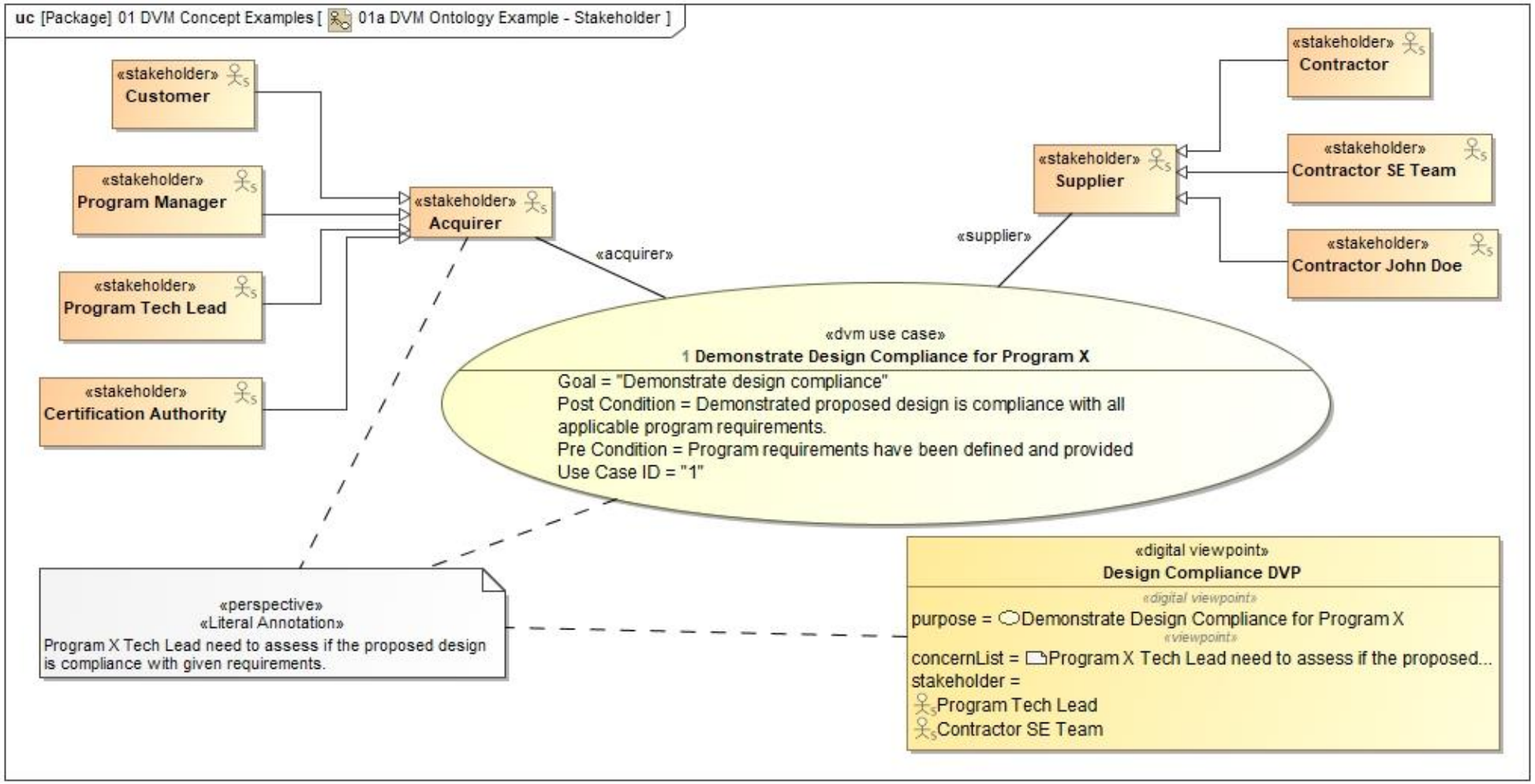
- Describe the stakeholders involved in a given exchange of digital information
- Can be applied to any stakeholders exchanging digital information, whether they are from the same or different organizations
- The perspective defines the specialized stakeholder needs that drive associated work activity and requirements for the digital view



Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

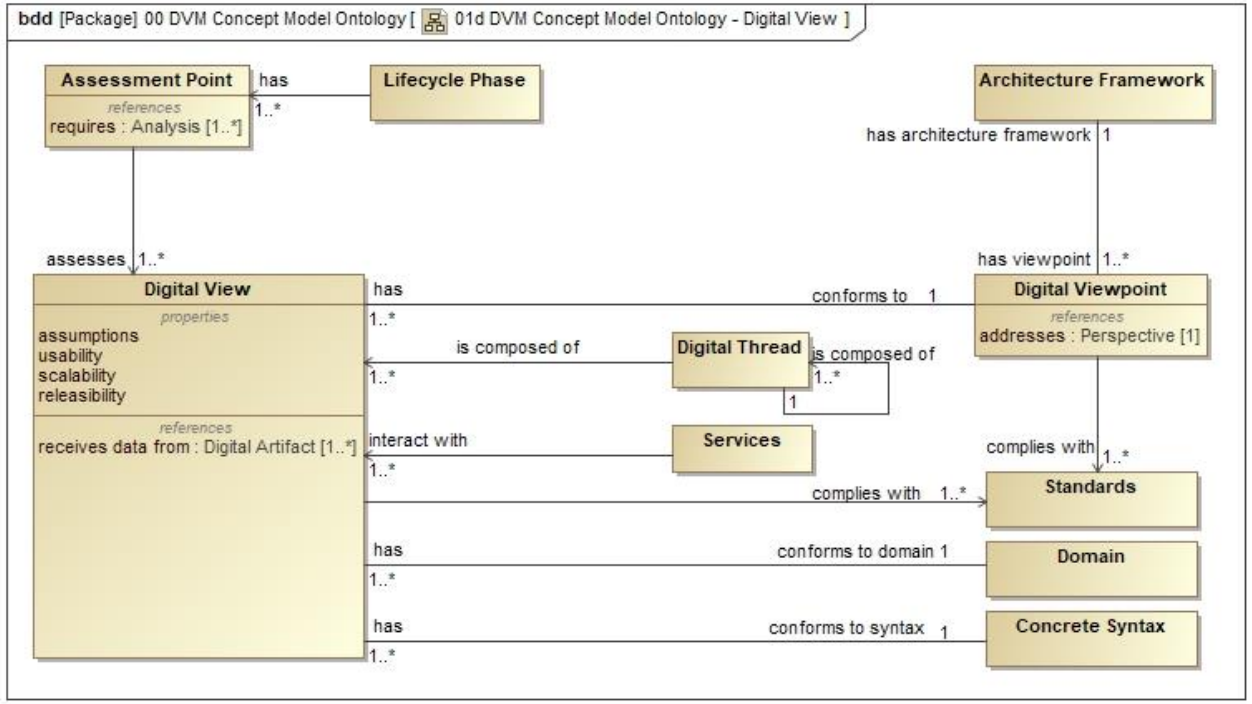
DVM: Stakeholder Concepts - Example



© 2022 Published and used by INCOSE with permission

DVM: Digital View Concepts Ontology

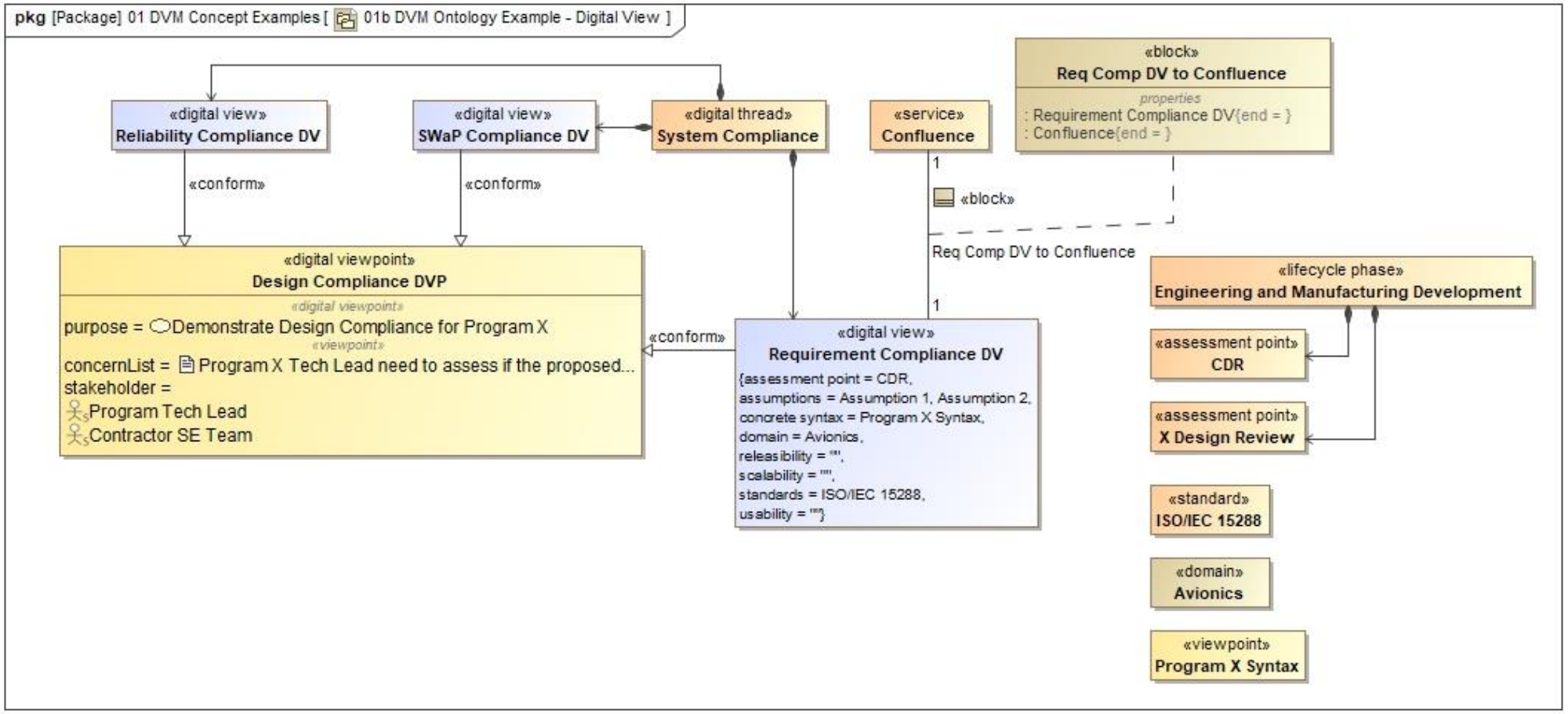
- This ontology specifies concepts used to describe
  - Specify concepts describing digital views
  - Specify applicable standards and syntax
  - Influence of digital views in system life cycle
- The relationship between digital views and viewpoints is specified
- New digital views and viewpoints can be conceptualized as extensions of these base concepts



Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

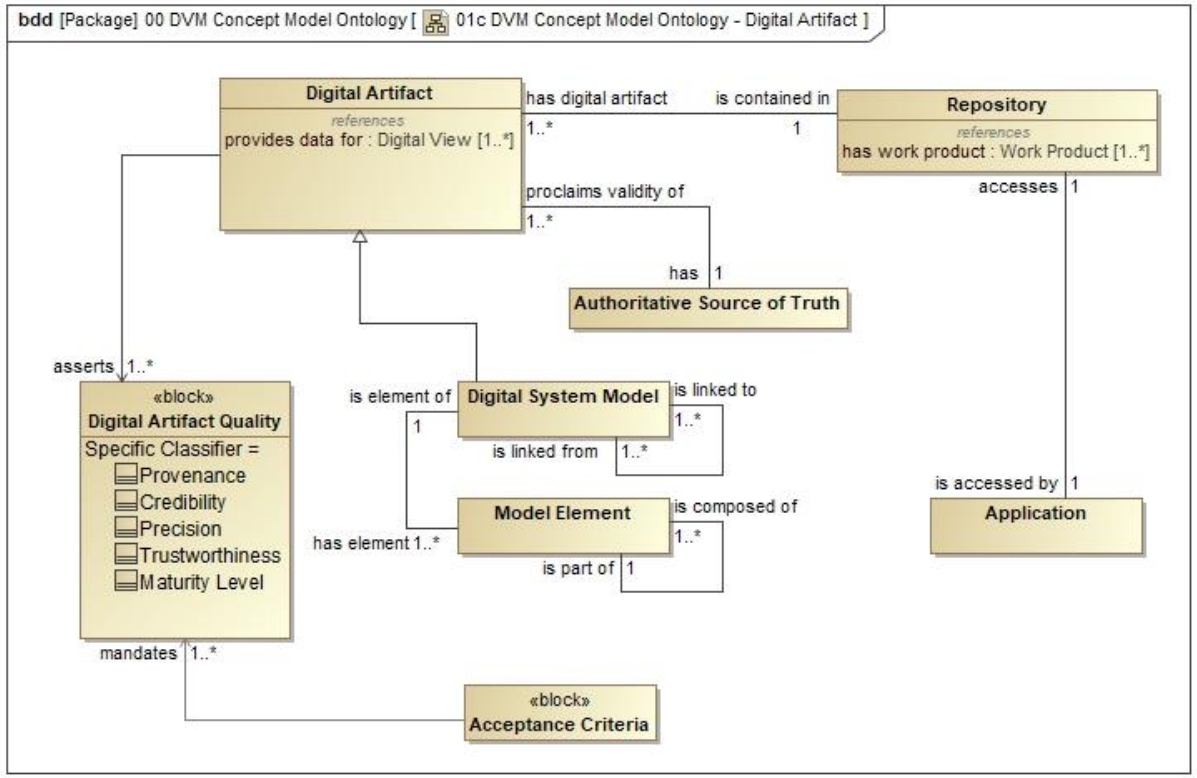
DVM: Digital View Concepts - Example



© 2022 Published and used by INCOSE with permission

DVM: Digital Artifact Concepts Ontology

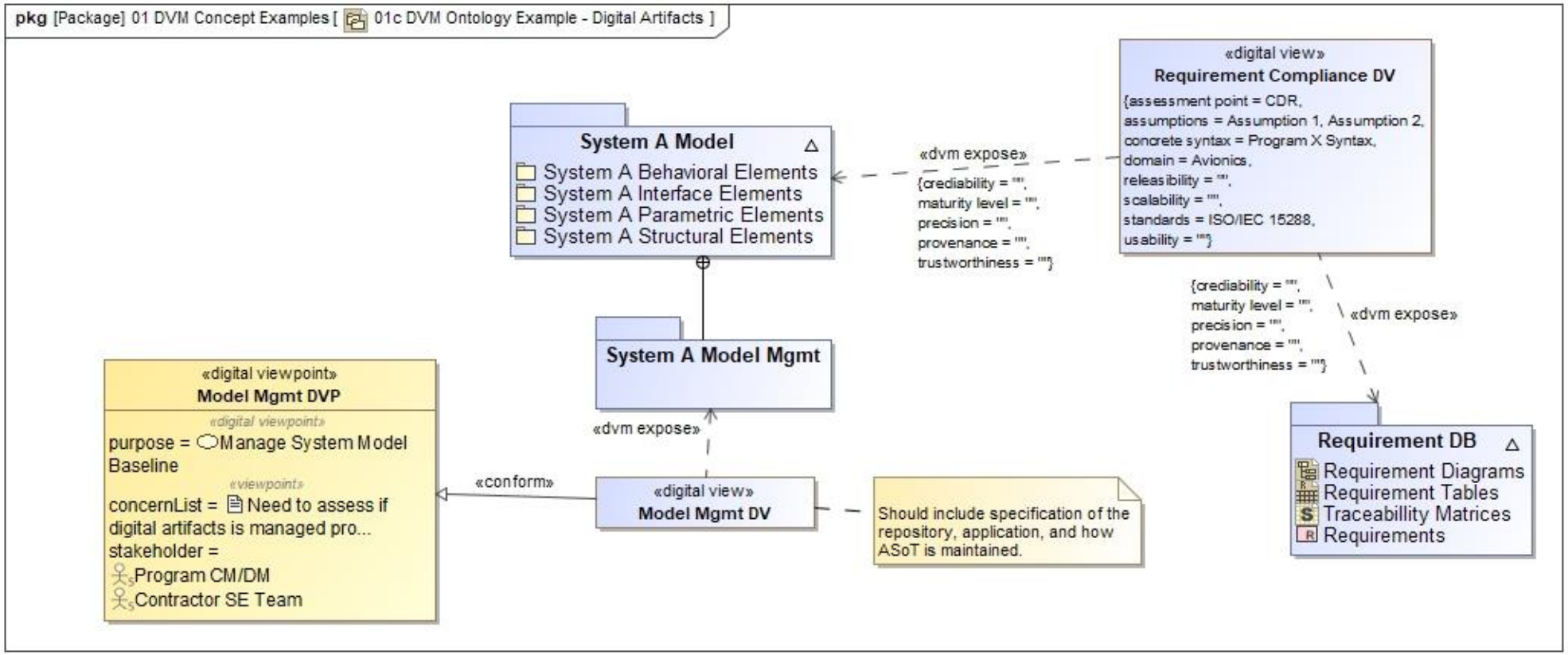
- Describe the kinds of digital information (models, databases, etc.) that comprise a digital artifact to be exchanged
- Shows how repositories and authoritative sources of truth critical in specifying pedigree of digital artifacts
- Enables specification of digital artifact quality mandate by acceptance criteria



Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

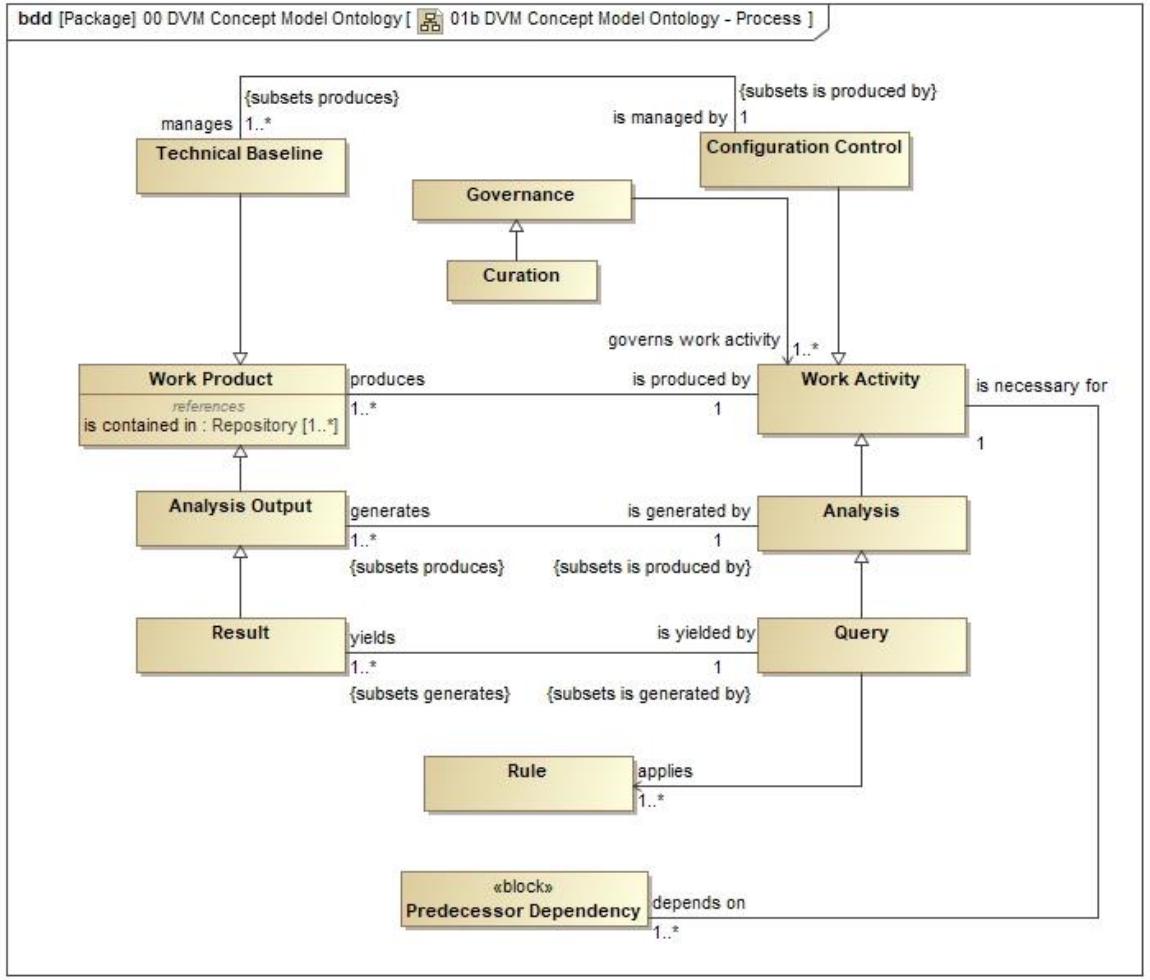
DVM: Digital Artifacts Concepts - Example



© 2022 Published and used by INCOSE with permission

DVM: Process Concepts Ontology

- This ontology specifies concepts used to describe work products and the activities that produce them
- Some specialized kinds of work products and activities can be specified
- The concepts of governance can dictate how work activity should be performed

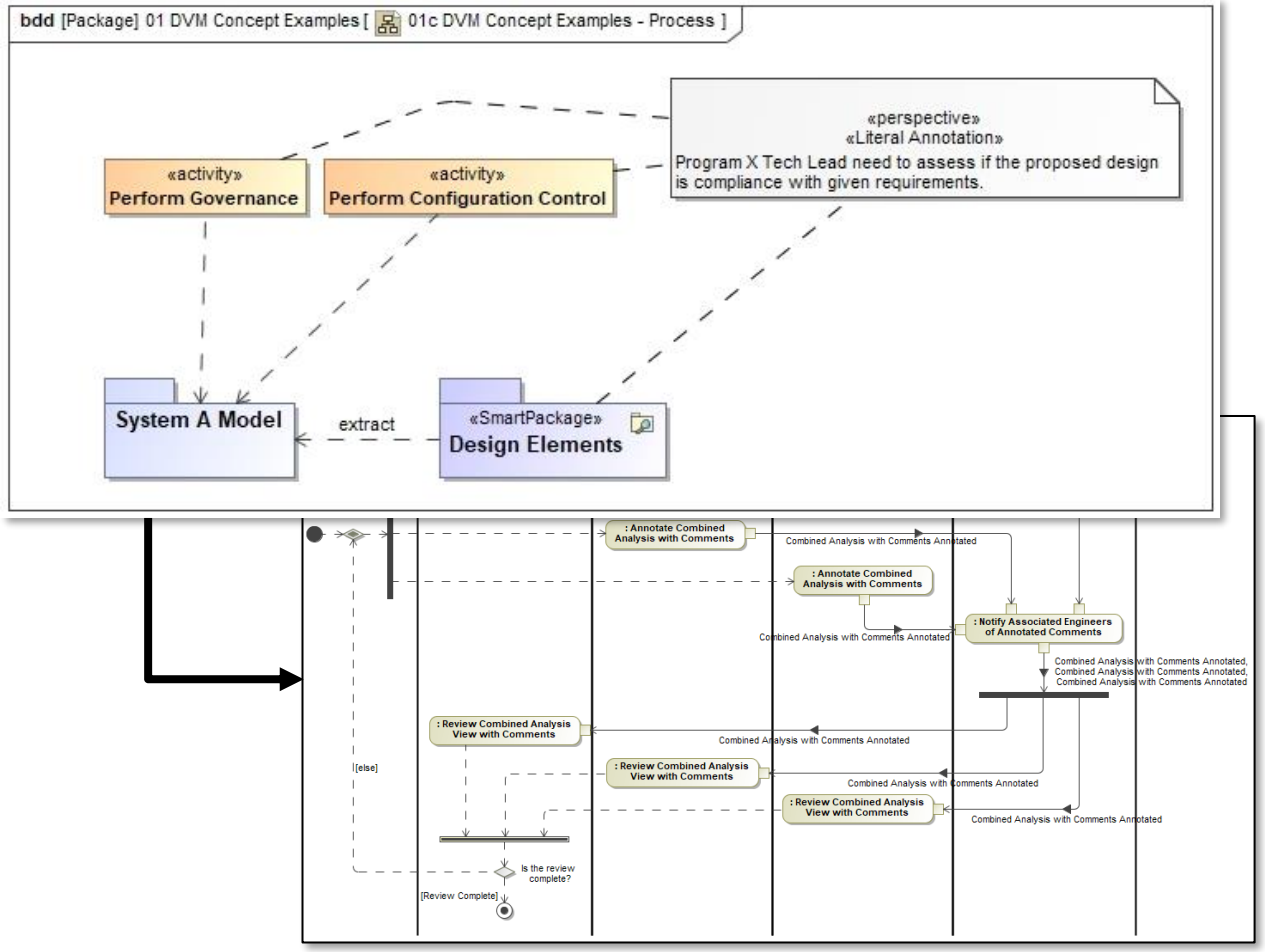


Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM: Process Concepts - Example

- Specified perspective influences how digital artifacts are produced
- Work process can be specified in series of activity flows
- Query is a type of work activity to define artifacts required for the perspective from a metamodel

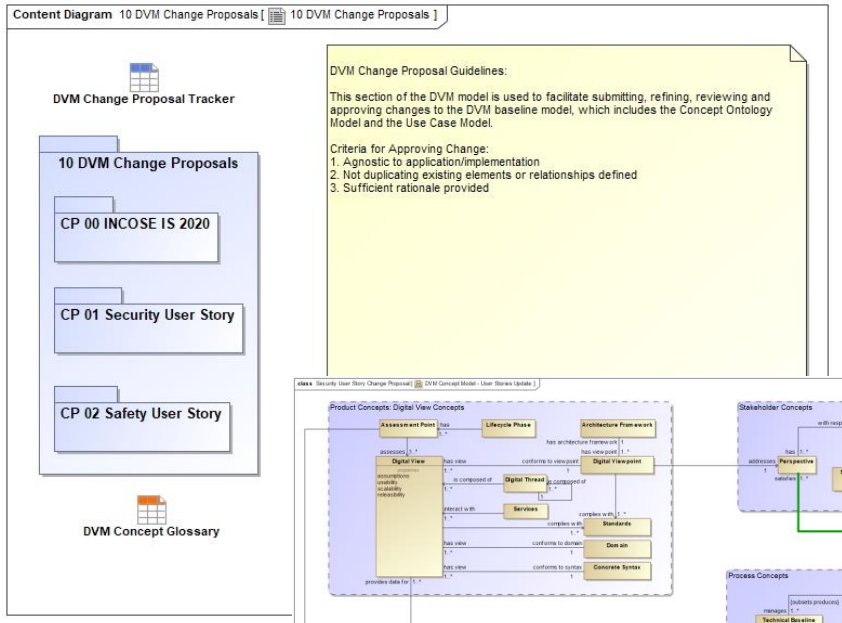


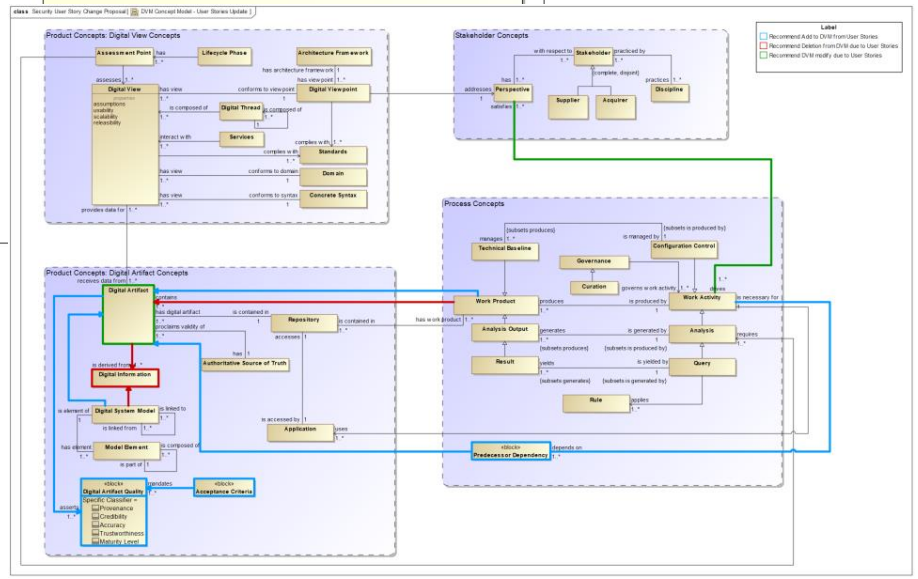
Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM Baseline Management Process (Preliminary)

- Support update to the DVM concept, or informing the DVM
- Proposed changes are tracked from major events, and through our biweekly meetings
- Preliminary process for reviewing and approving change proposals is established, include
  - Change Proposal Submission
  - Change Proposal Tracker
  - Baseline Control Board and Approval Process
- ISO change process will supersede once this becomes an approved ISO standard project



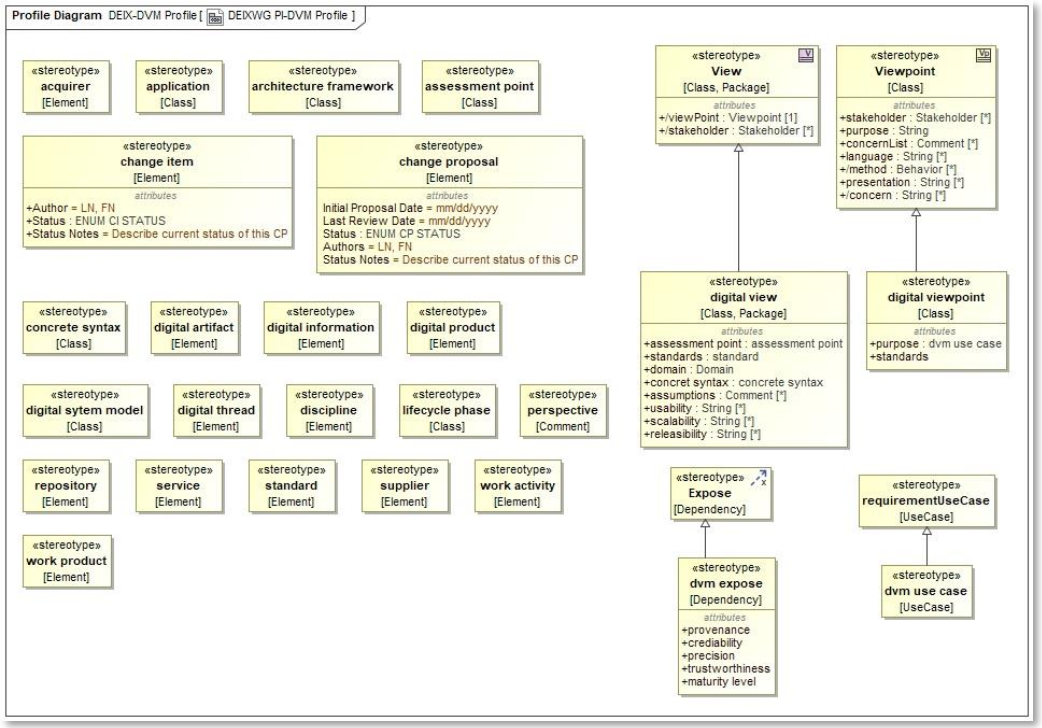


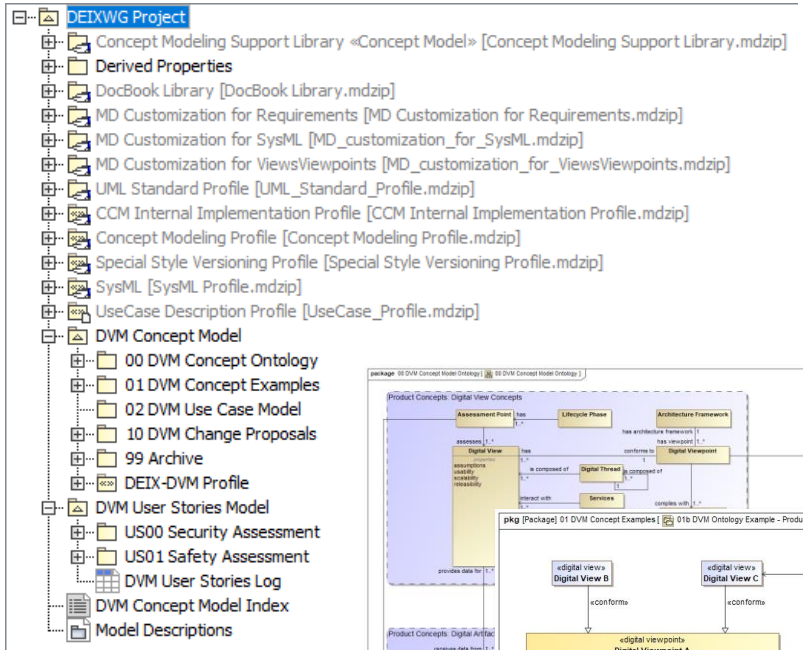
Annotated updates to the DVM

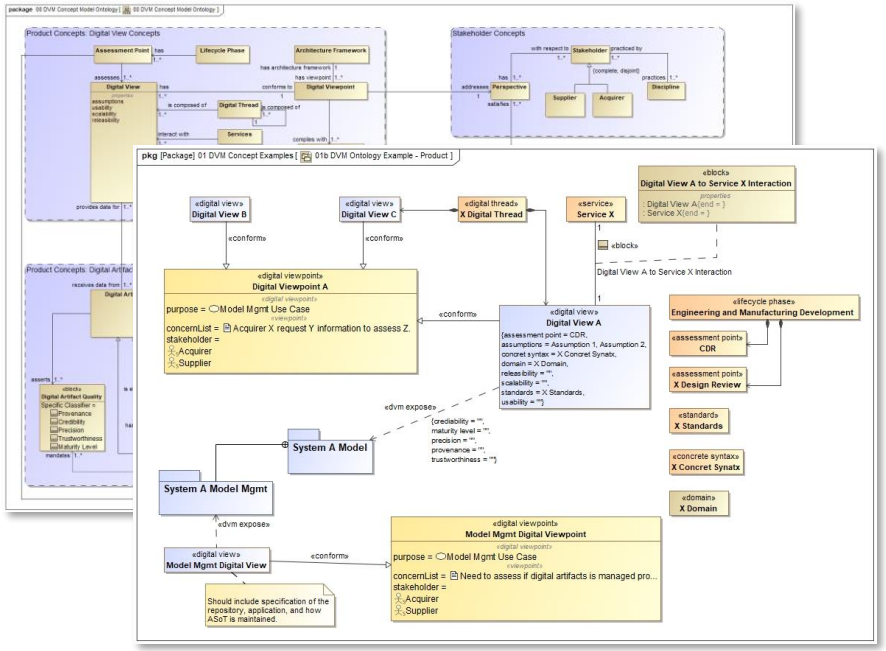
© 2022 Published and used by INCOSE with permission

DVM Products

- DVM Baseline Model (Rev A)
  - Includes a preliminary profile
- Access via INCOSE DEIX Teams



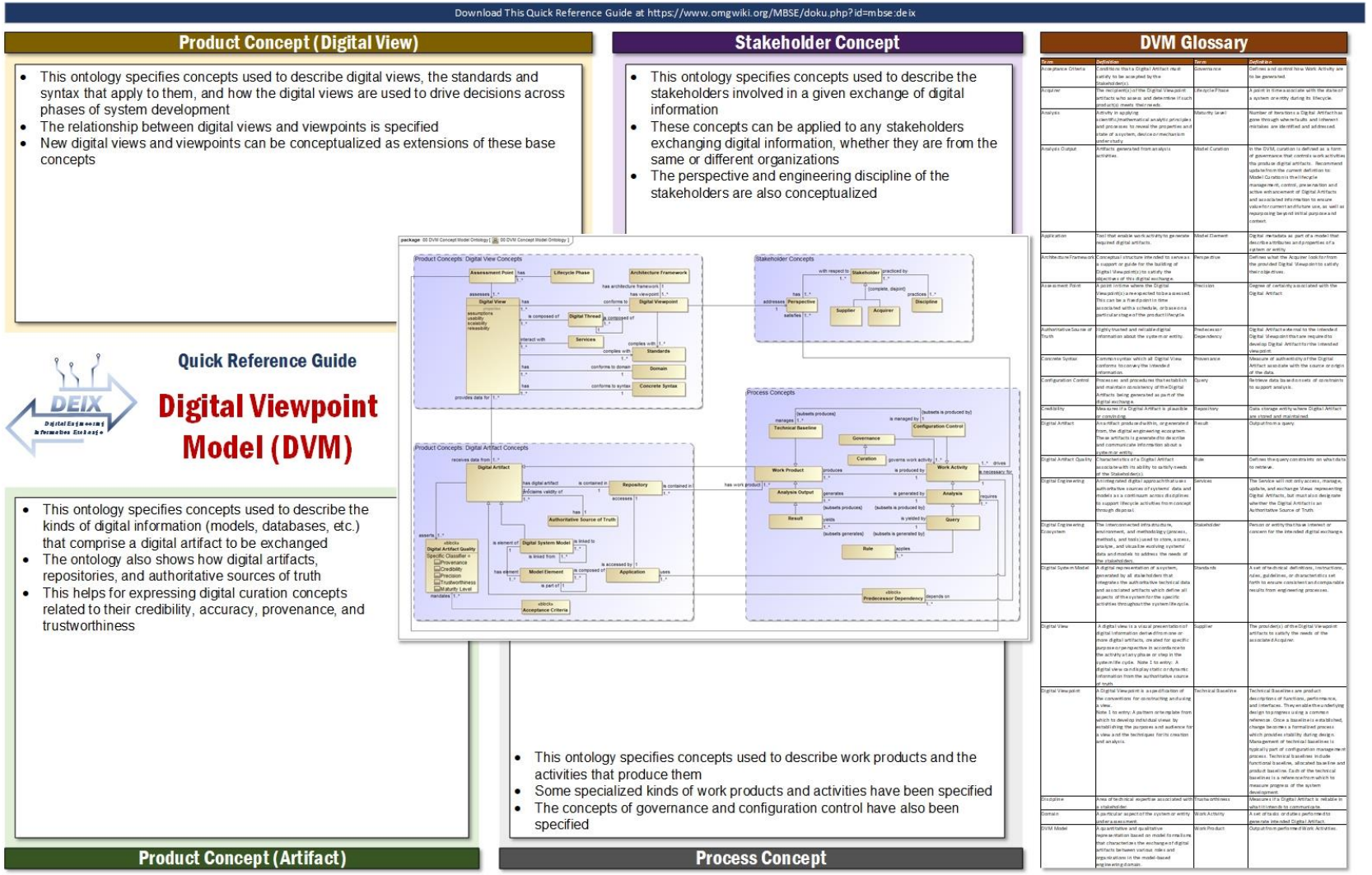




© 2022 Published and used by INCOSE with permission

DVM Products

- DVM Quick Guide



Distribution Statement A. Approved for public release

© 2022 Published and used by INCOSE with permission

DVM Products

- DVM Use Case Template
  - Facilitate the specification of user story that involves a digital exchange

Use Case ID:	
Use Case Name: *(Should be the use case goal as a short active verb phrase)*	
Goal In Context: *(Longer statement of the goal, if needed)*	
Precondition(s): *(Assumed state of the world at start)*	
Success End Condition: *(State of the world upon successful completion)*	
Failed End Condition: *(State of the world if goal abandoned)*	
Primary Actor(s): *(User(s) who have defined the user goal and often, but not always triggers the use case)*	
Supporting Actor(s): *(User(s) who provide an external service to the use case)*	
Trigger(s): *(Event(s) that start the use case)*	
Use Case Author(s): *(Name(s) and Organization(s))*	

Main Success Scenario:
(Steps of the scenario from trigger to goal delivery and any cleanup after)

Step #:	***Step Description:***
1.a	Systems Engineers develop the following in the Digital Engineering System (DES): • Aircraft-level Requirements • Preliminary System Architecture (Logical and Functional)
1.b	Safety Engineers provide the following to the Systems Engineers in the Digital Engineering System: • Preliminary Aircraft Safety Assessment in forms of requirement or constraints
1.c	Security Engineers provide the following to the Systems Engineers in the Digital Engineering System: • Preliminary Aircraft Security Risk Assessment in forms of requirement or constraints
2	Digital Engineering System generates a Combined Supporting Analysis for Functional Allocation View and provides the view to the System Engineers, Safety Engineers and Security Engineers
3	System Engineers, Safety Engineers and Security Engineers review the view content
4	System Engineers, Safety Engineers and Security Engineers annotate view content with comment and feedback in the Digital Engineering System
5	Digital Engineering System provides the updated view with the annotated comments to the System Engineer, Safety Engineer and Security Engineer
6	Systems Engineer updates Functional Allocation after agreement from all Associated Engineers in the Digital Engineering System

Extensions:
(Any alternative actions to a scenario step. State the affected step, condition and branching action.)

Affected Step #:	***Condition:***	***Branching Action:***
4, 5	Systems Engineer requires further feedback from the engineers before proceeding	• The use case steps 4 & 5 are revisited depending on the input views that need to be updated and re-generated
4, 5	Systems Engineer requires updated views from the Commenting Engineers before proceeding *(Not modeled for simplicity)*	• The use case steps 1-3 are revisited depending on the input views that need to be updated and re-generated

© 2022 Published and used by INCOSE with permission

DEIX Use Case Workshop Concept

Distribution Statement A. Approved for public release

DEIX Workshop Description

- Demonstrate a methodology for defining digital view requirements for a stakeholder purpose in a selected domain
- This methodology can be used by organizations to develop their own digital engineering metamodels

© 2022 Published and used by INCOSE with permission

DEIX Workshop – Methodology Overview

- The methodology has the following basic workflow:
  1. Identify the engineering processes of interest
  2. Define the use case descriptions and the process workflows
  3. Identify the required views from the process workflows
  4. Develop implementation plans and examples for the required views
  5. Identify updates for the digital engineering metamodel (DVM)
  6. Repeat for additional engineering processes and use cases

- For the workshop, we plan to demonstrate this workflow:
  - We've already developed a use case description and required views from a process in the aircraft manufacturing industry (steps 1-3)
  - We plan to demonstrate steps 4 and 5 in the workshop

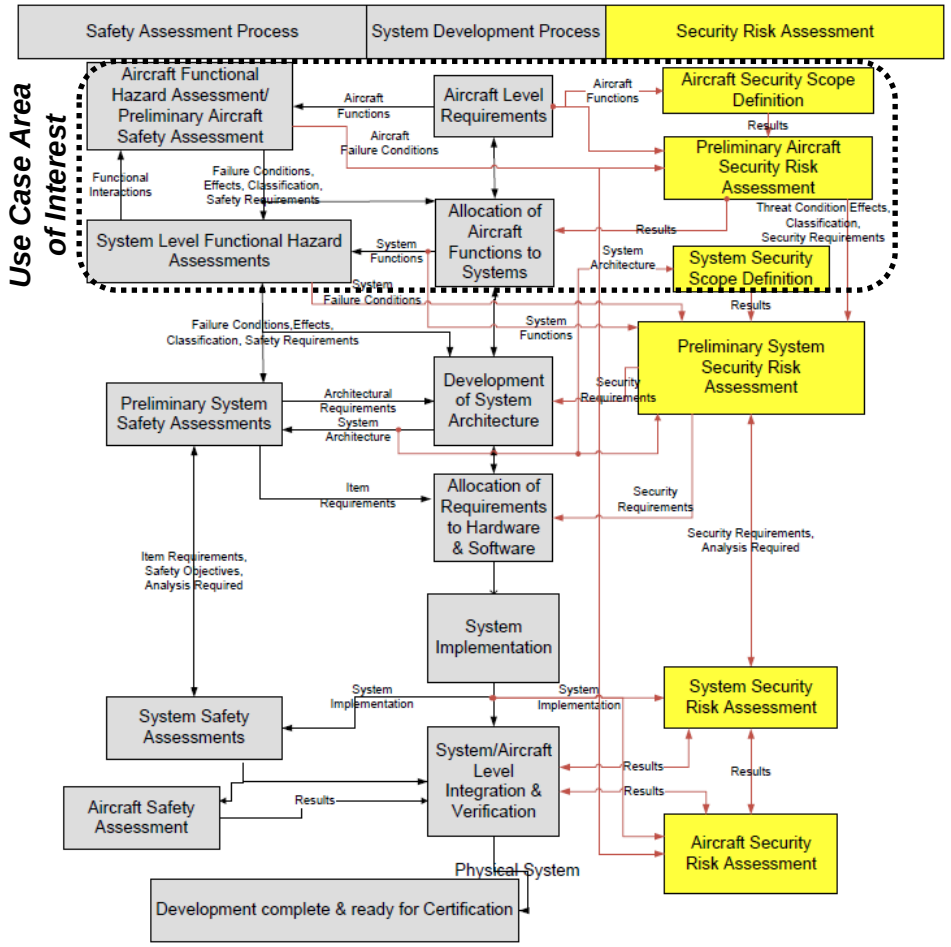
Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Process and Use Case of Interest

- The process of interest is the aircraft system development process combined with safety assessments and security risk assessments
  - This is adapted from EUROCAE's Airworthiness Security Process Specification (ED-202A)

- The use case of interest is "Develop the Functional Allocation incorporating Aircraft Safety and Security Risk Assessment Processes"
  - This is a subset of the full ED-202A process
  - Provides a unique challenge for information exchange
    - Not a traditional "point-to-point" exchange
      - e.g. Safety Engineer to Systems Engineer
    - Rather the use case includes "combined views" across the three domains (systems engineering, safety engineering and security engineering)

EUROCAE ED-202A Process Flow



Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Use Case Template

- For the workshop, we developed a use case template for the DEIXWG to use
  - Most of the attributes of the template are from Alistair Cockburn's Writing Effective Use Cases
  - Some of the attributes are custom attributes created to support better support the DEIXWG effort
  - Each attribute has a definition and instructions
- We used this template for the use case for the workshop

INCOSE DEIXWG Functional Use Case Definition

This form is to describe a functional use case in support of the INCOSE DEIXWG for the development of the Digital Viewpoint Model (DVM). This use case description describes the core functional attributes of a desired process with the intention of assisting the development of the DVM. Many of the use case attributes are taken from "Writing Effective Use Cases" by Alistair Cockburn with some alterations and additions for DVM development. This description must stay implementation-agnostic. This description DOES NOT describe what the DVM is capable of doing. This is only a mechanism to assist in the DVM's development.

Characteristic Information

Use Case ID:	1
Use Case Name: *(Should be the use case goal as a short active verb phrase)*	Develop the Functional Allocation incorporating Aircraft Safety and Security Risk Assessment Processes
Goal In Context: *(Longer statement of the goal, if needed)*	Systems engineering develops/refines the design and allocation of aircraft's system functions to the aircraft's systems guided by the information from the preliminary aircraft safety assessment and preliminary aircraft security risk assessment. This use case is an adaptation of the EUROCAE Airworthiness Security Process Specification (ED-202A). This use case focuses on a subset of the full process flow (see *DEIXWG Additional Information – Supporting Documentation*). This is a comprehensive adaptation of that process since the original EUROCAE ED-202A process is from the mindset of Security Engineering. This use case serves as a predecessor to the assignment of Development Assurance Level and Security Assurance Level.

Precondition(s): *(Assumed state of the world at start)*	• The following information has been defined:
	  ○ Aircraft-level Requirements
	  ○ Preliminary System Architecture (Logical and Functional)
	• The following assessments have been completed:
	  ○ Preliminary Aircraft Safety Assessment, which includes tailoring of applicable requirements/controls for the target system
	  ○ Preliminary Aircraft Security Risk Assessment, which includes tailoring of applicable requirements/controls for the target system
	• While system architecture is not baselined (Prior to PDR)

Success End Condition: *(State of the world upon successful completion)*	Updated functional allocation incorporating the preliminary aircraft safety and security risk assessments, with adequate substantiation information/data to

Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Use Case Template Attributes

- Some Use Case Template Attributes:
  - Use Case Name
  - Goal In Context
  - Precondition
  - Success End Condition
  - Failed End Condition
  - Primary Actor(s)
  - Supporting Actor(s)
  - Trigger(s)
  - Use Case Author(s)
  - Main Success Scenario
  - Applicable Technical Processes
  - Required Views

INCOSE DEIXWG Functional Use Case Definition

This form is to describe a functional use case in support of the INCOSE DEIXWG for the development of the Digital Viewpoint Model (DVM). This use case description describes the core functional attributes of a desired process with the intention of assisting the development of the DVM. Many of the use case attributes are taken from "Writing Effective Use Cases" by Alistair Cockburn with some alterations and additions for DVM development. This description must stay implementation-agnostic. This description DOES NOT describe what the DVM is capable of doing. This is only a mechanism to assist in the DVM's development.

Characteristic Information

Use Case ID:	1
Use Case Name: *(Should be the use case goal as a short active verb phrase)*	Develop the Functional Allocation incorporating Aircraft Safety and Security Risk Assessment Processes
Goal In Context: *(Longer statement of the goal, if needed)*	Systems engineering develops/refines the design and allocation of aircraft's system functions to the aircraft's systems guided by the information from the preliminary aircraft safety assessment and preliminary aircraft security risk assessment. This use case is an adaptation of the EUROCAE Airworthiness Security Process Specification (ED-202A). This use case focuses on a subset of the full process flow (see *DEIXWG Additional Information – Supporting Documentation*). This is a comprehensive adaptation of that process since the original EUROCAE ED-202A process is from the mindset of Security Engineering. This use case serves as a predecessor to the assignment of Development Assurance Level and Security Assurance Level.

Precondition(s): *(Assumed state of the world at start)*	• The following information has been defined:
	  ○ Aircraft-level Requirements
	  ○ Preliminary System Architecture (Logical and Functional)
	• The following assessments have been completed:
	  ○ Preliminary Aircraft Safety Assessment, which includes tailoring of applicable requirements/controls for the target system
	  ○ Preliminary Aircraft Security Risk Assessment, which includes tailoring of applicable requirements/controls for the target system
	• While system architecture is not baselined (Prior to PDR)

Success End Condition: *(State of the world upon successful completion)*	Updated functional allocation incorporating the preliminary aircraft safety and security risk assessments, with adequate substantiation information/data to

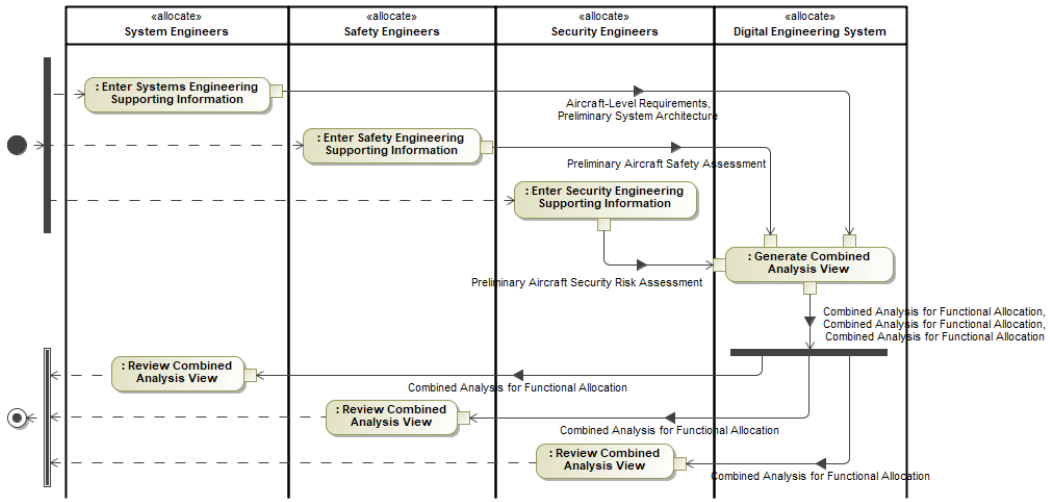
Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Use Case Main Success Scenario

- We wrote out the main success scenario for the use case in the template
- We developed a few diagrams as attachments to describe the detailed flow of the main success scenario

Scenario Information

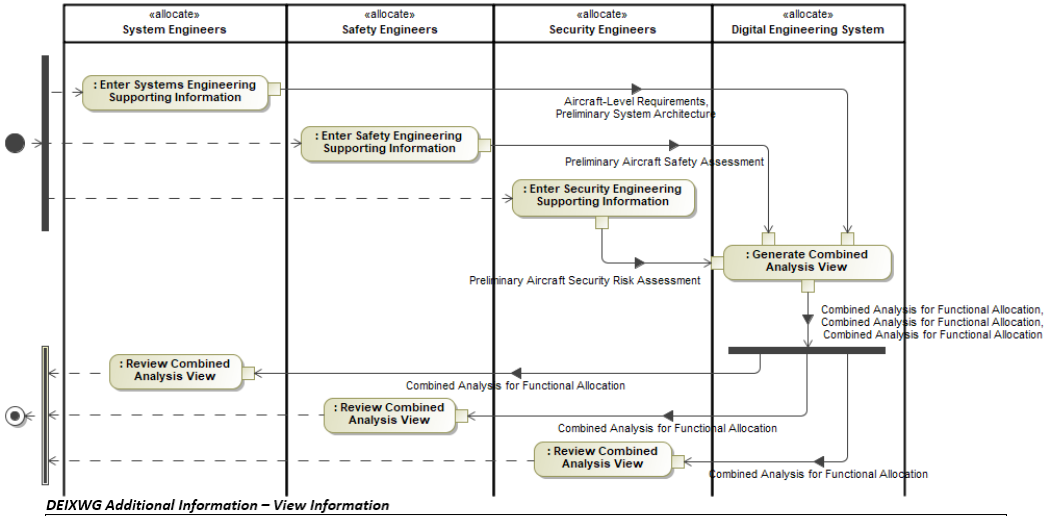
Main Success Scenario: *(Steps of the scenario from trigger to goal delivery and any cleanup after)*	
Step #:	***Step Description:***
1.a	Systems Engineers develop the following in the Digital Engineering System (DES): • Aircraft-level Requirements • Preliminary System Architecture (Logical and Functional)
1.b	Safety Engineers provide the following to the Systems Engineers in the Digital Engineering System: • Preliminary Aircraft Safety Assessment in forms of requirement or constraints
1.c	Security Engineers provide the following to the Systems Engineers in the Digital Engineering System: • Preliminary Aircraft Security Risk Assessment in forms of requirement or constraints
2	Digital Engineering System generates a Combined Supporting Analysis for Functional Allocation View and provides the view to the System Engineers, Safety Engineers and Security Engineers
3	System Engineers, Safety Engineers and Security Engineers review the view content
4	System Engineers, Safety Engineers and Security Engineers annotate view content with comment and feedback in the Digital Engineering System
5	Digital Engineering System provides the updated view with the annotated comments to the System



Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Required Views

- After we developed the detailed scenario flow, the information flows represent the views for the use case
- We defined a list of these required views from these information flows
  - We used the ED-202A to help us define the required view content
- For the workshop, we selected the "Combined Analysis for Functional Allocation" as the view for the workshop attendees to evaluate
  - It provides the DEIXWG a complicated view to evaluate



DEIXWG Additional Information – View Information

Required Views

(Any required information view in order to execute the use case. State the view name, description, view content, reviewing/consuming actor and producing actor.)

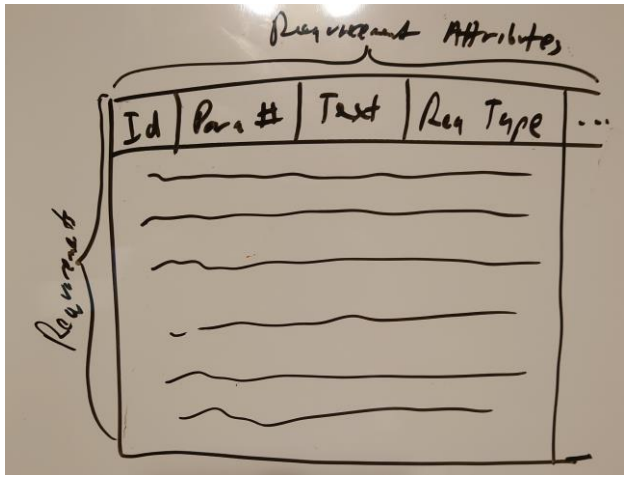
View Name:	*Description:*	*View Content*	*Reviewing / Consuming Actor:*	*Producing Actor:*
Aircraft-Level Requirements	The requirements that define the aircraft as top-level system of interest.	• Requirement Information (ID, Paragraph #, Text & Other Attributes)	**N/A for this UC* / *Captured by DES for ASOT**	System Engineers
Preliminary System Architecture (Logical and Functional)	The preliminary system architecture both logical and functional.	• Logical System Decomposition • Functional Decomposition	**N/A for this UC* / *Captured by DES for ASOT**	System Engineers
Preliminary Aircraft Safety Assessment	The preliminary assessment of aircraft's safety/functional hazards.	• Failure Conditions • Failure Effects • Affected System Functions • Safety Requirements	System Engineers	Safety Engineers
Preliminary Aircraft Security Risk Assessment	The preliminary assessment of aircraft's security risks.	• Security Scope (Environment & Perimeter) which defines this Assessment • Threat Conditions • Threat Effects • Affected System Functions • Security Requirements	System Engineers	Security Engineers
Combined Analysis for Functional Allocation	Combines the information from systems engineering, safety engineering and security engineering to assist with functional allocation.	• Affected System Functions • Related Safety & Security Requirements • Related Safety & Security Supporting Information (e.g. Failure Conditions, Failure Effects, Threat Conditions, Threat Effects, etc.)	• System Engineers • Safety Engineers • Security Engineers	• System Engineers • Safety Engineers • Security Engineers
Combined Analysis with Comments Annotated	Same as the "Combined Analysis for Functional Allocation" but with "Comment/Feedback Items" annotated.	• Combined Analysis for Functional Allocation • Attached Comment/Feedback Items	• System Engineers • Safety Engineers • Security Engineers	• System Engineers • Safety Engineers • Security Engineers
System Functional Allocation	The allocation of system functions to system components.	• System Function Mapping (Mapping of functions to system components)	**N/A for this UC* / *Captured by DES for ASOT**	System Engineers

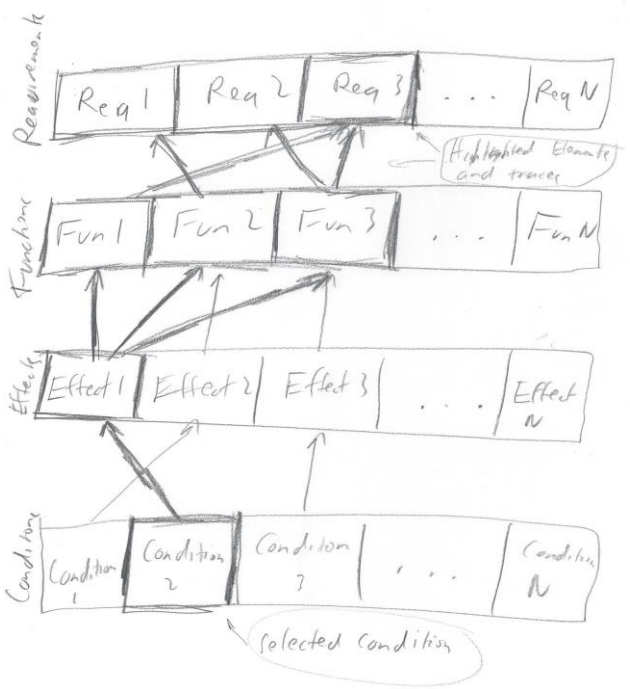
Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Sample Example Views

- Workshop attendees will come up with example implementations of the required view
  - Workshop attendees will have the completed use case template, required view information and any other attachments as reference
  - Workshop attendees will have materials (whiteboard, paper, pencils, etc.) to prototype sketch examples of the view
  - Workshop attendees will be broken up into groups and will collaborate with their fellow group members on their view examples

- Here are some potential examples using other required views from the use case

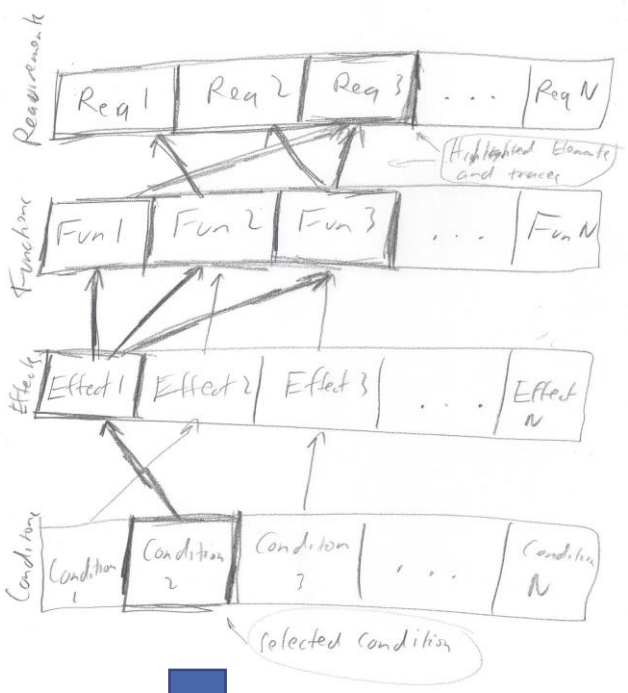


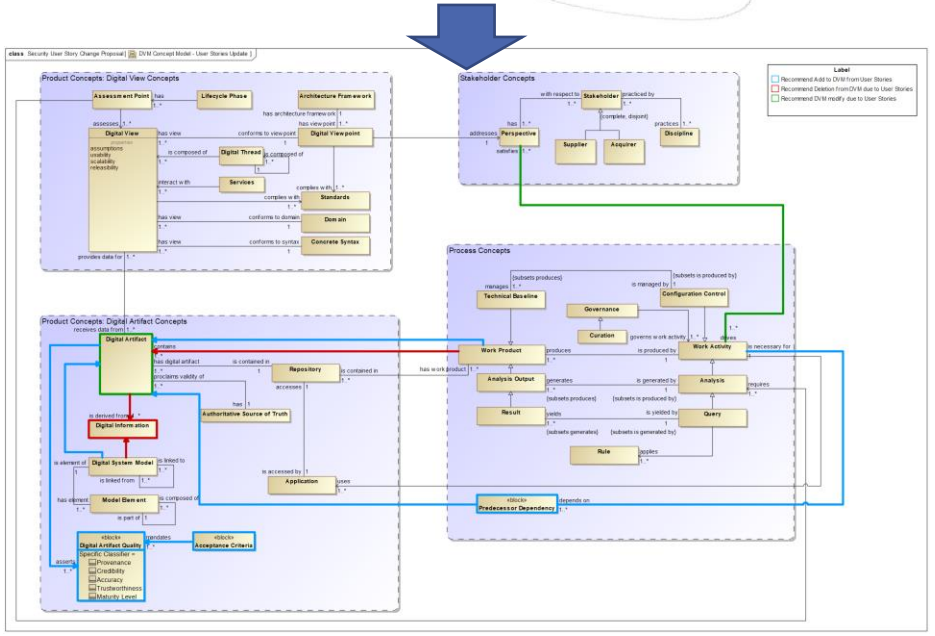


Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DEIX Workshop – Informing the DVM

- After developing their implementation examples, workshop attendees will use their example to inform the DVM
  - Workshop attendees will make recommendations to the DVM which align with their implementation
  - Since workshop attendees will be broken up into groups, the groups will get to compare their use case implementation and DVM recommendations with the other groups





Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

DVM – Next Steps

- Industry
  - Participate in future DVM meetings
  - Contribute to the DVM definition
  - Develop products to enable usage of the DVM
- DVM Use Case Workshop at INCOSE IW2023
- Support incorporation of DVM method to ISO 15288 standards; guidance document
- Forming a standard for the DVM concept itself; similar to ISO 42010

Distribution Statement A. Approved for public release
© 2022 Published and used by INCOSE with permission

References

Reference	Description
DEIX INCOSE Teams	https://incose2.sharepoint.com/:f:/r/sites/DEIXWG/Shared%20Documents/Standards%20Framework?csf=1&web=1&e=j3rb3C
Glossary of Key DEIX Terms	DEIX Topical Encyclopedia Entries (DEIXPedia)
Digital Engineering	Digital Engineering References on the OMG MBSE Wiki Page
DEIXWG on OMG MBSE Wiki	OMG Wiki Page for DEIXWG
INCOSE DEIXWG Page	INCOSE WG Page for DEIXWG

© 2022 Published and used by INCOSE with permission

Raytheon Technologies

Building a Digital Engineering Ecosystem using Syndeia

Julie DeMeester
Deborah Thomas
Raytheon Missiles and Defense

November 2022

© 2021 Raytheon Technologies Corporation.
All rights reserved.

Raytheon Approved for Public Release
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.

Digital Engineering Terminology

- The DoD defines digital engineering as an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.
- The DAU Glossary defines a digital engineering ecosystem as an interconnected infrastructure, environment, and methodology (process, methods, and tools) used to store, access, analyze, and visualize evolving systems' data and models to address the needs of the stakeholders.
- Digital threads are extensible analytics frameworks to connect models and all associated data, software, and functional support governing more than one system lifecycle phase with one-to-one real-world traceability.*
- Challenge: Different tools (data repositories) are used in the design, development, deployment and sustainment of a system. Many/Most of these tools do not integrate with each other, so we need an integration platform (or a digital engineering ecosystem) that can interconnect these tools.

*Dr. Will Roper, There is no Spoon: The New Digital Acquisition Reality

Raytheon Approved for Public Release
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.

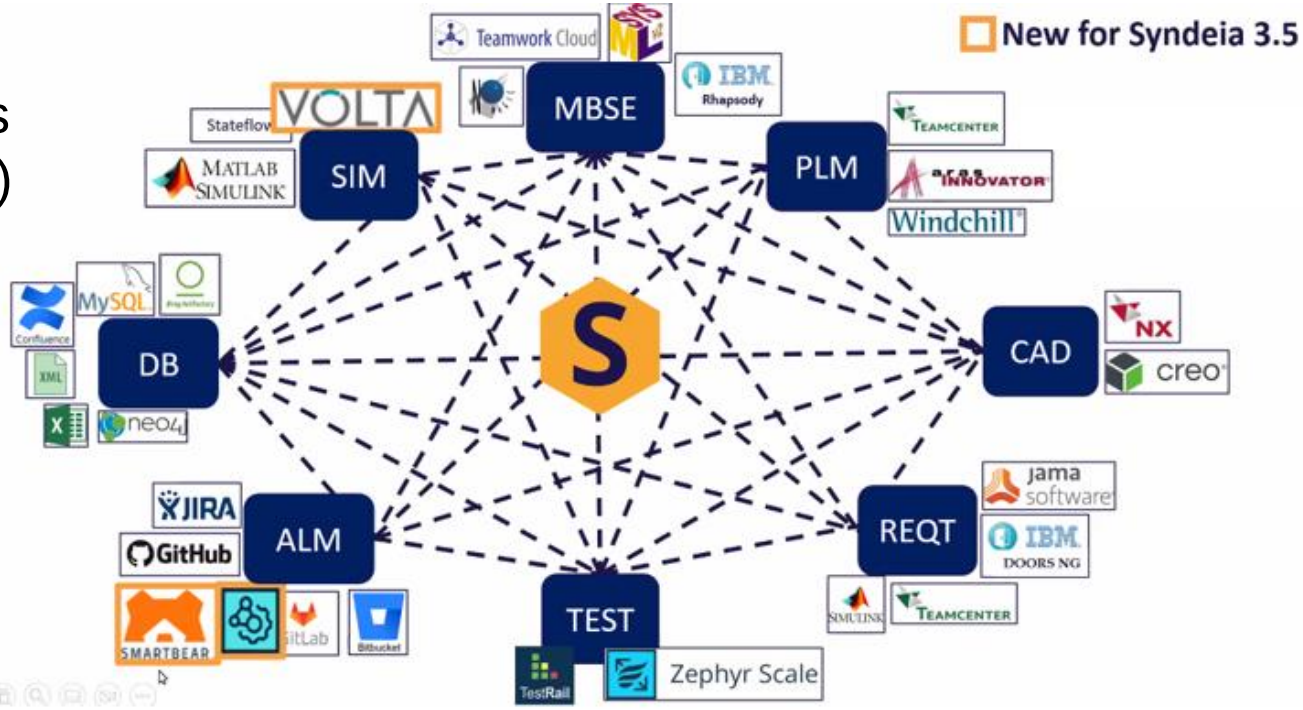
Digital Engineering Use Case

- Provide system stakeholders with visibility into the system.
- For example….
  - *Determine Impact of a Change to the System (e.g., Requirement, Model, Part)*
  - *Determine Impact of Simulation to the System (e.g., Validate or Invalidate a Requirement)*
- To do this, I will need a digital engineering ecosystem that …
  - *Enables the integration of data repositories, i.e., requirements database, SysML model, PLM system*
  - *Provides a framework for creating digital threads across data repositories*
  - *Provides a mechanism for Querying / Visualizing Digital Threads*
  - *Provides a way to Compare/Sync Data Repositories*
  - *Is able to perform model/data transformations, e.g., DOORS-Next Requirement -> SysML Requirement*

Raytheon Approved for Public Release
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.

Intercax's Syndeia Digital Engineering Platform

- Syndeia is a software that uses a SysML System Architecture model as the mechanism to coordinate with other models in other engineering tools (e.g., Creo, DNG) and data repositories (Simulink, MySQL)
- Syndeia provides capabilities for building, managing, analyzing, querying, and visualizing the digital thread of the product/system through its lifecycle.
- Syndeia builds on open standards (e.g. REST/HTTP, JDBC, and OSLC) and production ready APIs



Raytheon Technologies
Raytheon Approved for Public Release
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.

Why Syndeia ?

- Syndeia satisfied the program's digital engineering requirements
- Provided out-of-the-box integrations with the desired tools in our digital engineering environment
  - Cameo System Modeler, DOORS-Next, Creo, Teamcenter, others
- Not many commercially available digital engineering ecosystems to choose from in late 2020
- Intuitive user interface
- Lots of videos and tutorials for getting started

Raytheon Approved for Public Release
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.

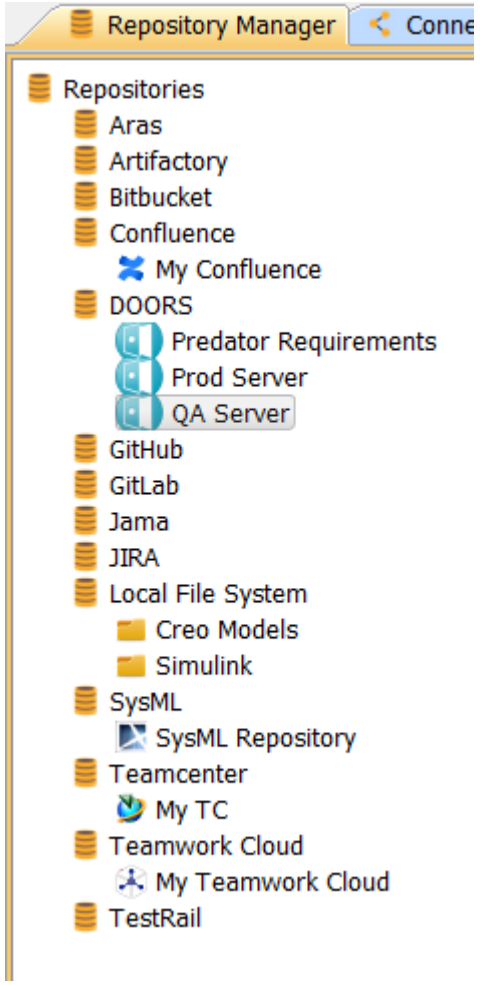
Syndeia Services

Syndeia Services	Description
Search	Query the entire digital design for related elements based on the search criteria. The search returns a list or graphical representation of design elements in each repository.
Connect	Create a persistent connection between selected design elements within their respective configuration controlled repository.
Access	Allow the user to access the design element in its native format and tool if the user has the required access permissions.
Transform	Transform a design element from one format to another. For example, a transform allows a user to create SysML requirements from DOORS-NG requirement modules.
Compare	Allows the user to compare a digital thread with the current design data in the SSoT identifying differences.
Synchronize	Allows the user to accept and update one design element based on a change in another element. For example, if the current requirement in DOOR-NG has changed, the user can accept and update the corresponding requirement in the SysML model.

Raytheon Approved for Public Release
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.

Syndeia Digital Ecosystem Environment

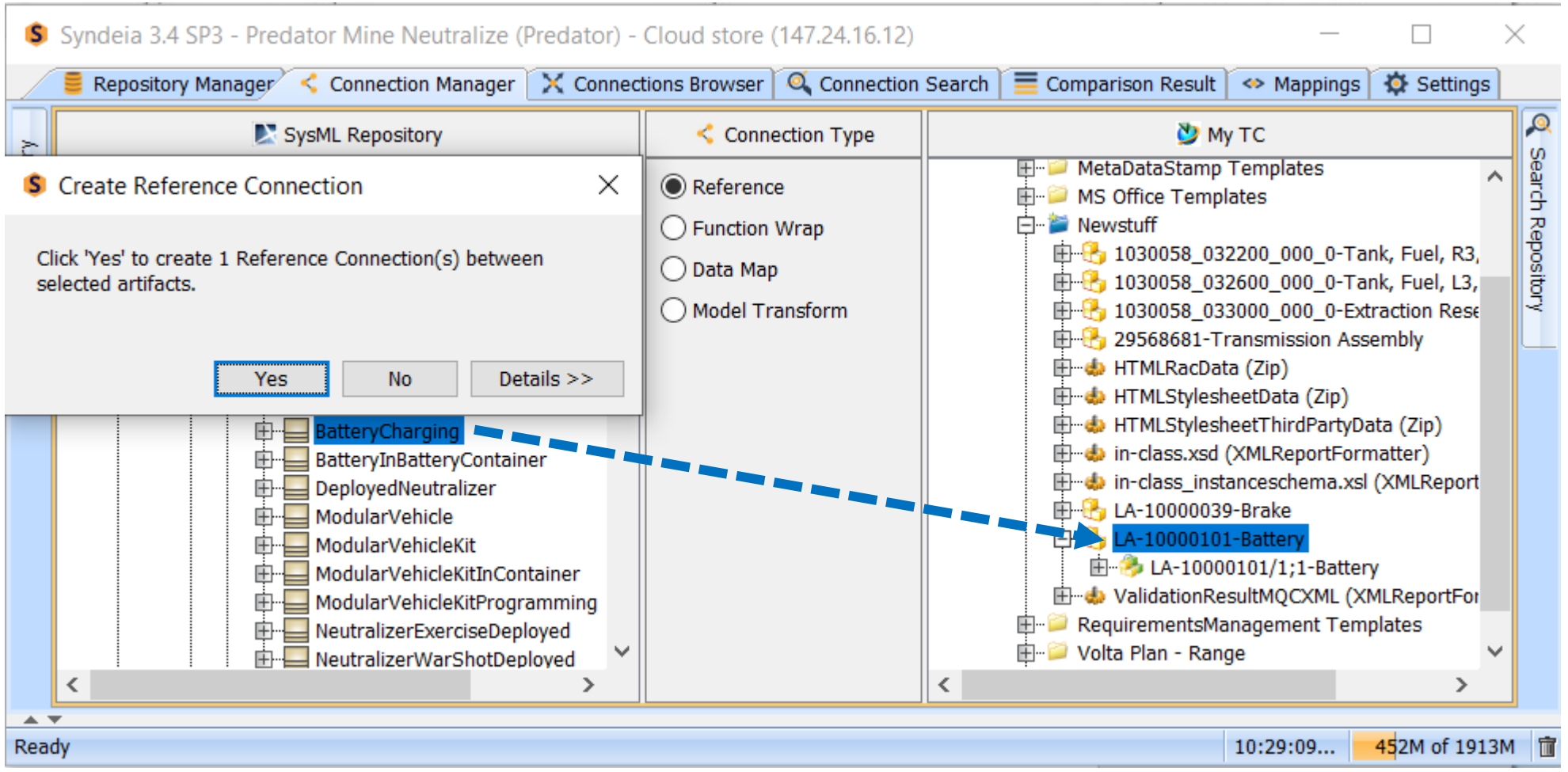
- Syndeia v3.4 MagicDraw Plugin and Syndeia Cloud
- Program's Data Repositories
  - Cameo EA and Teamwork Cloud
  - DOORS-NG
  - Teamcenter
  - Creo
  - Jira
  - GitHub
  - MySQL
  - Volta (MDAO) coming in v3.5
  - Matlab/Simulink
  - Excel



Raytheon Approved for Public Release
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.

Syndeia Reference Connections

- Drag and Drop Reference Connection aka Digital Threads are created between engineering artifacts. For example, a Creo model or part (managed in Teamcenter) and a SysML block.

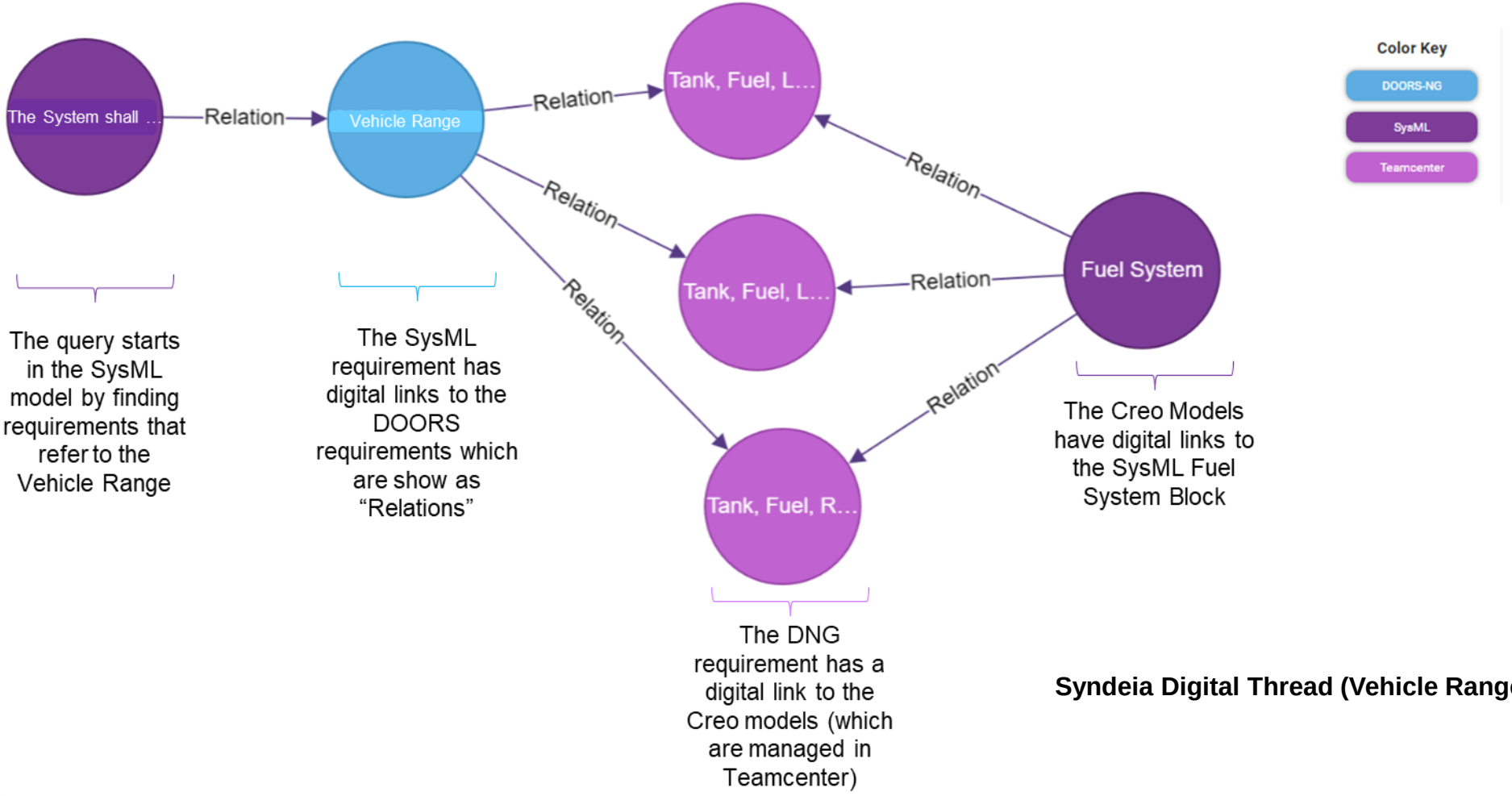


Raytheon Technologies

Raytheon Approved for Public Release
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.

Syndeia Digital Thread Example

This Syndeia digital thread query shows the digital thread for the Vehicle Range from its system requirement, to the DOORS-Next performance requirement to the digital design models (e.g., Creo) to the physical block in the SysML model. Note that the Creo models are configured managed in Teamcenter. This digital thread is used to conduct impact analysis. For example, if the vehicle requirement changes, we can understand the downstream impacts.



Syndeia Digital Thread (Vehicle Range Example)

Raytheon Technologies
Raytheon Approved for Public Release
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.

Impressions

- Syndeia is good at connecting artifacts across different engineering repositories, e.g., DNG, Teamcenter, etc.
- Meets the current needs of our programs.
- Cameo is being used as the main user interface to coordinate with other models in other engineering domains, e.g., DNG, Creo, etc.
- Syndeia Web Console is the main user interface to visualize digital thread
- “Local Repositories” should not be used (because they are local!)
- Besides Syndeia Reference Connections (digital threads), Syndeia provides a useful model transformation between DNG requirements and SysML requirements
  - Syndeia provides other types of transformations, such as SysML IBD <-> Simulink but this may blur the lines between which model is the source of truth
- Defined process for creating “reference connections” is required
  - Who creates and manages the links
  - so that directionality of the link is consistent (or it gets confusing when you are visualizing the graph)
- Syndeia provides a lot of videos and training material

Raytheon Approved for Public Release
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.

Digital Engineering Lessons Learned

- Define the process for creating “reference connections”
  - Who creates and manages the links
  - Directionality of the link are consistent. Note: SysML is always identified as the source of the link.
- Identify what types of links (digital threads) you want to create. For example:
  - Create reference connections from DOORS-NG functional requirement(s) to its SysML <<functional>> block to show a <<satisfy>> relationship
  - Create reference connections from a Teamcenter part/item/assembly to a <<physical>> SysML block to show a <<satisfy>> relationship
- Establish operational and QA environments for Syndeia
  - For testing out new patches and upgrades
  - QA environment for training / experimentation
- Use caution if using “Local Repositories” (because they are local!)
- Configuration manage your data repositories
  - Teamwork Cloud for Cameo
  - Global Configuration Management (GCM) for DOORS-Next

Raytheon Approved for Public Release
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.

Digital Engineering Lessons Learned (continued)

- Use Syndeia Dashboard for adding repositories and defining reference connections
  - Syndeia Dashboard uses URLs to connect to data repositories
  - Creating reference connection is drag and drop action
- Use Syndeia Web Console for visualizing digital threads.
  - Syndeia Web Console uses web interface to connect to data repositories
  - Creating reference connections is based on a series of menu items (that can be confusing)
- Once you get a data repository connected it will show up in both the Dashboard and the Web Console.
- Customer wanted “digital thread” as a deliverable, but customer did not have or would have Syndeia as part of its digital acquisition environment. Workaround was to export reference connections in Excel and deliver that.

Raytheon Approved for Public Release
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.

Digital Engineering Lessons Learned (continued)

- Use Syndeia Dashboard for adding repositories and defining reference connections
  - Syndeia Dashboard uses URLs to connect to data repositories
  - Creating reference connection is drag and drop action
- Use Syndeia Web Console for visualizing digital threads.
  - Syndeia Web Console uses web interfaces to connect to data repositories
  - Creating reference connections is based on a series of menu items (that can be confusing)
- Once you get a data repository connected, it will show up in both the Dashboard and the Web Console.
- Customer wanted “digital thread” as a deliverable, but customer did not have or would have Syndeia as part of its digital acquisition environment. Workaround was to export reference connections in Excel and deliver that.

Raytheon Approved for Public Release
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.

Bio

- Julie DeMeester is an Engineering Fellow with Raytheon Missiles and Defense in Tewksbury, Massachusetts. Julie has been with Raytheon for over 16 years and has worked Enterprise and System of Systems Architecture on a variety of Raytheon Programs. Julie is currently actively involved in Raytheon's Model Based Engineering and Digital Engineering Initiatives.
- Contact Information
  - julied@raytheon.com (978) 604-4234
- Deborah Thomas is a Raytheon Missiles and Defense senior technical leader supporting the Land Warfare and Missile Defense department from her Alabama remote location. Deborah is a Model Based Systems Engineering (MBSE) and Engineering Digital Thread subject matter expert and co-chair of the Raytheon MBSE Technical Interchange Group.
- Contact Information
  - Deborah.R.Thomas@RTX.com (256) 361-8374

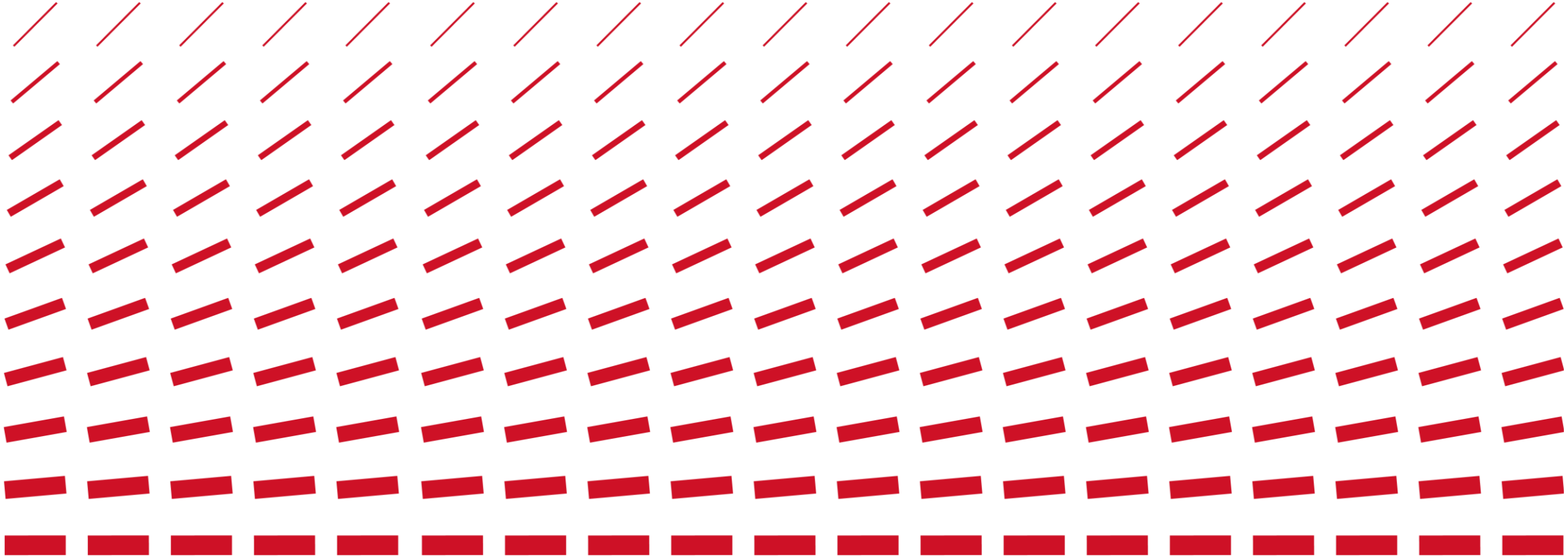
Raytheon Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Abstract

A Digital Engineering (DE) ecosystem provides the interconnected infrastructure used to store, access, analyze, and visualize evolving systems' engineering artifacts (models and data) throughout its lifecycle. It is comprised of interconnected digital models, data repositories and engineering environment that enables the creation of the systems' digital thread. Model Based Engineering (MBE) is a critical component to our DE approach. MBE is an integrated engineering approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal. This presentation will discuss creating a digital engineering ecosystem using Syndeia from Intercax and the associated digital engineering use cases and processes for creating the digital thread.

Raytheon Approved for Public Release
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.



Raytheon Technologies

Raytheon Approved for Public Release
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 GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Improved Data Fusion in Digital Twins: A Requirements Analysis

Laura Hugill
PhDc, The George Washington University
Principal Systems Engineer, Raytheon Solipsys

Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Overview

- Digital Twins in Defense
- Data Fusion Techniques
- Requirements
- Path Forward

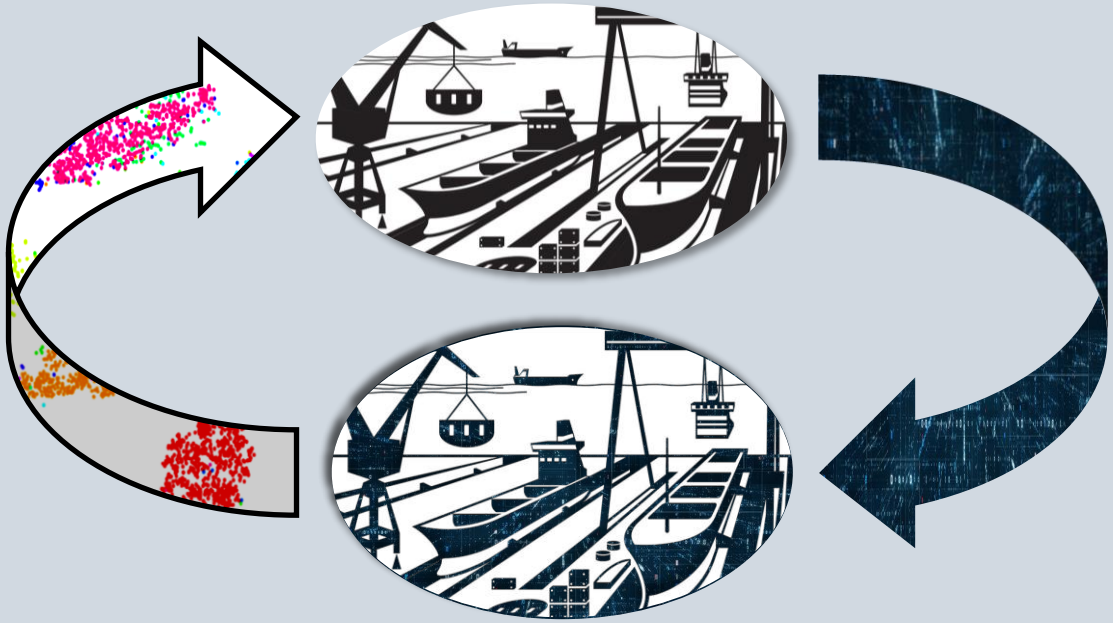
Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Digital Twins (DTs)

Digital instantiation of a physical system with synchronized, bidirectional data sharing

- Modeling and Simulation
- Integration and Test
- Maintenance
- Optimization



Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

DTs in US Defense Industry

applied sciences

MDPI

Article

Developing a Digital Twin and Digital Thread Framework for an 'Industry 4.0' Shipyard

Toh Yen Pang [1,*], Juan D. Pelaez Restrepo [1], Chi-Tsun Cheng [1]

[1] School of Engineering, RMIT University, B
juan.pelaez.restrepo@rmit.edu.au (J.D.P.R.)
s3588698@student.rmit.edu.au (A.Y.); s377
[2] MEMKO Systems, Melbourne, VIC 3000, A
* Correspondence: tohyen.pang@rmit.edu.a

Abstract: This paper provides an overvi
thread technology in industrial operatio
advantage of improving the efficiency o
important element of the Industry 4.0 d
that are generated and collected by a di
storage. The paper aims to report on th
digital twin and digital thread for better
the production process and performance
digital twin/thread framework incorpora
in which these two components rely on th
flow and exchange to drive innovation.
that include organizational architecture l
software requirements. It is envisaged
optimization of operational processes and
in an Industry Shipyard 4.0.

Keywords: digital twin; digital thread; fra

check for updates

Citation: Pang, T.Y.; Pelaez Restrepo, J.D.; Cheng, C.-T.; Yasin, A.; Lim, H.; Miletic, M. Developing a Digital Twin and Digital Thread Framework for an 'Industry 4.0' Shipyard. *Appl. Sci.* **2021**, *11*, 1097. https://doi.org/10.3390/app11031097

1. Introduction

Navy Optimizing Shipyards With Digital Twin Technology

BY YASMIN TADJDEH

The Navy's public shipyards — which repair the service's submarines and aircraft carriers — are aging and facing obsolescence issues. To revitalize the yards and improve infrastructure, the Navy is in the midst of a multi-billion-dollar optimization overhaul that will employ digital twin technology to map out areas most in need of changes.

The Shipyard Infrastructure Optimization Program, or SIOP, is a 20-year, $21-billion effort to modernize the four public yards in Norfolk, Virginia; Pearl Harbor, Hawaii; Portsmouth, Virginia; and Puget Sound, Washington.

"We've got dry docks that are over 100 years old," said Steve Lagana, program manager for the SIOP office. "We have buildings that are over 100 years old."

Rep. Rob Wittman, R-Va., ranking member of the House Armed Services subcommittee on seapower and projection forces, said the yards are in dire need of an upgrade.

"When you travel to our public shipyards, it is sobering to see the age of the dry docks, … the limited capability of the dry docks, and also the age of the shops that are there," he said during the Surface Navy Association's annual conference in January, which was held virtually due to the COVID-19 pandemic.

This creates substantial efficiency issues, he noted.

"If you go to a place like Norfolk Naval Shipyard, and you're working on ture is intrinsically linked to performance and in 2017 began laying the groundwork for the SIOP program, which officially began in the summer of 2018, Lagana said.

"This really is an … industrial manufacturing optimization program with a focus on productivity in the shipyards and how that affects the overall national defense," he said. "How do we get submarines in and out of shipyards as efficiently as possible, so the fleet commanders have the assets they need to do their mission?"

Critical to the effort is a modeling-and-simulation technology known as digital twins which digitally replicates an object, place or building, said Stephanie Douglas, executive director for logistics, maintenance and industrial operations at Naval Sea Systems Command.

"The modeling and simulation is really key as it allows us the opportunity to figure out how to optimize flow, not only within the shops, but around the yards to provide the most efficient and productive layout for operations within the shipyard," she said. "We're already seeing some really exciting things come out of the modeling-and-simulation piece of it in terms of opportunities."

The service reached out to fication of that, we will start into that effort," he said.

Norfolk is also moving along well, he added.

Lagana noted that all the yards will have their digital twins up and running this year.

The service is already gleaning a great deal of information from Pearl Harbor's digital twin, he said.

"We're definitely getting some better insight into some potential tweaks in infrastructure," he said. "With any analysis, you kind of want to find that sweet spot, that knee in the curve to where can I get the most efficiencies with the best return on investment."

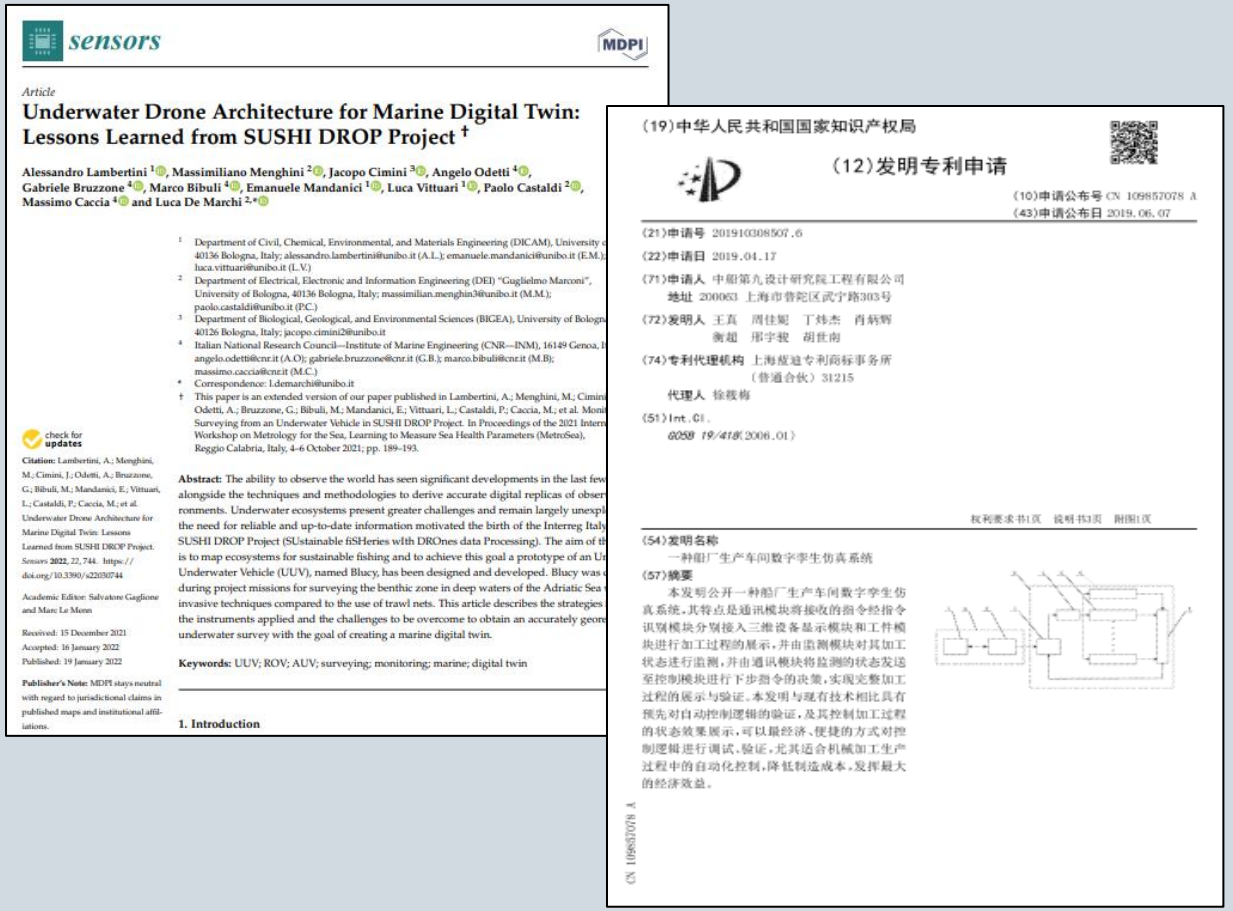
In some cases, the Navy is finding that

The Los Angeles-class fast-attack submarine USS Olympia arrives at Puget Sound Naval Shipyard.

- Naval Shipyards
- Intrusion Detection Control Systems
- Antisubmarine Warfare Sensors
- Cybersecurity Initiatives

Global Defense Instantiations of DTs

- **Italy** – Researching underwater drone digital twins
- **China** – Filed patent for shipyard digital twin architecture
- **Russia** – Promoting digital twin use within the Russian military-industrial complex



sensors

MDPI

Article

Underwater Drone Architecture for Marine Digital Twin: Lessons Learned from SUSHI DROP Project †

Alessandro Lambertini [1], Massimiliano Menghini [2], Jacopo Cimini [3], Angelo Odetti [4], Gabriele Bruzzone [4], Marco Bibuli [4], Emanuele Mandanici [1], Luca Vittuari [1], Paolo Castaldi [2], Massimo Caccia [4] and Luca De Marchi [2,*]

[1] Department of Civil, Chemical, Environmental, and Materials Engineering (DICAM), University of 40136 Bologna, Italy; alessandro.lambertini@unibo.it (A.L.); emanuele.mandanici@unibo.it (E.M.); luca.vittuari@unibo.it (L.V.)
[2] Department of Electrical, Electronic and Information Engineering (DEI) "Guglielmo Marconi", University of Bologna, 40136 Bologna, Italy; massimilian.menghin3@unibo.it (M.M.); paolo.castaldi@unibo.it (P.C.)
[3] Department of Biological, Geological, and Environmental Sciences (BIGEA), University of Bologna 40126 Bologna, Italy; jacopo.cimini2@unibo.it
[4] Italian National Research Council—Institute of Marine Engineering (CNR—INM), 16149 Genoa, I angelo.odetti@cnr.it (A.O); gabriele.bruzzone@cnr.it (G.B.); marco.bibuli@cnr.it (M.B); massimo.caccia@cnr.it (M.C.)
* Correspondence: l.demarchi@unibo.it
† This paper is an extended version of our paper published in Lambertini, A.; Menghini, M.; Cimini Odetti, A.; Bruzzone, G.; Bibuli, M.; Mandanici, E.; Vittuari, L.; Castaldi, P.; Caccia, M.; et al. Moni Surveying from an Underwater Vehicle in SUSHI DROP Project. In Proceedings of the 2021 Intern Workshop on Metrology for the Sea, Learning to Measure Sea Health Parameters (MetroSea), Reggio Calabria, Italy, 4–6 October 2021; pp. 189–193.

check for updates

Citation: Lambertini, A.; Menghini, M.; Cimini, J.; Odetti, A.; Bruzzone, G.; Bibuli, M.; Mandanici, E.; Vittuari, L.; Castaldi, P.; Caccia, M.; et al. Underwater Drone Architecture for Marine Digital Twin: Lessons Learned from SUSHI DROP Project. *Sensors* **2022**, *22*, 744. https://doi.org/10.3390/s22030744

Academic Editor: Salvatore Gaglione and Marc Le Menn

Received: 15 December 2021
Accepted: 16 January 2022
Published: 19 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: The ability to observe the world has seen significant developments in the last few alongside the techniques and methodologies to derive accurate digital replicas of obser ronments. Underwater ecosystems present greater challenges and remain largely unexpl the need for reliable and up-to-date information motivated the birth of the Interreg Italy SUSHI DROP Project (SUstainable fiSHeries wIth DROnes data Processing). The aim of t is to map ecosystems for sustainable fishing and to achieve this goal a prototype of an U Underwater Vehicle (UUV), named Blucy, has been designed and developed. Blucy was during project missions for surveying the benthic zone in deep waters of the Adriatic Sea invasive techniques compared to the use of trawl nets. This article describes the strategies the instruments applied and the challenges to be overcome to obtain an accurately geore underwater survey with the goal of creating a marine digital twin.

Keywords: UUV; ROV; AUV; surveying; monitoring; marine; digital twin

1. Introduction

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109857078 A
(43)申请公布日 2019.06.07

(21)申请号 201910308507.6

(22)申请日 2019.04.17

(71)申请人 中船第九设计研究院工程有限公司
地址 200063 上海市普陀区武宁路303号

(72)发明人 王真 周佳妮 丁炜杰 肖炳辉
衡超 邢宇骏 胡世南

(74)专利代理机构 上海蓝迪专利商标事务所（普通合伙） 31215
代理人 徐筱梅

(51)Int.Cl.
G05B 19/418(2006.01)

权利要求书1页 说明书3页 附图1页

(54)发明名称

一种船厂生产车间数字孪生仿真系统

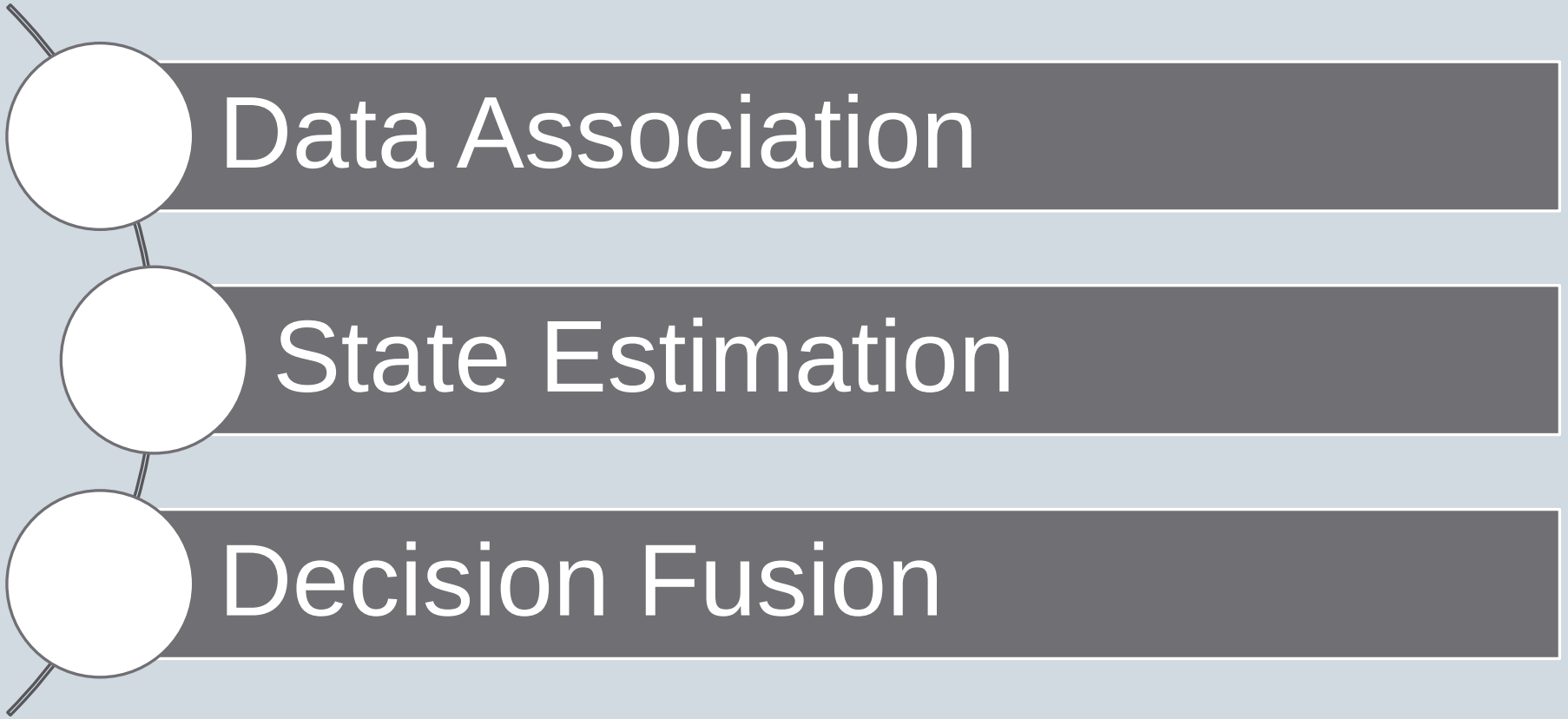
(57)摘要

本发明公开一种船厂生产车间数字孪生仿真系统。其特点是通讯模块将接收的指令经指令识别模块分别接入三维设备显示模块和工件模块进行加工过程的展示，并由监测模块对其加工状态进行监测，并由通讯模块将监测的状态发送至控制模块进行下步指令的决策，实现完整加工过程的展示与验证。本发明与现有技术相比具有预先对自动控制逻辑的验证，及其控制加工过程的状态效果展示，可以最经济、便捷的方式对控制逻辑进行调试、验证，尤其适合机械加工生产过程中的自动化控制，降低制造成本，发挥最大的经济效益。

CN 109857078 A

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Data Fusion Techniques



Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Gaps within Developed DTs

Digital twins in many defense systems lack data fusion frameworks

- Unable to support the integration of data and analytics towards an automated solution
- No room for processing of asynchronous information
- Patchwork limits functionality, resulting in DTs that have low survivability and maintainability rates

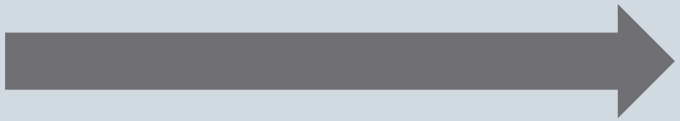
Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

DT Gaps to Requirements

Noted Gaps:

1. Data Framework
2. Data Management
3. System Data Integration
4. Convergence
5. Optimized Analytics



Requirements:

1. Data Framework
2. Data Management
3. System Data Integration
4. Convergence
5. Optimized Analytics

Distribution Statement A. Approved for public release

Data Lifecycle

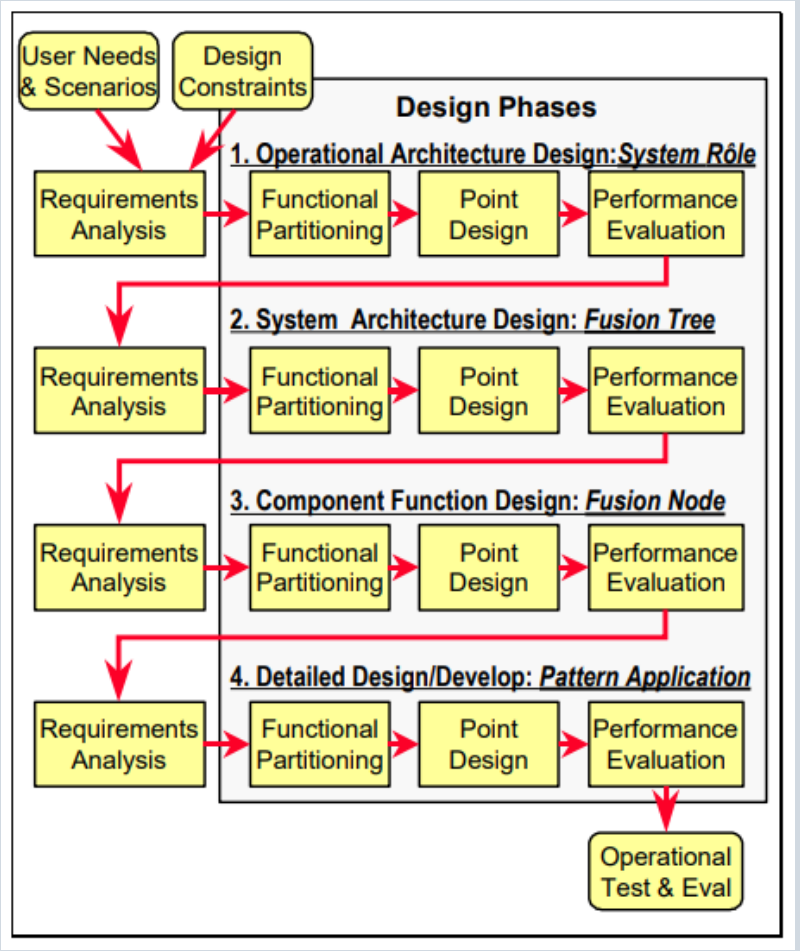
Can use data fusion process in conjunction with data lifecycle to form the basis of requirements analysis

Distribution Statement A. Approved for public release

Requirements Analysis

Requirements analysis can be broken down at four design phases of the data fusion process:

1. **Operational Architecture Design**
2. **System Architecture Design**
3. **Component Function Design**
4. **Detailed Design and Development**



Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Path Forward

1. Use open-source DT resources to perform system level product decomposition at operational architecture design level
2. Determine requirements for data fusion network system architecture design
3. Create a requirements design of data fusion nodes at the component function level, with data flow specifications among digital twin system components
4. Extend requirement analysis for detailed design elements of digital twins
5. Review existing data fusion networks within DTs to illustrate the functionality of the performed requirements analysis

Distribution Statement A. Approved for public release

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Questions?

Laura Hugill

PhDc – The George Washington University

Principal Systems Engineer, Raytheon Solipsys

Email: laurahugill@gwu.edu

Distribution Statement A. Approved for public release

Application of the Digital Thread through the Digital Engineering Framework for Integration and Interoperability

Authors: Daniel Dunbar, Mark Blackburn, Thomas Hagedorn, Dinesh Verma

Presenter: Daniel Dunbar
PhD Candidate – Stevens Institute of Technology
ddunbar1@stevens.edu

NDIA 25th Annual Systems and Mission Engineering Conference
November 2, 2022

Approved for Public Release

Digital Engineering

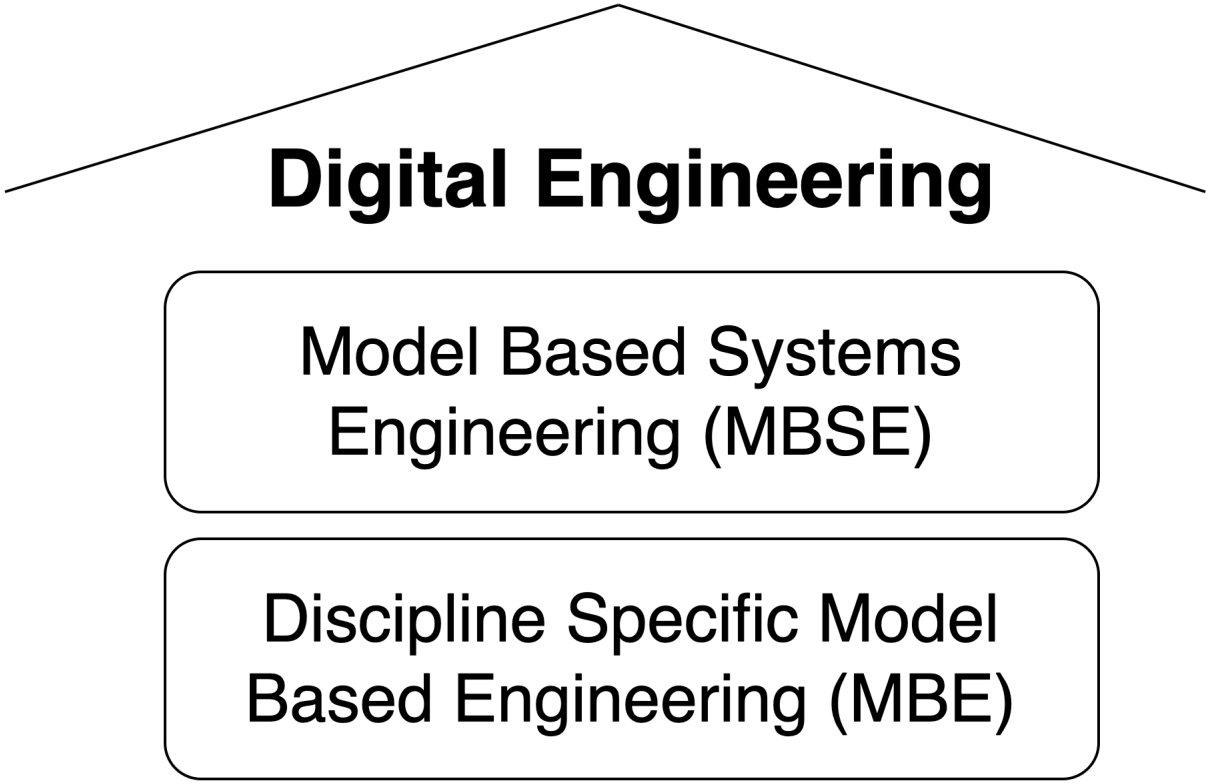
- Umbrella Domain - Broad Terms
- Characterized by ”authoritative sources of system data and models”
- Commonly uses an Authoritative Source of Truth (AST)
- Recognizes shared parameters across a variety of individual models

Research Question

- How do you effectively implement a forward-looking AST that enables a Digital Thread

Answer

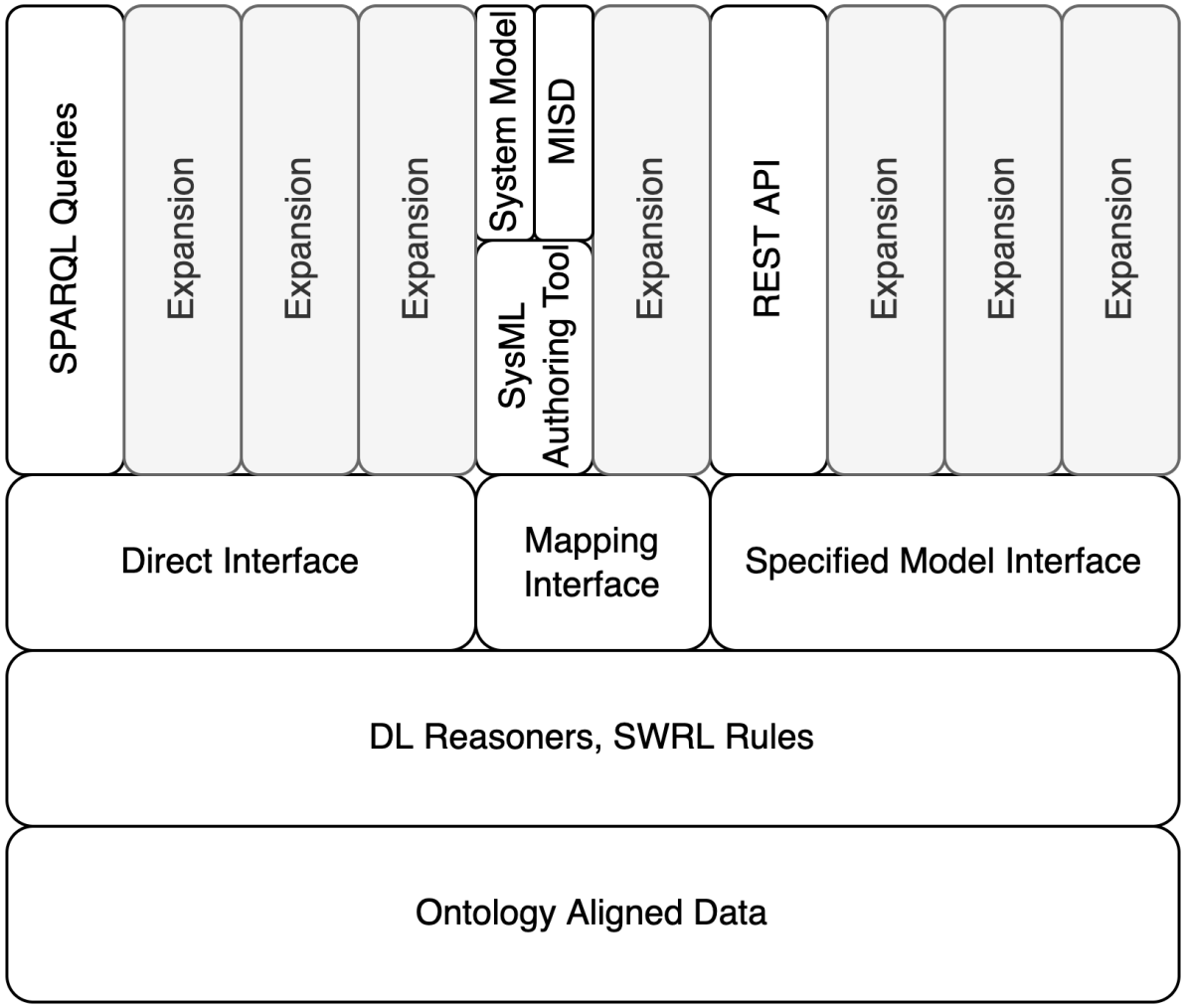
- Digital Engineering Framework for Integration and Interoperability (DEFII)



https://ac.cto.mil/wp- content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf

DEFII Framework

Digital Engineering Framework for Integration and Interoperability



- Foundation: Formal ontologies and data aligned to them
- Reasoners enrich data through axioms and rules setup in ontologies themselves

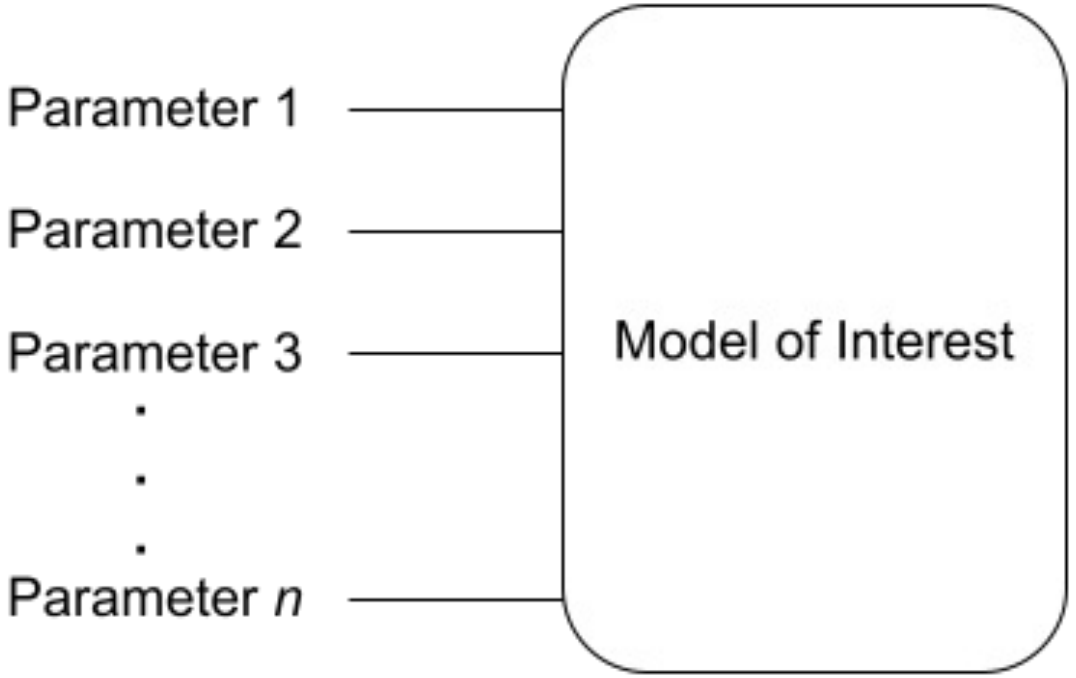
Three Notional Interfaces

- **Direct Interface**: Direct invocation of the Semantic Web Technology (SWT) stack
- **Mapping Interface**: Tool Dependent Mapping
  -> Begins with tool and moves toward ontology
- **Specified Model Interface**: Tool Independent Access to ontology aligned data
  -> Begins with ontology and exposes data towards tools

(Dunbar et al., 2022)

Model Interface Specification Diagram (MISD)

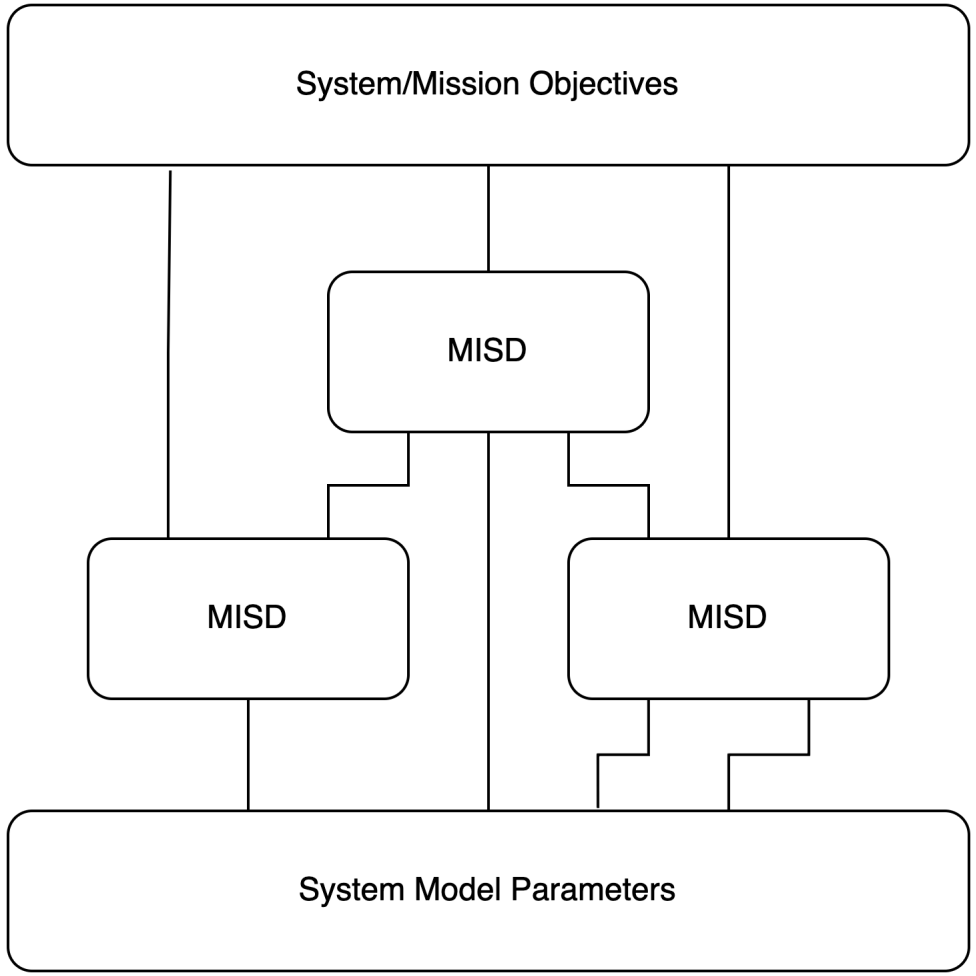
- Creates tool agnostic interface for further design, analysis, and reporting tasks
- Bridge between ontology-aligned triple store and use of models of interest
- Based on Matt Cilli's approach to Assessment Flows
- Formalizes Model Data
- Specifies models – not tools



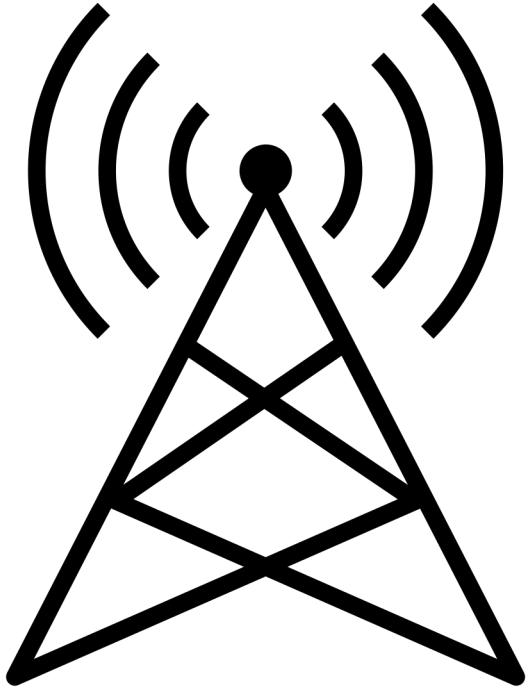
(Cilli, 2015) (Dunbar et al., 2022)

Assessment Flow Diagram (AFD)

- An Assessment Flow Diagram (AFD) aggregates several individual Models of Interest
- Shared parameters across models are explicitly identified



Telecom Use Case



Radio Tower Site – Three Models (Simplified)

Coverage Analysis

- Tx Power
- Transmission Line Type
  - Mainline
  - Shelter Jumper
- Transmission Line Length
  - Mainline
  - Shelter Jumper
- Antenna Type
- Antenna Height
- Frequency Band

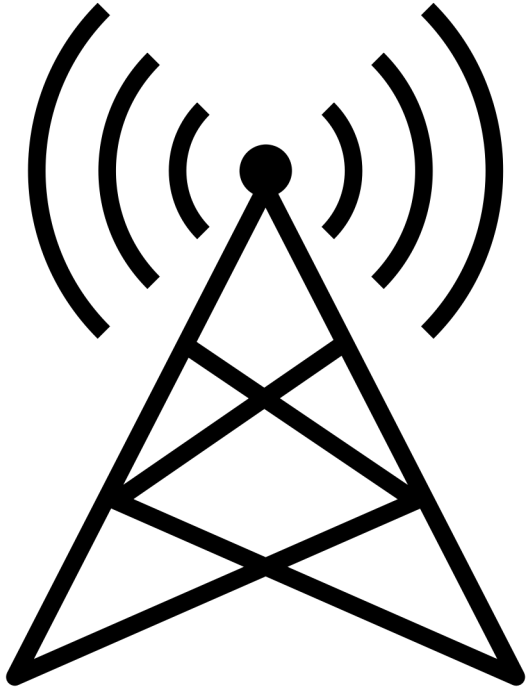
Tower Structural Loading Analysis

- Antenna Type
- Antenna Height
- Transmission Line Type
- Coverage Approval

FCC Licensing Application

- Tower Identifier
- Frequency Information
- Effective Radiated Power (ERP)

Telecom Use Case



Radio Tower Site – Three Models (Simplified)

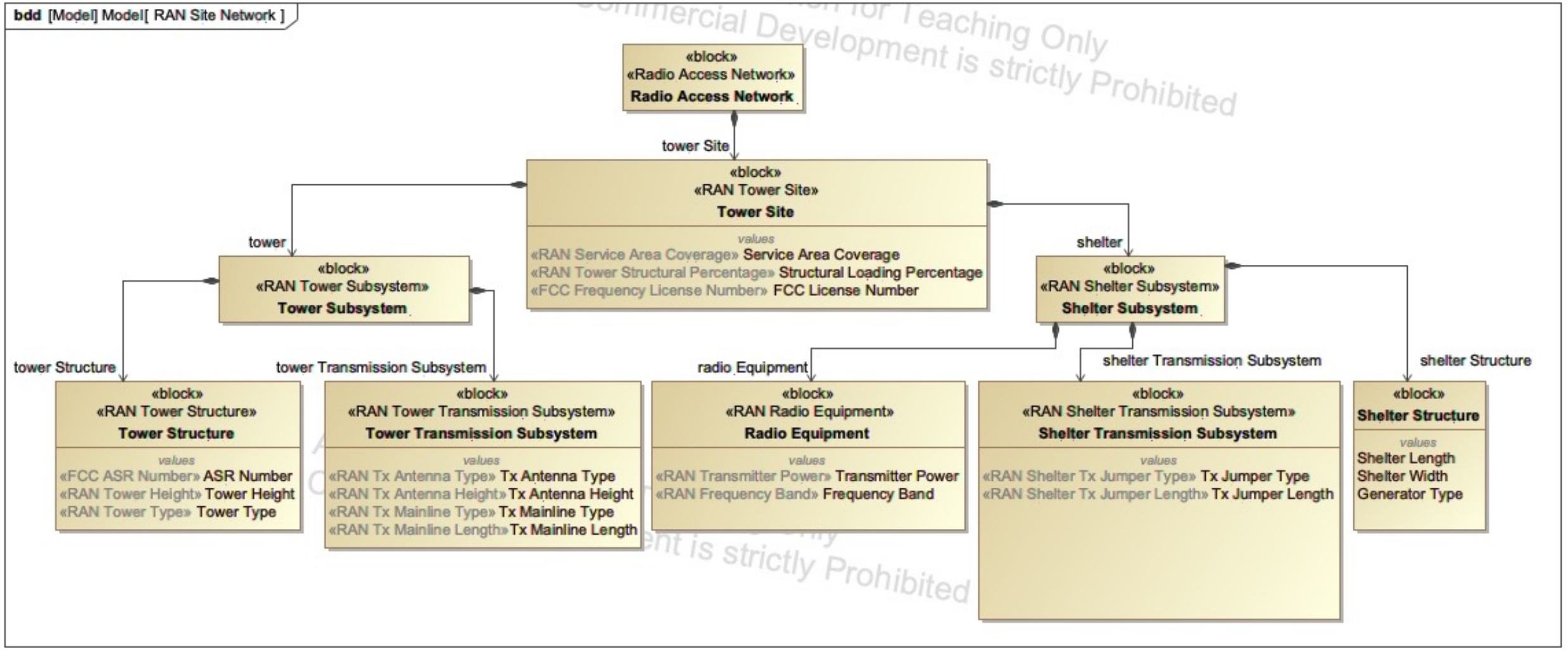
Coverage Analysis
- Tx Power
- Transmission Line Type
  - Mainline
  - Shelter Jumper
- Transmission Line Length
  - Mainline
  - Shelter Jumper
- Antenna Type
- Antenna Height
- Frequency Band

Tower Structural Loading Analysis
- Antenna Type
- Antenna Height
- Transmission Line Type
- Coverage Approval

FCC Licensing Application
- Tower Identifier
- Frequency Information
- Effective Radiated Power (ERP)

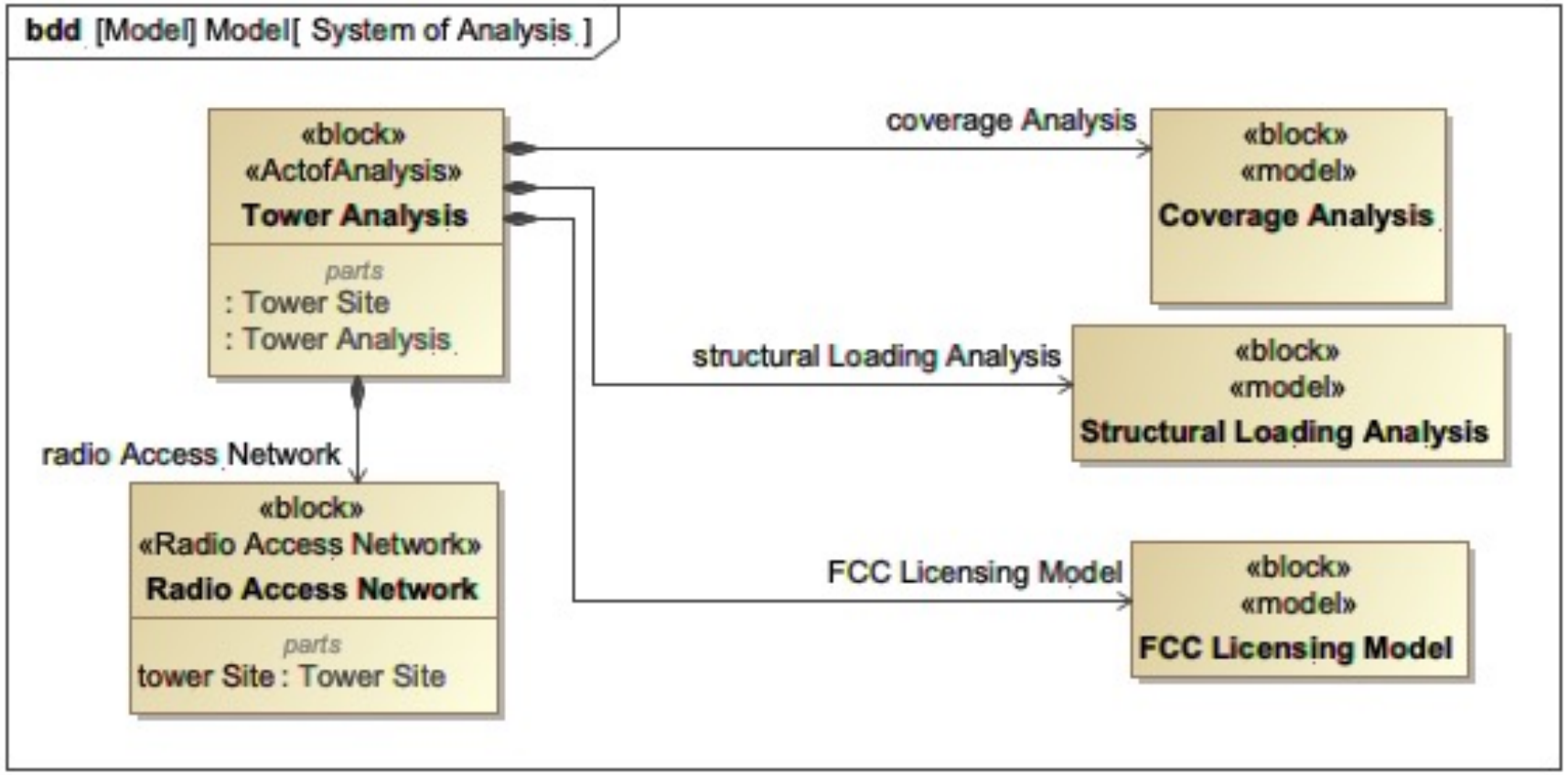
Radio Tower Site – Top Level Objectives
- Service Area Coverage Metric
- FCC License Number
- Structural Loading Percentage

Telecom System Under Design BDD

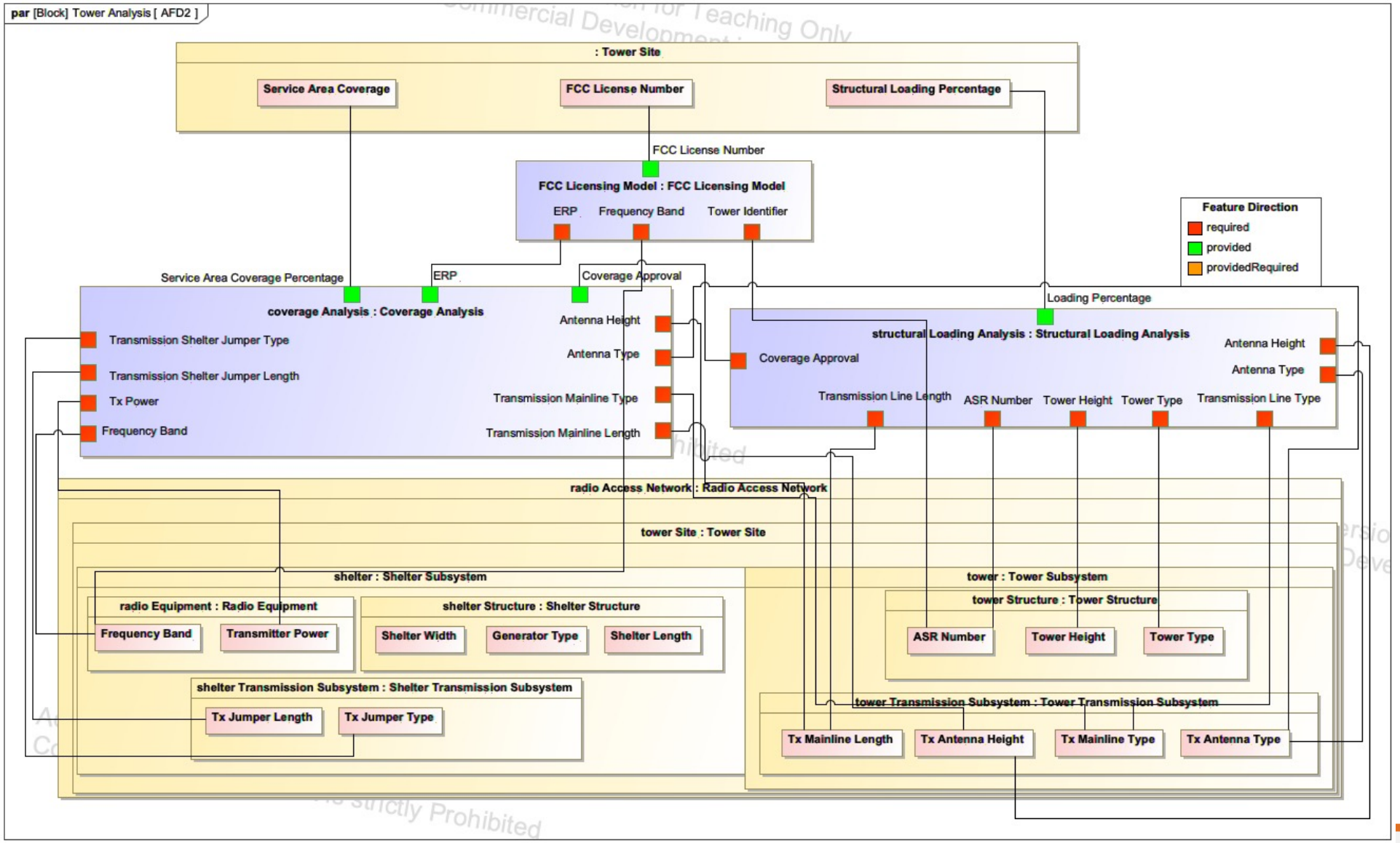


Commercial Development is strictly Prohibited for Teaching Only

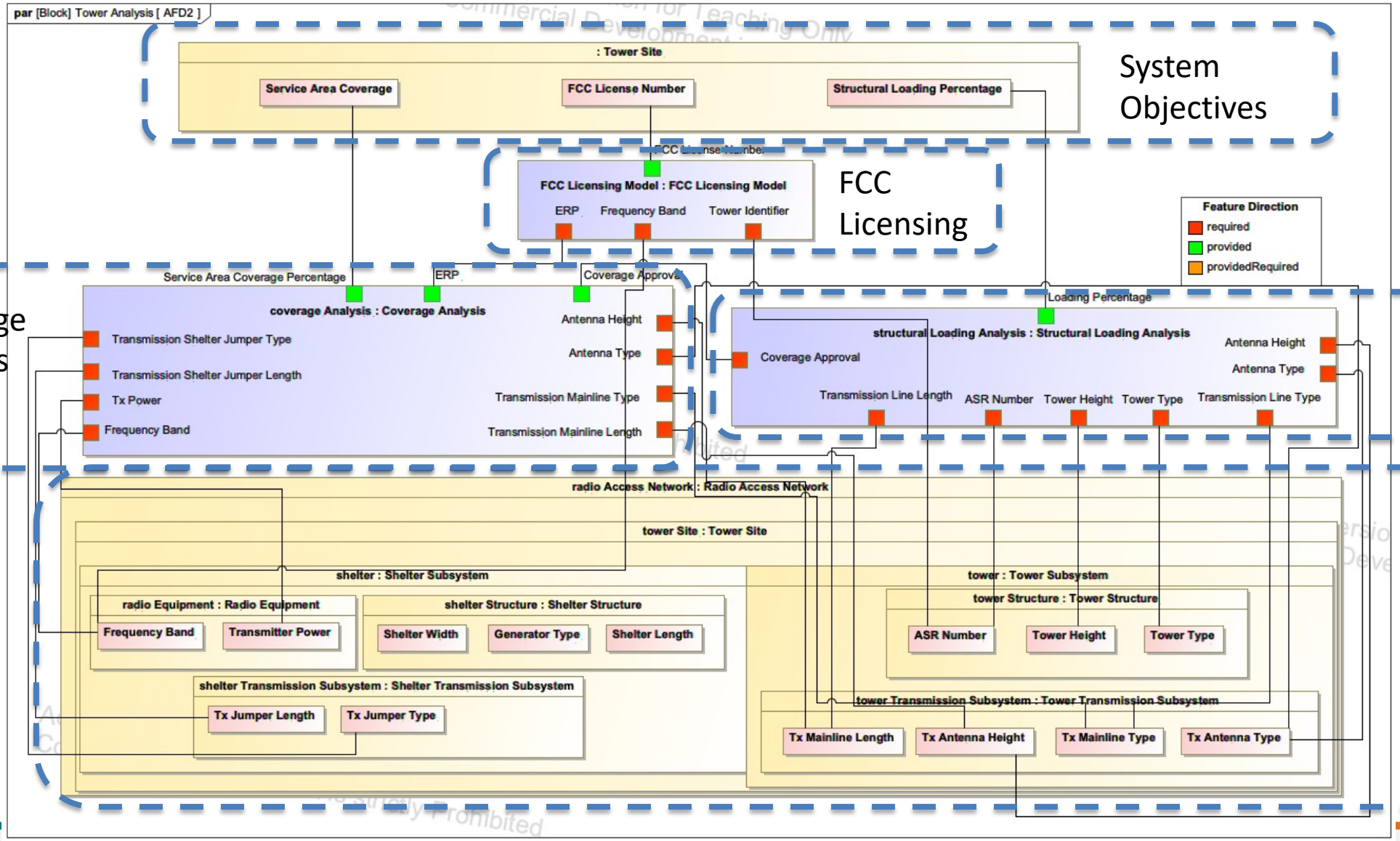
Tower System of Analysis BDD



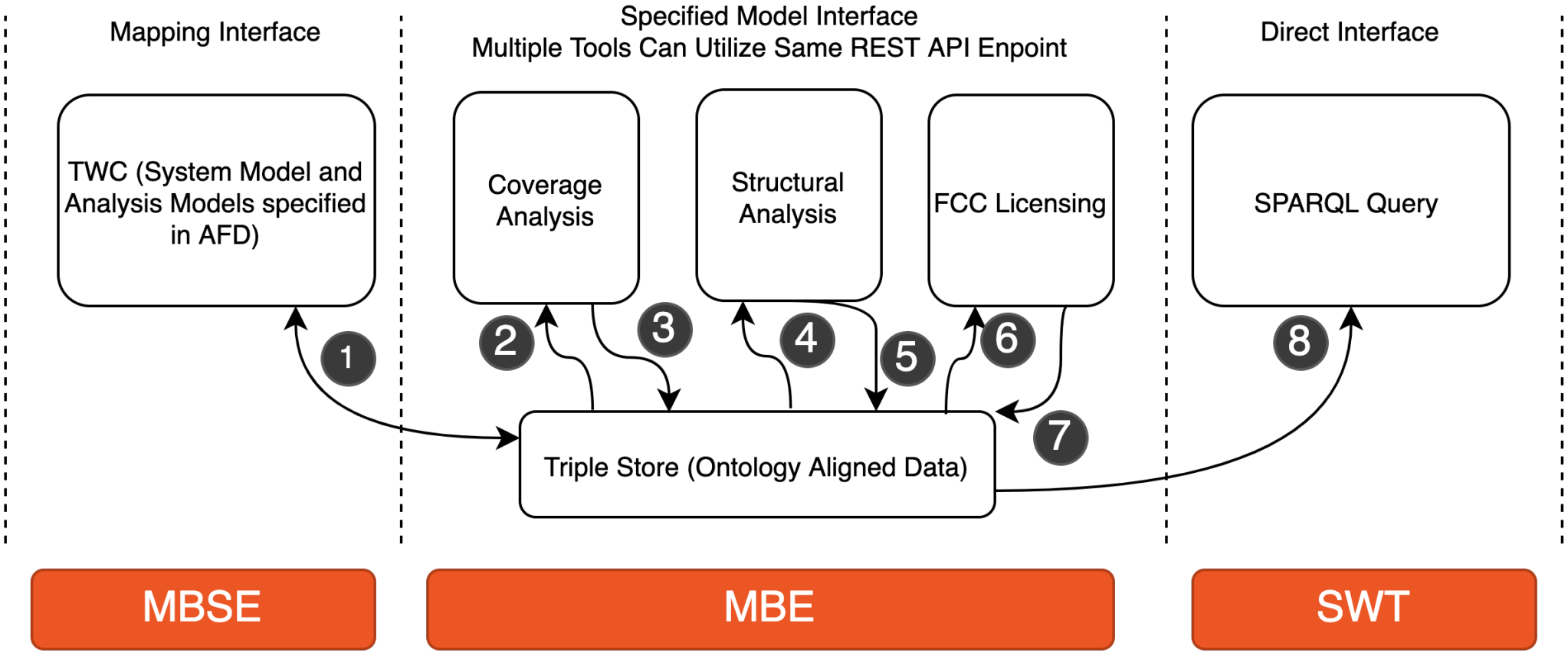
System of Analysis Assessment Flow Diagram (AFD)



System of Analysis Assessment Flow Diagram (AFD)



Digital Thread

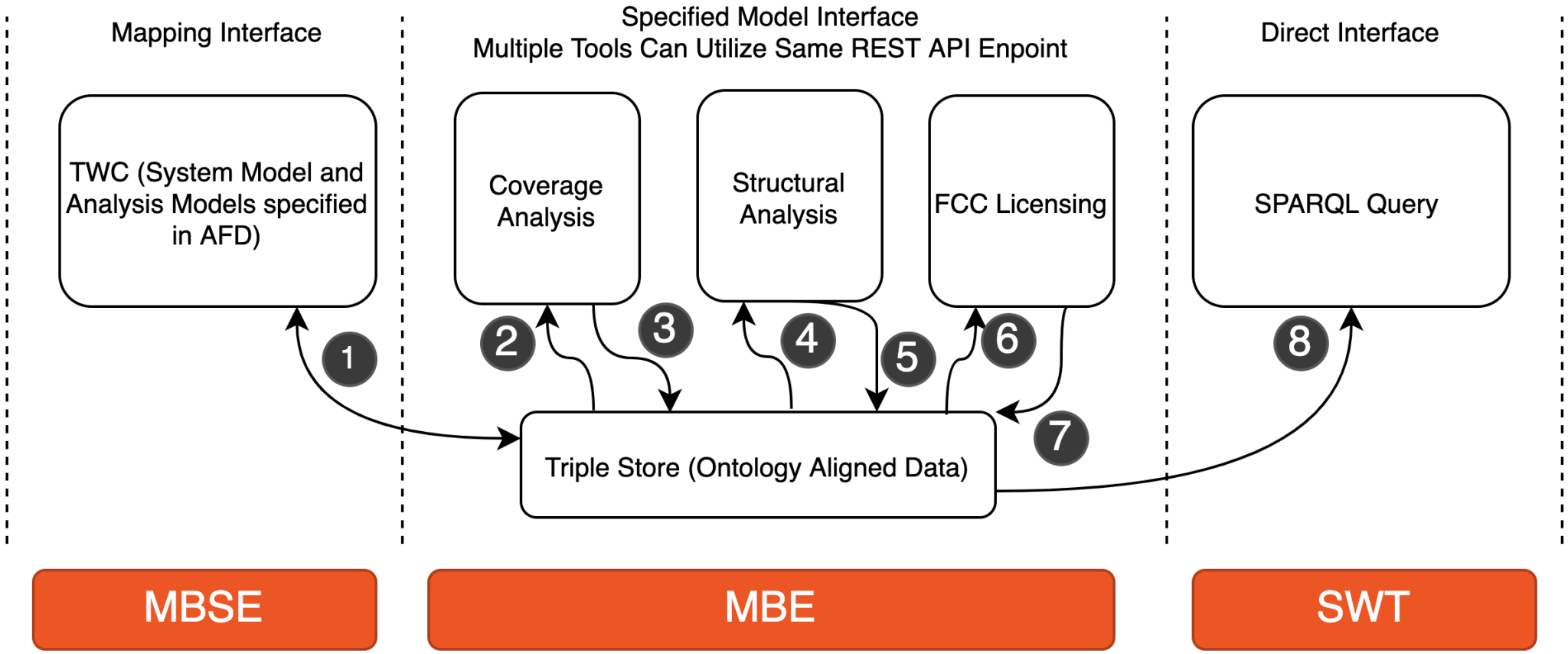


REST API Service

- Individual models or entire AFD can be called via REST API endpoint
- Straightforward integration with external tools due to ubiquity of http services
- Multiple tools can use same REST API endpoint


```
{
    "Coverage Analysis": {
        "Transmission Shelter Jumper Type": "0.25",
        "Transmission Shelter Jumper Length": "20",
        "Tx Power": "100",
        "Frequency Band": "700",
        "Transmission Mainline Length": "350",
        "Transmission Mainline Type": "1.25",
        "Antenna Type": "SC479-HF1LDF",
        "Antenna Height": "325",
        "Coverage Approval": "False",
        "ERP": "",
        "Service Area Coverage Percentage": ""
    },
    "Structural Loading Analysis": {
        "Coverage Approval": "False",
        "Transmission Line Length": "350",
        "ASR Number": "A25J6Y",
        "Tower Height": "400",
        "Tower Type": "Guyed",
        "Transmission Line Type": "1.25",
        "Antenna Type": "SC479-HF1LDF",
        "Antenna Height": "325",
        "Loading Percentage": ""
    },
    "FCC Licensing Model": {
        "ERP": "",
        "Frequency Band": "700",
        "Tower Identifier": "A25J6Y",
        "FCC License Number": ""
    }
}
```

Digital Thread



Conclusion

- DEFII Framework provides a graph-based method for integrating tools
- Users can configure the DEFII framework via SysML models – broad SWT knowledge across workforce unnecessary
- Digital Thread can be implemented using an ontology-aligned AST and standard interface types

Future Work

- Explore additional functionality enabled by a graph representation of the system
- Explore additional functionality enabled by formal ontological knowledge representation

References

Cilli, Matthew V. “Improving Defense Acquisition Outcomes Using an Integrated Systems Engineering Decision Management (ISEDM) Approach.” ProQuest Dissertations and Theses, 2015. http://ezproxy.stevens.edu/login?url=https://www.proquest.com/dissertations-theses/improving-defense-acquisition-outcomes-using/docview/1776469856/se-2?accountid=14052.

Dunbar, Daniel, Thomas Hagedorn, Mark Blackburn, John Dzielski, Steven Hespelt, Benjamin Kruse, Dinesh Verma, and Zhongyuan Yu. “Driving Digital Engineering Integration and Interoperability Through Semantic Integration of Models with Ontologies,” 2022. arXiv. https://arxiv.org/abs/2206.10454.

Wagner, David A., M. B. Bennett, R. Karban, N. Rouquette, S. Jenkins, and M. Ingham. “An Ontology for State Analysis: Formalizing the Mapping to SysML.” In *2012 IEEE Aerospace Conference*, 1–16. Big Sky, MT: IEEE, 2012. https://doi.org/10.1109/AERO.2012.6187335.

stevens.edu

Daniel Dunbar
ddunbar1@stevens.edu

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

U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND AVIATION & MISSILE CENTER

An Update to the Comprehensive Architecture Strategy (CAS) and its Supporting Architecture Processes and Body of Knowledge (BoK)

Scott Wigginton

Experimental Developer

Technology Development Directorate

03 Nov 2022

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

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

CURRENT DOD SYSTEMS ENVIRONMENT

Only Constant for DoD Systems is CHANGE!

Military systems **must rapidly adapt** to maintain operational relevance

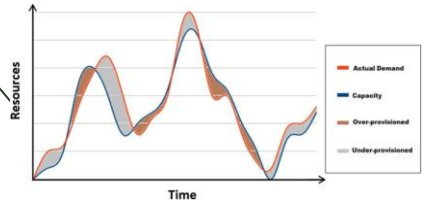
Evolving Threats

Strategic and Tactical Innovation

Rapid Technological Change

Increased Leverage of COTS

Resource and Demand Uncertainty

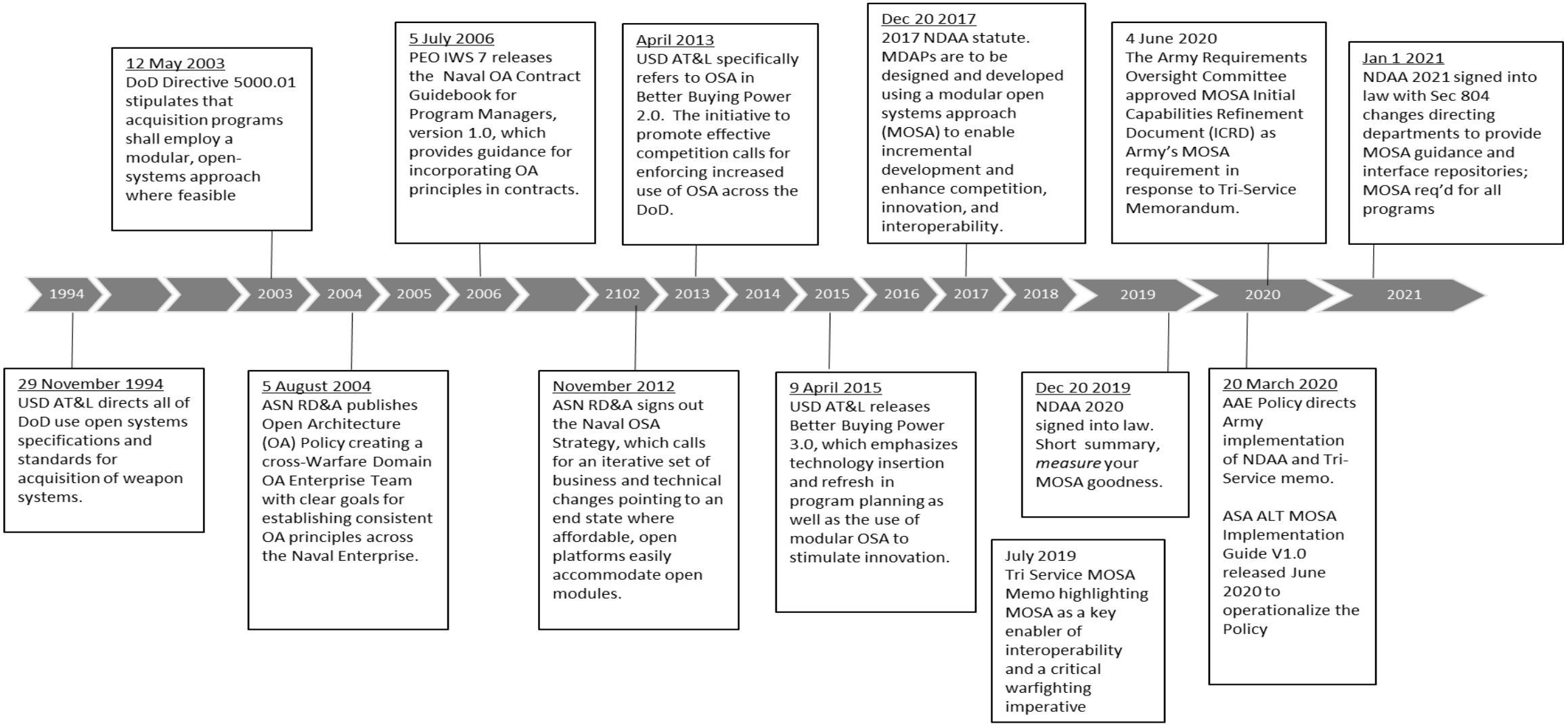


Modular Open Systems Approach (MOSA) is Key to Achieving Systems Resilient to Change

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

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

WE'VE BEEN TOLD TO DO MOSA FOR A LONG TIME



But we haven't been told how; nor do we have good metrics

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

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

IF MOSA IS THE ANSWER; WHAT ARE THE CHALLENGES?

(1) “We must inspect what we expect”, and architecture is key to MOSA

(2) We must inspect architectures to ensure MOSA is realized

(3) We lack process for deep architectural inspection across lifecycle

(4) We lack engineering foundation for architectural inspections

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

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

COMPREHENSIVE ARCHITECTURE STRATEGY (CAS)

- CAS is a strategy to address architecting for MOSA objectives
- Business Goals are the baseline to define and empower a MOSA
- An overarching architectural approach to Enterprise and Product Line management to enable rapid capability reuse and deployment across systems resulting in significant cost, schedule, and warfighting advantages
- Used to guide development of architectures that support a MOSA

The AVE architecting processes presented today evolved from the CAS

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

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

ARCHITECTURE VERIFICATION ENVIRONMENT (AVE) VISION

Mission

Provide capabilities to **inspect architectures** and their derivations for an **ability to handle future uncertainty** which drives system changes

Early Lifecycle Assessment of how well an architecture will enable a system to handle lifecycle change

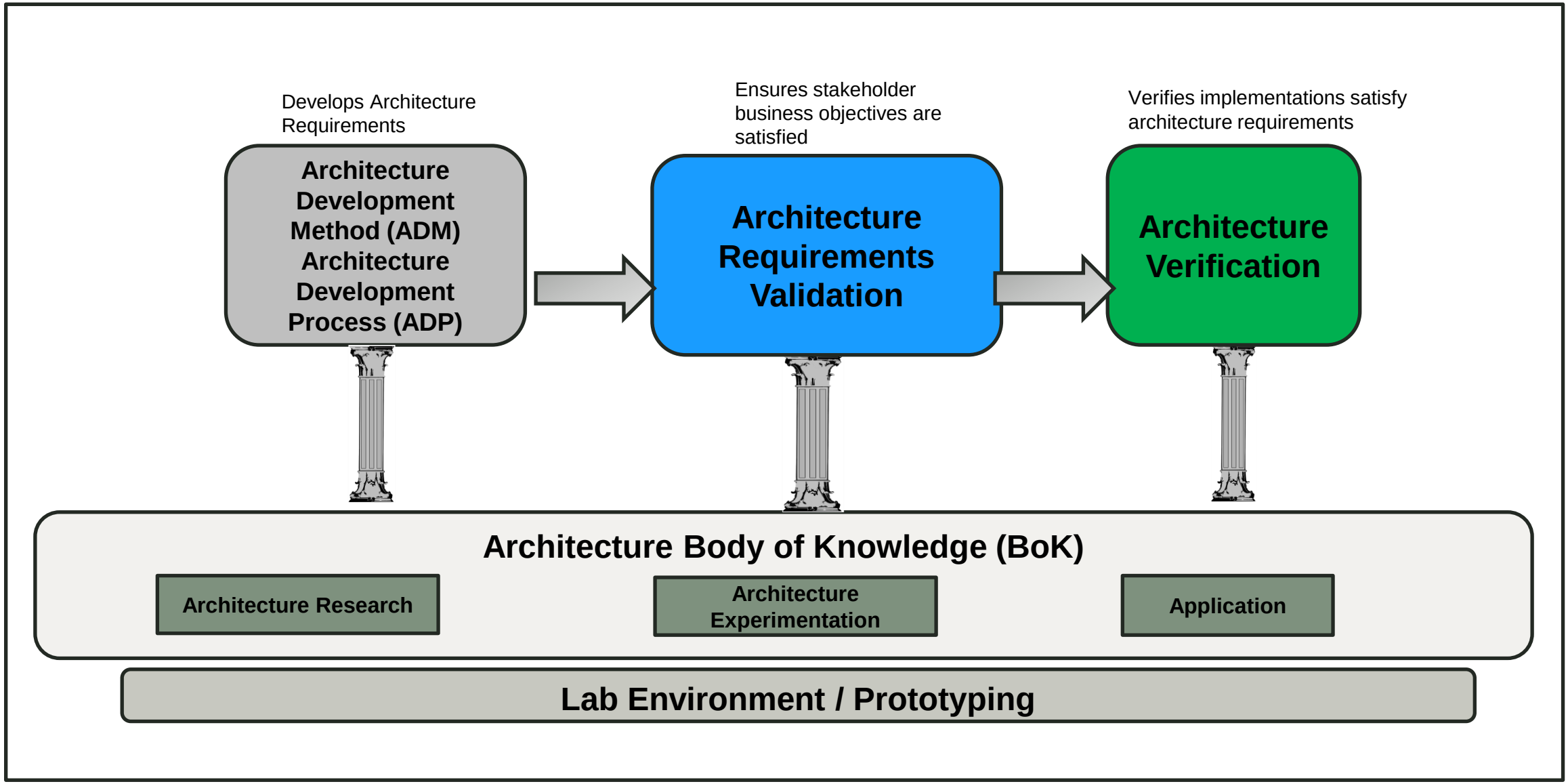
Ensure Derivations Maintain Architecture intent, decisions, and conceptual/logical instantiations

Assess SW/HW Implementations for predicted or specified response to lifecycle changes

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

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

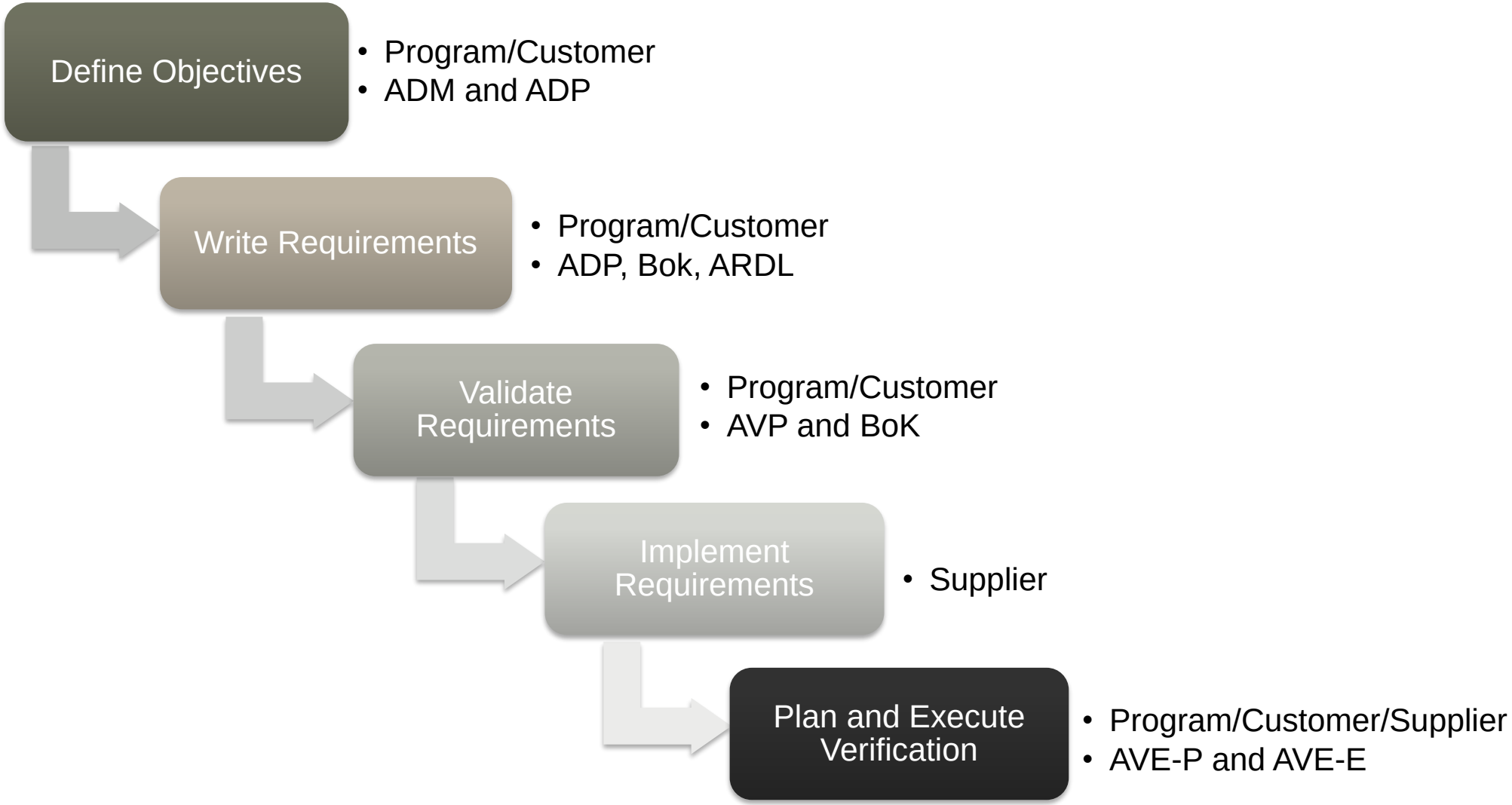
AVE OVERVIEW



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

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

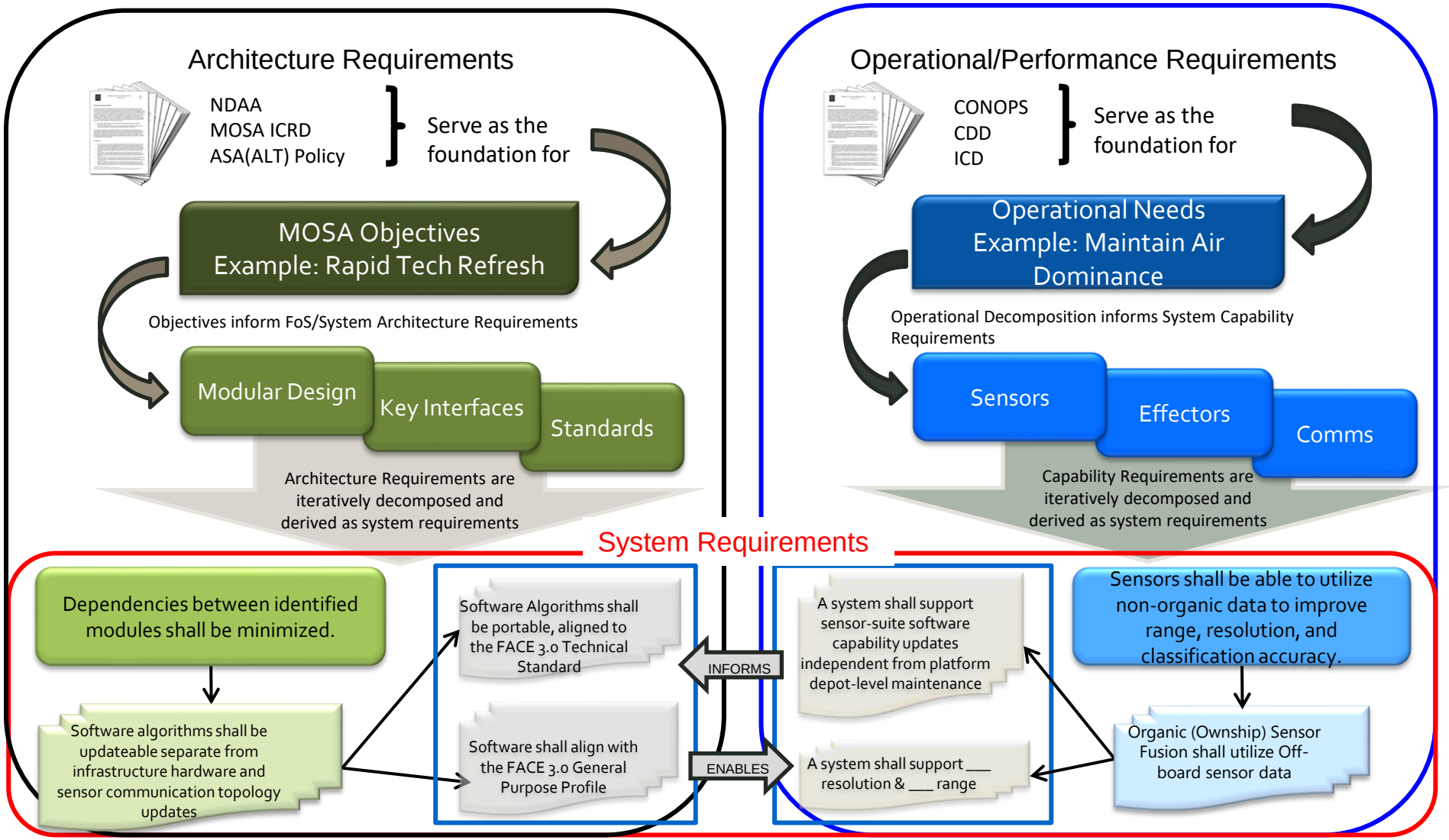
ARCHITECTURE LIFECYCLE PROCESSES



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

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

ARCHITECTURE REQUIREMENTS EXAMPLE

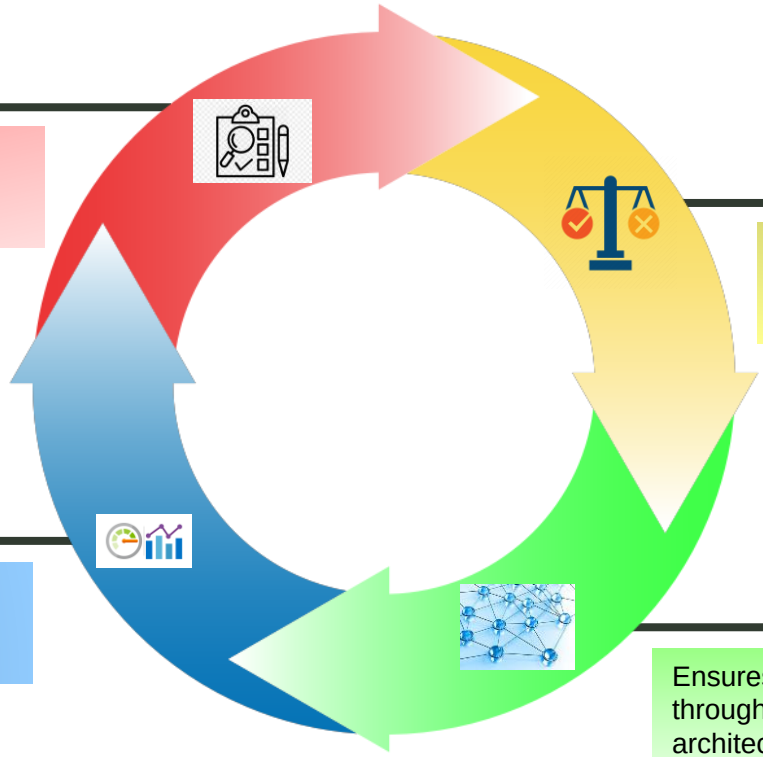


Distribution Statement A: Approved for public release. Distribution is unlimited.

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

ARCHITECTURE REQUIREMENTS VALIDATION

GOAL: Early assessment of architecture and design's ability to enable system evolution w.r.t. MOSA Objectives within required business and technical criteria



Requirements Well-Formedness Checks

Ensures requirements are clear, appropriate, and cohesive to communicate intent as system evolves

Strategic Architecture Decision Analysis

Assesses strategic architecture decisions for their ability to enable program MOSA objectives

Architecture Traceability Analysis

Ensures architecture is maintained through refinement (e.g., requirements, architectures, design) across the lifecycle

Architecture Metrics Assessment

Shows how well architecture instantiations are expected to handle evolution through change

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

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

VERIFICATION PLANNING AND EXECUTION

Architecture Verification Planning covers:

- Architecture Scenario development
- Create Architecture Test cases
- Determine Test method (inspect, analyze, demonstrate, test)
- Determine resources needed (humans, software, tools, hardware, lab, etc.)

Architecture Verification Execution covers:

- Execute Test method
- Capture results
- Analyze results
- Make assessment

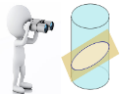
Assess SW/HW Implementations for predicted or specified response to lifecycle changes

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

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

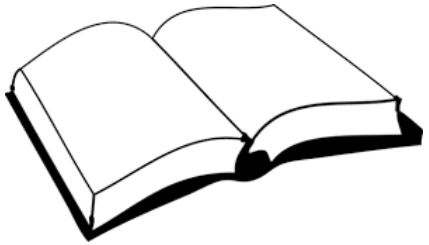
ENGINEERING FOUNDATION OF THE BODY OF KNOWLEDGE

- Standardized Business Drivers
- Standardized Quality Attributes (QA)

- Standardized Architecture Mechanisms
- Policy and Regulatory Statements
- Business Drivers to QA Relationships
- QA to Mechanism Relationships (early draft)
- QA to QA Relationships (early draft)
- Standard Architecture Viewpoints and Aspects 
- Example Architecture Requirements

Incorporated Into

Architecture Book of Knowledge (BoK)



Used for

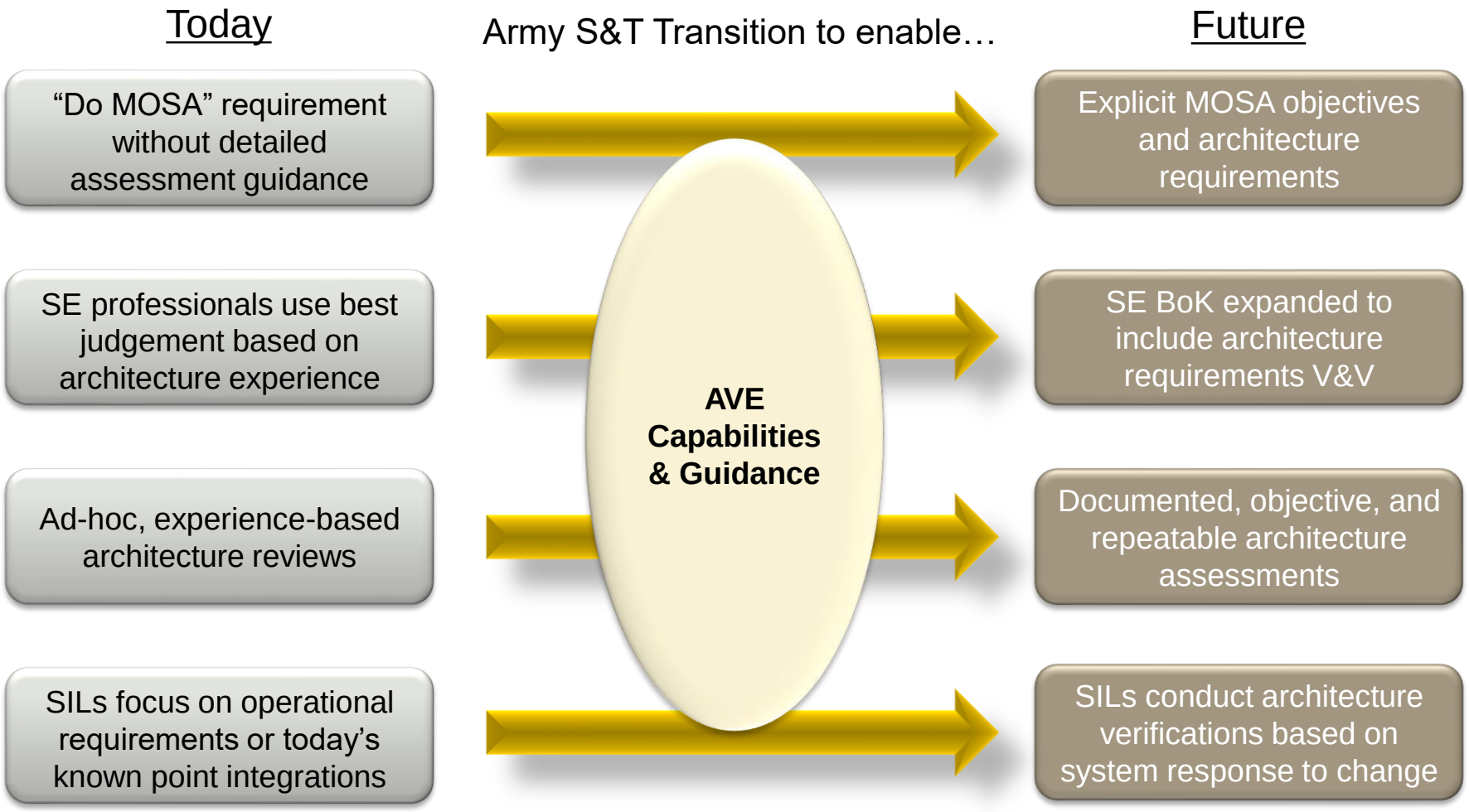
Architecture V&V Processes

- Architecture Requirements Validation
- Architecture Implementation Verification

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

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

AVE SUMMARY



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

An Overview of the Directed Energy Weapon Systems Modular Open Systems Approach Reference Architecture (DEWS MOSA RA)

Directed Energy Weapons

- Directed Energy Weapons (DEW) utilize beams of energy to destroy, damage, or disrupt a target. Examples include lasers, high power microwaves (HPM), and particle beams. They offer:
  - Potential to "Bend" the Cost Curve
  - Deep Magazines with Rapid Reload and Reduced Logistics
  - Highly reduced collateral damage
  - Precision Effects / Adjustable Effects
  - Engagement at the Speed of Light
  - Air / Land / Sea Platforms

DE-MSHORAD
Army
Laser

SSL-TM
Navy
Laser

THOR
Air Force/Army
HPM

HiJENKS
Air Force/Navy
HPM

AHEL
SOCOM
Laser

Distribution A: Approved for Public Release

DEWs Are Arriving and Being Used

- **ODIN – Optical Dazzling Interdictor, Navy**
  - Low-power laser system for dazzling of Unmanned Aerial System (UAS)-mounted Electro-Optical (EO)/Infrared (IR) sensors
  - First three systems installed on DDG51 Flt IIA ships, five more to be installed through 2023
- **HELIOS, Navy**
  - cUAS, cFIAC, 60 kW, Lockheed
  - To be installed on DDG51 Flt IIA ship in FY22
- **SSL-TM – Solid State Laser- Technology Maturation, Navy**
  - cUAS, cFIAC, 150 kW, Northrup
  - Installed on USS Portland (LPD 27) in 2019, deploys in 2021
- **CLAWS – Compact Laser Weapons System, Marines**
  - cUAS, 5 kW, Boeing, 5 systems, in CENTCOM
  - Integrated with Army C-RAM C2 system and radar
- **HELWS – High Energy Laser Weapons System, Air Force**
  - cUAS, 10 kW, Raytheon
  - 1 unit in CENTCOM
- **THOR – Tactical High Power Microwave Operational Responder, Air Force**
  - cUAS, Raytheon, OCONUS evaluation later this year
- **DE M-SHORAD** – Maneuvering Short Range Air Defense, Army
  - Experimental prototype with combat capability : 50 kW-Class laser for cUAS, cRAM, cRW
  - Prototype demo FY21, 1st Platoon (4 platforms) fielded FY22
- **IFPC-HEL – Fixed/Semi-Fixed Site Protection, Army**
  - Lab demo FY22: 300 kW-Class laser for cUAS, cRAM, cCM will inform prototyping effort
  - Joint range demonstration with Navy HELCAP in FY23, 1st Platoon (4 platforms) fielded FY24

Distribution A: Approved for Public Release

Directed Energy Weapon System (DEWS) MOSA Reference Architecture

- Directed energy systems are becoming technically mature, on the verge of being more widely deployed
- Services and programs all going in their own direction – and there is no OSA for DEWS

Needs

- MOSA-based approach to "guide and constrain" development and procurement
- Well-defined, government "owned" open interfaces between modules
- Developer-independent modules
- Service- and Host Platform-independent OSA

To Enable

- Rapid, cost-effective, and supportable DEWS fielding (reduced time from R&D, to prototyping, to integration, to DT and OT)
- Extend service life of systems through incremental upgrades (including from third-party sources)
- Industrial base expansion and engagement → ecosystem (economies of scale)
- Aligned R&D investment
- Reuse across programs and Services

Distribution A: Approved for Public Release

DEWS MOSA Reference Architecture Stakeholder Organizations

Steering Committee

- OSD R&E and DE JTO
- MDA/DVD
- Navy PEO IWS 2.0
- Air Force AFLCMC/XA
- Army RCCTO

Performing Organization

- The MITRE Corporation

Working Group

Air Force:
- AFLCMC/EBZA
- AFRL RD

Army:
- HQDA RCCTO
- SMDC

Navy
- NAVSEA 05Z/05W
- NSWC DD and NSWC CD
- ONR

DoD:
- MDA/DVD
- OSD Power Beaming

Others:
- IBAS INSITUWARE
- MANTECH/Penn State URC

Distribution A: Approved for Public Release

DEWS RA Vision, Goals, Enablers

Key
Vision
Goals
Enablers

Directed Energy Weapon programs leverage a broadly applicable Reference Architecture, founded on MOSA principles, that accelerates innovation, expedites development, and increases the reuse of standard elements

Broadly Applicable

a) Stakeholder definition of CV-1, QAs, Use Cases, Architecture Principles
b) Agnostic with respect to operating environment
c) Agnostic with respect to host platform

Based on MOSA Principles

a) Leverage open/commercial standards and OSAs
b) Non-proprietary, supplier-agnostic module & interface definitions
c) Protect supplier IP and employs balanced Data Rights within modules
d) Large and small business are full partners in architecture development and governance
e) Create new only when necessary
f) Conformance Certification

Accelerate Delivery of Innovation

a) Follow "gray box" concept (architecture defines what the modules and interfaces do, not how they do it)
b) Provide alternative methods to instantiate near-term and future-focused technologies
c) Ensure small businesses- are fully enfranchised
d) Evolvability is incorporated

Expedite Acquisition

a) Reduce traditional weapon system integration & test time
b) Vendor-agnostic open reference architecture allows government to leverage multiple industry partners
c) Allow faster insertion of new tech from best of breed
d) Enable small businesses-developed enhancements at reduced costs

Increase Reuse

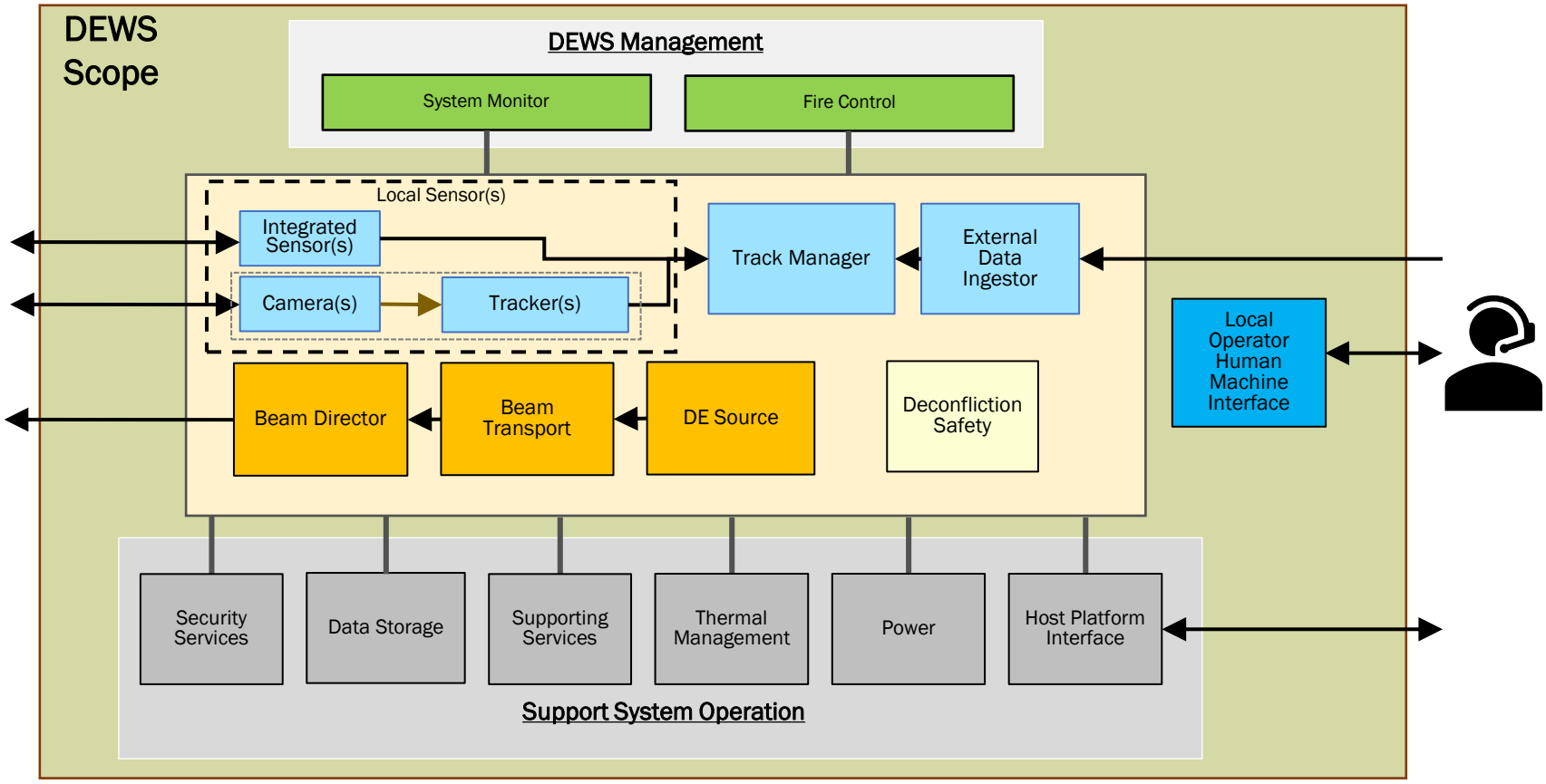
a) Facilitate backward compatibility
b) Open business model
c) Portable modules enables cross-weapon portfolio application to reduce design time for new systems

Distribution A: Approved for Public Release

Learn from Systems under Development

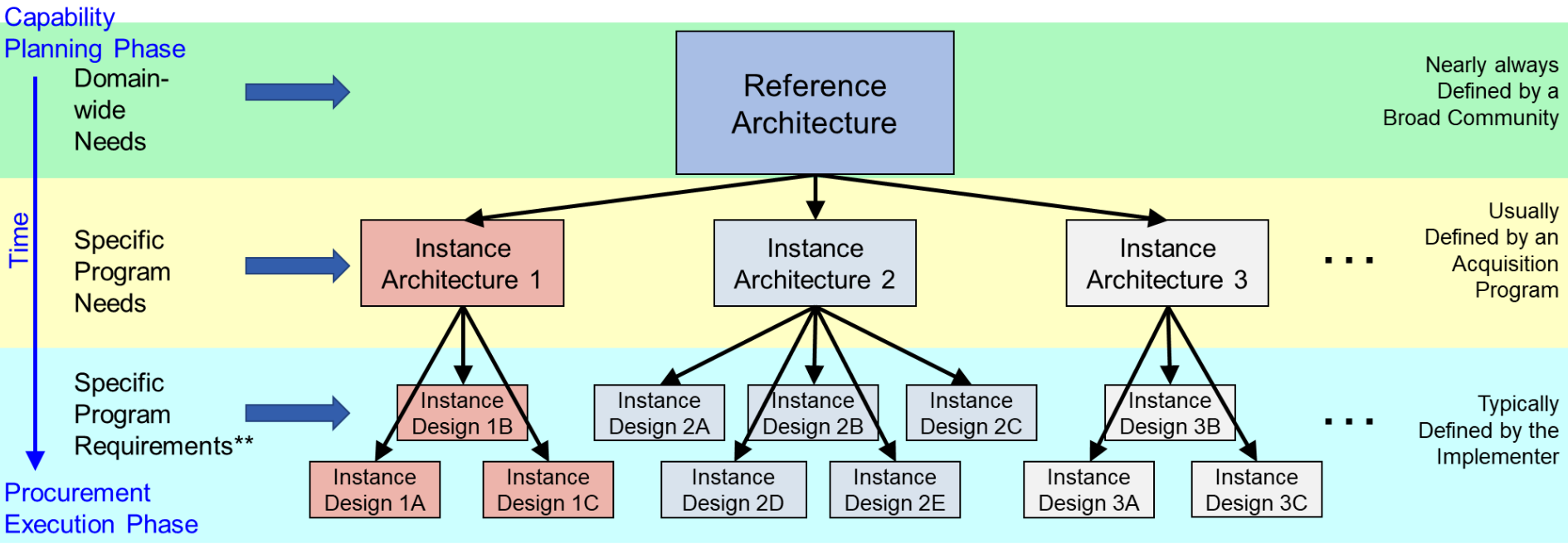
Program Name	Service	Type	Domain	Government Lead	Industry Partners
Bane	Navy	HPM	Land	Dahlgren DEW Office (DEWO)	
Tactical High-Power Microwave Operational Responder (THOR)	USAF	HPM	Land	AFRL	BAE Systems (BAE), Leidos, Verus Research
DE-Maneuver Short Range Air Defense (MSHORAD)	Army	HEL	Land	Army RCCTO	Kord Technologies (Kord)
Indirect Fire Protection High Energy Laser (IFPC-HEL)	Army	HEL	Land	RCCTO, OSD, SMDC	Dynetics (a Leidos Co.), Lockheed Martin Corporation (LMC), MZA Associates Corporation (MZA)
High Power Joint Electromagnetic Non-Kinetic Strike (HiJENKS)	Navy: ONR USAF: AFRL	HPM	Air	Dahlgren /Kirtland	LMC
Self-protect High Energy Laser Demonstrator (SHiELD)	USAF	HEL	Air	AFRL	LMC and Northrop Grumman
Airborne High Energy Laser (AHEL)	USAF	HEL	Air	AF Special Operations Command (AFSOC)	
High Energy Laser with Integrated Optical-dazzler and Surveillance (HELIOS)	Navy	HEL	Sea	PEO IWS 2	LMC
Layered Laser Defense (LLD)	Navy	HEL	Sea	ONR	LMC
Solid State Laser Technology Maturation (SSL-TM)	Navy	HEL	Sea	Dahlgren	NG

DEWS Open Reference Architecture Modules



* Showing only a small subset of interfaces to ensure clarity of the graphic

How a Reference Architecture* fits into the Development Process



---

* The Reference Architecture will evolve over time as experience from its use is folded back into it

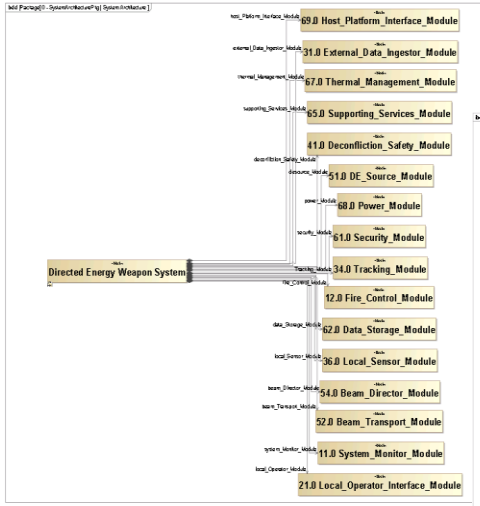
** Selection of the Implemented Design will be based on factors such as price/performance trades, SWaP, etc.

Derived from SOSA 101

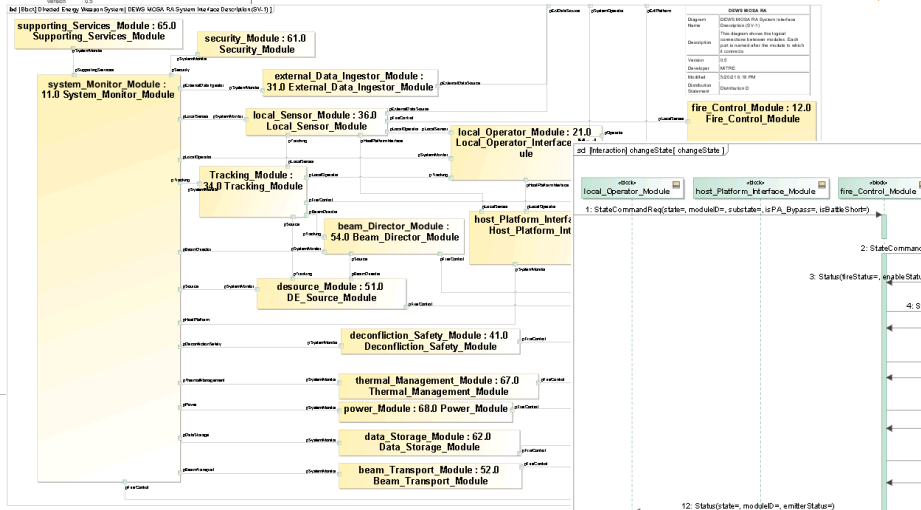
DEWS MOSA Reference Architecture Model

- The DEWS MOSA RA will be provided as a Digital Engineering product, directly usable as a base for implementing programs
- Accompanying documentation will provide guidance on use, including with other standards

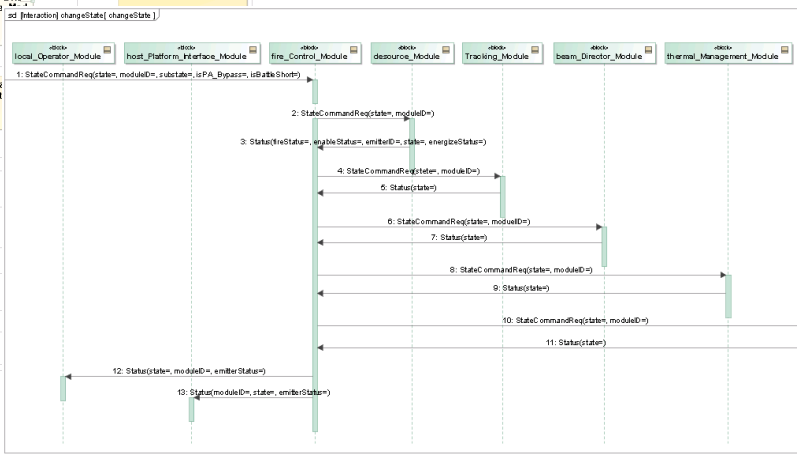
System Architecture



System Interfaces

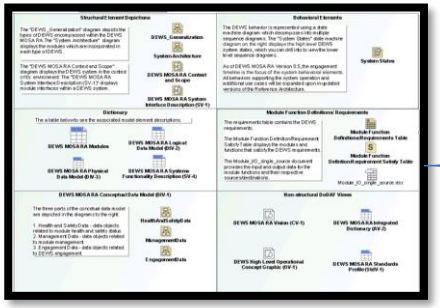


System Behavior



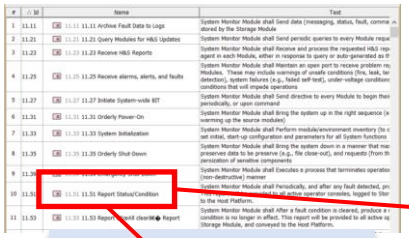
Distribution A: Approved for Public Release

DEWS RA Model Components

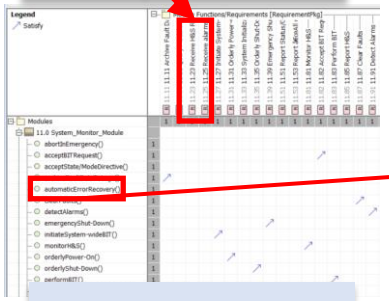


Landing Page to Navigate the Reference Architecture

Requirements

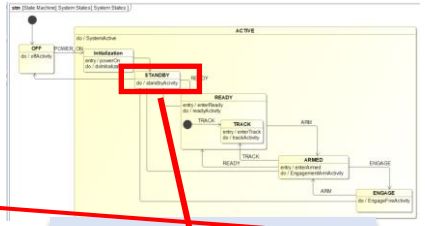


Module Interface Requirements

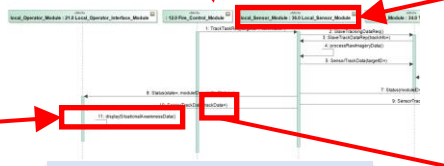


Module Functions

Behavioral



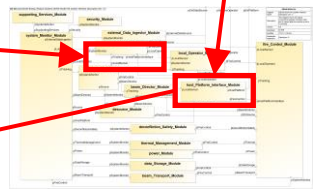
State Machine



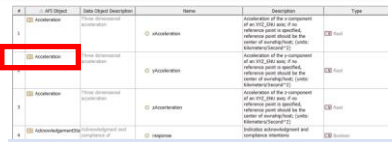
Sequence Diagram

Structural

System Architecture

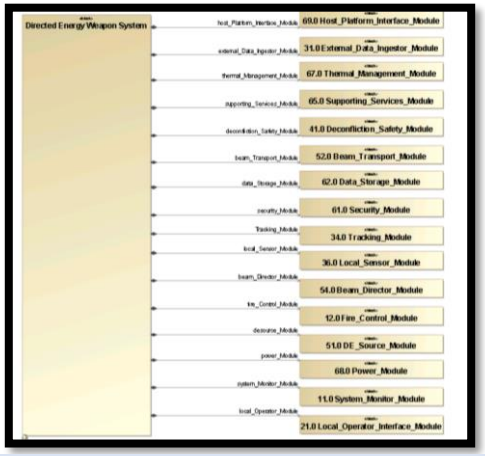


System Interface Description

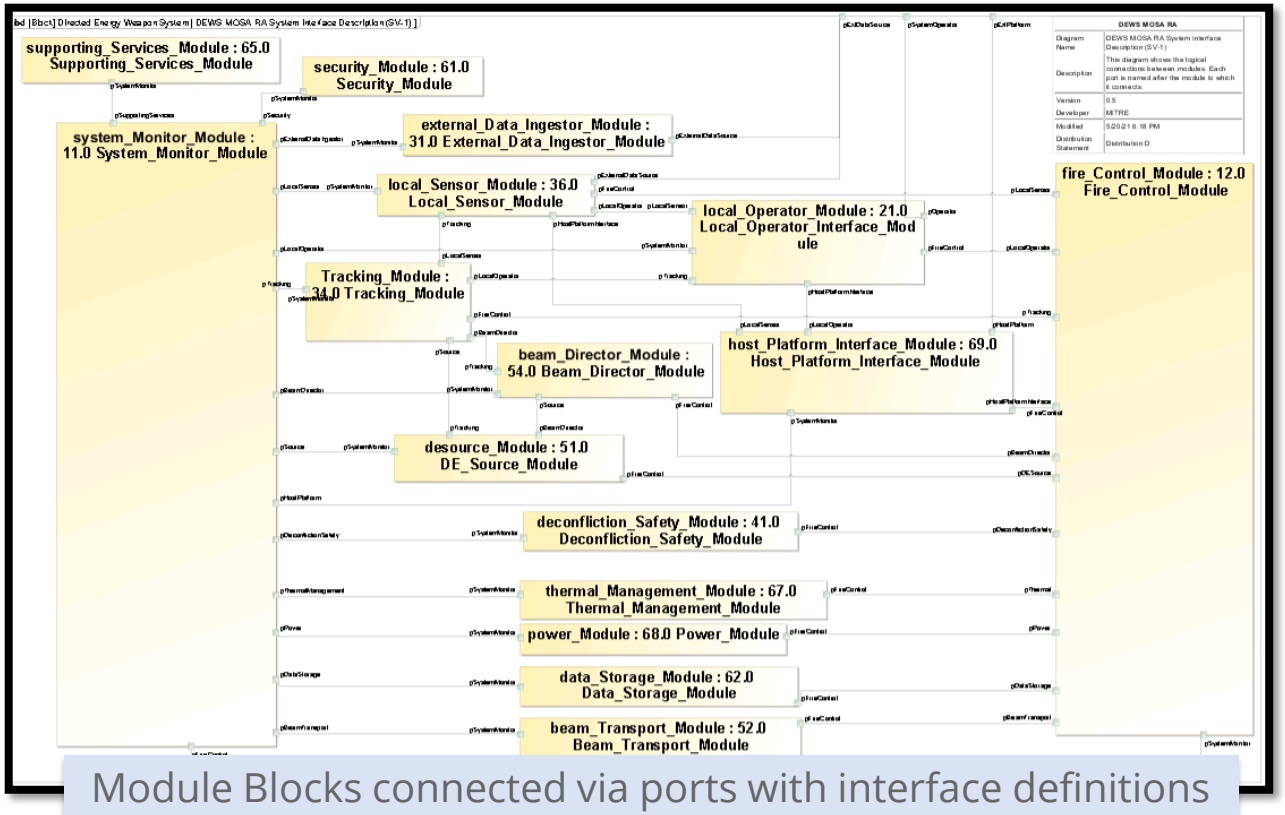


Data Model

DEWS RA Module System Architecture



Module Definitions



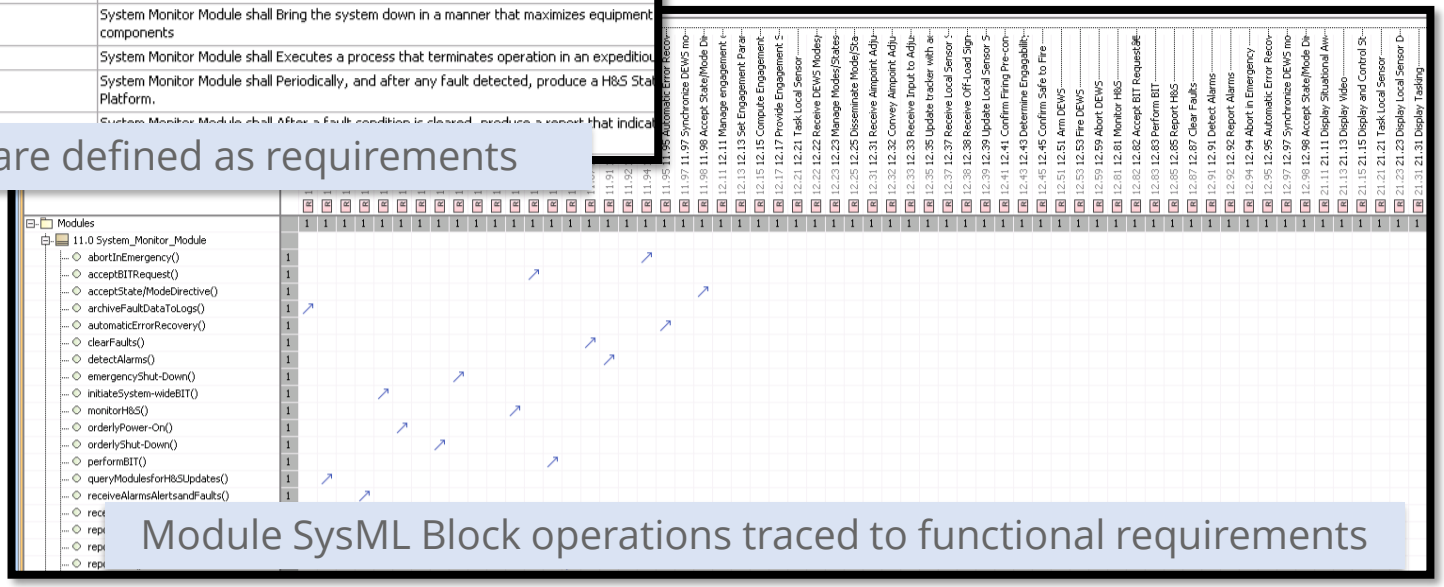
Module Blocks connected via ports with interface definitions

Distribution A: Approved for Public Release

Functional and Interface Requirements

#	Id	Name	
1	11.11	11.11 11.11 Archive Fault Data to Logs	System Monitor Module shall Send data (messaging, status, fault, command, etc.) and vide
2	11.21	11.21 11.21 Query Modules for H&S Updates	System Monitor Module shall Send periodic queries to every Module request routine H&S re
3	11.23	11.23 11.23 Receive H&S Reports	System Monitor Module shall Receive and process the requested H&S reports (that come fr
4	11.25	11.25 11.25 Receive alarms, alerts, and faults	System Monitor Module shall Maintain an open port to receive problem reports from any ar failures (e.g., failed self-test), under-voltage conditions, interlock trips, or other condition
5	11.27	11.27 11.27 Initiate System-wide BIT	System Monitor Module shall Send directive to every Module to begin their BIT process, up
6	11.31	11.31 11.31 Orderly Power-On	System Monitor Module shall Bring the system up in the right sequence (enabling cooling be
7	11.33	11.33 11.33 System Initialization	System Monitor Module shall Perform module/environment inventory (to confirm all are on-
8	11.35	11.35 11.35 Orderly Shut-Down	System Monitor Module shall Bring the system down in a manner that maximizes equipment components
9	11.39	11.39 11.39 Emergency Shut-Down	System Monitor Module shall Executes a process that terminates operation in an expeditiou
10	11.51	11.51 11.51 Report Status/Condition	System Monitor Module shall Periodically, and after any fault detected, produce a H&S Stat Platform.
11			

Module functions are defined as requirements



Module SysML Block operations traced to functional requirements

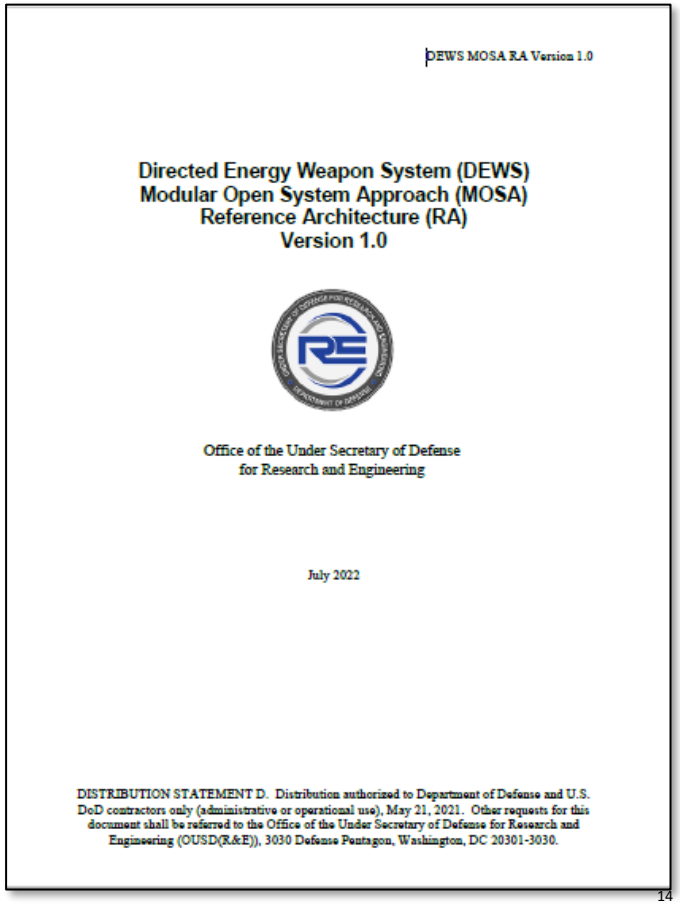
Reference Architecture Released to Government and Industry

Version 1.0 of the Reference Architecture released 22 July 2022

- Reference Architecture Document
- Digital Model and Tools
- Supplemental Material
  - Implementation Guidance
  - Alignment Assessment Guidance
  - Acquisition Guidance

Incorporated feedback from government and industry based on version 0.7 of the Reference Architecture

- Industry review via RFI
- Held an Industry Day on November 4, 2021
- Received hundreds of feedback comments
- Dialog with submitters to address questions



DEWS MOSA RA Version 1.0

Directed Energy Weapon System (DEWS)
Modular Open System Approach (MOSA)
Reference Architecture (RA)
Version 1.0

Office of the Under Secretary of Defense
for Research and Engineering

July 2022

DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only (administrative or operational use), May 21, 2021. Other requests for this document shall be referred to the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), 3030 Defense Pentagon, Washington, DC 20301-3030.

Distribution A: Approved for Public Release

How to Use the DEWS MOSA RA

- To obtain the DEWS MOSA RA, contact dewsra@mitre.org

- The DEWS RA is complementary to other standards
  - Each platform may have an architecture
  - Integration standards may be used across the wider system
  - DEWS RA v1.0 does not specify hardware-level implementation of interfaces, cabling, and module hosting; look to hardware standardization for these

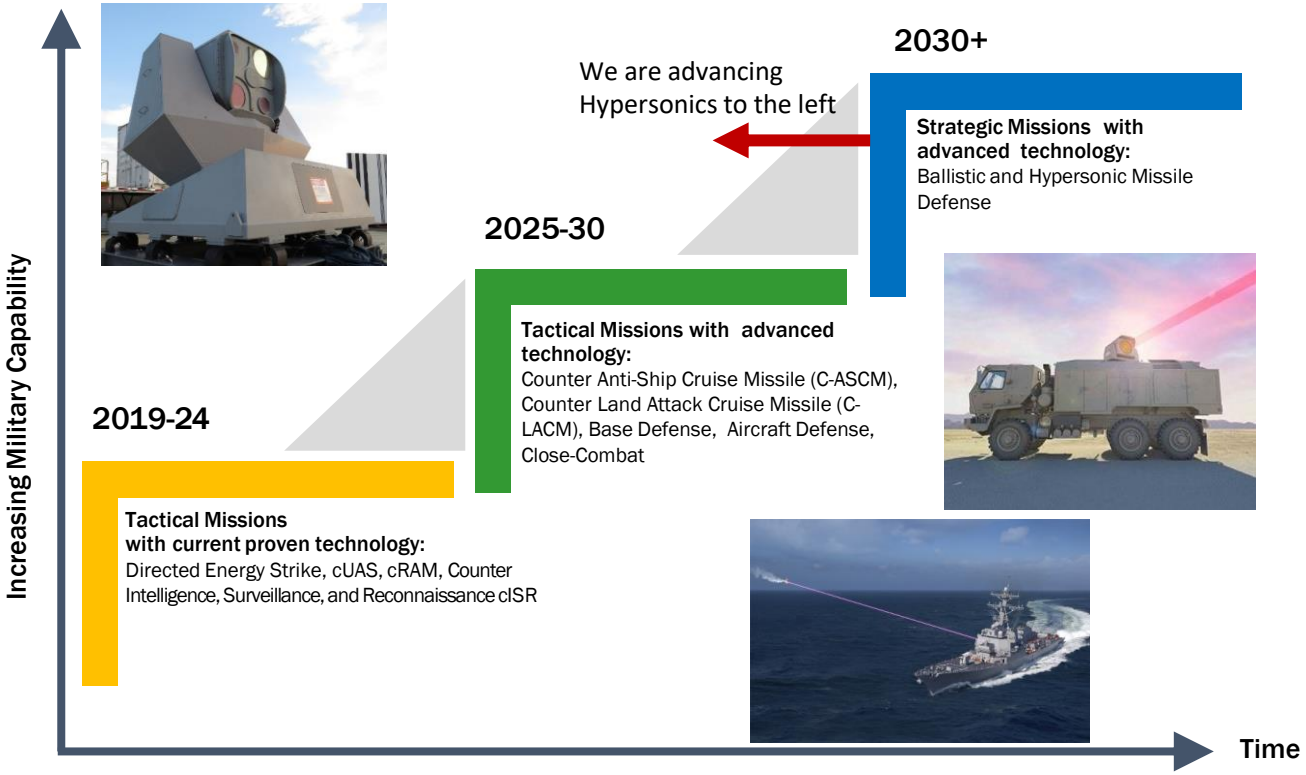
- The MBSE model provides base objects which can be specialized, extended, and refined to provide instance-specific modeling elements.

Distribution A: Approved for Public Release

DEW Roadmap: Mission Growth From Simple To Complex, & Short Range To Long

Key Aspects

- Achieve military dominance in every mission area where DEW makes technical sense
- Develop operational experience, knowledge, and confidence through operational demonstrations
- Advance and mature the technology to increase lethality, expand the mission set, and counter future adversaries
- Deliver new military capabilities with proven technology



Achieving MOSA Benefits
A Decision Framework For Choosing MOSA Metrics

What Questions Should We Be Asking?

"Change begins with inquiry, and Leading with Questions jump-starts the process with its practical approach for leaders who want to develop and ask questions that provoke reflection, get meaningful information, and initiate action."

Leading with Questions: How Leaders Find the Right Solutions By Knowing What To Ask, Michael Marquardt

Steve Henry
tamu1971@msn.com

Bob Scheurer
Robert.P.Scheurer@boeing.com

Ed Moshinsky
ed.moshinsky@gmail.com

Joseph Bradley
josephbradley@leadingchangellc.net

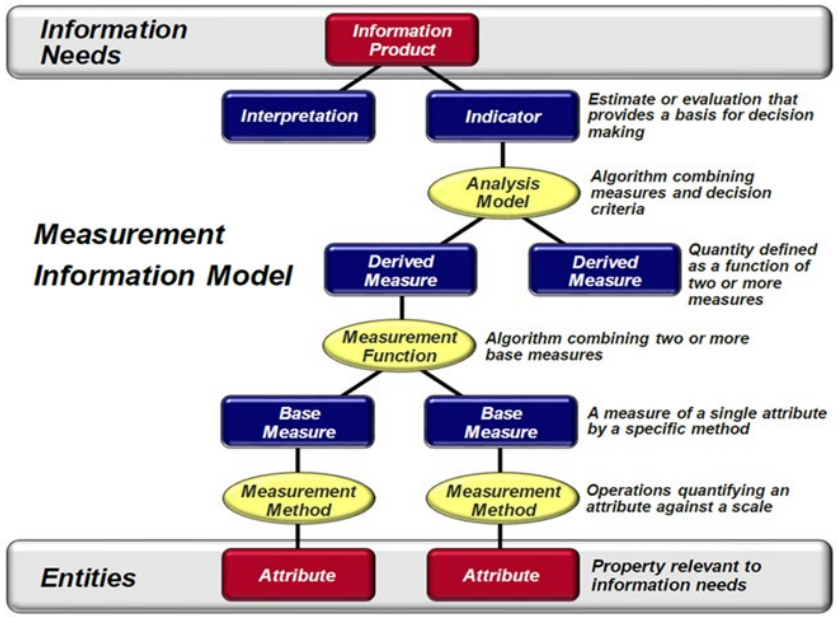
Version 25, 23 Oct 22

Approved for Public Release

How Can We Define MOSA Success?

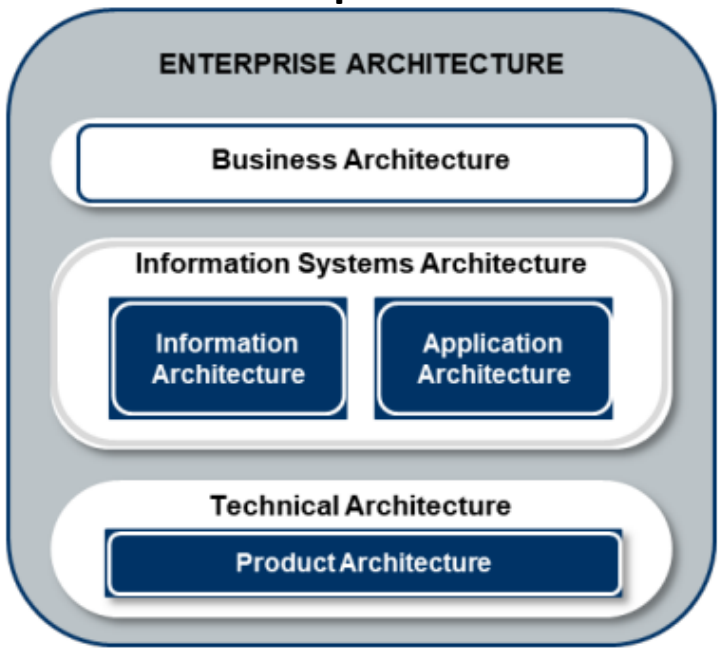
Practical Software and Systems Measurement Continuous Iterative Development Measurement Framework, V 2.1

MOSA Metrics



MOSA Reference Frameworks in Defense Acquisition Programs, May 2020

MOSA Implementation



Decision/ Knowledge Management

Project Assessment and Control

Measurement

Project Planning

MOSA Objectives and Enablers

Continuous Competition
Reference Architectures
Mission Integration
Interoperability
Cost Savings
Product Life cycle
Operational Flexibility
Commonality
Rapid Tech Refresh
CM
Profit
Interfaces
Integration
Open Standards
ROI
Revenue Growth
Standards Conformance
Enabling Environment
Modular Design
Affordability
Reuse
Supply Chain

DoD Modular Open System Approach Ecosystem

What are the Different Stakeholders Views of MOSA Success?

Policy and Guidance Effectiveness and Achievement of MOSA Benefits

MOSA Strategy to Achieve Desired Benefits - Cost, Schedule, Performance, Speed of Change and MOSA Enabling Environment Process Controls

Availability of Staffing Resources and Skills to Support Effective Requirements Development and Planning

Modular Design - MBSE, Resilient Architecture, Open Standards, Design Interfaces, Modularity, Integration, Verification, Product Line Engineering and Interoperability

Statutory, Policy, Standards Conformance, High Quality, and Configuration Management

Continuous Competition, Contract Performance, and MOSA Enabled Supply Chain

DoD and Commercial Contract Opportunities, Revenue Growth, Profit, and Return on Investments

Adapted: Under Secretary of Defense for Research and Engineering, Modular Open System Approach

How Do We Achieve MOSA Success?

MOSA Enablers

Mature Systems Engineering

- Acquisition and Supply Processes
- Organizational Project Enabling Processes
- Technical Management Processes
- Technical Processes

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition

Digital Engineering Environment
"Authoritative Source of Truth"

Establish Enabling Environment

Employ Modular Designs

Designate Key Interfaces
Use Open Standards
Certify Conformance

Mission Integration Management

DoD MOSA Benefits

Enhance competition open architecture with severable modules, allowing components to be openly competed

Enable cost savings/cost avoidance reuse of technology, modules, and/or components from any supplier across the acquisition life cycle

Facilitate technology refresh delivery of new capabilities or replacement technology without changing all components in the entire system

Incorporate innovation operational flexibility to configure and reconfigure available assets to meet rapidly changing operational requirements.

Improve interoperability allow severable software and hardware modules to be changed independently

Adapted: Under Secretary of Defense for Research and Engineering, Modular Open System Approach

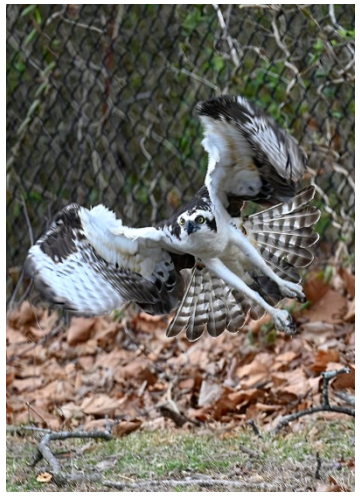
Measurement Selection/Tailoring Lessons Learned

"What Gets Measured Get Done"

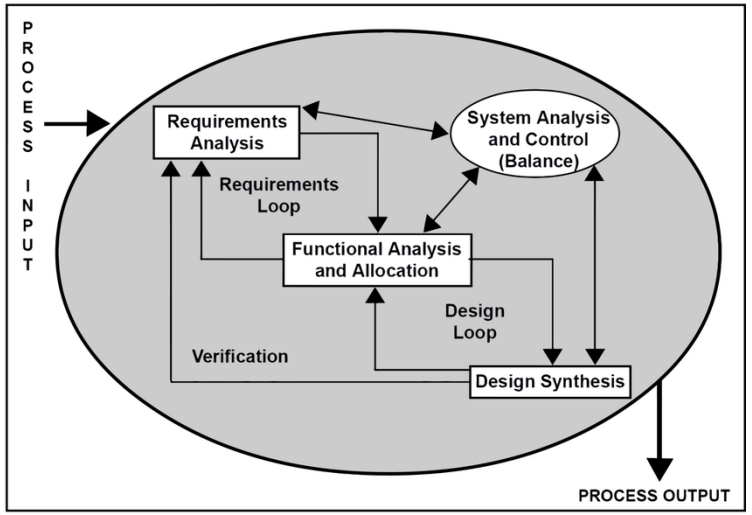
- Develop and track metrics to control processes, measure against goals and objectives, and make decisions
  - **How do we know we will succeed?**
  - **If a metric won't help make a decision, you don't need it**
- There will be fact of life metric "taxes" from external sources
  - **How does your customer user the information and metrics?**
- Metrics tracked and owned at Program, Functional, and IPT levels
  - **What information is needed to do the job at all levels of the organization?**
- Define a minimum core set -- teams may want/need more
- Goal:
  - **Focus on Your Goal and Desired Benefit**
  - **Obtain Delivery Velocity/Meet Commitments**
  - **Ensure Quality**
  - **Enable Insight**

Metric Selection Philosophy is a Forcing Function

Sample MOSA Benefit Measurement Use Cases

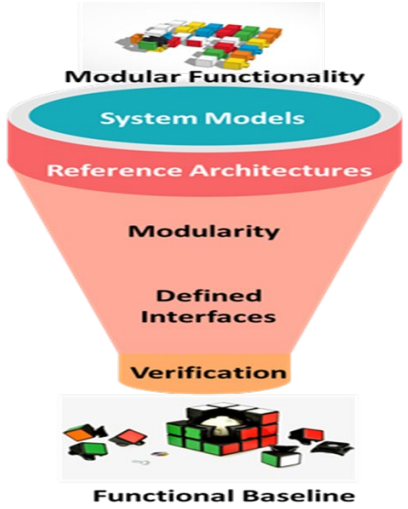


MOSA in Nature



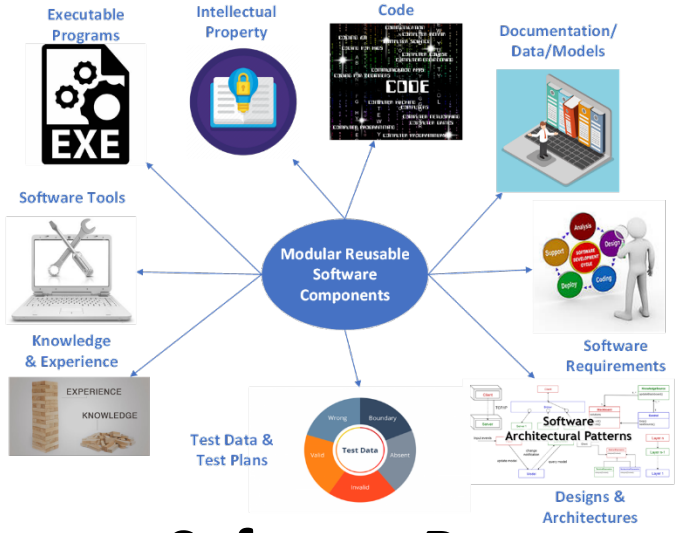
Systems Engineering Life Cycle MOSA Implementation

GATM Business Case – Collins KC-135



Interoperability

What other Use Cases do we need?



Software Reuse

Osprey Nest MOSA

Modular Component Integration

What's Important to the Osprey?

Loosely Couple Nest Architecture

Conformance With Accepted Open Standards and Key Interfaces

Lifecycle Modular Part Supply Chain

Rapid Technical Refresh

Abundant Food

Multi-level Security

Operational Flexibility

Osprey MOSA Enabling Environment

MOSA Benefit

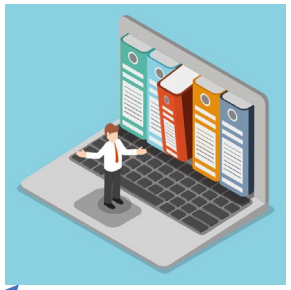
How do We Measure the Benefits of SW Reuse?

Executable Programs

Intellectual Property

Code

Documentation/ Data/Models

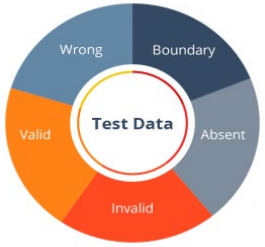


Software Tools

Modular Reusable Software Components

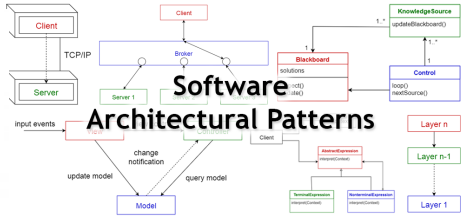
Knowledge & Experience

Test Data & Test Plans



Software Requirements

Designs & Architectures



Potential MOSA Reuse Benefit Metrics

- Release Frequency
- Cycle Time Reductions
- Schedule Reductions
- Cost Avoidance
- Team Velocity
- Technical Refresh Innovation Adoption Frequency
- Mean Time to Repair/Replace
- Return on Investment

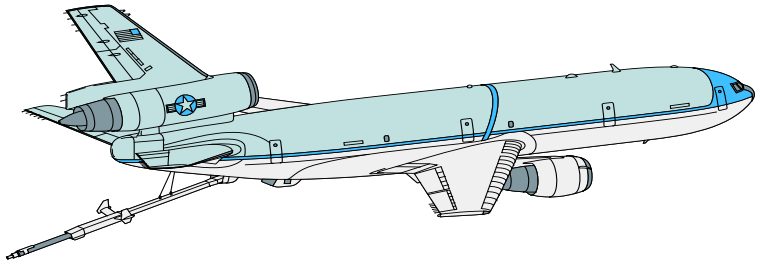
Global Air Traffic Management (GATM) Mission Needs and MOSA Business Case

Communication
Digital Radios to Handle Reduced Channel Spacing and Datalink

Navigation
Better Horizontal and Vertical Position Accuracy to Meet Required Navigation Performance in Reduced Separation Environment

Surveillance
Enhanced Situational Awareness, Collision Avoidance and Automatic Position Reporting Via Datalink

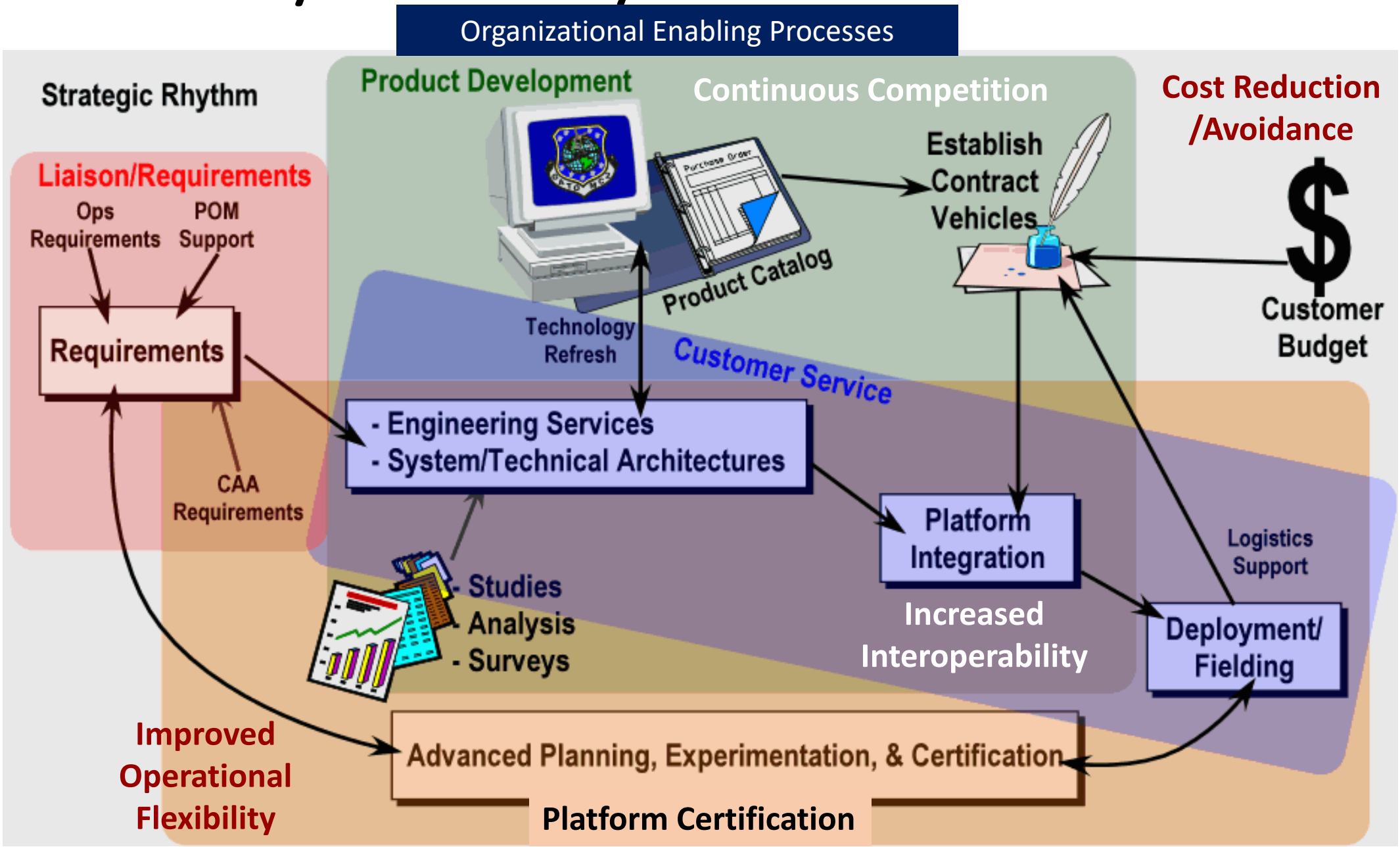
Air Traffic Management
Transition From Air Traffic Control to Management Using New Procedures and Automation



- **$2.5 B Program**
- **28 Aircraft Programs**
- **20+ Modular Components**
- **Published International/ FAA Standards**
- **Immediate Operational Impacts**
- **Short Implementation Schedule**

Failure to comply with international aviation flight standards and equipage will result in restrictions in worldwide airspace and decreased combat capabilities

GATM System Of Systems SPO CONOPS



What Were the GATM Stakeholder MOSA Success Metrics?

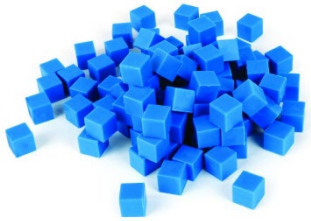
GATM Program Office	Aircraft Program Office	Major Command
GATM Acquisition Capability Time Lines • Cycle Time (Time from RFP Release to Contract Award) – component availability • Competition Frequency Planned vs Actual	**Aircraft GATM Integration/ Deployment Timelines** • On time GATM Component Delivery vs need • Aircraft GATM Integration Cycle Times	**Aircraft GATM Deployment Timelines** • GATM Equipage % by Fleet Burndown • Denied Airspace Access Backlog

Competition Cost Savings
• Component Unit Pricing Catalog versus IDIQ Bid Prices
• Component Unit Pricing Trends over time
• Component Repair Cost
• Quantity Buy Savings
• Integration Competition Cost Savings
	Aircraft GATM equipage cost
	• Aircraft Integration Cost Funding Shortfalls
	  • Integration Competition Cost Savings
	  • Integration Cost Avoidance
	• GATM Component Unit Pricing Trends over time
	• GATM Component Repair Cost
		Total GATM Program Cost
		• Aircraft Integration Cost vs Committed
		• Sustainment Cost Reductions
		  • Mean Time Between Failures
		  • Mean Time to Repair
		• GATM Competition Cost Savings
		• Commonality Across Platforms
		• Lifecycle Cost

Speed of Delivery • Delivery Time vs Contract • Mean Time to Repair and Return • Surge Repair Delivery Times	**Speed of Delivery** • Average GATM Component Delivery time from time of order • Aircraft GATM Modification Cycle Time Trends	**Speed of Delivery** • Aircraft GATM Equipage vs Need Timelines • Mean Time to Repair and Return
Aircraft Conformance to GATM Standards • USAF GATM Conformance Requirements • Component Standards Conformance • Aircraft GATM Conformance burn down	**Aircraft Conformance to GATM Standards** • Aircraft GATM Conformance burn down • Aircraft Safety Standards Conformance • System Suitability and Effectiveness Measures	**Aircraft Conformance to GATM Standards** • Airspace Access Standards Conformance • Mission Limitations Burndown • Operations That Can Be Executed vs Committed

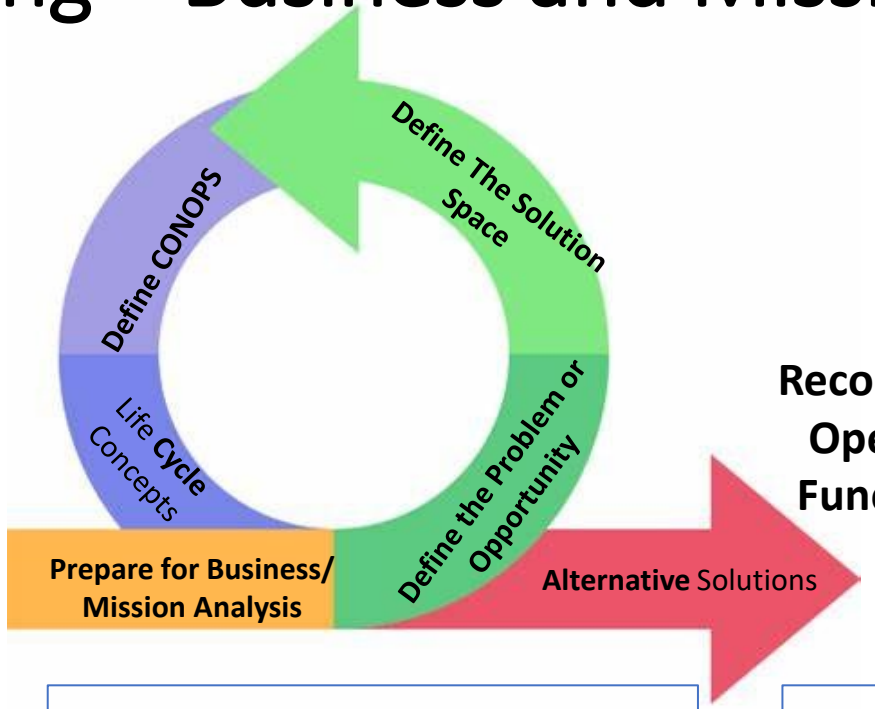
Systems Engineering Life Cycle MOSA Implementation
Systems Engineering – Business and Mission Analysis

Modular Parts



Modular Functionality

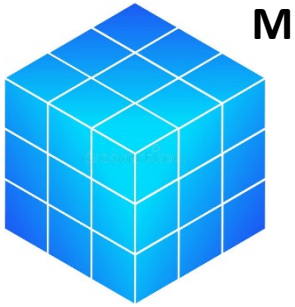
It starts with Mission Engineering



Alternative Solutions

Reconfigurable Operational Functionality

Multi-Function



Scaled Single Function

MOSA Information Needs

- Organization Strategic Plan
- Program/Mission Constraints
- Mission characterization
- MOSA Candidate solutions
- Reuse Opportunities
- MOSA Benefits opportunities
- Solution Modularity to support CONOPS, Technical Refresh and Competition
- Mandatory Standards and Reference Architectures

Process MOSA Outputs

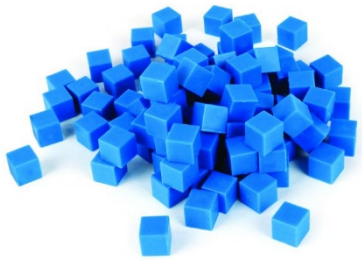
- Stakeholder identification
- Preliminary Life Cycle Concepts
- Problem & MOSA Opportunity Statement
- MOSA Business/IP Requirements
- Preliminary MOSA Benefit evaluation criteria
- MOSA Requirements Traceability
- MOSA Implementation Plan

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition

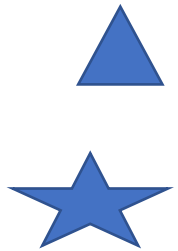
Preliminary MOSA Measurements/Metrics

- **Burndown**
  - MOSA Enabling Environment Backlog
  - Interoperability Gaps Backlog Solution Interfaces
  - Data Standard Compliance Backlog
  - Technical Debt
  - Intellectual Property
- **Committed vs Delivered**
  - Solution Reuse Cost Avoidance
  - Competition Savings Committed vs Achieved
- **Cumulative Flow**

Stakeholder Needs and Requirements



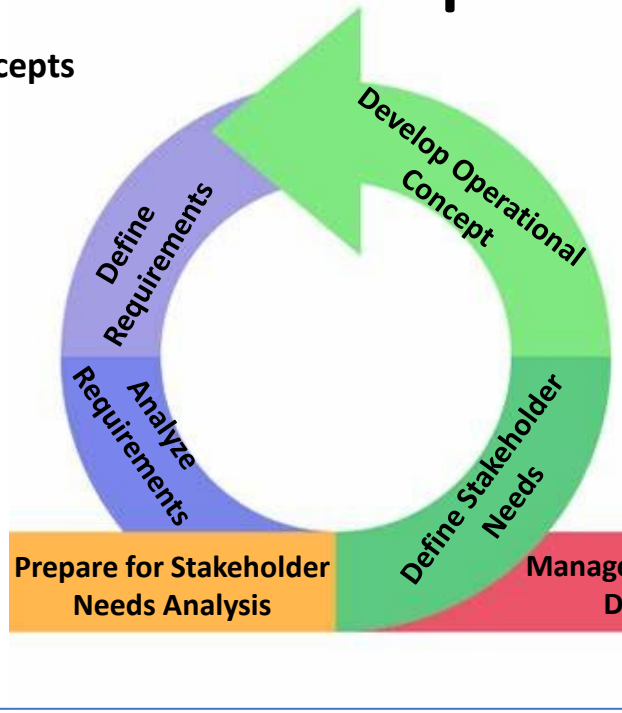
Modular Parts



Modular Concepts

Modular Functionality

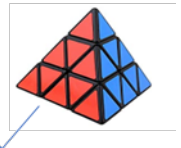
Interfaces

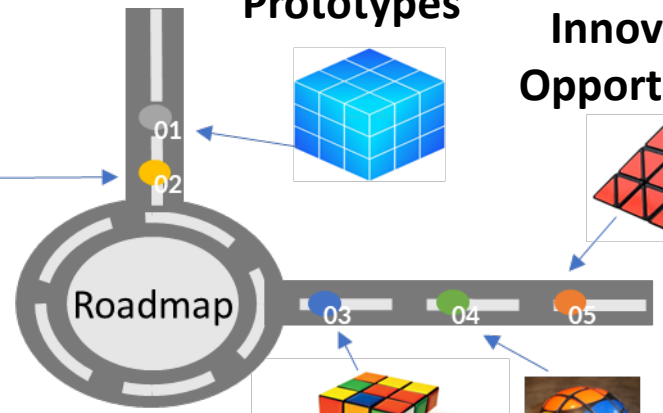


Initial MVP

Rapid Prototypes

Continuous Innovation Opportunities





Lower Cost

Frequent Releases

Modular Operational Agility

Technical Refresh Competition

MOSA Information Needs

- Identify and define constraints on a system
- Identify the MOSA tenets that address the stakeholder needs and the MOSA benefits that will be achieved

Process MOSA Outputs

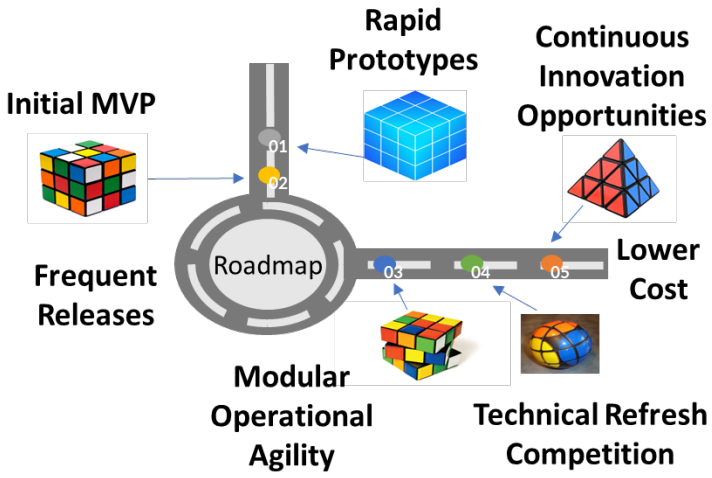
- Stakeholder agreement that their needs, expectations, and interoperability are reflected adequately in the requirements
- Define a representative set of scenarios to identify all required capabilities and MOSA needs that correspond to anticipated operational and other life-cycle concepts.
- Test methodologies to verify MOSA compliance
- Approved Information Support Plan (ISP)

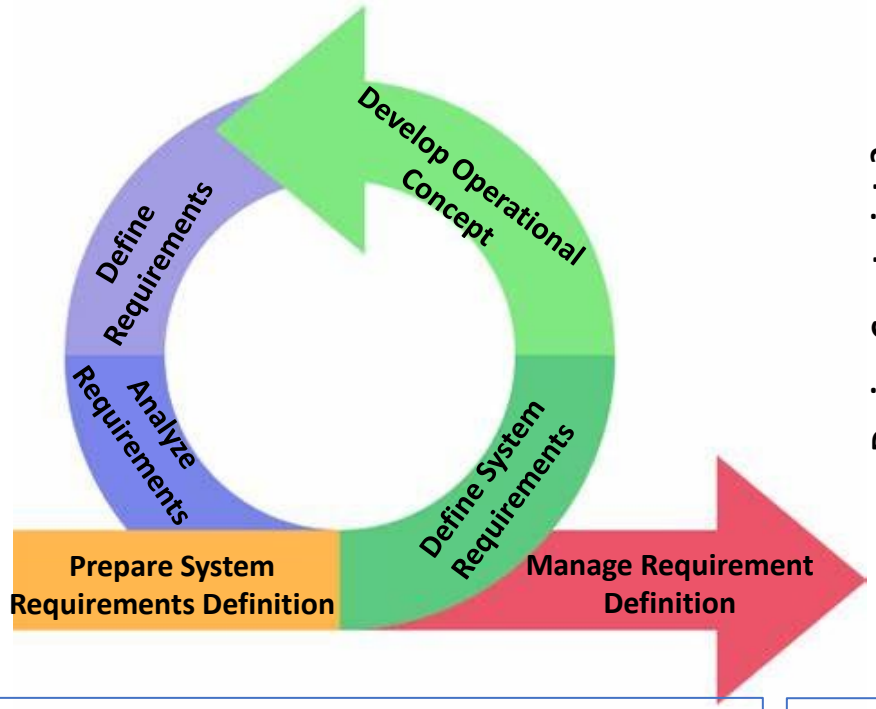
MOSA Measurements/Metrics

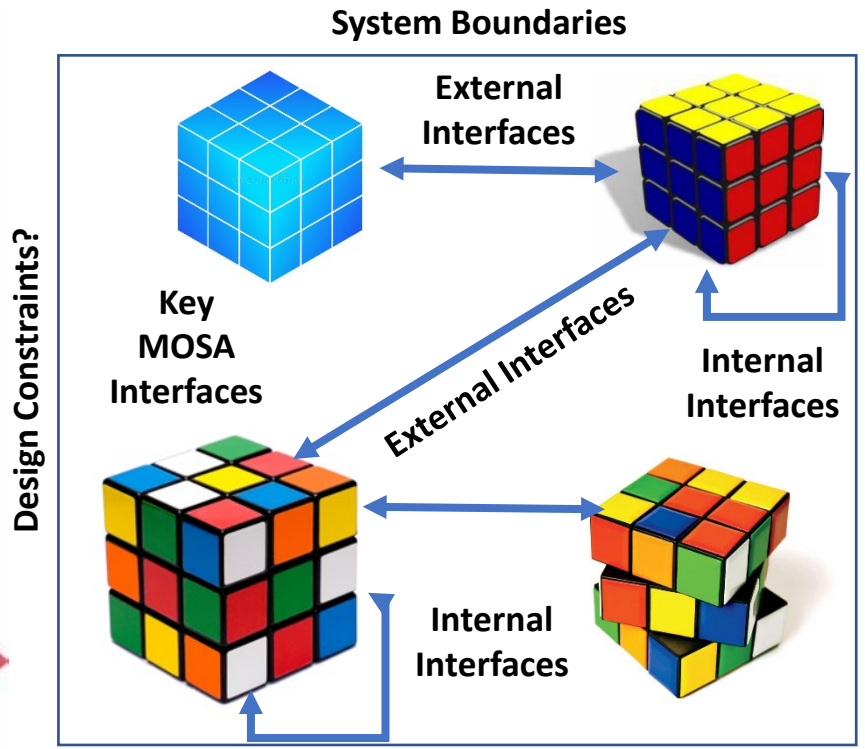
- **Burndown**
  - Conditions Which Operations Can Be Executed Burndown or **Committed vs Delivered**
  - Interoperability Gap Backlog
  - Desired system or system of systems operational configurations backlog
- ***Committed vs Delivered*** *or* ***Cumulative Flow***
  - MOSA Interfaces Standards Identification
  - Requirements Verification Traceability Matrix (RVTM)

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition & AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

Systems Requirements Definition







MOSA Information Needs

- Document system description, including system interfaces, functions and boundaries, for a system solution
- Define system requirements (functional, performance, process, non-functional, and interface) and design constraints

Process MOSA Outputs

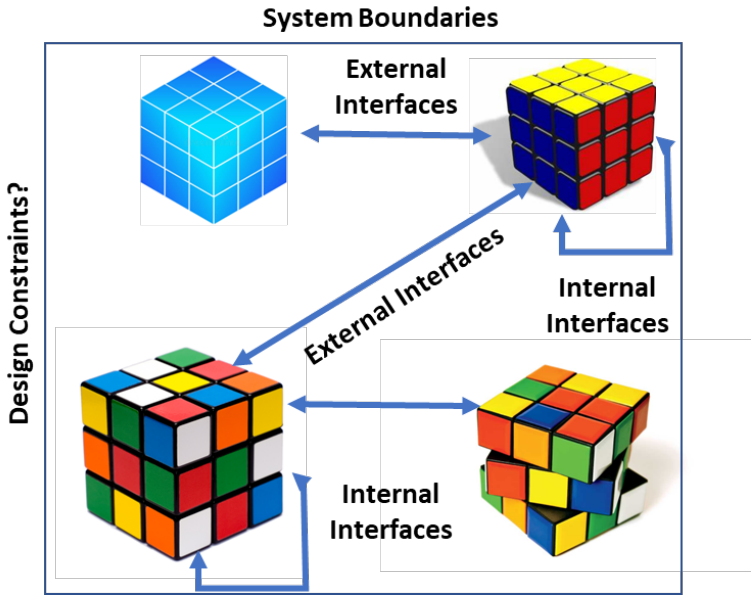
- System functional definition
- Approved System/MOSA Requirements
- System functional interface identification
- System of System interface definition(s)
- MOSA requirements verification criteria
- Updated RVTM

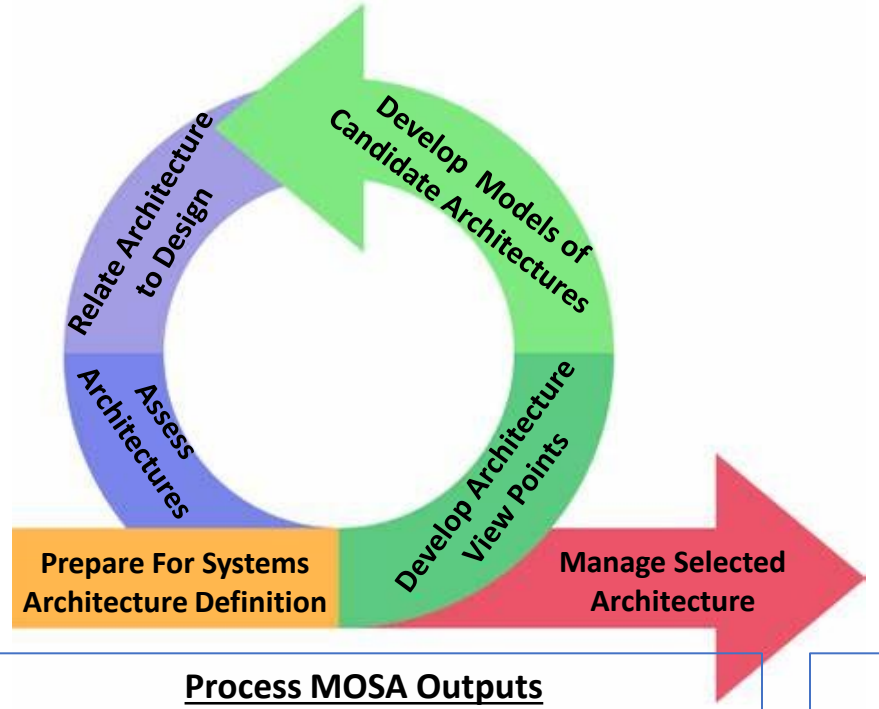
MOSA Measurements/Metrics

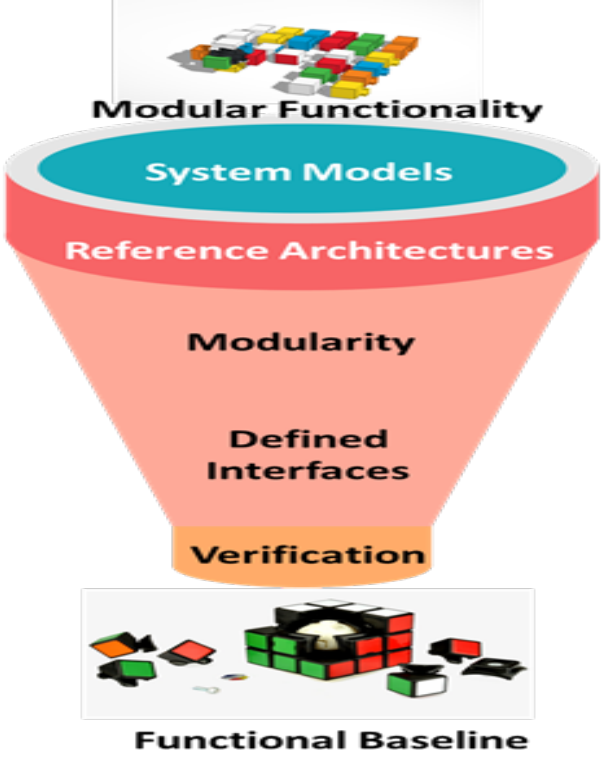
- **Definition Cumulative Flow**
  - Systems Requirement System Interface Identification - Internal and external; Artificial Intelligence; Machine to Machine…
  - Update MOSA Verification Criteria/RVTM
- **Burndown**
  - Status MOSA functional requirements definition
- **Committed vs Delivered**
  - Interoperability Performance Measures
  - MOSA Benefit Performance Measures

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition & AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

Architecture Definition







MOSA Information Needs

- Define context, boundaries, and external interfaces of the system
- Develop/reuse architecture views and models of the system(s)
- Identify system elements and their interfaces
- Alignment of the architecture with requirements and design MOSA characteristics to be achieved.

Process MOSA Outputs

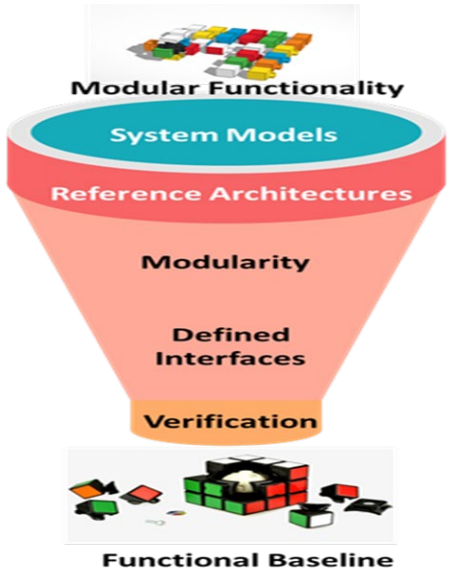
- System functional definition
- System Requirements
- System functional interface identification
- System of System interface definition(s)
- Standard/Reference Architecture Selection
- MOSA requirements verification criteria
- Updated RVTM
- Modular Open System Architecture Selection
- Rational for MOSA design choices
- Functional Baseline

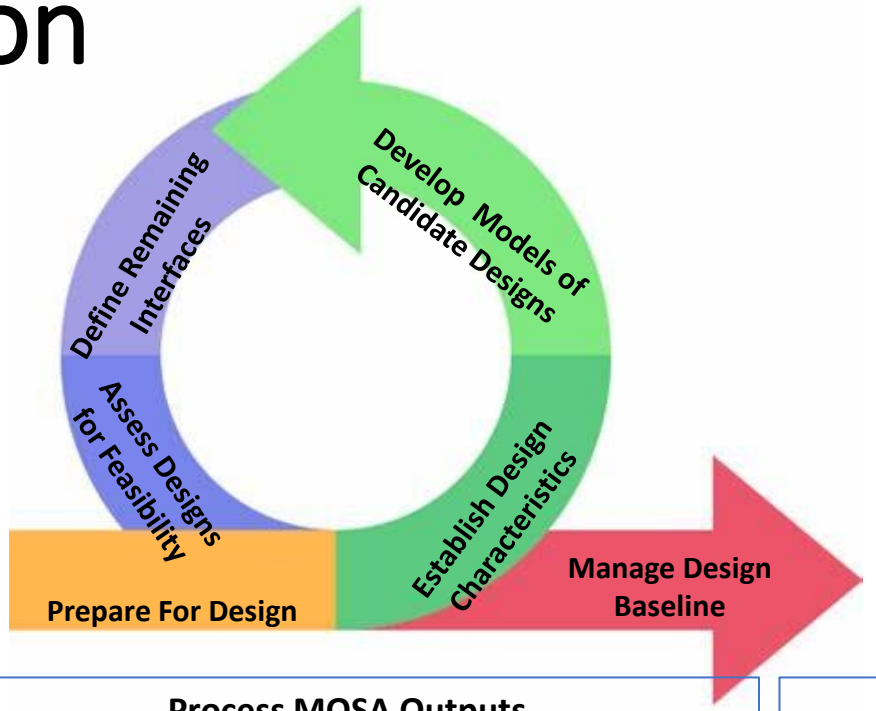
MOSA Measurements/Metrics

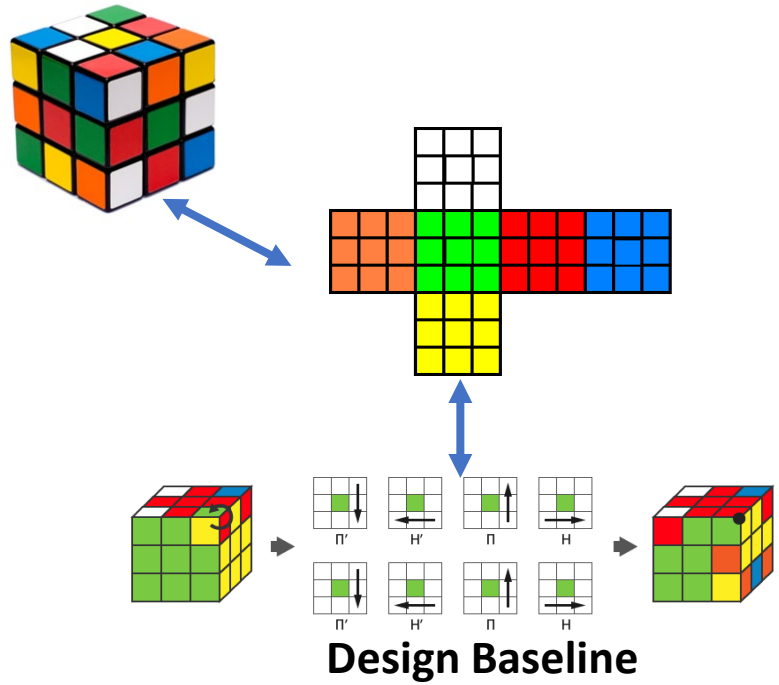
- **Cumulative flow**
  - Functional allocation and analysis
  - System Model completion
- **Burndown**
  - Selected Reference Architecture and Standards conformance
  - System interfaces definition backlog
- **Committed vs delivered**
  - Modularity
  - Cohesion and Coupling
  - Cyclomatic Complexity
  - Change and Propagation

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition & AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

Design Definition







MOSA Information Needs

- System models Maturity
- MOSA Design documentation
- Design rational
- MOSA and Digital Engineering enabling environment
- MOSA Requirements Traceability
- Design Baseline(s)

Process MOSA Outputs

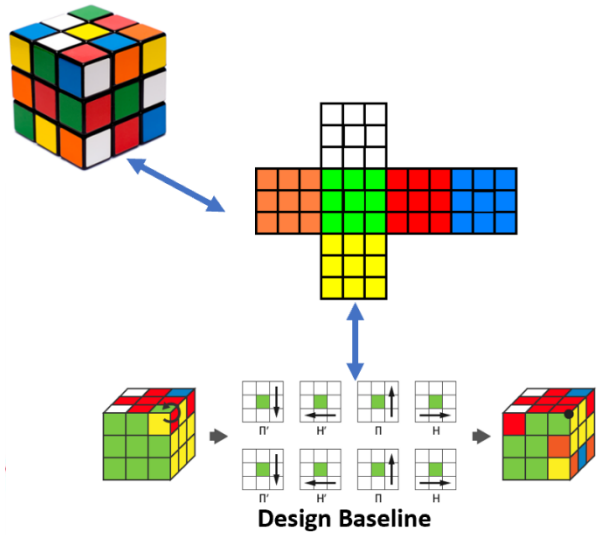
- Defined modular design characteristics of each system element
- Defined and standardize Interfaces (ICD/API) between system elements composing the system to allow for opportunities of future modernization
- Digital modular design artifacts
- MOSA enabling environment necessary for design definition and implementation
- Demonstrated modularity/standards to support desired competition and technical refresh

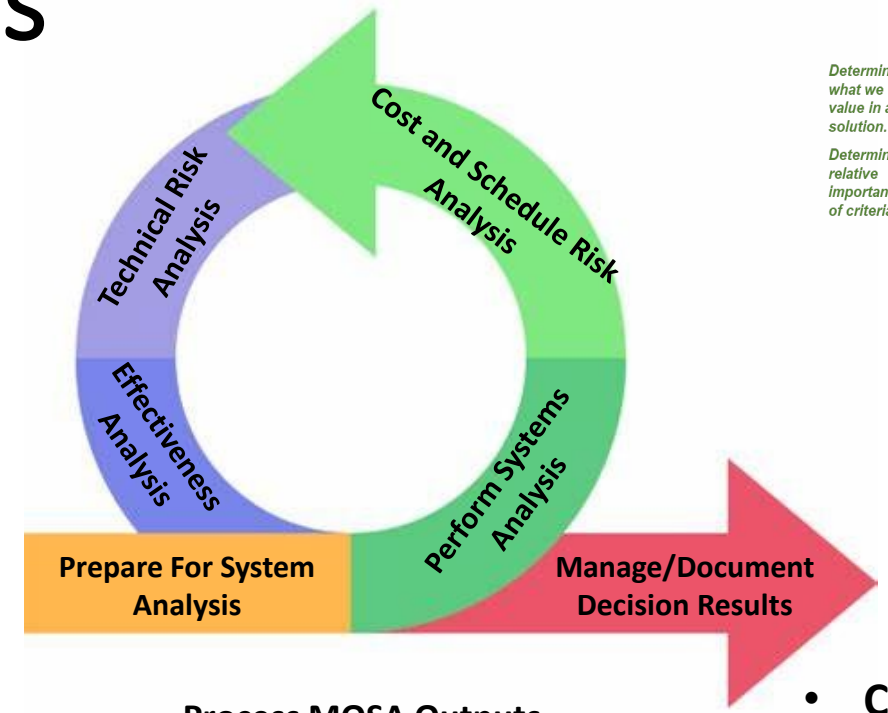
MOSA Measurements/Metrics

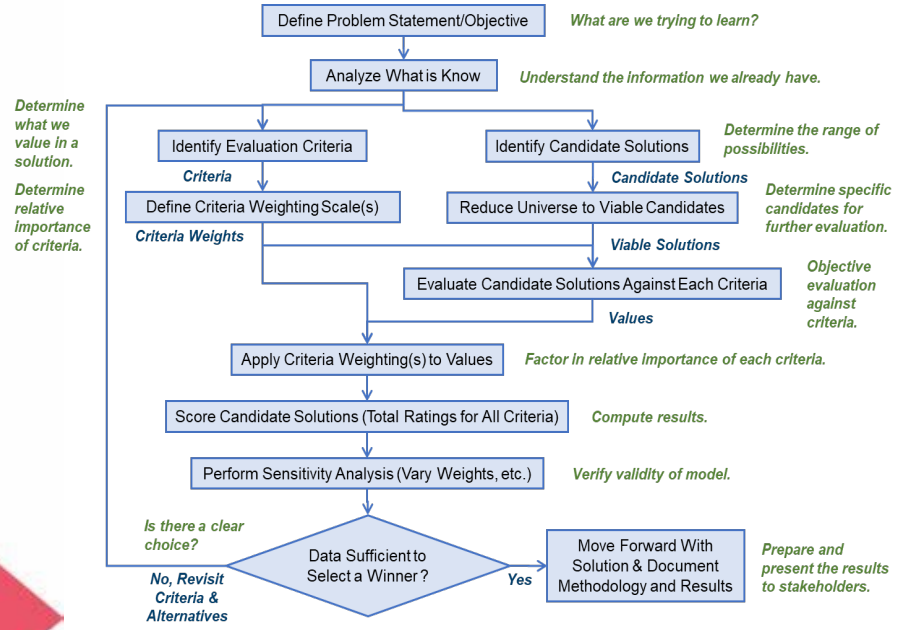
- **Committed vs Delivered**
  - MOSA/Digital Engineering enabling environment
  - Modularity
  - Competition Effectiveness
  - Conditions Which Operations Can Be Executed
- **Burndown or Cumulative Flow**
  - Design Baseline Documentation Backlog
  - Standards Compliance backlog Burndown external/internal interface definitions
- **MOSA Design Performance Metrics**
  - Life Cycle Cost Trends
  - Mean Time to Repair/Recover
  - Integration/Reuse Readiness Levels

Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition & AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

System Analysis







MOSA Information Needs

- MOSA Decisions requiring alternative analysis are identified.
- Alternative courses of to achieve MOSA benefit goals.
- Preferred MOSA course of action
- The resolution, decision rationale and assumptions for MOSA are recorded
- Modular Open Systems Approach into program protection review and analysis

Process MOSA Outputs

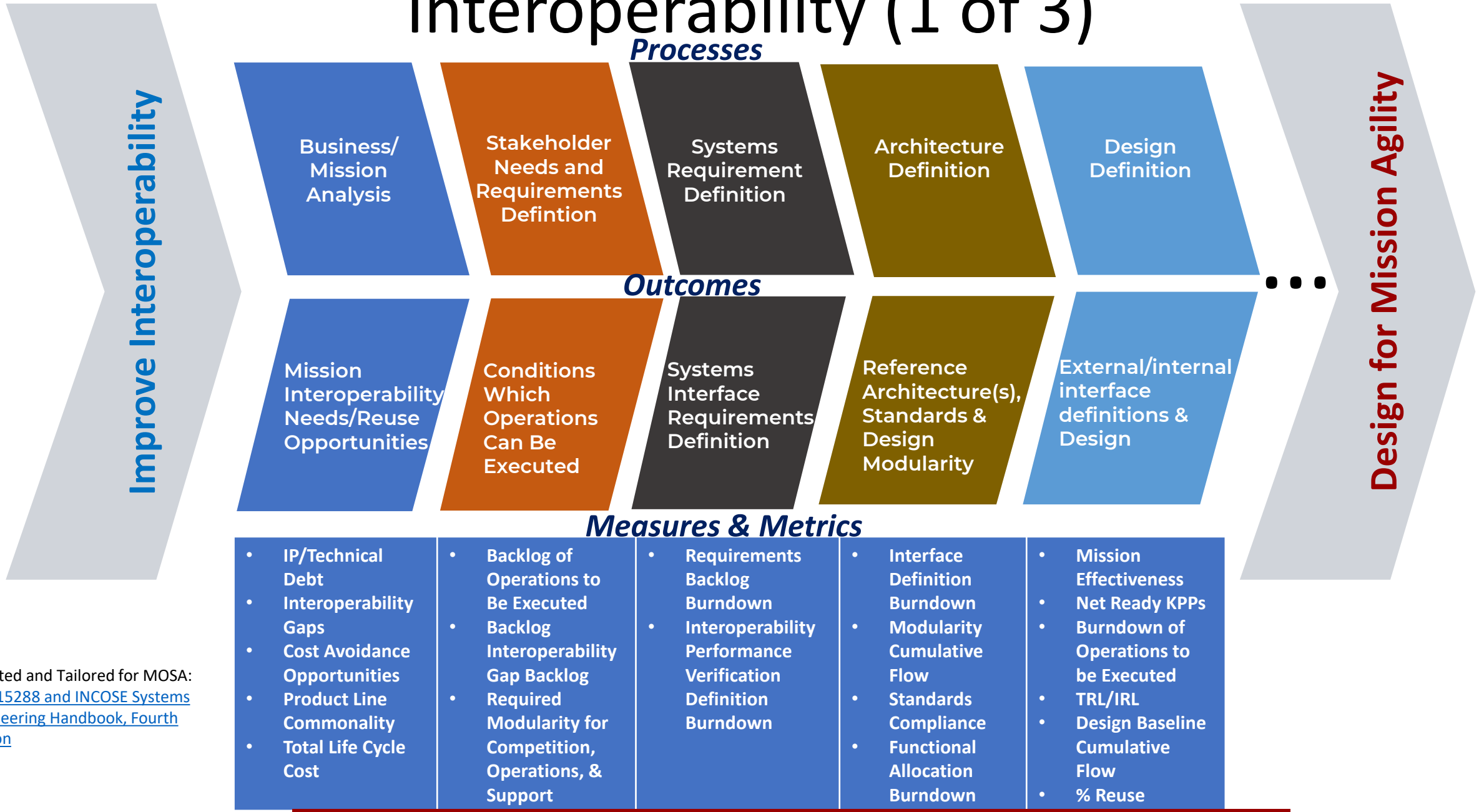
- MOSA competition strategy
- MOSA Technical Refresh Strategy
- Updated MOSA Implementation Plan & SEP/SEMP
- MOSA success measures
- Listing of selected standards and rationale for why they were chosen
- Listing of considered standards that were not selected and why they were not chosen

MOSA Measurements/Metrics

- **Committed vs Delivered**
  - Technology, Integration, and Reuse Readiness Levels
  - Conditions Which Operations Can Be Executed Cost Risk/Affordability Assessments
  - Lifecycle Cost Target Commitments
  - Reuse Cost Savings
- **Schedule/Cost Risks Assessment Trends**
- **Competition Effectiveness**
  - % of BOM Value Competed
  - % of BOM Components with Adequate Competition for Technical Refresh
  - Competition Frequency Planed vs Actual
  - Competitive Cost Savings Committed vs Achieved

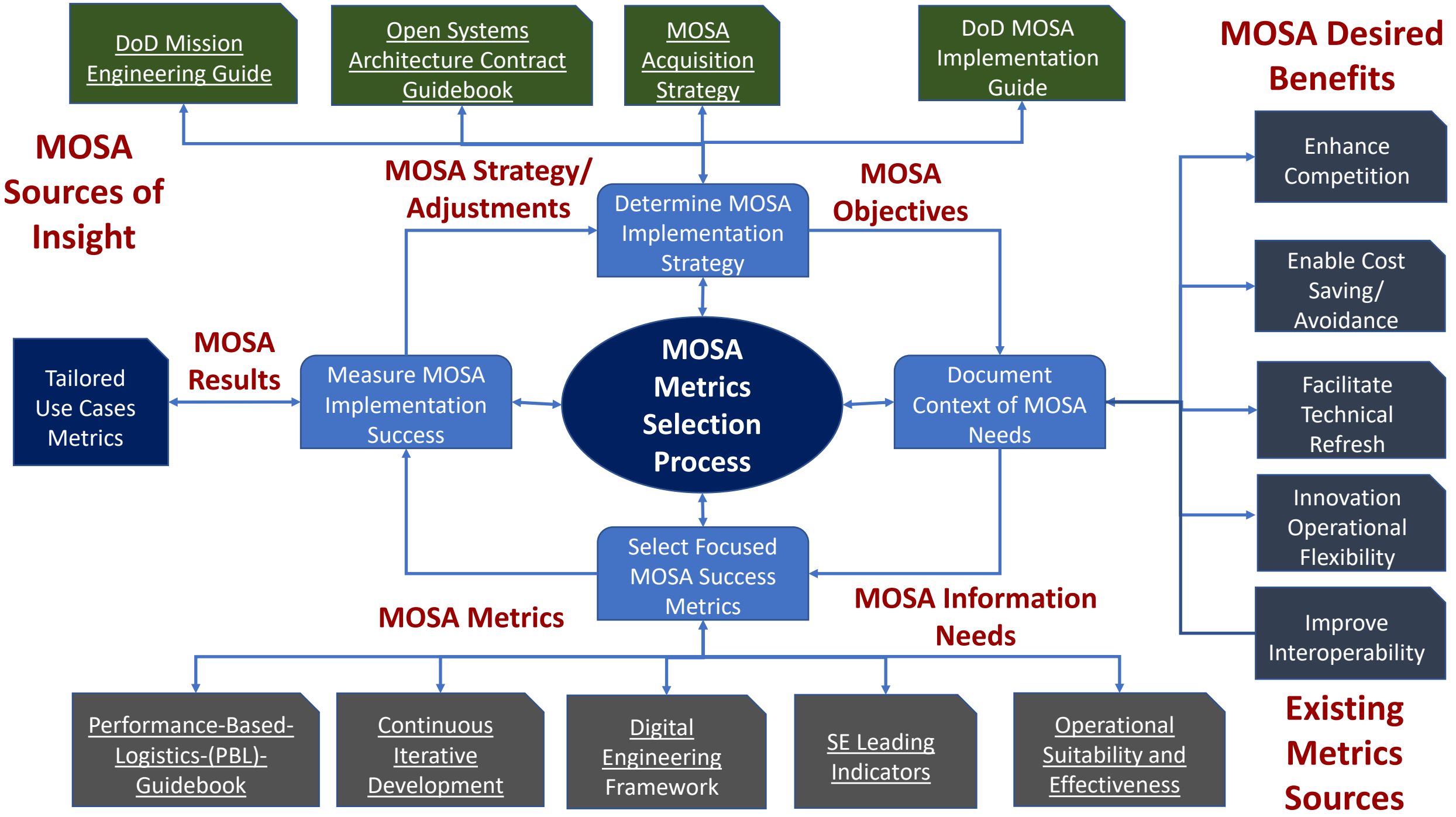
Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition & AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

Interoperability (1 of 3)



Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition

What measures enable informed design decisions?


DoD Mission Engineering Guide
Open Systems Architecture Contract Guidebook
MOSA Acquisition Strategy
DoD MOSA Implementation Guide
MOSA Sources of Insight
MOSA Strategy/ Adjustments
MOSA Objectives
MOSA Desired Benefits
Determine MOSA Implementation Strategy
Enhance Competition
Enable Cost Saving/ Avoidance
Facilitate Technical Refresh
Innovation Operational Flexibility
Improve Interoperability
Tailored Use Cases Metrics
MOSA Results
Measure MOSA Implementation Success
MOSA Metrics Selection Process
Document Context of MOSA Needs
Select Focused MOSA Success Metrics
MOSA Metrics
MOSA Information Needs
Performance-Based-Logistics-(PBL)-Guidebook
Continuous Iterative Development
Digital Engineering Framework
SE Leading Indicators
Operational Suitability and Effectiveness
Existing Metrics Sources

MOSA Metrics Selection Framework Guide Status / Help Needed

- ✓ Identified Most Likely MOSA Use Cases
  - Primarily Acquirer-Centric
  - Some Supplier-Centric
  - More Use Cases Possible Over Time
- ✓ Identified MOSA Sources Selection Process
- Determining MOSA Metric Candidates Superset (Currently 100's) – In Progress
  - Extracted from Leaves in the Mind Mapping of the MOSA Info Sources/Benefits
  - Significant Commonality Emerging in Metrics Types (Similar to Distribution Function)
- Distilling Superset to Most Common Metrics – Initiating
  - Expect a Limited Number of Common Metric Types (Likely a Few Dozen)
  - Unique, Individual Metrics for MOSA to be Developed, as Needed
  - Similar to Digital Engineering Metrics
- Drafting MOSA Metrics Implementation Guide – In Progress
  - Similar to Digital Engineering Metrics Implementation Guide

Help Needed for Validating MOSA Metrics Most Viable Product (i.e., the Most Common MOSA Metrics and Plan for Implementation)

International Council on Systems Engineering

SE Handbook

National Defense Industrial Association

NDIA MOSA White Paper Final Release NDIA Architecture Committee 2020

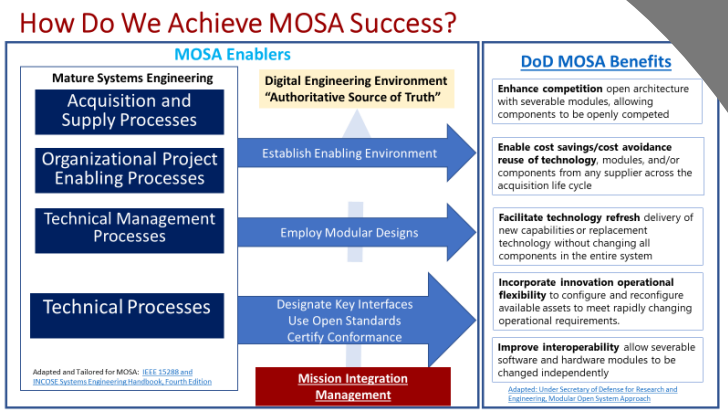
Practical Software & Systems Measurement

Practical Software and Systems Measurement Continuous Iterative Development Measurement Framework

DI-MGMT-82099, Open System Management Plan

Determine MOSA Implementation Strategy

- **Enhance competition**
  - GATM Business Case
  - CANES Business Case
  - MOSA in Source Selection
  - Architecture Modularity
- **Enable Cost Savings/Avoidance**
  - Software Reuse
  - Reuse Readiness Levels
- **Facilitate Technical Refresh**
- **Incorporate innovation operational flexibility**
- **Improve Interoperability**
- **SE Life Cycle MOSA Implementation**



Selection Framework

Document Context of Modularity/Openness Needs

Select Focused MOSA Value Success Metrics

Measure MOSA Implementation Success

Any Questions?

NDIA MOSA Metrics Selection Framework Guide

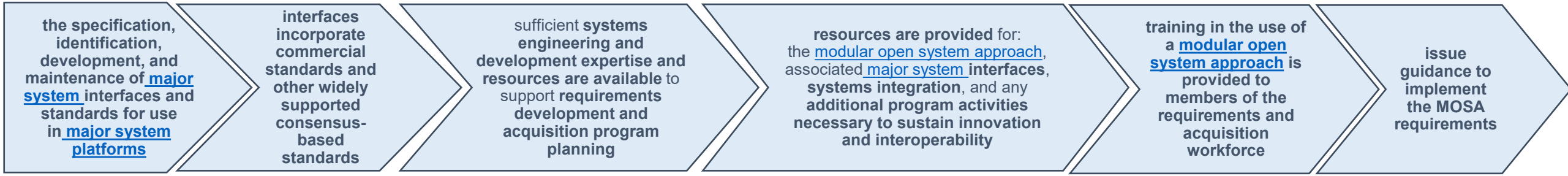
Backup

What are Your Program MOSA Requirements?

DoD Modular Open Systems Approach (MOSA) Statutory Requirements

- 10 USC 3771: Rights in technical data: regulations
- 10 USC 3772: Rights in technical data: provisions required in contracts
- 10 USC 3773: Domestic business concerns: programs for replenishment parts
- 10 USC 3774: Major weapon systems and subsystems: long-term technical data needs
- 10 USC 3775: Definitions
- 10 USC 4401: Requirement for **modular open system approach** in major defense acquisition programs
- 10 USC 4402: Requirement to address modular open system approach in **program capabilities development and acquisition weapon system design**;
- 10 USC 4403: Requirements relating to **availability of major system interfaces and support** for modular open system approach definitions

DoD MOSA Requirement Cliff Notes



MOSA Enhance Interoperability Overview

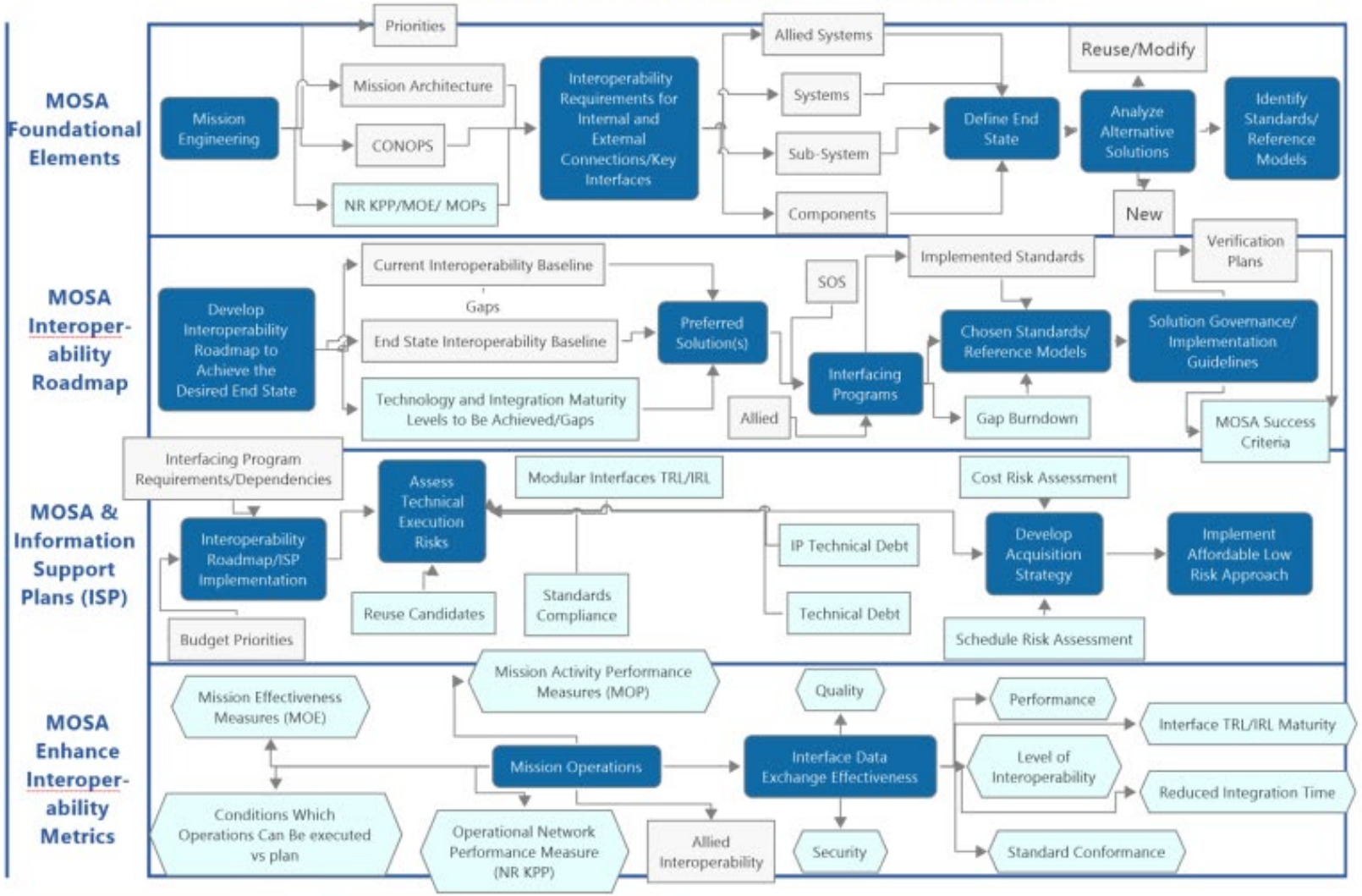
Information Needs

What are our Interoperability Needs

What is required to provide the needed interoperability?

How do we provide the needed interoperability?

How can MOSA's contribution to interoperability mission and interface's success be measured?



Information Needs

What Standards and Reference Models Do We use?

What are the system data exchanges and associated measures and metrics?

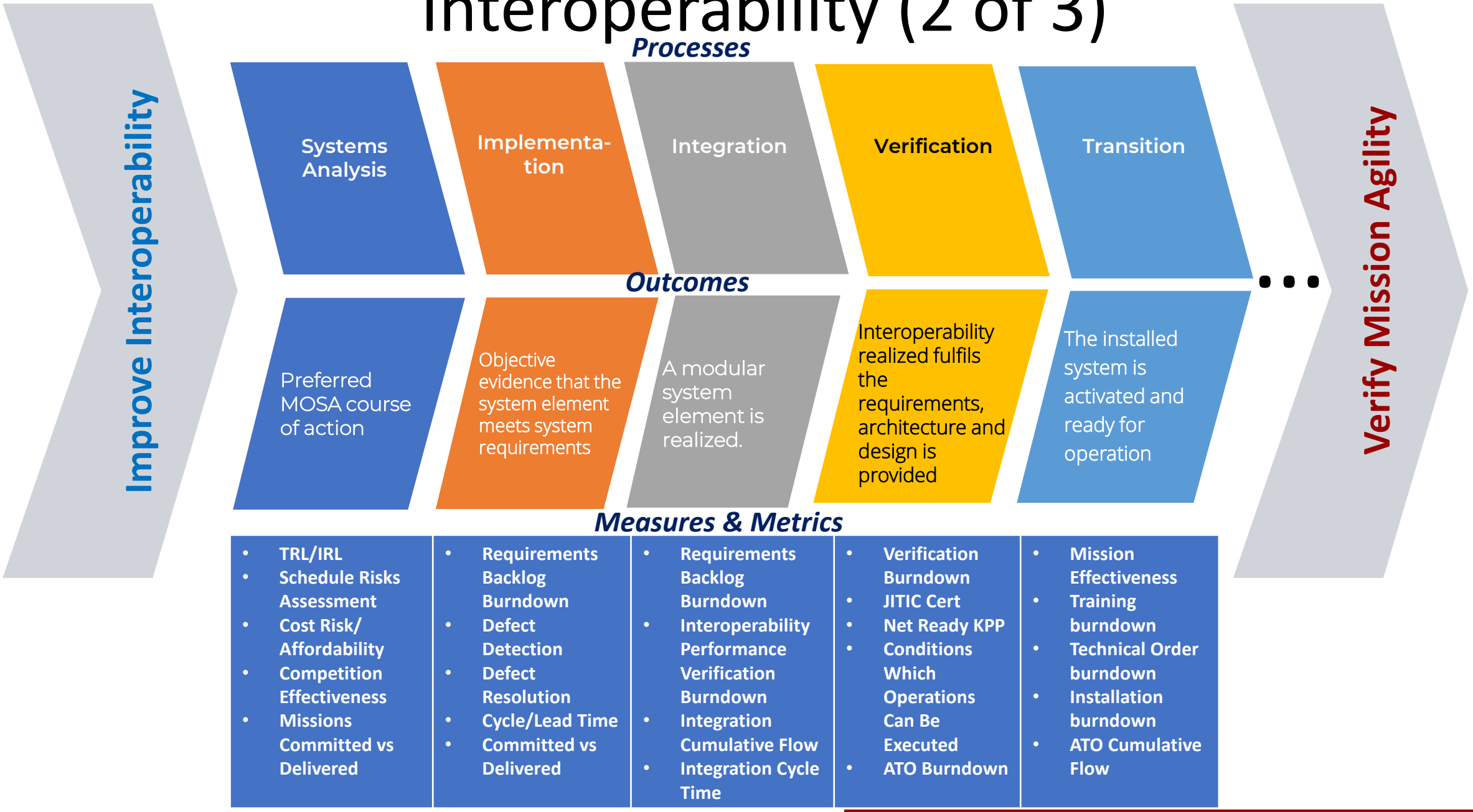
How will we achieve and maintain the Joint interoperability certification?

Which of these metrics apply to you and your current program?

Steve Henry
TAMU1971@msn.com

MOSA Interoperability Metrics | MOSA Interoperability Readiness Metrics | MOSA Interoperability Focus | MOSA Interoperability Information Needs

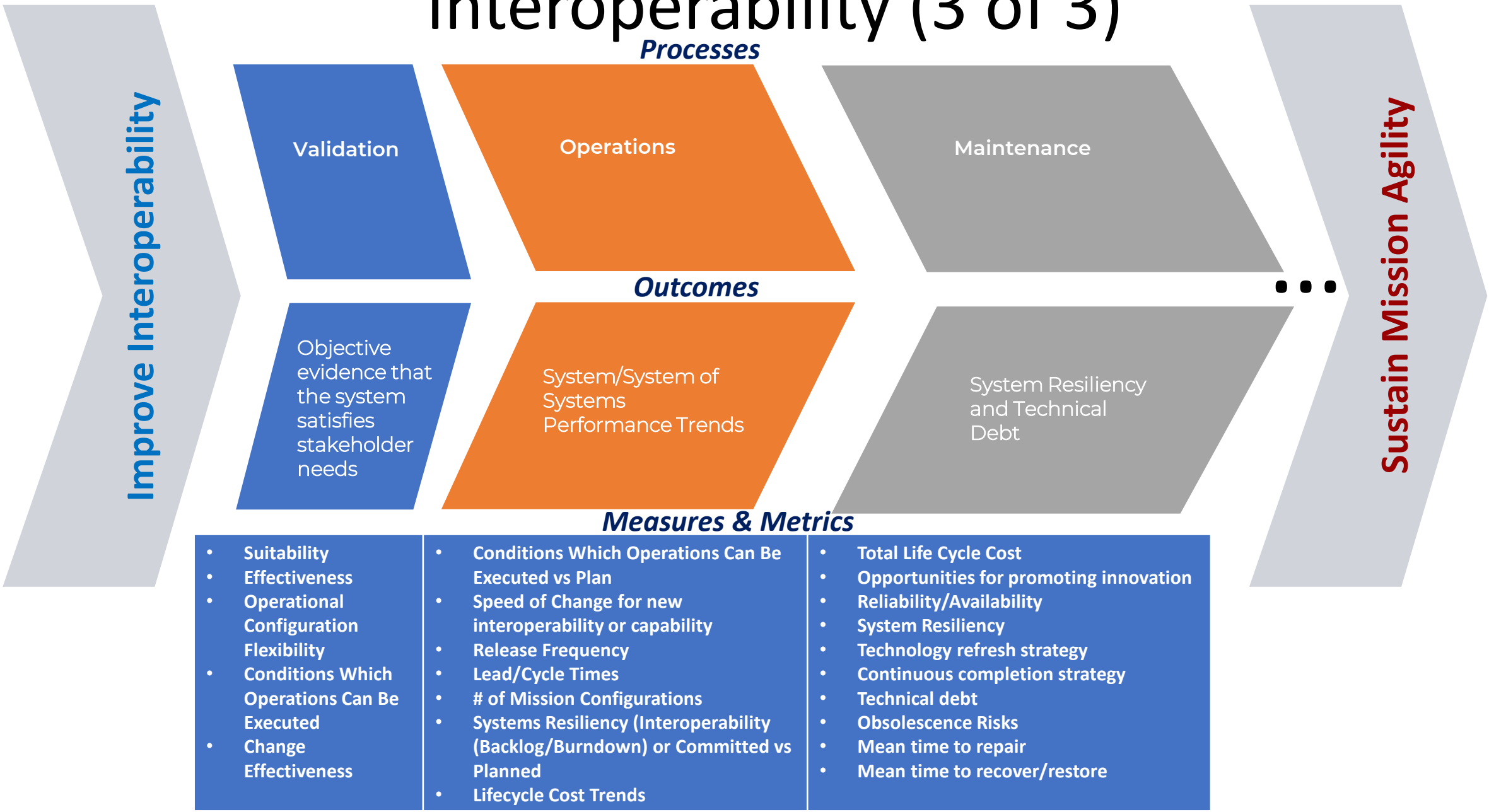
Interoperability (2 of 3)



Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition

What measures tell us we are ready to deploy?

Interoperability (3 of 3)



Measures & Metrics

• Suitability • Effectiveness • Operational Configuration Flexibility • Conditions Which Operations Can Be Executed • Change Effectiveness	• Conditions Which Operations Can Be Executed vs Plan • Speed of Change for new interoperability or capability • Release Frequency • Lead/Cycle Times • # of Mission Configurations • Systems Resiliency (Interoperability (Backlog/Burndown) or Committed vs Planned • Lifecycle Cost Trends	• Total Life Cycle Cost • Opportunities for promoting innovation • Reliability/Availability • System Resiliency • Technology refresh strategy • Continuous completion strategy • Technical debt • Obsolescence Risks • Mean time to repair • Mean time to recover/restore

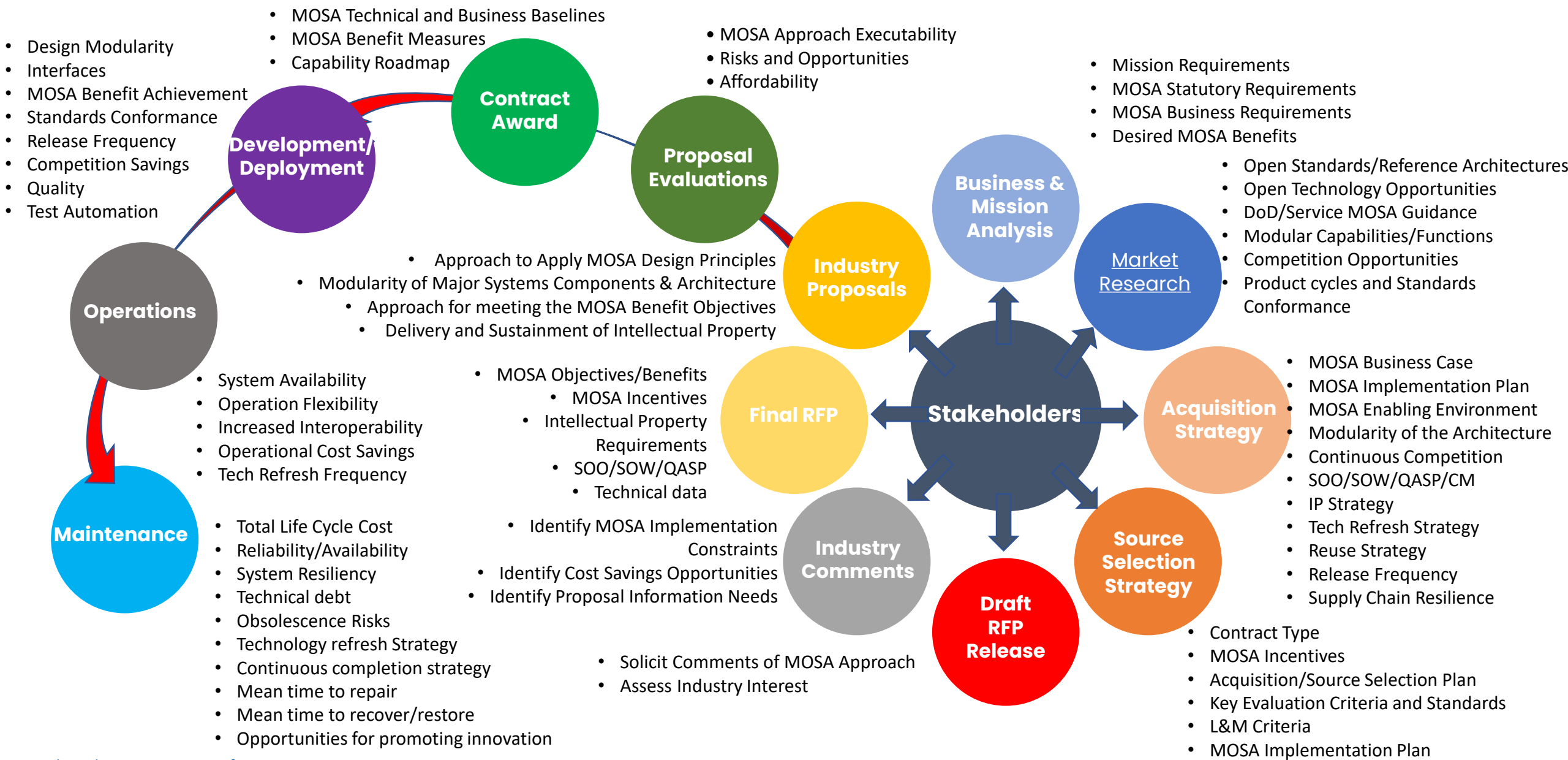
Adapted and Tailored for MOSA: IEEE 15288 and INCOSE Systems Engineering Handbook, Fourth Edition

What measures tell us we are still meeting requirements and achieving the benefits?

How Did GATM Implement its MOSA Approach?

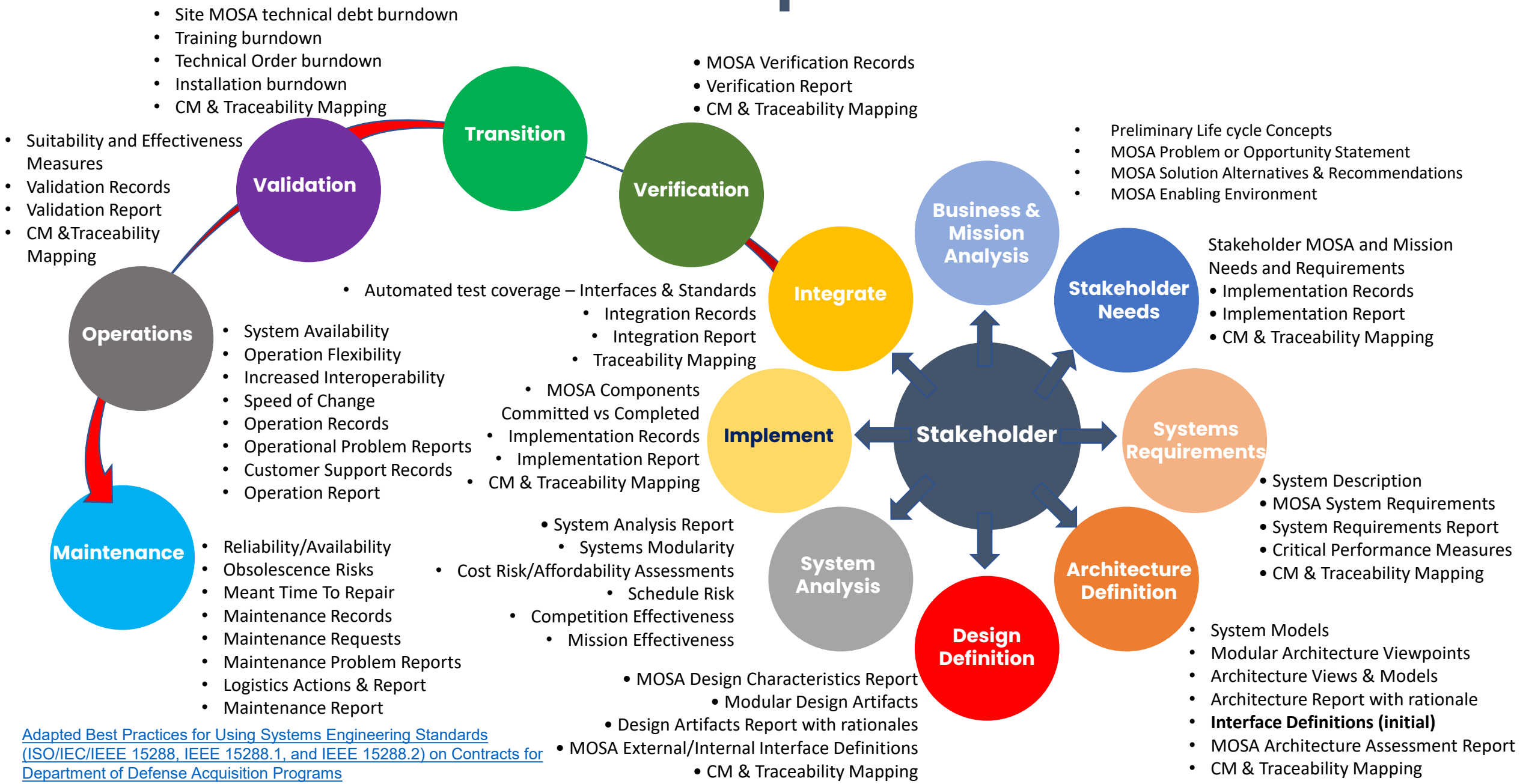
MOSA Implementation Actions	Outcome
1. Standardize interface specifications to allow of opportunities for future modernization	Use Open Standards: Open standards allows developers to leverage commercially developed technologies, increasing competition. Additionally, they offer faster upgrades at reduced cost and complexity. Fielded systems are more affordable and maintainable. **GATM adopted open AEEC, RTCA/ARINC Standards for all GATM components Add action** **The GATM components are the foundation for growth to the ADS-B capabilities**
2. Maintain a digital engineering MOSA authoritative source of truth	Combine model based techniques, digital practices, and computing infrastructure to enable delivery of high pay off solutions to the warfighter at the speed of relevance. Improves technical, contract, and business practices through an authoritative source of truth and digital artifacts. **GATM Configuration baselined for all components on vendor web site. GATM Program Office maintained specifications/requirements by country, one stop ordering, and engineering support on-line.**
3. Specify all interfaces by identifying connections between the systems and systems of systems building blocks	Decouple the interface and Service implementation so that they can maintain separate life cycles. In order for components to decouple their inner workings from each other but be able to leverage the capability provided by each highly cohesive service, developers expose openly available key interfaces to other components. **The GATM MOSA approach followed the ICAO CNS/ATM architecture and modernization roadmap.**
4. Plan Program to Achieve the MOSA Objectives	Describes the developer's approach for using modular design, standards-based interfaces, and widely-supported, consensus-based standards to achieve defined MOSA and Mission objectives. **The CNS/ATM Vendors are authorized by the FAA to produce TSO certified components have a modular card that provides the open interface between the component and the aircraft.**
5. Modularize by decomposing system Capabilities into functional modules	Accurately isolate functionality during the design process to simplify development, maintenance, changes and upgrades. **Each GATM component and its associated functions are modular, built to the standards, and certified**
6. Define Interface specifications by capturing how functional modules work	Decouple the interface and Service implementation so that they can maintain separate life cycles. In order for components to decouple their inner workings from each other but be able to leverage the capability provided by each highly cohesive service, developers expose openly available key interfaces to other components. **The GATM IDIQ contract allows the addition of upgraded products and capabilities as long as the original interface and capabilities are retained.**
7. Verify conformance to selected MOSA standards	Certify Conformance: Developers need to verify and validate their MOSA strategy and requirements, ensuring conformance to selected internal and external open interface standards. **The GATM aircraft integration contracts required procurement of compliant components from the GATM IDIQ contract and GATM accreditation GATM standards conformance by the GATM Program Office. Conformance certification enabled access to airspace worldwide.**

MOSA Business Strategy Implementation



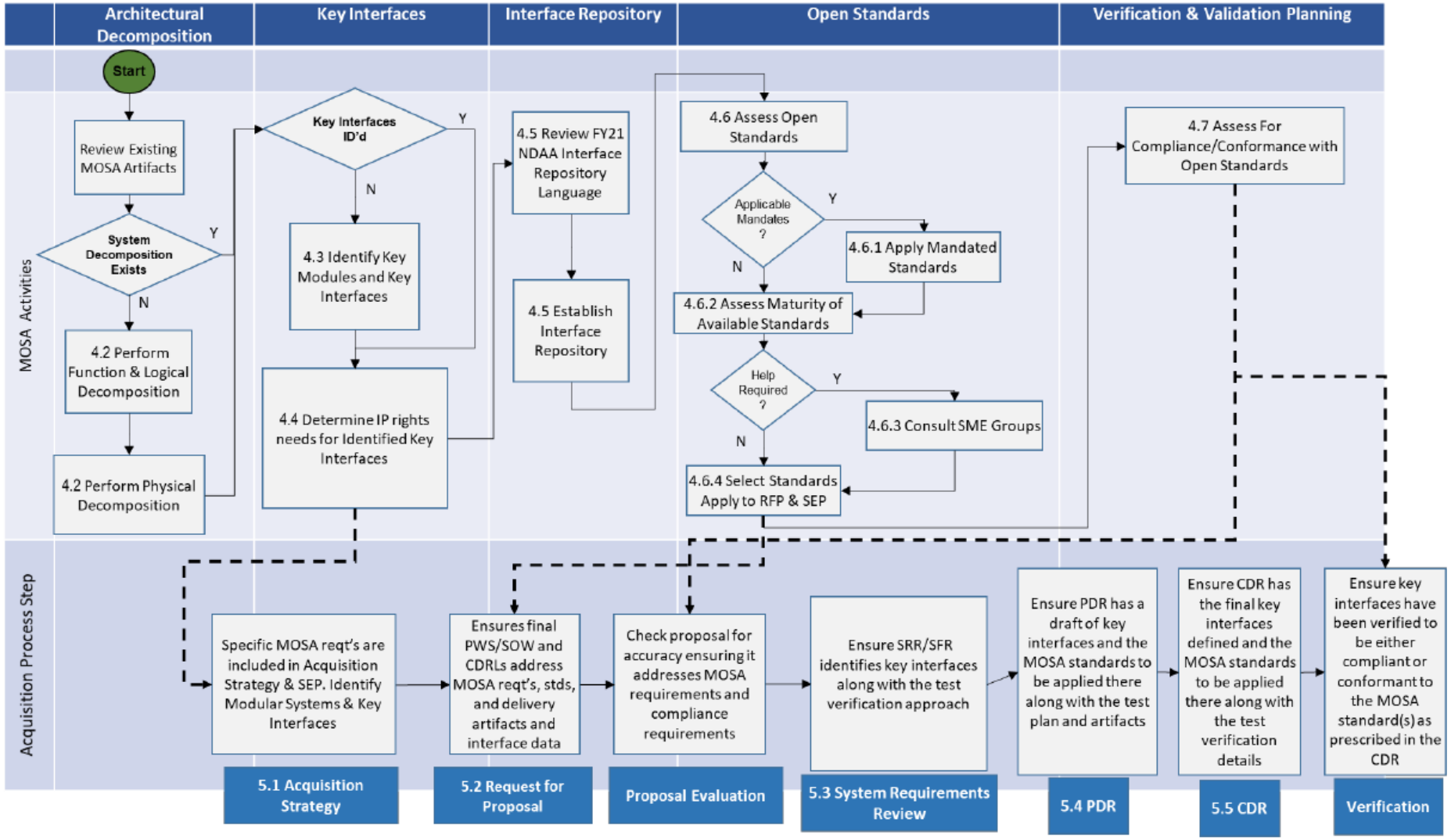
Adapted: DAU Acquisition of Services

MOSA Technical Implementation Flow



[Adapted Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on Contracts for Department of Defense Acquisition Programs]

USAF MOSA Starting Point for New Programs



AIR FORCE MATERIEL COMMAND (AFMC) GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN SYSTEMS APPROACHES IN WEAPON SYSTEMS

USAF MOSA Starting Point for Legacy Programs

Key Questions

- What is the Expected Service Life of the system?
- Is the modification replacing obsolete components?
- Can the modification be executed in such a way as to open a portion of the overall architecture?
- What future modifications are projected for the weapon system?
- What is the threat environment for the weapon system?

Tailor the MOSA Approach and Measurements to Address the MOSA Benefit Objectives

Legacy MOSA Approach

- Apply MOSA principles to their development and modification efforts
- Connect MOSA techniques to Digital Transformation and Model Based Acquisition objectives.
- Align with DoD, Department of the Service, and Major Command MOSA policy requirements
- Decompose MOSA concepts into actionable steps that can be tailored to fit program needs and constraints
- Align with traditional Acquisition schedule milestones and Adaptive Acquisition Framework alternatives including Agile Acquisition approaches

Metrics Selection Example
Enhance Competition – MOSA Approach

- **Source Selection Evaluation Criteria – Selected MOSA Objective**
  - **Architecture Completeness:** The extent to which the offeror's MOSA systems engineering and business approach and schedule demonstrate an appropriate balance of cost, schedule, and performance risk to implement and sustain the proposed MOSA approach throughout the lifecycle.
  - **Digital Engineering and Modeling:** The extent offerors Open System Management Plan and System Engineering Master Plan addresses the program MOSA requirements, identifies relevant modular systems/components and intellectual property required to meet MOSA objectives throughout the lifecycle
  - **Past Performance -** The Offeror shall provide details of your company's experience with implementing MOSA and achieving the benefits of MOSA on similar efforts
- **MOSA Information Needs/Measures**
  - Source Selection
    - Functional Architecture Completeness and Volatility
    - Committed vs Completed
    - Model Traceability
  - Execution
    - Functional Architecture Completeness and Volatility
    - Model Traceability
    - Architecture MOSA Requirements Implementation – Burndown, Cumulative Flow, Committed vs Delivered
    - Intellectual Property Committed Vs Completed
    - Technical Debt Burndown
  - Sustainment
    - Functional Architecture Completeness and Volatility
    - Technical/IP Debt – Committed vs Delivered, Burndown

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Digital Engineering (DE) Tool Selection Criteria

Daniel Hettema

Director, Digital Engineering, Modeling and Simulation (DEM&S)

Office of the Executive Director, Systems Engineering and Architecture

Office of the Under Secretary of Defense for Research and Engineering

SETA Support: Emily Bak, Jeffery Nartatez, Frank Salvatore

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Agenda

- Purpose & Scope
- Approach
- POAM
- Initial Criteria
- Criteria Crosswalk
- Sample Criteria
- Digital Engineering Body of Knowledge (DEBoK)
- Next Steps

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Purpose & Scope

- Purpose: Provide guidance to DE architects, planners and implementers focused around making tool decisions to align engineering with enterprise goals for digital transformation.
- What it is not? - Policy, list of tools or vendors, trade study tool, "single point solution/one size fits all"
- Scope: Establish DE tool agnostic selection criteria aligned with
  - DoD DE strategy, DE fundamentals, DE ecosystem requirements
  - DoD Defense Industrial Base lessons learned and best practice
  - Provide reference products in the DEBoK
- So what?
  - Improved vendor tool interoperability
  - Shared collaborative environment
  - Expanded commonality across enterprise solutions
  - Increase in automation

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Approach

Define Purpose

Define Scope and Plan
- Define product boundaries
- Establish initial guidance

Define and Organize Criteria
- Brainstorm
- Alignment
- Crosswalk criteria against: strategy, requirements, fundamentals
- Aggregate into organized list of questions

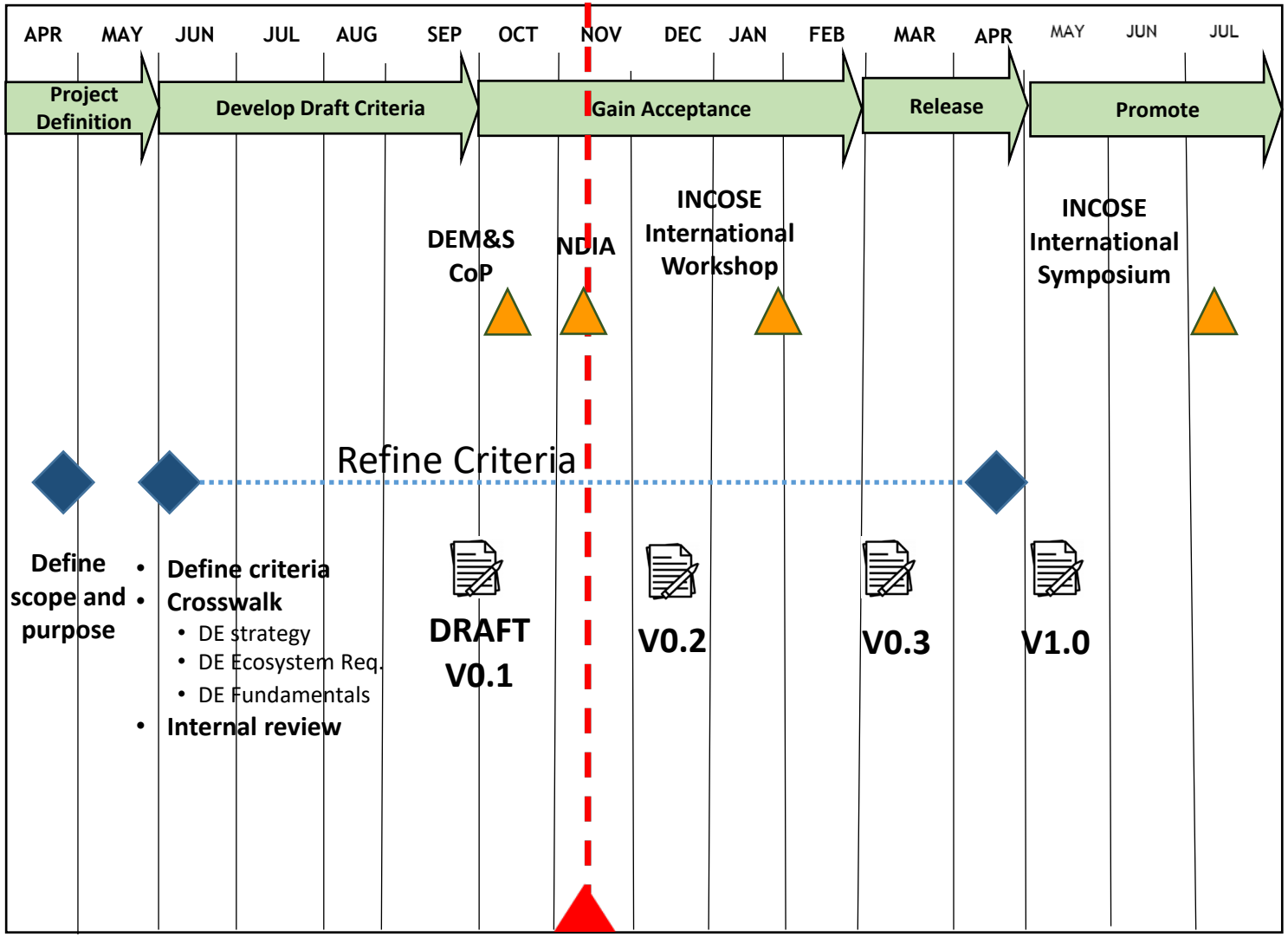
Gain Acceptance
- Internal review
- DEM&S CoP
- NDIA SME conference
- INCOSE IW

Develop Usage Guidance
- Finalize criteria
- Use cases
- User guidance

Release, Promote and Adoption
- Publicly available on the DEBoK
- Include in info share briefs
- Training
- Acceptance
- Command media

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Tool Selection Criteria POAM



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Initial Criteria Focus, Not Comprehensive

- Integration with existing tools
- Data: Continuity, authoritative, curation and shared
- Full traceability of tool execution, product and legacy (digital thread, cross domain, etc.)
- Tool product credibility: Automated verification and validation
- Data management adherence (Configuration Management (CM), Data Management (DM), logistics, quality, etc.)
- Long-term archival/retrieval (obsolescence, tool supportability)
- Standards adherence
- Automation – reporting, notification, handoffs, etc.
- Licensing: Enterprise-wide, creative licensing strategies
- Collaboration and sharing (Intellectual Property (IP), data rights, access control, etc.)

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Criteria Alignment – Strategy, Fundamentals & Requirements

OUSD(R&E)

DE Ecosystem Generic Requirements

OUSD(R&E)

DE Fundamentals

DE Tools Criteria

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Strategy: What, Not How

Describes 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

DE Strategy Link

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

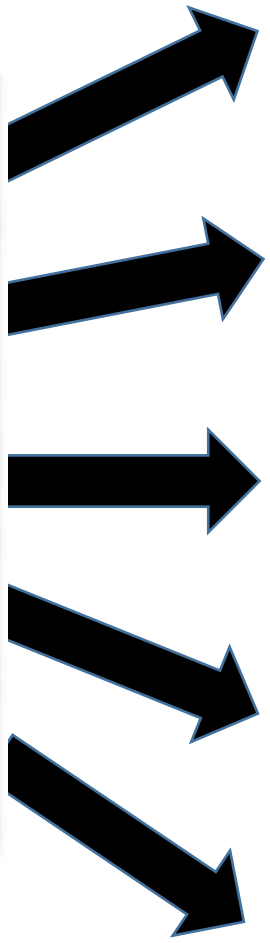
Combine standard representations of a system (s), with computers, additional computational techniques as a continuous, complete and evolving ecosystem to provide data for data-informed decisions and interactive visualizations to a continuum of questions

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Strategy Crosswalk

DE Strategy

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

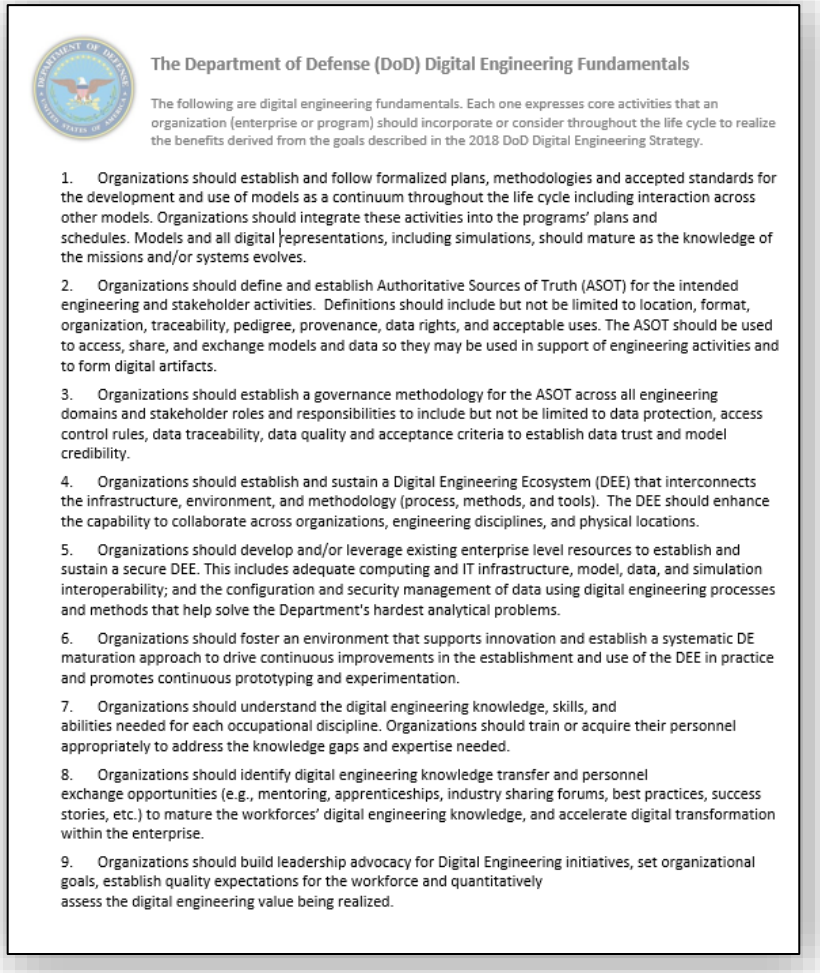


Sample DE Tool Criteria

- Supports the development of models
- Support interoperability with other models (management, design, manufacturing, system, business, product support)
- Supports establishing access and controls.
- Supports the management of models as the authoritative source of truth
- Provides AI/ML capabilities
- Supports advanced human machine interfaces
- Support enterprise and flexible licensing agreements with minimal constraints on data exchange/sharing.
- Supports change management activities
- Supports Enterprise level reporting and communications

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Fundamentals



The Department of Defense (DoD) Digital Engineering Fundamentals

The following are digital engineering fundamentals. Each one expresses core activities that an organization (enterprise or program) should incorporate or consider throughout the life cycle to realize the benefits derived from the goals described in the 2018 DoD Digital Engineering Strategy.

1. Organizations should establish and follow formalized plans, methodologies and accepted standards for the development and use of models as a continuum throughout the life cycle including interaction across other models. Organizations should integrate these activities into the programs' plans and schedules. Models and all digital representations, including simulations, should mature as the knowledge of the missions and/or systems evolves.

2. Organizations should define and establish Authoritative Sources of Truth (ASOT) for the intended engineering and stakeholder activities. Definitions should include but not be limited to location, format, organization, traceability, pedigree, provenance, data rights, and acceptable uses. The ASOT should be used to access, share, and exchange models and data so they may be used in support of engineering activities and to form digital artifacts.

3. Organizations should establish a governance methodology for the ASOT across all engineering domains and stakeholder roles and responsibilities to include but not be limited to data protection, access control rules, data traceability, data quality and acceptance criteria to establish data trust and model credibility.

4. Organizations should establish and sustain a Digital Engineering Ecosystem (DEE) that interconnects the infrastructure, environment, and methodology (process, methods, and tools). The DEE should enhance the capability to collaborate across organizations, engineering disciplines, and physical locations.

5. Organizations should develop and/or leverage existing enterprise level resources to establish and sustain a secure DEE. This includes adequate computing and IT infrastructure, model, data, and simulation interoperability; and the configuration and security management of data using digital engineering processes and methods that help solve the Department's hardest analytical problems.

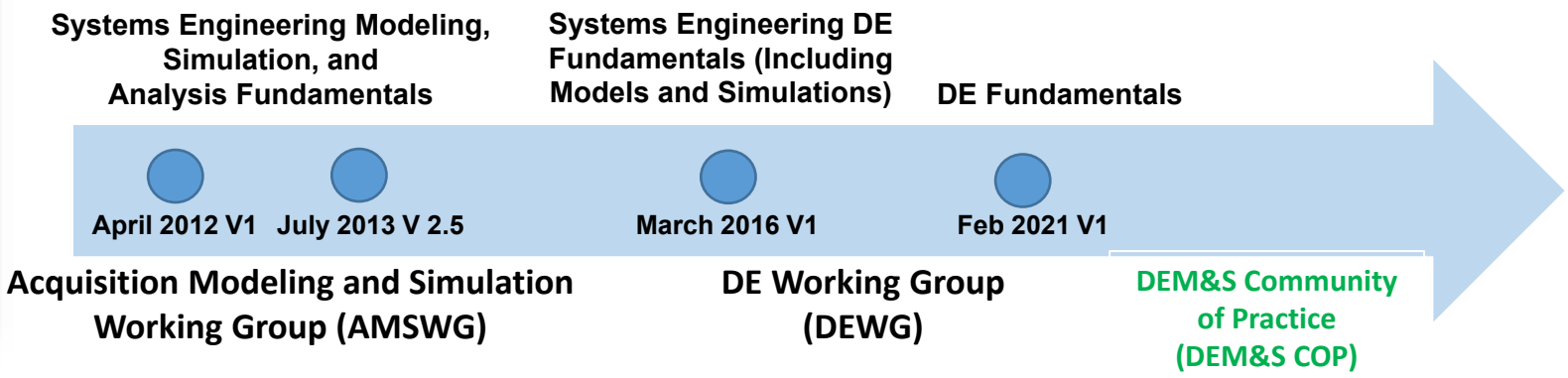
6. Organizations should foster an environment that supports innovation and establish a systematic DE maturation approach to drive continuous improvements in the establishment and use of the DEE in practice and promotes continuous prototyping and experimentation.

7. Organizations should understand the digital engineering knowledge, skills, and abilities needed for each occupational discipline. Organizations should train or acquire their personnel appropriately to address the knowledge gaps and expertise needed.

8. Organizations should identify digital engineering knowledge transfer and personnel exchange opportunities (e.g., mentoring, apprenticeships, industry sharing forums, best practices, success stories, etc.) to mature the workforces' digital engineering knowledge, and accelerate digital transformation within the enterprise.

9. Organizations should build leadership advocacy for Digital Engineering initiatives, set organizational goals, establish quality expectations for the workforce and quantitatively assess the digital engineering value being realized.

- The DE Fundamentals are a one-page reference that expresses core activities that an organization (enterprise or program) should incorporate or consider throughout the life cycle to realize the benefits derived from the DoD DE Strategy.
- Where can you find it?
  - Public access: https://ac.cto.mil/wp-content/uploads/2022/03/DE-Fundamentals-2022.pdf
- Product Heritage and Pedigree



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Fundamentals

DE Fundamentals Snapshot

Organizations should establish and sustain a Digital Engineering Ecosystem (DEE) that interconnects the infrastructure, environment, and methodology (process, methods, and tools).

The DEE should enhance the capability to collaborate across organizations, engineering disciplines, and physical locations.

Organizations should develop and/or leverage existing enterprise level resources to establish and sustain a secure DEE.

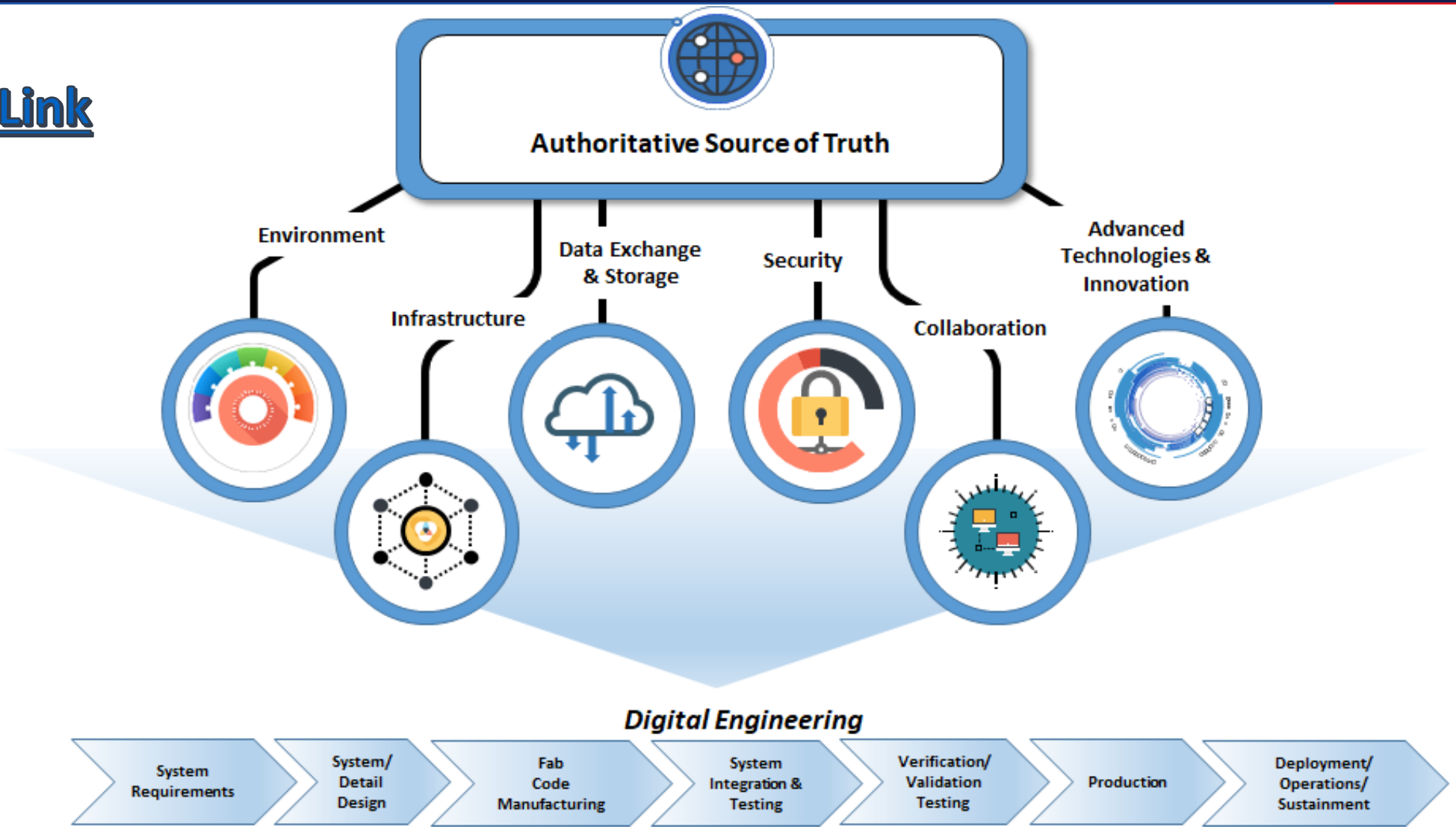
DRAFT Sample DE Tool Criteria

- Facilitate data formats/standards to include pedigree and provenance, meta-data, or appropriate traceability needed.
- Tools need to be compatible with the organizations existing infrastructure and environment.
- Tools should support continuous validation includes self-checking to enforce adherence to semantics and syntax. Supports error checking
- Tool supports automated notification of changes and discussion or activity happening within it.
- Tools should support planning and scheduling of modeling, simulation, and digital engineering activities.

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Ecosystem Requirements

DEBoK Link



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DE Ecosystem Requirements

DE Ecosystem baseline requirements	
Category	**Sub-Category**
Adv Tech & Processes	Processes
Adv Tech & Processes	Technologies
Collaboration	Resources
Collaboration	Users
Data	Curation
Data	Exchange
Data	Storage
Environment	Licensing
Environment	Portability
Environment	Support
Environment	Visualization
Infrastructure	Hardware/Computing
Infrastructure	Networks
Infrastructure	Software
Security	Access Control
Security	Classification
Security	Cybersecurity

Sample DE Tool Criteria

Capable of cross platform capabilities, tool to tool interaction, integration.

Enable automation of data exchange between users.

Interface capabilities to export data easily in varying different formats

Supports DoD Data Strategy VAULTIS goals

Support legacy and new technology- part of extensibility

Supports automated data tagging, metadata entry for curation of resulting work products. This will aid in configuration management and curation of work products.

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Sample Criteria - As Factors in Your Decision Making

- **Does your tool have a governance process?**
  - Does the tool support version control with a controlled process?
  - Is the tool vendor committed to long term sustainability?
  - Is the tool compatible with the organization's existing tools?
- **Does your tool support integration of models?**
  - Does the modeling environment support integration of modeling tools?
  - Does the modeling tool support interfacing and integration with other models ?
  - Can the models be used on other operating systems?
- **Does your tool support access control?**
  - Does the tool only allow authorized users to edit?
  - Does the tool support "read-only" capabilities?
  - Does your tool have user group access control?
  - Is there controls on access down to the attribute level?
- **Does your tool provide cross tool /platform integration?**
  - Does the tool support API/ interfacing (standard plug-ins) for tool-to-tool interaction?
  - Can the tool be used on multiple platforms and operating systems?
  - Does the tool support forward and backwards capabilities?

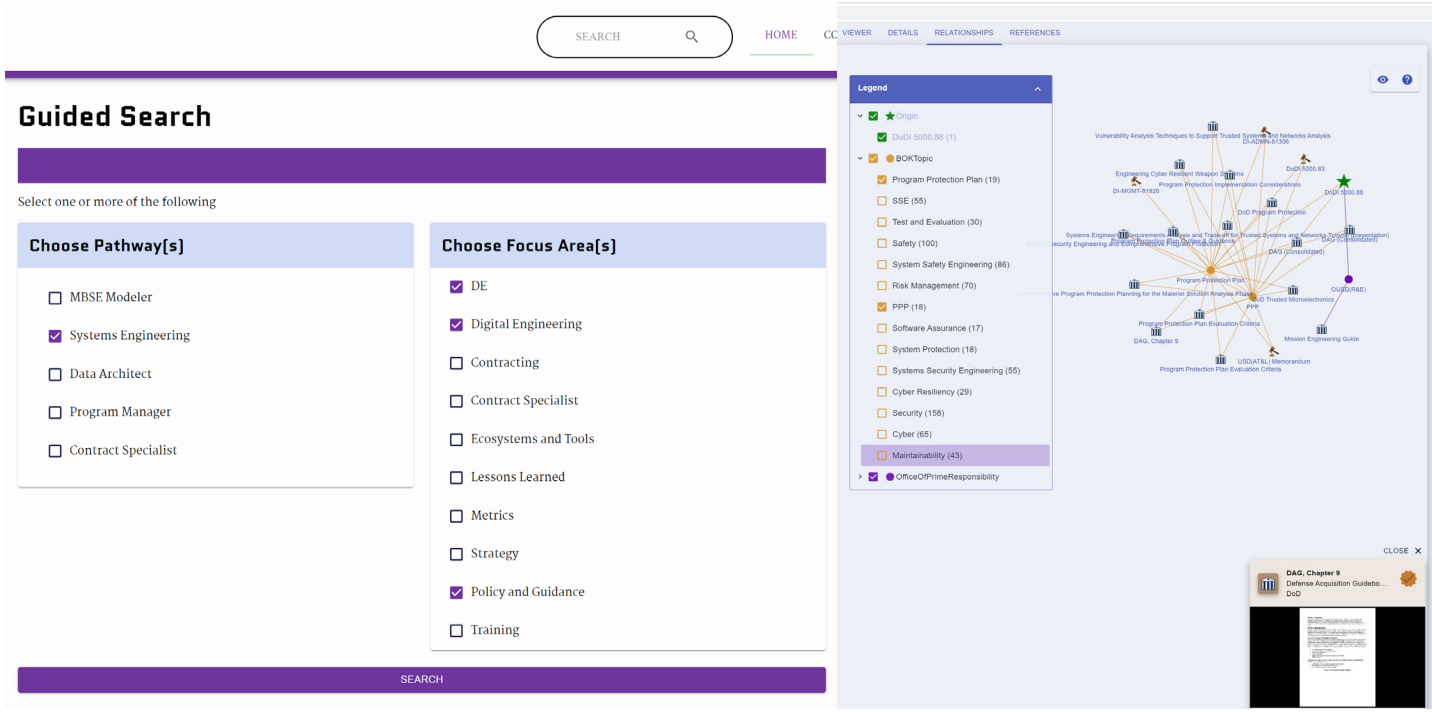
Work in progress, preparation for INCOSE International Workshop

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

DEBoK

- Tools selection criteria will be available on the DEBoK
  - The DEBoK is a public-facing platform for authoritative DE referential resources
  - Provides collaboration for the DE community
- Please visit us at: de-bok.org

DEBoK
Digital Engineering Body of Knowledge



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Next Steps and Request for Input/Feedback

We are looking for your feedback, support & guidance:

- Comments, Recommendations
- Similar activities
- Similar artifacts
- Established baseline set of tool criteria

Next Steps:

- Derive preliminary criteria guidance (ongoing)
- Complete draft criteria guidance OSD internal review
- INCOSE IW collaboration
- Public release

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Questions, Outreach for Collaboration

- Provide us your feedback and any input you might have
- Provide your recommendations with supporting rationale for consideration in future revisions
- If you have artifacts, please send them to:

osd.mc-alex.ousd-r-e.mbx.deboksupport@mail.mil

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Contact

Office of the Under Secretary of Defense for Research and Engineering
osd.r-e.comm@mail.mil | Attn: SE&A
https://www.cto.mil
https://ac.cto.mil/engineering

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3011

Agile/MOSA/Microservice Architectures Stronger Together

Kurt Mohr & Darryl Nelson
RI&S Engineering

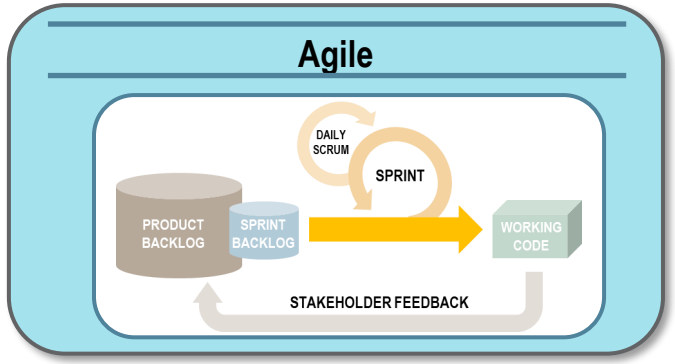
November 2, 2022

© 2022 Raytheon Technologies Corporation.
All rights reserved.

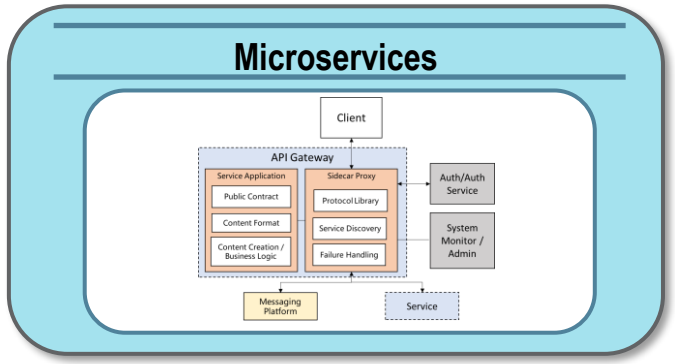
Raytheon Technologies Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Agenda

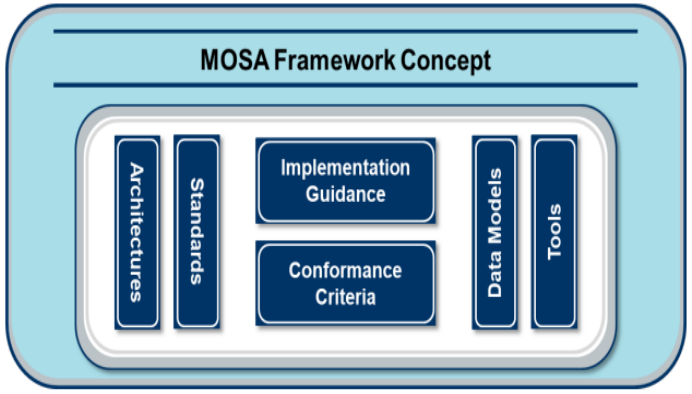
- **Establish a Lexicon** – defining Agile, Microservices, and MOSA
- **Speed of Agility** - agility and speed are keys to successful deployment of incremental capabilities
- **Microservice interfaces** - microservice architectures can represent both major and minor interfaces
- **Interface Stability of MOSA** - MOSA, with more stringent interface adherence at the major level, may be viewed as conflicting with rapid changes and trial and error of Agile
- **Adaptability vs. Stability** - using microservices to develop rapidly adaptable systems in an agile manner while meeting the MOSA requirements of modular design at the major system level, using consensus -based standards, and having severability at all levels of the architecture
- **Architectural Strategies** - architectural strategies for internal and external interfaces, and interface compatibility/extensibility
- **Reference Architecture** – what does 'good' look like
- **Commercial Examples** - interface stability at the major system level while providing adaptability and modularity at the lower levels of system architectures
- **DevSecOps** - enable speed and agility of microservice architectures while ensuring the quality of service required for MOSA system architectures



+



+



https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

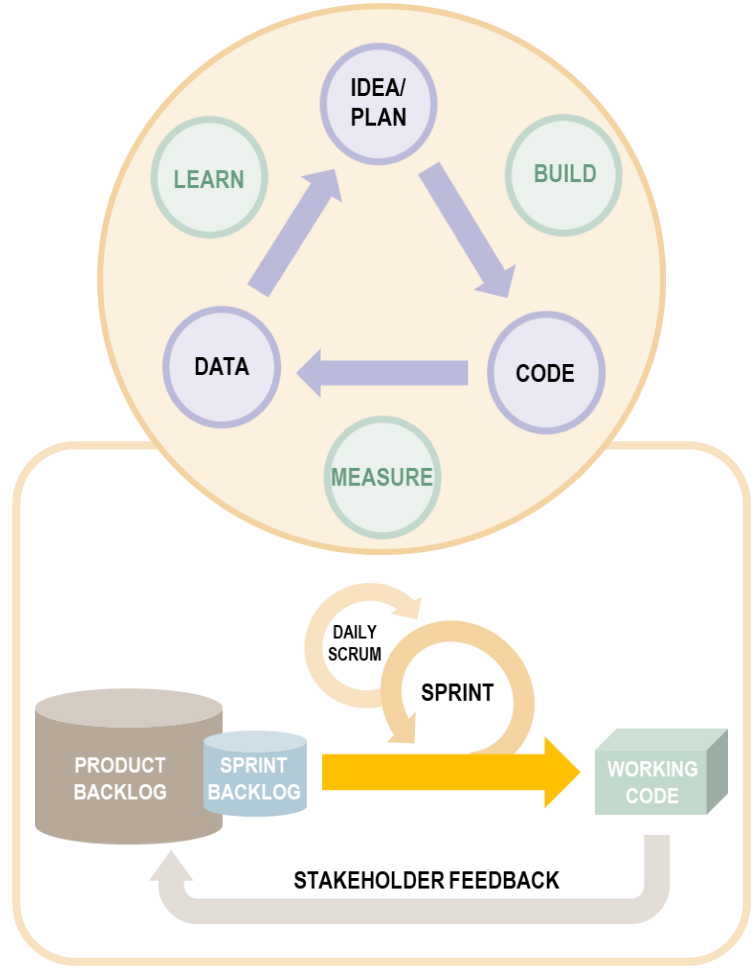
Lexicon - Agile

- Many Agile methodologies, but same basic values:
  - **Individuals and interactions** over processes and tools
  - **Working software** over comprehensive documentation
  - **Customer collaboration** over contract negotiation
  - **Responding to change** over following a plan

agilemanifesto.org/

- Focus on **Agility**
  - Ability to move or adapt quickly
  - Better Software through tight Feedback Loops for Rapid Adaptation
  - Facilitates fast learning

- Allows **rapid change** based on new information and discovery
  - Learning lessons and trying new approaches (retrospectives)
  - Buying down risk through experimentation (prototyping)



Agility is about adapting rapidly and not being tied to an original plan

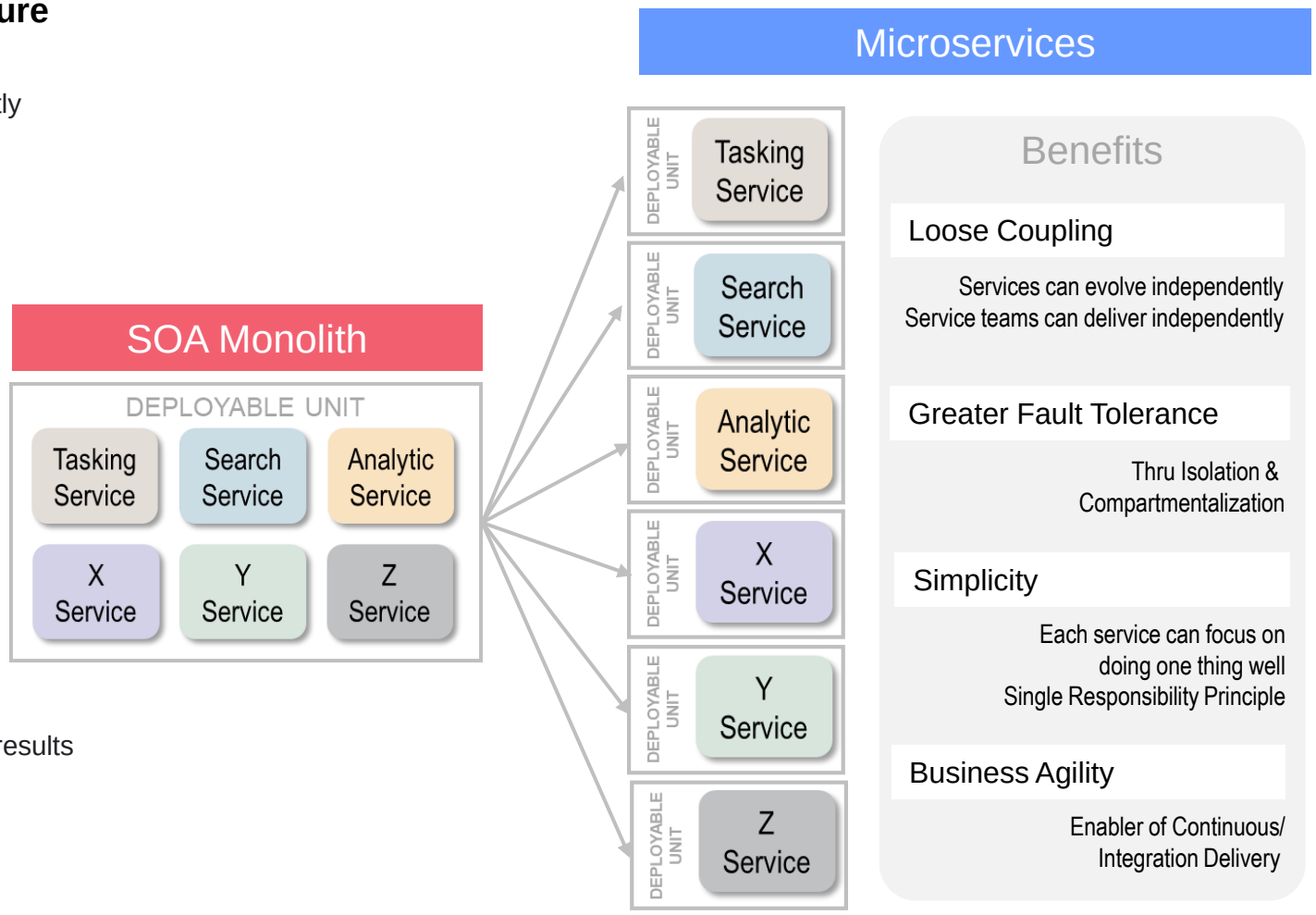
Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Lexicon – Microservice Architecture

- **Next evolution of Service-Oriented Architecture (SOA) to Microservices**
  - Suites of software applications composed of independently deployable services
  - Loosely coupled services
  - Fine-grained, meaning small in size and scope
  - Light-weight protocols
  - Independently managed
  - Delivering systems as a set of constrained, granular, independent collaborating services

- **Value of Microservice Architectures**
  - Enforces Isolation for resilience and elasticity
  - Ability to create and deploy fixes independently
  - Limiting the reach of defects
  - Minimizes the need for specialized personnel knowledge
  - Can be assembled in different ways to produce different results
  - The independent services can be composed together to cooperate, providing sophisticated business services



Microservice Architectures maximizes the number of 'services' to build on

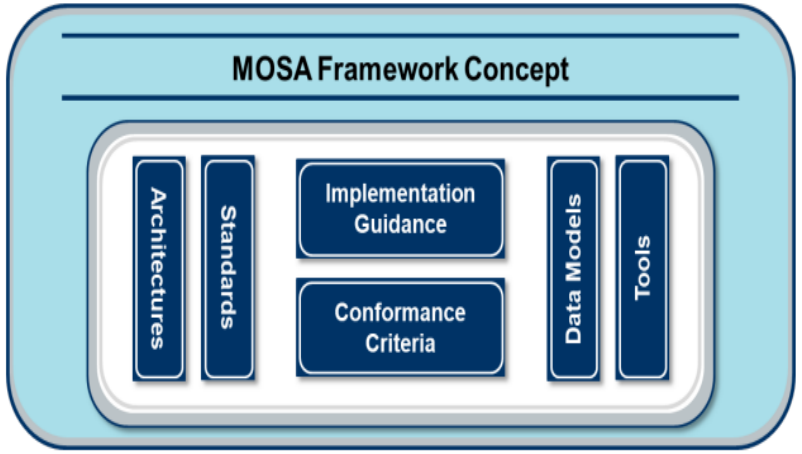
Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

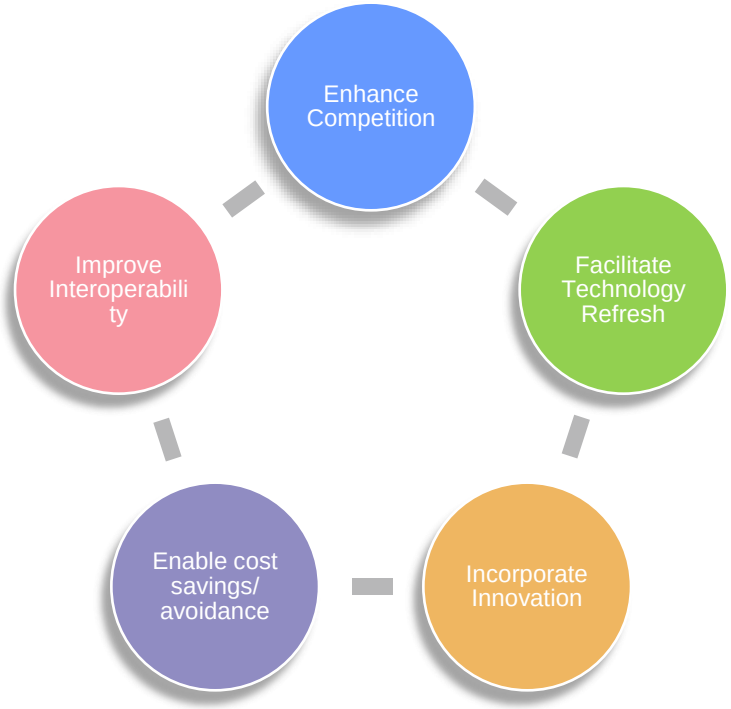
Lexicon - MOSA

- **MOSA Definition**
  - A modular design that uses major system interfaces between major platforms/systems/components
  - Ensures major system interfaces use widely supported and consensus-based standards
  - Allows major system components severability at the appropriate level to be added/removed/replaced
- **MOSA intent is to:**
  - Support a more rapid evolution of capabilities and technologies throughout the product life cycle
  - Ensure architecture modularity, open systems standards, and appropriate business practices.
- **Expectation is MOSA delivers:**
  - Enhance competition
  - Facilitate technology refresh
  - Incorporate innovation
  - Enable cost savings/cost avoidance
  - Improve interoperability

References
- https://www.dsp.dla.mil/Programs/MOSA/
- https://ac.cto.mil/mosa/



https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf



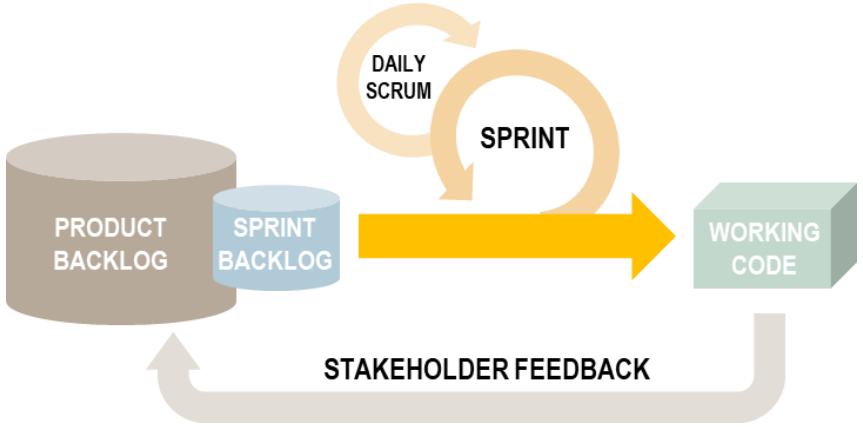
MOSA employs standards to allow component replacement

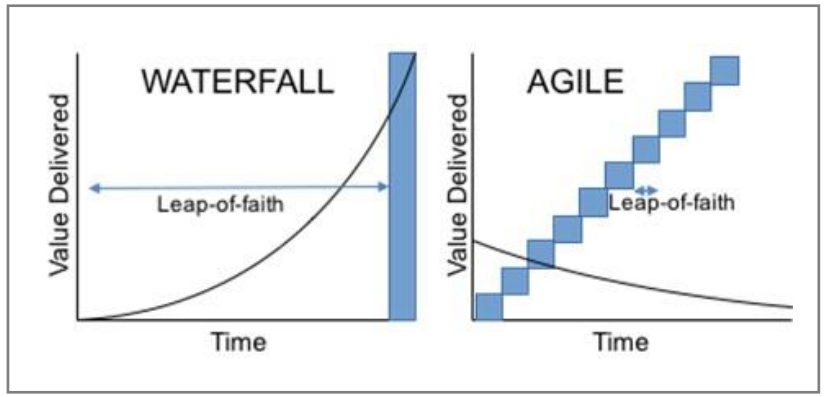
Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Speed of Agility

- **Agile methodologies deliver capabilities quickly at lower risk**
  - Incremental deliveries on a regular cadence
  - Short cycle times get things to users for evaluation
- **Experimentation allows new technologies to be evaluated**
  - "Fail Fast" methodology to determine what works and what doesn't
  - No long development cycles
- **Minimal Viable Product (MVP) can be found and refined**
  - Many times the "most important features" evolve
  - Eliminating unnecessary features can save cost and schedule
- **Testing early and often reduces tail end schedule risk**
  - "Test gets compressed" mentality changes to "shift left"





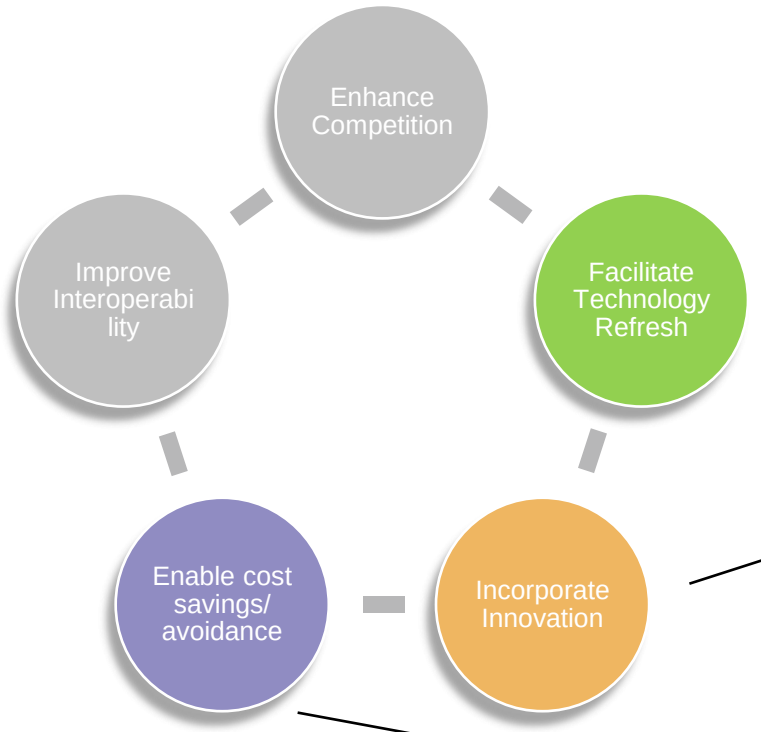
Dr Ian Mitchell, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons https://commons.wikimedia.org/wiki/File:Waterfallvsagile.jpg

Agile shortens timelines to get things into customer's hands

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Agility + MOSA – Contradictory or Complimentary?



Facilitate technology refresh

- Agility can shorten technology refresh cycles

Incorporate innovation

- Experimentation and team-driven priorities enables innovation

Enable cost savings/cost avoidance

- Risk mitigation and rapid fielding support cost avoidance through early testing
- Customers can focus on MVP

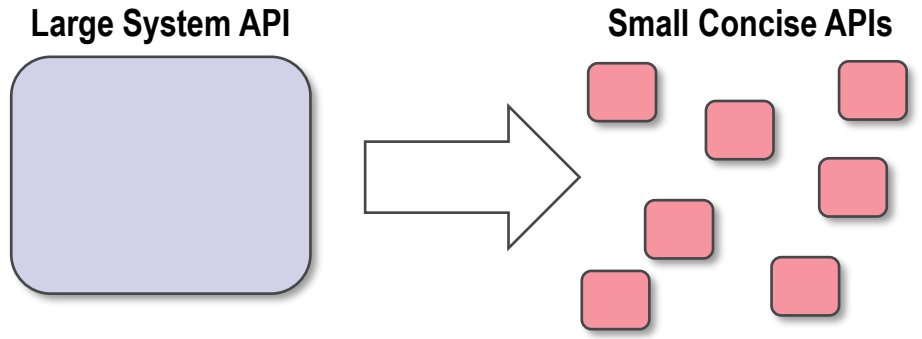
Agility provides several of the outcomes MOSA seeks to achieve

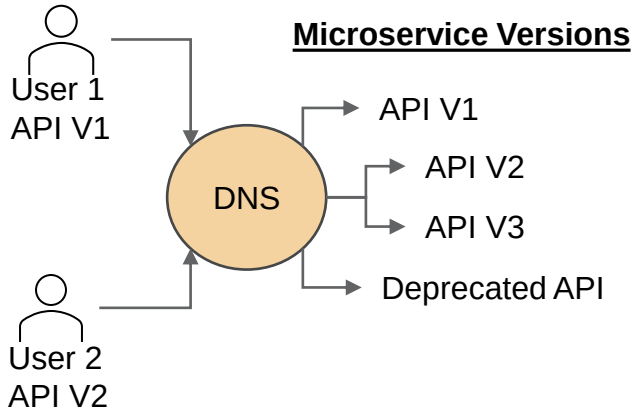
Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Microservice Flexibility

- **Microservices have individual interfaces**
  - Instead of one large interface, many smaller ones
  - Small, concise interfaces are easier to understand
- **Deployment can be targeted**
  - Deploying a single service for a test or a set for added functionality
- **Interface changes don't require all parties aligning schedules**
  - Interfaces can be versioned and operate concurrently
  - Deprecating old interfaces gives time for callers to adapt
- **Changing out a microservice provider is low impact**
  - Can operate the old and new concurrently
  - Changing the endpoint can be as easy as a DNS entry



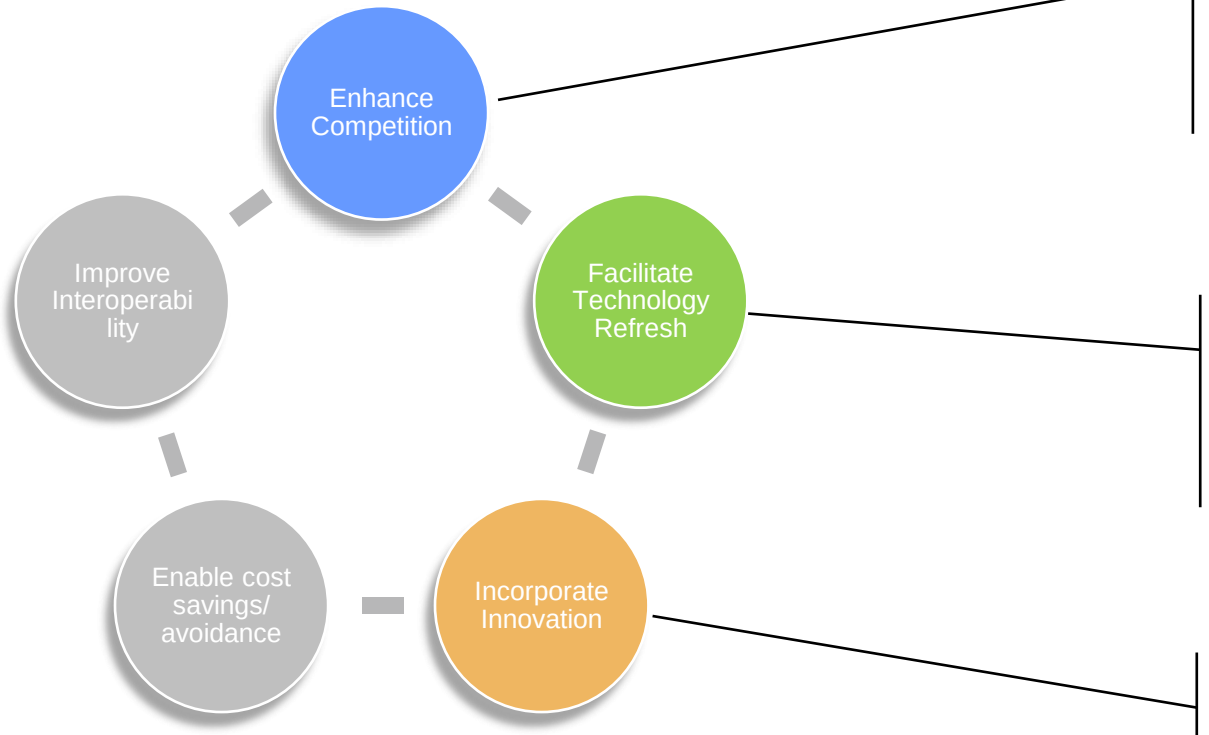


Microservice architectures decouple implementation from interface

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Microservices + MOSA – Can they live together?



Enhance competition

- Microservices allow competing services to be evaluated
- Services can live side by side for comparison or use

Facilitate technology refresh

- New versions can co-exist with older ones for refresh
- Microservices can be updated independently

Incorporate innovation

- Services enable deployment of MVP with rapid iteration

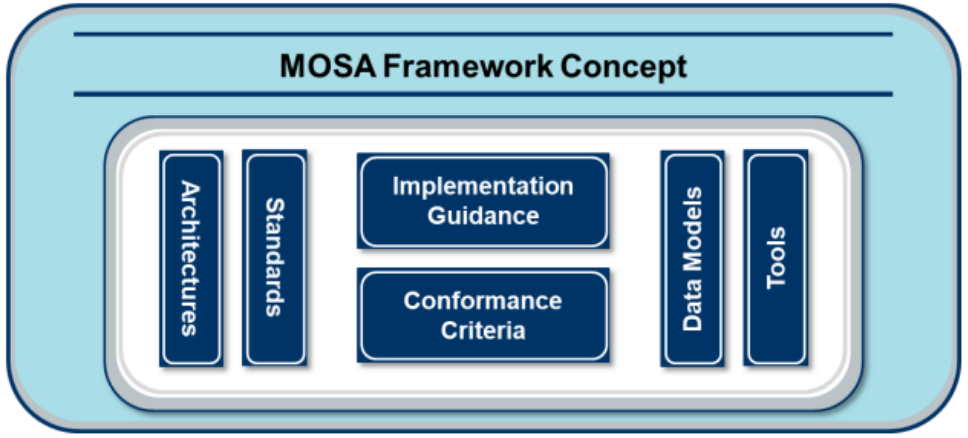
Microservices have the potential to aide MOSA objectives

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

MOSA Interface Stability

- **But MOSA is looking for interface stability, right?**
  - A modular design that uses **major system interfaces** between major platforms/systems/components
  - Ensures major system interfaces use **widely supported and consensus-based standards**
  - Allows **major system components severability** at the appropriate level to be added/removed/replaced
- **MOSA focuses on the major systems**
  - MOSA is silent on the minor systems and components
  - There is no clear definition of “major”
- **Interfaces are tightly controlled and versioned**
  - Allowing ad-hoc updates would be chaotic at best
  - Version changes go through multiple reviews with many stakeholders



Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs, Deputy Director for Engineering, Office of the Under Secretary of Defense for Research and Engineering, Director of Defense Research and Engineering for Advanced Capabilities, May 2020, Distribution Statement A. Approved for public release. Distribution is unlimited.
https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf

MOSA’s key concerns are major interface boundaries

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Adaptability vs. Stability

Adaptability

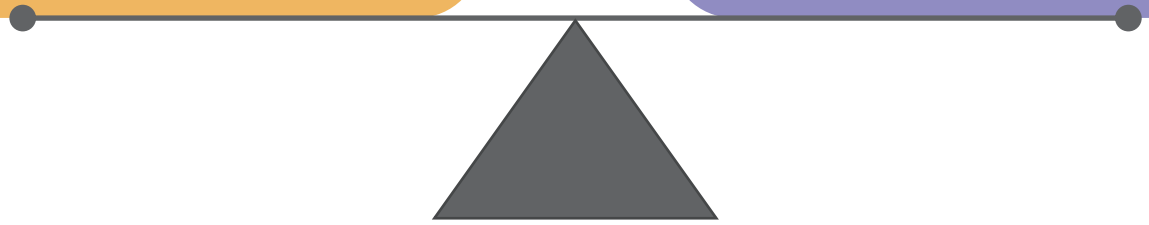
Agile and Microservices provide **adaptability**

- Both in implementation details and interface changes
- Adding new services or updating them rapidly
- Running concurrently or deviating for specific needs
- Accepting trial and error to 'learn' the best approach
- Technology change at the most granular level
- Every microservice is replaceable

Stability

MOSA provides interface **stability**

- Rarely changing interfaces
- Generally, one implementation in the system at a time
- Technology refresh of large system components
- Competition at the macro level



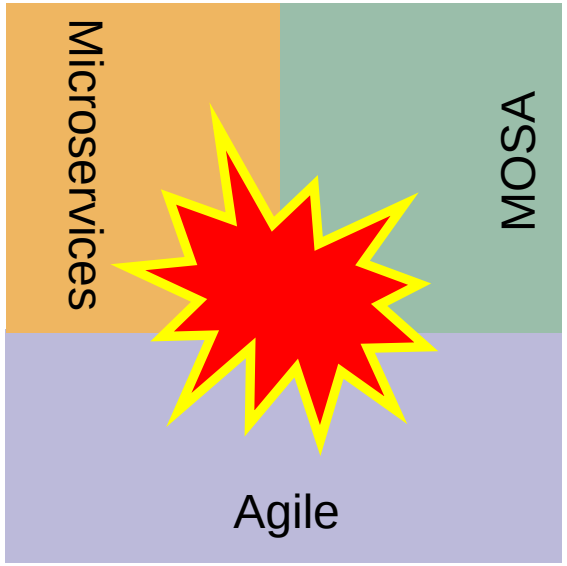
Ease of change vs. the stability for long contract cycles seem to be at odds

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

So Do they Conflict?

- **Microservices allows for frequent interface changes**
  - Agile allows for interfaces to be updated regularly
  - MOSA does not allow for interfaces to change in weekly Agile cycles
- **Agile experimentation isn't consensus-based**
  - MOSA relies on consensus for interfaces
  - Microservice changes could be 'tried' in an agile increment with a subset of callers
- **MOSA is serving a wide range of stakeholders**
  - Agile has stakeholders, but it does not require consensus
  - Microservices could have different versions for different stakeholders

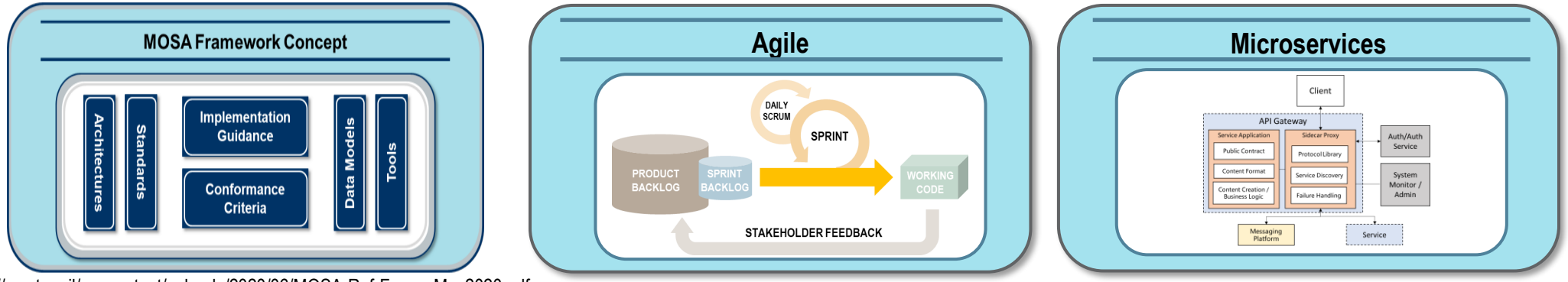


So Agile and Microservices work, but not with MOSA?

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Same Objectives, Different Approach



https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf

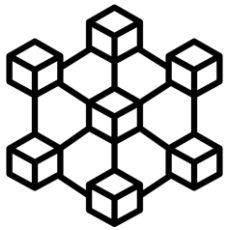
- **While the approaches differ, there are significant synergies**
  - Changes at the micro-level don't need to be coordinated
  - Microservices can be callers of major interfaces
- **Competition enhancement at all levels**
  - MOSA brings it at major components
  - Microservice architectures compete deeper in the architecture
  - "Competition" can be capability, not just provider, using Agile
- **Interoperability can be enhanced**
  - Rapid microservice adapters can insulate from major changes through design patterns
    - Façade pattern, Delegation pattern, and Proxy pattern
  - Interface versioning can be implemented quickly in Agile

Combining Agile, MOSA, and Microservices are Different but Complementary Approaches
They Serve the Same Objectives

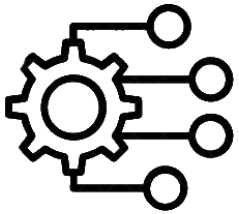
Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Architectural Strategies



- **Defining Major and Minor Interfaces**
  - Architecturally defining which interfaces are major and thus MOSA
  - Providing API registration for interface selection of minor interfaces
  - Using extensible interface protocols
    - E.g. Adding optional content to JSON messages



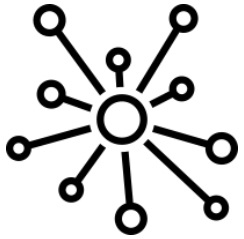
- **Intelligent Routing**
  - Routing data based on the recipient's needs
  - Changing routing rules to old or new service implementations
  - Identifying interfaces that are backwards compatible or where multiple versions could co-exist

Multiple strategies can be used to marry the approaches

Raytheon Technologies Approved for Public Release
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.

Architectural Strategies cont.

- **Data Adaptation**
  - A microservice can be inserted to adapt new interface calls to old
    - E.g. Stripping new fields so that a recipient can continue to function
  - Developed, tested, and deployed quickly through Agile
  - When the recipient is ready for the new interface, the microservice is disabled or updated



- **Maximizing Stateless Processing**
  - Decoupling data state between components to reduce major interface dependency
  - Using proxy interfaces to deal with 'extra' data across major interface points

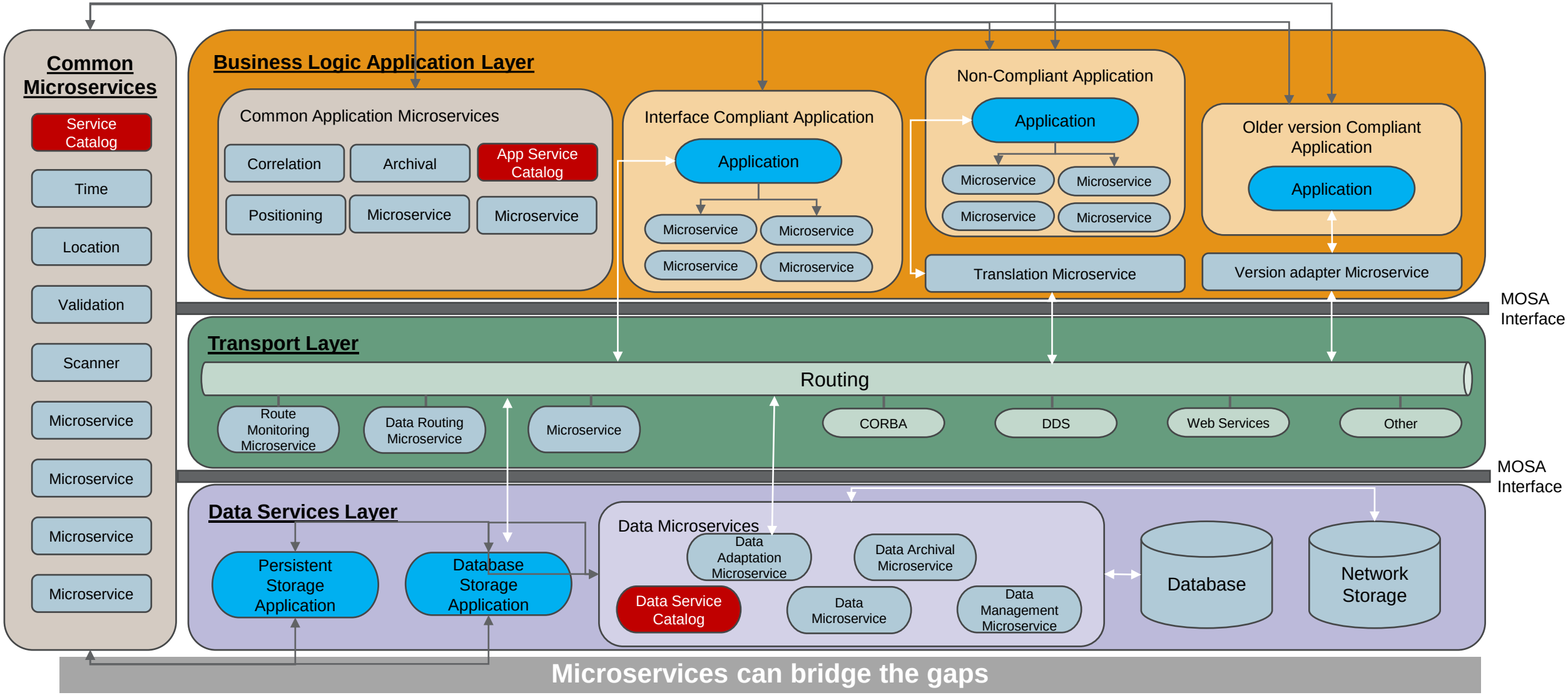
- **Using Big Data Approaches**
  - Segregating responsibilities to the lowest levels
  - Using data aggregation services to initiate major interface calls

MOSA objectives are all about dependencies, minimize those

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

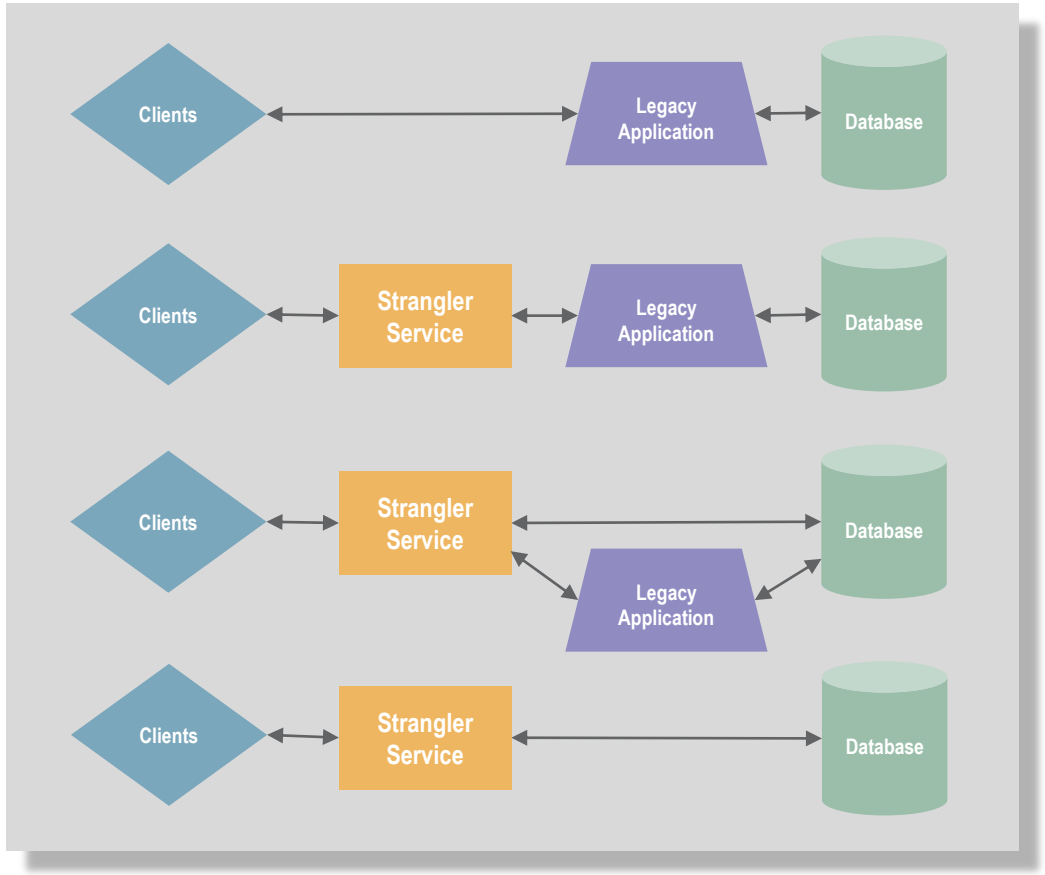
Reference Architecture



Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Strangler Pattern: Incremental Modernization



1. Original legacy application
2. Strangler as a pass through
3. Strangler taking over some responsibilities
4. Complete transition to Strangler

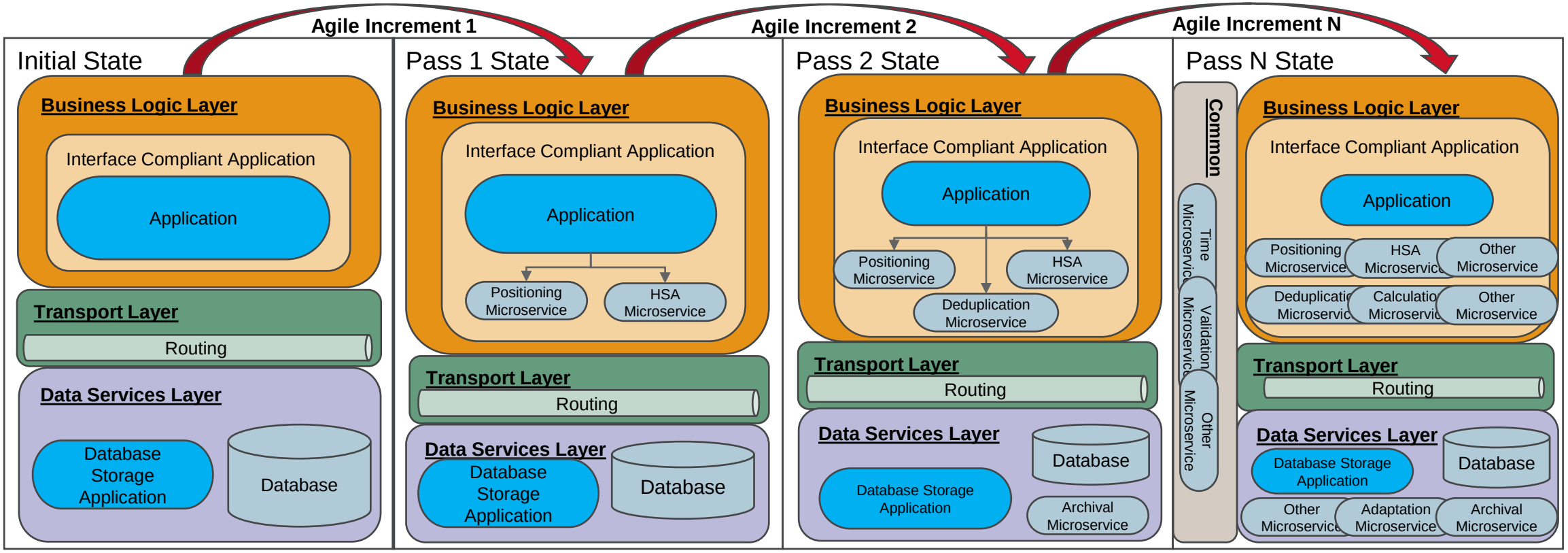
A *software pattern* of incremental migration of a legacy system by replacing existing functionalities with new applications and services in a phased approach.

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Agile Migration Paths

- Use Strangler pattern for incremental modernization to an application by adding microservices
- Agile methods provide boundaries to limit risk each increment



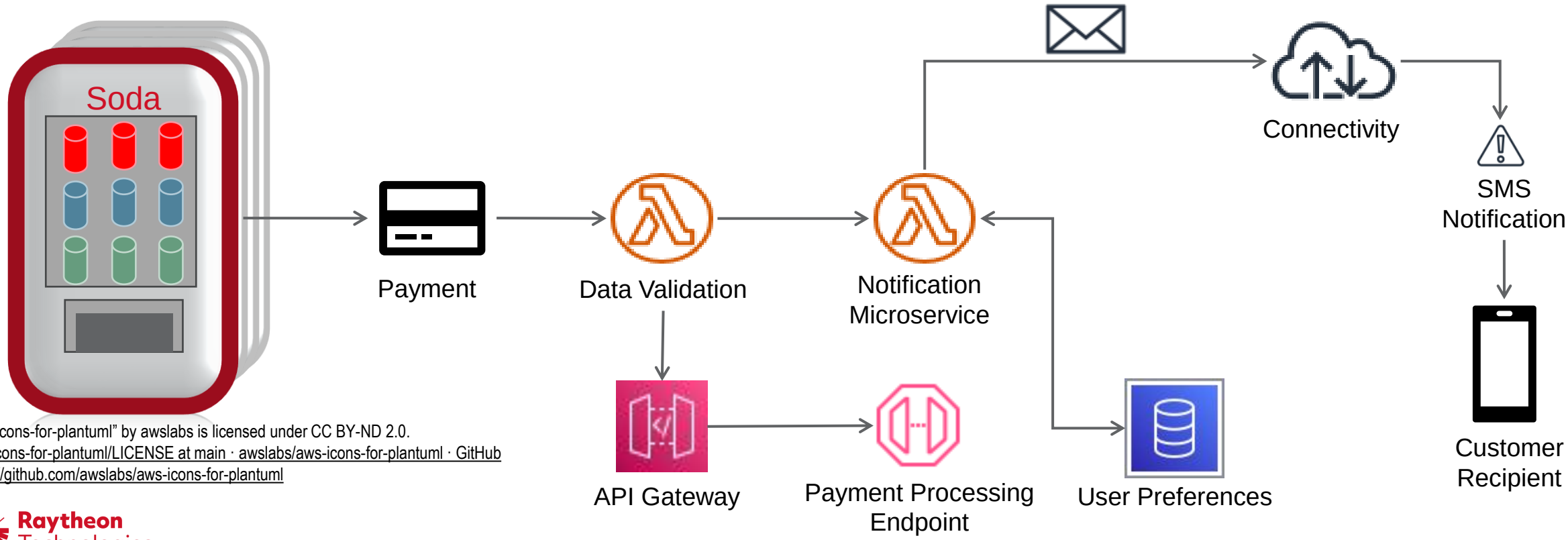
Migration doesn't have to be a "big bang"

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Commercial Example

- **Soda manufacturer vending machines**
  - Vending machines call microservice
    - Implemented as Lambda function
  - Data is conformed to major payment APIs
  - Newer vending machines updated to use latest interface features
  - Microservices send notifications to users

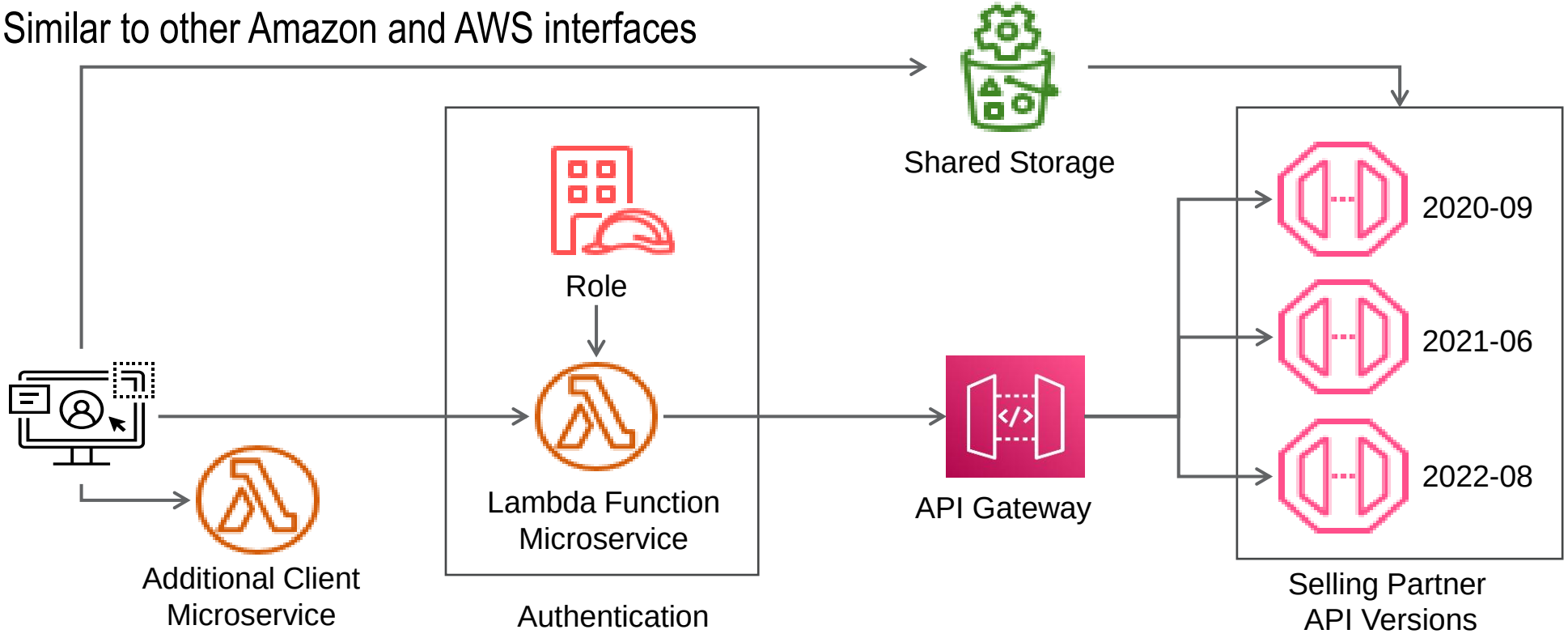


"aws-icons-for-plantuml" by awslabs is licensed under CC BY-ND 2.0.
aws-icons-for-plantuml/LICENSE at main · awslabs/aws-icons-for-plantuml · GitHub
https://github.com/awslabs/aws-icons-for-plantuml

Raytheon Technologies Approved for Public Release
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.

Commercial Example

- **Amazon Selling Partner interface**
  - Supports multiple versions of agreed to static interfaces
  - Concurrent execution routed by URL
  - Similar to other Amazon and AWS interfaces
  - Data adaptation and role restrictions
  - Callers can easily abstract their version away



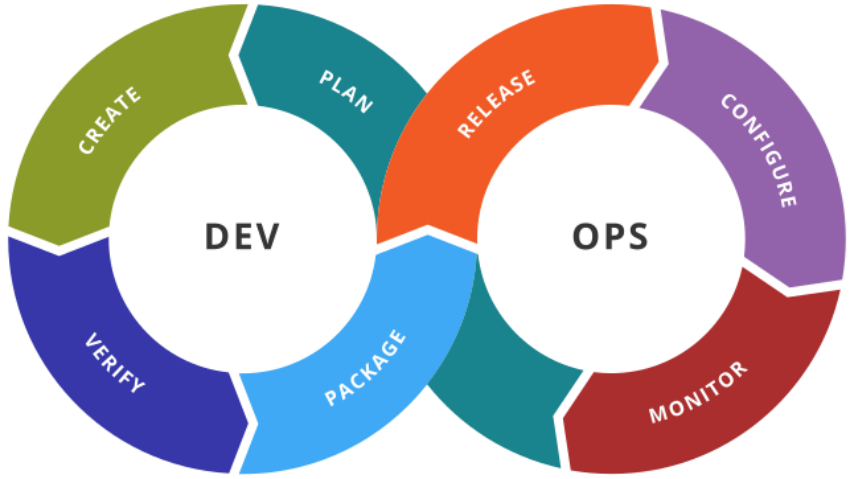
"aws-icons-for-plantuml" by awslabs is licensed under CC BY-ND 2.0.
aws-icons-for-plantuml/LICENSE at main · awslabs/aws-icons-for-plantuml · GitHub
https://github.com/awslabs/aws-icons-for-plantuml

Raytheon Technologies
Raytheon Technologies Approved for Public Release
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.

What about DevSecOps?

DevSecOps allows rapid deployment with reduced risk posture

- Deploys micro-services at the lower levels while maintaining interface code stability
- Reduces risk of full system deployments
- Significantly reduces or eliminates downtime for deployments



Kharnagy, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons
https://upload.wikimedia.org/wikipedia/commons/0/05/Devops-toolchain.svg

Improves security posture

- Allows targeted patching of critical security changes
- Enables automated security testing on granular level

Automated verification finds issues early

- Validates that the interfaces didn't change
- Regression tests the microservice functionality
- Allows validation of multiple versions concurrently in operations

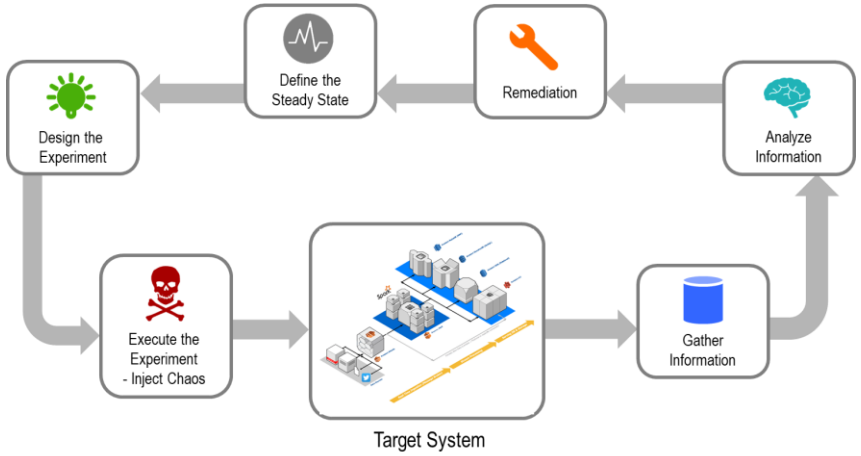
DevSecOps supports MOSA, Agile, and Microservice approaches

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Microservice Recommendations

- ***UX is Not Just for UI's***: Design the interface contract FIRST with stakeholders
  - Tools: e.g. Swagger
- **Patterns**: Use them!
  - Recommended book: https://www.manning.com/books/soa-patterns
- Use **Frameworks**
  - e.g. Spring
- **No one tool is right for every job**
- Adopt and Integrate ***Chaos Engineering***
  - *Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's capability to withstand turbulent conditions in production.*[1]



[1] https://principlesofchaos.org/

Raytheon Technologies
Raytheon Technologies Approved for Public Release
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.

Raytheon Technologies

Raytheon Technologies Approved for Public Release
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.

Authors

Kurt Mohr

Kurt Mohr is an Engineering Fellow with over 20 years in Software Engineering and Architecture spanning both commercial and defense. He has a strong background in multiple Agile development methodologies including Scrum, Kanban, and Scaled Agile. Kurt is the Software Technical Director for Raytheon Intelligence & Space Common Engineering. Kurt has architectural experience with all forms of software systems including cloud, bare metal, and embedded as well as highly scalable distributed computing.

Darryl Nelson

Darryl Nelson is the Technology Director for *Data Engineering and Advanced Software* at Raytheon Intelligence & Space. Darryl's previous roles include Chief Engineer, Corporate Technology Area Director, and Chief Scientist. He currently specializes in scalable system architectures with a focus on operationalizing AI, distributed data management, and continuously evolving software systems. Darryl is a US Army veteran with an interest in the impact of software on the future of warfare.

Raytheon Technologies Approved for Public Release
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.

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Modular Open Systems Approach Implementation Guidebook

Ms. Nadine Geier
Director, Systems Engineering
Office of the Executive Director, Systems Engineering and Architecture (SE&A)
Office of the Under Secretary of Defense for Research and Engineering

CLEARED
For Open Publication
Oct 04, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Agenda

- **Background**
- **Congressional Interest**
- **MOSA Vision**
- **Policy and Guidance… Where Is MOSA?**
- **Working Groups and Industry Engagements.. Bringing the Information Together**
- **MOSA Implementation Guidance**
  - Why a Guidebook?
  - Scope
  - Overview
- **What's Next?**

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Background

Modular Open Systems Approach (MOSA) requirements are codified in law (10 United States Code (U.S.C) §4401 – §4403) for Department of Defense (DoD) acquisition weapon systems

- All program managers can benefit from considering the requirements for modularity and open standards
  - DoD program sponsors and their associated Milestone Decision Authority (MDA) need consistent, quantitative, and repeatable measures to assess their program's compliance with statute
  - These measurements in turn will better enable them to continuously support DoD missions within a rapidly evolving battlespace

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Congressional Interest: MOSA in Development of Weapon Systems

- **2016:** OUSD(R&E) established MOSWG to address standards and architectures (FY15 NDAA Sec. 801)
- **2017:** Congressional requirement for MOSA in Major Defense Acquisition Programs (MDAPs) (FY17 NDAA Sec. 805)
- **2018**: MOSWG Tri-Service MOSA Tiger Teams spearheaded Service-specific guidance
- **2019:** Congressional direction to deliver MOSA Implementation guidance (FY20 NDAA Sec. 840)
- **2020:** OUSD(R&E) MOSWG identified, ranked, prioritized DoD MOSA pain points, and established Tiger Teams
- **2021:** Congressional requirement for establish a MOSA-enabled interface repository to access interfaces and relevant documentation (FY21 NDAA Sec. 804)

MOSA is consistently an RDT&E item of interest for both the HASC and SASC with numerous references in law mandating the enforcement of MOSA Implementation in DoD weapon systems

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

MOSA Vision

Ensure DoD architectures are modular and open to enhance competition, incorporate innovation, and support interoperability and rapid insertion of technology in DoD acquisitions

- Acquire systems that can be upgraded or modified to incorporate new technologies and respond to emerging threats
- Rely on architectures accessed from authoritative sources of truth that identify system components, component capabilities, the interfaces and standards used between components to identify upgradeable systems and reusable components.
- Identify standards which facilitate modularity and openness to enable consistent component replacement and interoperability
- Use relevant technology forecasts to field systems using tailorable modular and open system approaches for technology insertion that contribute to system success

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Policy and Guidance… Where Is MOSA?

Office of the Secretary of Defense

- Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs – *May 2020*
- DoDI 5000.88 Engineering of Defense Systems – *November 2020*
- Engineering of Defense Systems Guidebook – *February 2022*
- Systems Engineering Guidebook – *February 2022*

United States Air Force

- Air Force Data Rights Guidebook – *July 2019*
- Air Force AFI-63-101/20-101 Integrated Life Cycle Management – *June 2020*
- Air Force Material Command (AFMC) Guidebook for Implementing Modular Open Systems Approaches in Weapon Systems – *September 2022*
- PEO Specific Guidance

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Policy and Guidance… Where is MOSA?

United States Army

- Modular Opens Systems Approach Implementation Guide, Office of the Chief Systems Engineer – *June 2020*
- PEO Specific Guidance
  - PEO IEW&S
  - PEO GCS
  - PEO AVN

United States Navy

- Navy NAVSEA 9040.3A Acquisition and Management of Product Model and other Technical Data – *March 2013*
- PEO-Specific Guidance

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Working Groups and Industry Engagements.. Bringing It All Together

Modular Open Systems Working Group

MOSWG Pain Points

MOSWG developed a set of pain points with input from the industrial base and Military Department to address challenges in implementing MOSA in defense acquisition.

MOSWG Tiger Teams

MOSWG formed set of tiger teams to address each pain point and to develop deliverables that will support MOSA implementation in defense acquisition. Deliverables include a MOSA lexicon, recommendations to enable MOSA in acquisition, and an updated approach to assessing MOSA implementations.

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Working Groups and Industry Engagements.. Bringing It All Together

Enabling MOSA

- Need addressed: Common method to describe MOSA in architectures
- Products: Architecture functional decomposition guidance for MOSA

Implementing MOSA

- Need addressed: Common examples and target architectures to aid modular and open system architecture
- Products: Supplemental reference architecture and interface repository ~~guidance~~ for developing MOSA reference implementations

Contracting for MOSA

- Need addressed: Access to updated contracting requirements & processes for implementing MOSA
- Products: Contracting guidance for implementing MOSA

Assessing MOSA

- Need addressed: Quantitatively evaluate of MOSA
- Products: Method and assessment criteria to quantitatively evaluate MOSA in designs, tech approach and business strategies

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Working Groups and Industry Engagements.. Bringing it all Together

Defining MOSA

- Need addressed: Codify common definitions to guide MOSA design
- Products: Instructional Guidance with a taxonomy and lexicon for the implementation of MOSA

Access and Discovery of Standards to Enable MOSA

- Need addressed: Access to MOSA related standards and specifications
- Products: Solutions for identifying and accessing both government and industry standards that enable MOSA

Training and the MOSA Community of Practice

- Need addressed: Advance the state of MOSA training and MOSA Community of Practice
- Products: Modernized MOSA Community of Practice (CoP) site and updated DAU MOSA Training

Community Outreach

- Need addressed: Provide community of interest with regular MOSA-related updates
- Products: MOSA Newsletter and a curated MOSWG repository

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Working Groups and Industry Engagements.. Bringing it all Together

Executive Director of Systems Engineering & Architecture

Office of the Under Secretary of Defense
- United States Navy
- United States Army
- United States Air Force

OSD Assistance

Industry & Academia Engagement encouraged

Implementation
- Team Member(s) n, Org

Assessments
- Team Member(s) n, Org

Enabling
- Team Member(s) n, Org

Contracting
- Team Member(s) n, Org

Outreach
- Team Member(s) n, Org

Standards
- Team Member(s) n, Org

Define MOSA
- Team Member(s) n, Org

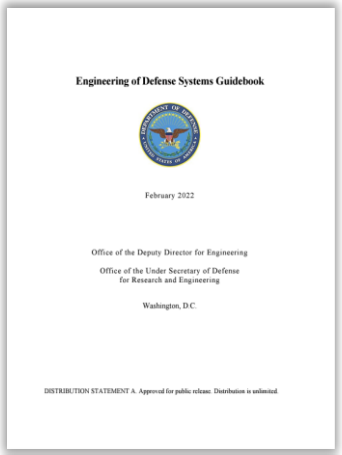
Cybersecurity
- Team Member(s) n, Org

MOSWG Other Focus Interests
- MOSA Business Case
- MOSA Conformance
- MOSA Training
- Reference Architectures

Future Pain Point
Tiger Teams, TBD

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

MOSA Implementation Guidebook
Why a Guidebook?


Engineering of Defense Systems Guidebook

February 2022

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

Washington, D.C.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Modular Open Systems Approach (MOSA)
Reference Frameworks in Defense Acquisition Programs

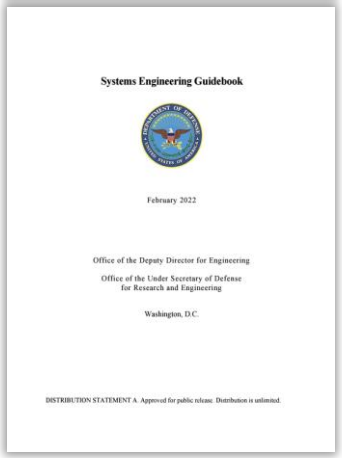
May 2020

Deputy Director for Engineering

Office of the Under Secretary of Defense for Research and Engineering,
Director of Defense Research and Engineering for
Advanced Capabilities

Washington, D.C.

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 20-S-1273.

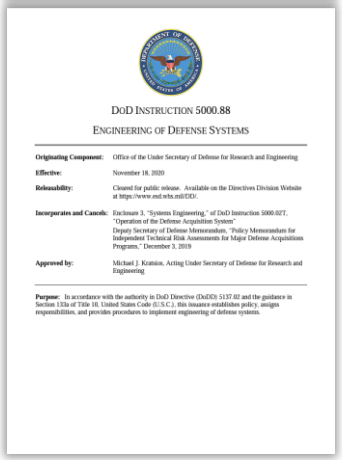

Systems Engineering Guidebook

February 2022

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

Washington, D.C.

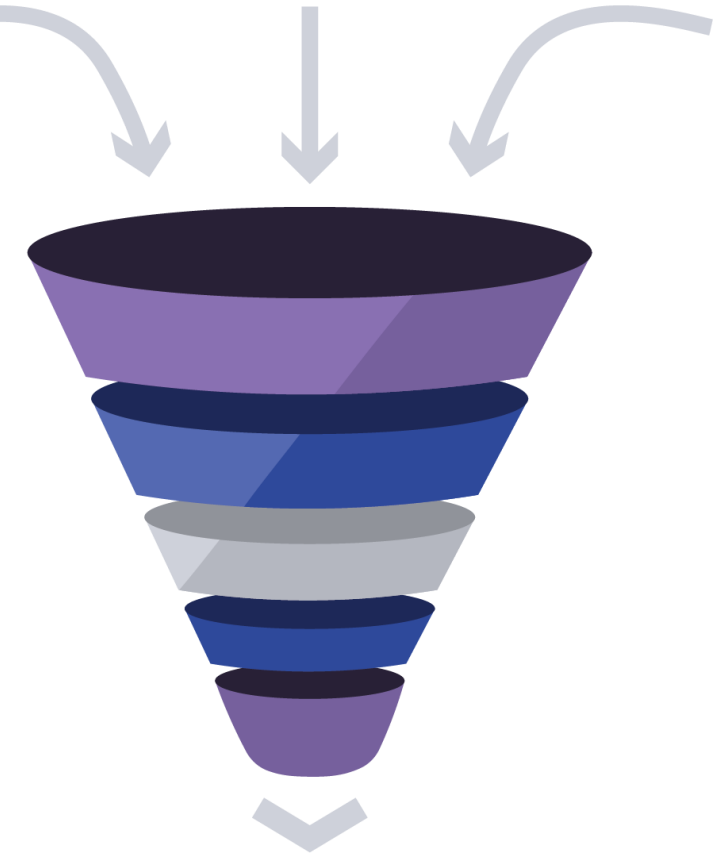
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.


DoD Instruction 5000.88

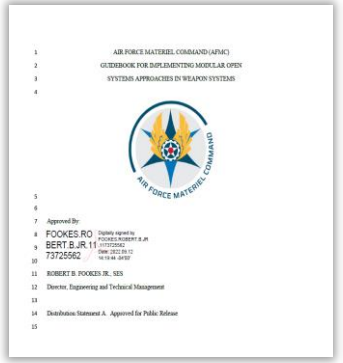
Engineering of Defense Systems

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	November 18, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Enclosure 3, "Systems Engineering," of DoD Instruction 5000.02T, "Operation of the Defense Acquisition System" Deputy Secretary of Defense Memorandum, "Policy Memorandum for Independent Technical Risk Assessments for Major Defense Acquisitions Programs," December 3, 2019
Approved by:	Michael J. Kratsios, Acting Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02 and the guidance in Section 133a of Title 10, United States Code (U.S.C.), this instruction establishes policy, assigns responsibilities, and provides procedures to implement engineering of defense systems.



Synergistic guidance for MOSA Implementation

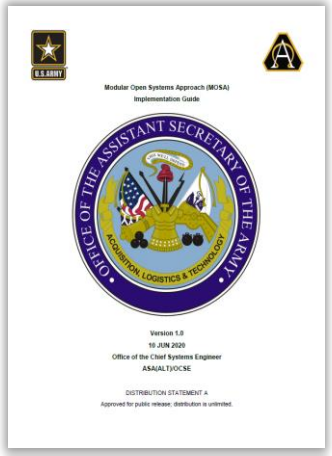

AIR FORCE MATERIEL COMMAND (AFMC)
GUIDEBOOK FOR IMPLEMENTING MODULAR OPEN
SYSTEMS APPROACHES IN WEAPON SYSTEMS

Approved By:

FOOKES.RO BERT.B.JR.1 73725562

ROBERT B. FOOKES JR., SES
Director, Engineering and Technical Management

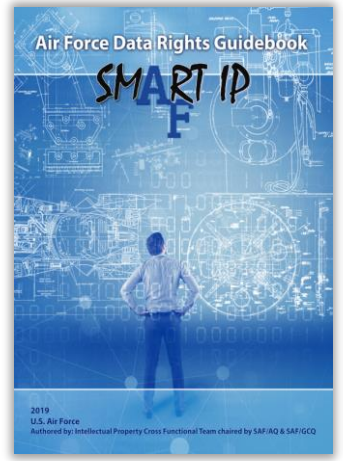
Distribution Statement A. Approved for Public Release

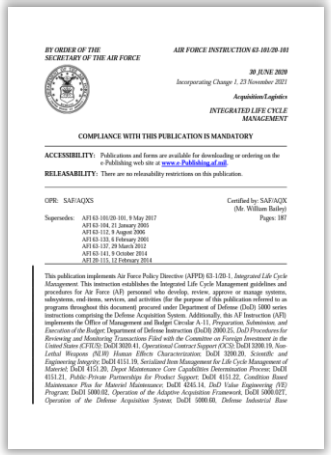

Modular Open Systems Approach (MOSA)
Implementation Guide

OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION, LOGISTICS & TECHNOLOGY

Version 1.0
10 JUN 2020
Office of the Chief Systems Engineer
ASA(ALT)/OCSE

DISTRIBUTION STATEMENT A
Approved for public release; distribution is unlimited.




BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 63-101/20-101

30 JUNE 2020

Incorporating Change 1, 23 November 2021

Acquisition/Logistics

INTEGRATED LIFE CYCLE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at www.e-Publishing.af.mil.

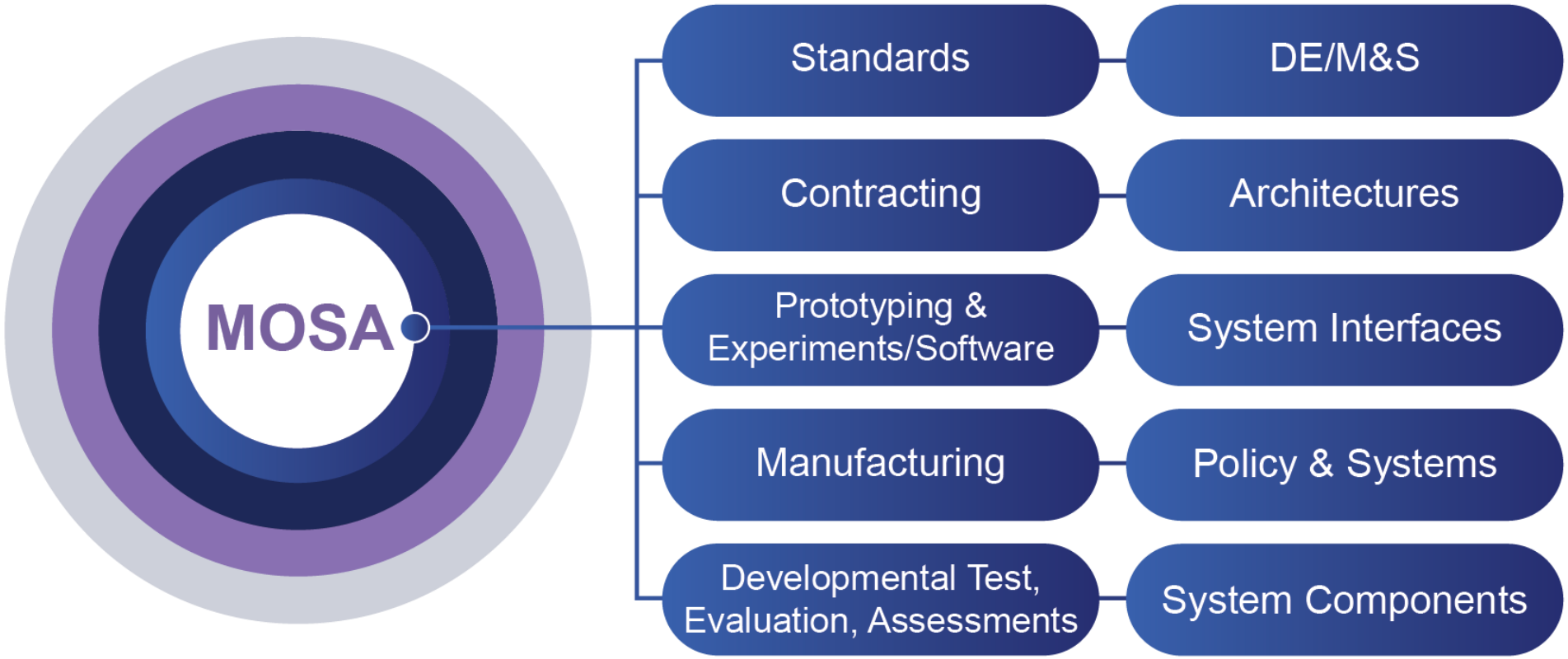
RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/AQXS — Certified by: SAF/AQX (Mr. William Bailey)

Supersedes: AFI 63-101/20-101, 9 May 2017 — Pages: 181
AFI 63-104, 21 January 2005
AFI 63-112, 9 August 2006
AFI 63-133, 6 February 2001
AFI 63-137, 29 March 2012
AFI 63-141, 9 October 2014
AFI 20-115, 12 February 2014

This publication implements Air Force Policy Directive (AFPD) 63-1/20-1, *Integrated Life Cycle Management*. This instruction establishes the Integrated Life Cycle Management guidelines and procedures for Air Force (AF) personnel who develop, review, approve or manage systems, subsystems, end-items, services, and activities (for the purpose of this publication referred to as programs throughout this document) procured under Department of Defense (DoD) 5000 series instructions comprising the Defense Acquisition System. Additionally, this AF Instruction (AFI) implements the Office of Management and Budget Circular A-11, *Preparation, Submission, and Execution of the Budget*; Department of Defense Instruction (DoDI) 2000.25, *DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)*; DoDI 3020.41, *Operational Contract Support (OCS)*; DoDI 3200.19, *Non-Lethal Weapons (NLW) Human Effects Characterization*; DoDI 3200.20, *Scientific and Engineering Integrity*; DoDI 4151.19, *Serialized Item Management for Life Cycle Management of Materiel*; DoDI 4151.20, *Depot Maintenance Core Capabilities Determination Process*; DoDI 4151.21, *Public-Private Partnerships for Product Support*; DoDI 4151.22, *Condition Based Maintenance Plus for Materiel Maintenance*; DoDI 4245.14, *DoD Value Engineering (VE) Program*; DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*, DoDI 5000.02T, *Operation of the Defense Acquisition System*; DoDI 5000.88, *Defense Industrial Base*

MOSA Implementation Guidebook Scope



Coalesce MOSWG Tiger Team products, Military Department (MILDEP) MOSA exemplars and industry recommendations for MOSA implementation

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

MOSA Implementation Guidebook Overview

Topics
MOSA-enabling Standards and Specifications
Contracting
Lexicon
Exemplars
Industry Recommendations
Architectures
Training and Education
Designated Interfaces

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

MOSA Implementation Guidebook Timeline

- **Phase 1 – June 2022**
  - Kickoff meeting
  - Assigning writing sections of Implementation Guidebook
- **Phase 2 – August 2022**
  - Status meeting #1
  - Review of status of sections
- **Phase 3 – September 2022**
  - Status meeting #2
  - Submission of draft sections for consolidation and comment/review

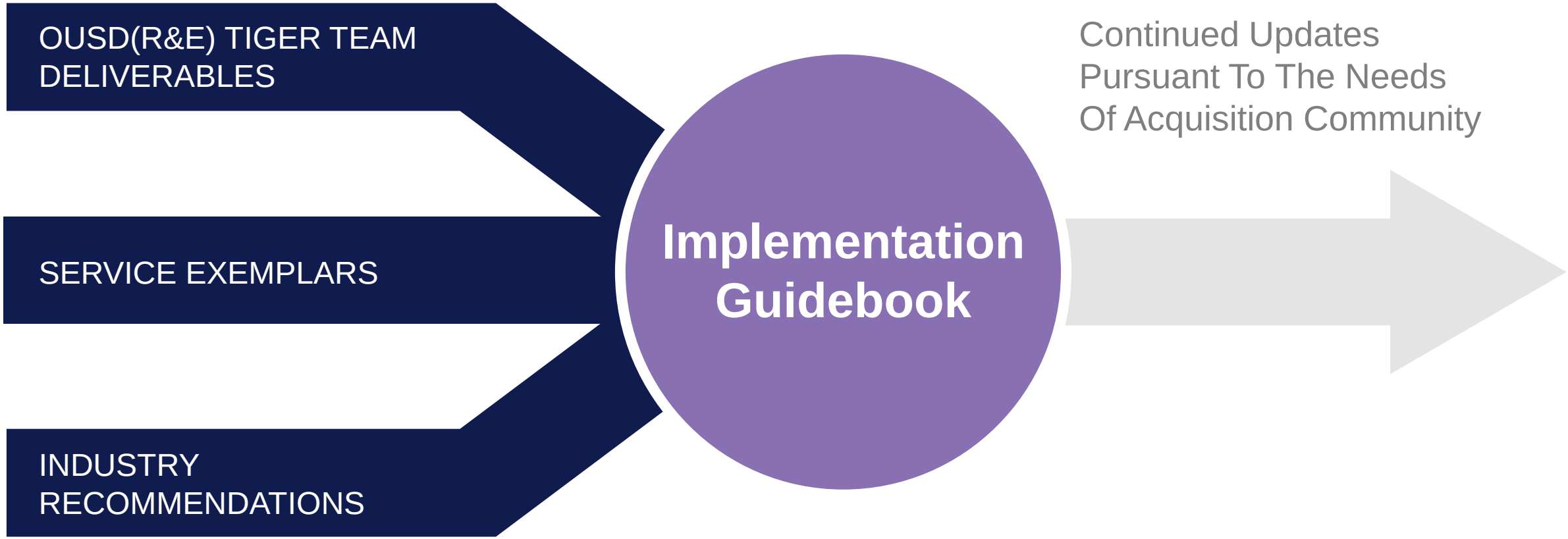
Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

MOSA Implementation Guidebook Timeline

- **Phase 4 – October/November 2022**
  - Status meeting #3
  - Discussion/Adjudication of comments and edits
- **Phase 5 – December 2022/January 2023**
  - Status meeting #4
  - Discussion/Adjudication of comments and edits
- **Phase 6 – December 2022/January 2023**
  - Final submission of assigned guidebook sections
  - Technical Edit review
  - Public Affairs Submission
  - Release to https://cto.mil

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

What's Next?



Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Collaboration Opportunities

- **Bi-monthly MOSWG**
  - Third Wednesday of every other month
  - https://intelshare.intelink.gov/sites/moswg/_layouts/15/start.aspx#/
- **Monthly Tiger Teams**
  - Implementing MOSA Tiger Team
  - Contracting for MOSA Tiger Team
  - MOSA Training/CoP Tiger Team
- **DAU hosted Community of Practice**
  - https://www.dau.edu/cop/mosa/Pages/Default.aspx
- **SE Modernization Body of Knowledge – MOSA section *(forthcoming)***

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

Contact

Office of the Under Secretary of Defense for Research and Engineering

osd.r-e.comm@mail.mil | Attn: SE&A

https://www.cto.mil

https://ac.cto.mil/engineering

Distribution Statement A. Approved for public release. Distribution is unlimited. (# 23-S-0001)

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Systems Engineering Modernization Across the Lifecycle

SERC SEMOD Lifecycle Mental Model

Ms. Nadine Geier

Director, Systems Engineering

Office of the Executive Director, Systems Engineering and Architecture

Office of the Under Secretary of Defense for Research and Engineering

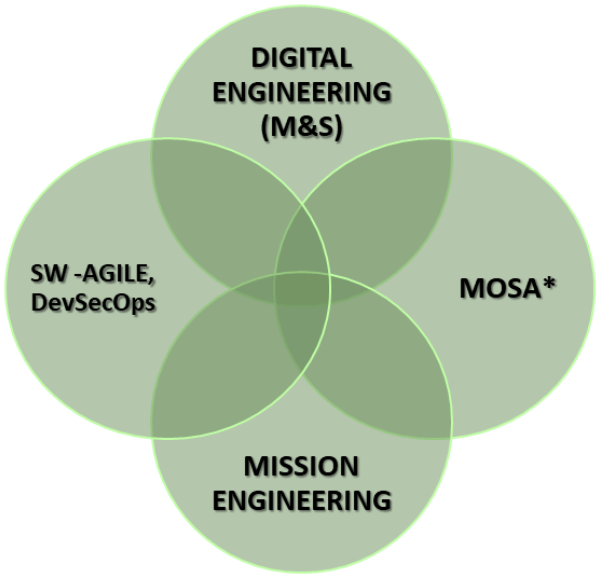
Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SE Modernization Problem Statement

SE Modernization Problem Statement

"There is a lack of an integrated approach to implementation of SE Focus Areas that is creating a delay in full implementation of the Digital Transformation which is necessary to ensure the relevant guidance, skills, and training are available to deliver a robust, disciplined approach to weapon systems acquisition."

SE Modernization Focus Areas (Initial Scope)



Collaborating with Government, Industry & Academia

Cross-Cutting Key Enablers

Architecture	Modeling Mission & Platform levels, embracing Reference Architectures
Model-Based Systems Engineering (MBSE)	Enterprise-wide implementation; models as Source of Truth
SOS/Enterprise Collaboration & Data	Understand/Assess cross-platform capabilities
Engineering Workflow	Evolving SE processes to model based, including V&V, R&M
Workforce Training & Culture	A focused approach to workforce initiatives that enable culture change & skills gap

ENABLERS RESULTED FROM INITIAL OUTREACH/INFORMATION SESSIONS

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Questions Used for Phase 1 Information Sessions

What role does **systems thinking** play

CURRENT STATE

What is the **Current State** of Systems Engineering in DoD?

What are the **enablers** to modernization?

What are the **barriers** to modernization?

How do we create an **SE Modernization Enterprise**?

COLLABORATION

How do we **increase collaboration** & **knowledge sharing**?

Who are potential **partners**/information sources?

How can we leverage **NDIA, INCOSE & consortiums** (or other government-industry groups)?

INNOVATION

What is the **Future State** of SE?

How do we **bring innovation to the SE environment** (process, artifacts, reviews, etc.)?

How do we know that we have achieved our goal? What are the **indicators of success**?

How do we **shift the culture** to embrace modernization principles and practices?

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Responses from INCOSE Workshops/Information Sessions

CURRENT STATE

- **Lack integration of engineering and other competencies** (science, safety, software, security, programmatic)
- **Lack means & funding for collaboration**
- **Lack of governance** (data and models)
- **Lack change momentum** (status quo dominates)
- **Digital artifacts become static -** lose dynamic content as the design progresses
- **Shortage of experienced practitioners**
- **Lack a digital process flow handbook(s),** a digital workflow with traceability to domains

COLLABORATION

FUTURE STATE

- ✓ **Seamless interoperability and integration** of all engineering disciplines
- ✓ **Greater (digital) integration of SE &** other disciplines including project management
- ✓ **Continuous engineering** across the globe communicating seamlessly and remotely
- ✓ **Digital twin(s) -** holistic for system life cycle
- ✓ **The equivalent of a DevOps revolution** cutting across disciplines & lifecycle
- ✓ **"How to model" is a core competency** for more than just the engineering community
- ✓ **Tool maturity -** more open, interoperable, usable, standardized

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

NDIA Activities Advance the SEMOD Initiative

SEMOD Focus Areas

- **MOSA**
  - SE Division (SED) produced MOSA White Paper
  - ✓ Developed MOSA Metrics guidance for programs
- **Agile Software/ System Development**
  - ✓ Agile Deliveries for Agencies, Programs, & Teams (ADAPT) Committee focused on promoting Agile System Development and DevSecOps for programs
  - ✓ Joint SED/ Integrated Program Management Division (IPMD) working group on Agile Program Execution
- **Digital Systems Engineering (DSE)**
  - ✓ SED-level working group addressing evolution of MBSE to DSE
- **Mission Engineering (ME)**
  - SED-level working group studying ME implementation
  - ✓ Conducted Survey of Industry's Mission Engineering capabilities
  - Provided review/ recommendations to DoD ME Guidebook update

SEMOD Cross-Cutting Key Enablers

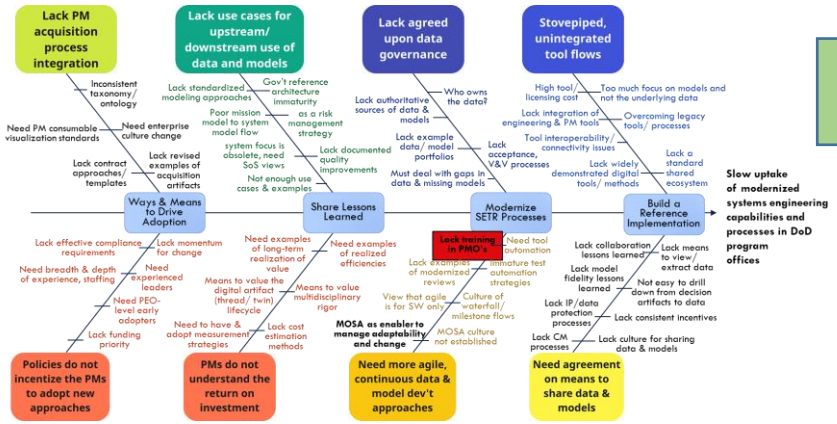
- **Architecture**
  - ✓ SE Division (SED) Architecture Committee leads system architecture focus
- **MBSE**
  - SED Modeling & Simulation Committee leads MBSE focus
- **SoS/ Enterprise Collaboration & Data**
  - ✓ System of Systems (SoS) Committee leads this area
  - ✓ System Security Engineering Committee leads focus on Enterprise Collaboration & Data
- **Workforce Training & Structure**
  - ✓ SED Education & Training Committee leading SEMOD/Digital Acquisition Thread study

✓ *Denotes subject of a 2022 NDIA S&ME Conference presentation*

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SEMOD FY22/23 Lines of Effort

SEMOD Pain Points



ALIGNED TO

SEMOD Lines of Effort

- SEMOD BoK & Community of Practice
- Policy & Guidance Review & Update
- Model Based Artifacts & Workflow
- Framework (Workflow Mapping & Roadmaps)
- Digital Acquisition Thread
- Workforce: DE/SE Topic Workshops & Webinars

EACH PAIN POINT ADDRESSED BY MULTIPLE LINES OF EFFORT

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SERC SEMOD GOALS

1. **Build an Integrating Framework** that incorporates key activities across these domains and focus areas.
2. **Align and Integrate Systems Engineering Practices** to specific acquisition pathways.
3. **Develop a set of Artifacts and associated Meta-Data** for a categorization and information framework that captures policy, guidance, and lessons learned into a body of knowledge.

As we developed the integration framework, we realized the “mental models” and related language of DoD systems Engineering were still too rooted in large scale major capability acquisitions and document-driven processes. We needed to re-envision the purpose and goals of modernized “digital” SE practices.

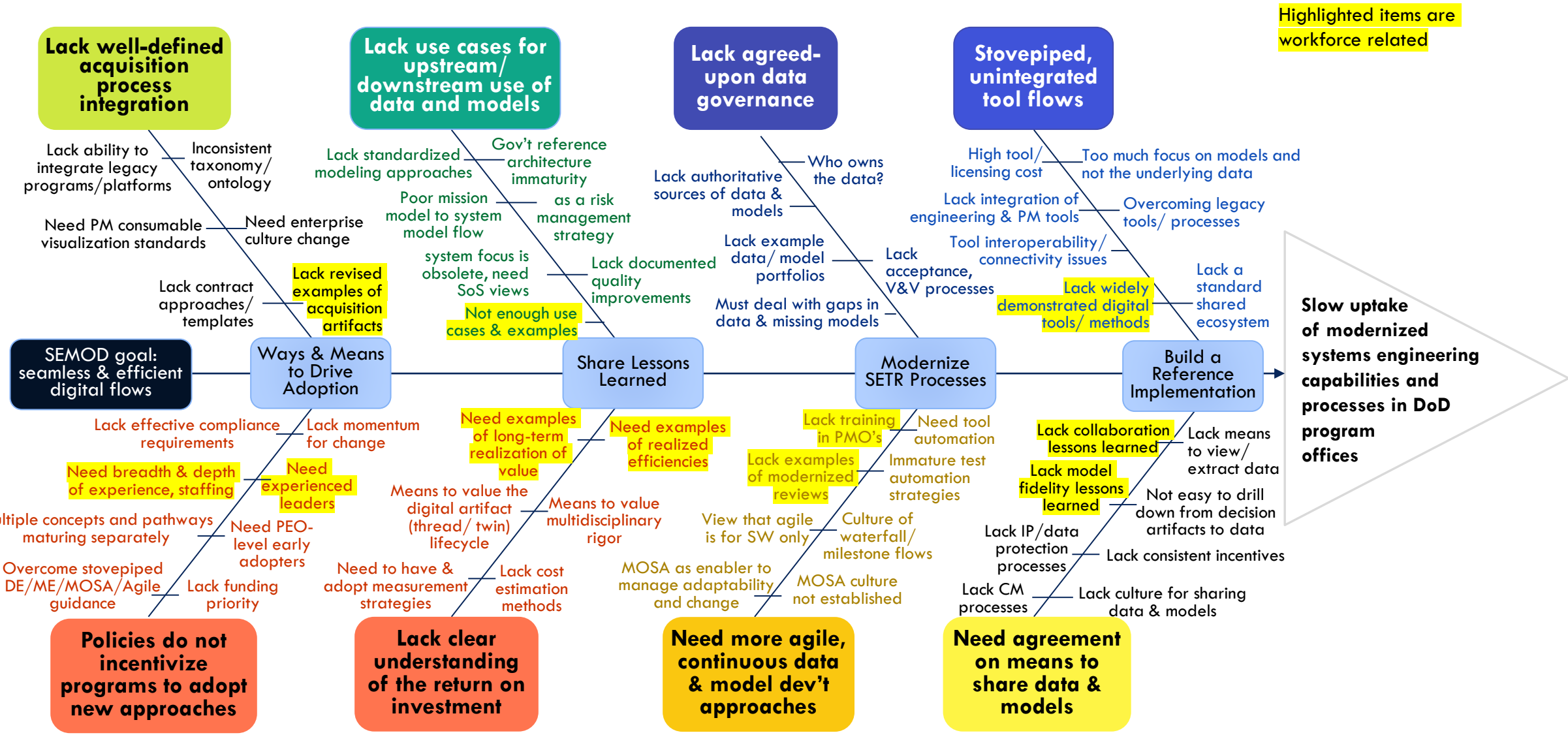
Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SEMOD Pain Points

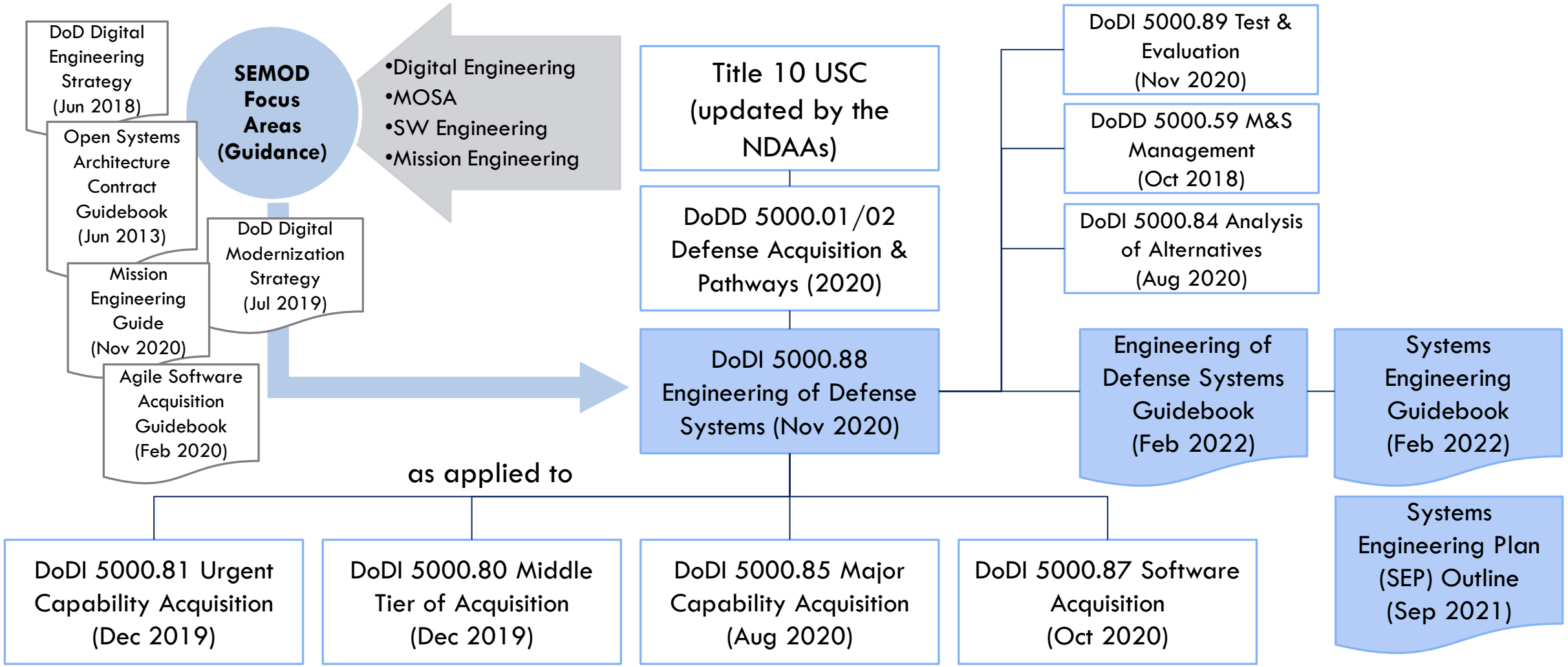
- Causally Related
- Derived from Workshops and Discussions with stakeholders
- Using the Integration Framework
- Address the slow uptake of modernized systems engineering processes
- Shown in the Fishbone diagram (next chart)
- Driven by the goal of seamless and efficient digital flows from data to decision artifacts and from decision artifacts back to data.

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

PAIN POINTS FISHBONE



POLICY DERIVATION



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

FOCUS AREA INTEGRATION – INTENT OF POLICY AND GUIDANCE

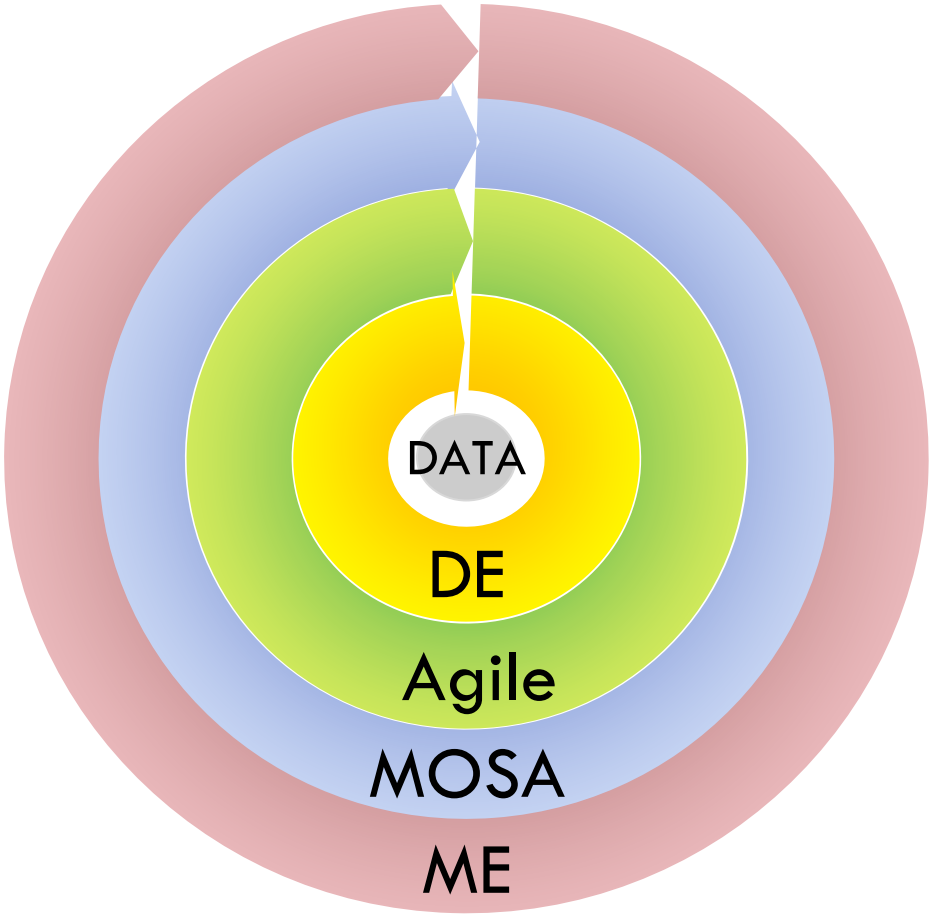
Digital Engineering (DE): implement "an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support lifecycle activities from concept through disposal." Enabler to manage lifecycle efficiency.

Agile/DevOps: begin with a high-level capture of business/ technical needs, continually implement and deploy to define & build value. Enabler to manage risk.

Modular Open Systems Approach (MOSA): use modular design, control interfaces, adopt open standards, measure conformance. Enabler to manage adaptability and change.

Mission Engineering (ME): continually provide engineered mission-based outputs to inform requirements, prototypes, design, and investment. Enabler to manage portfolios.

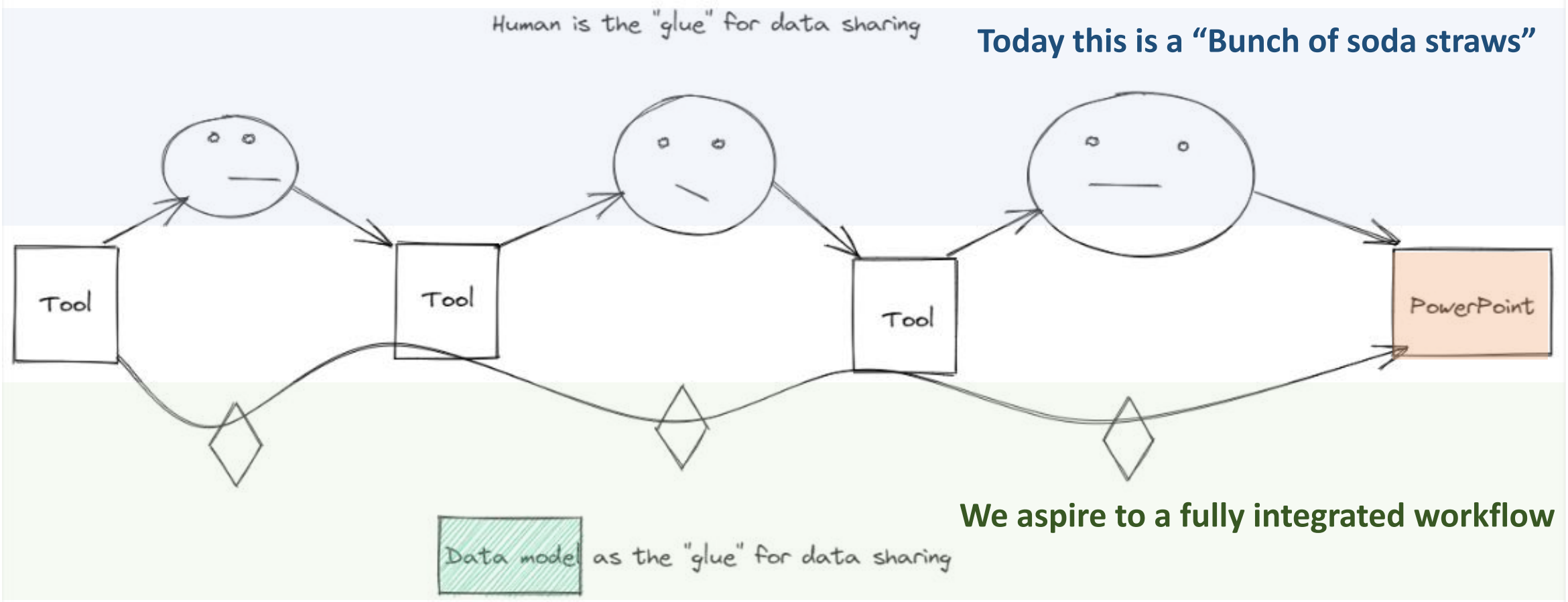
DoD Data Strategy: "data as a strategic asset"



The 4 focus areas generate a layered, continual, and data-centered model

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

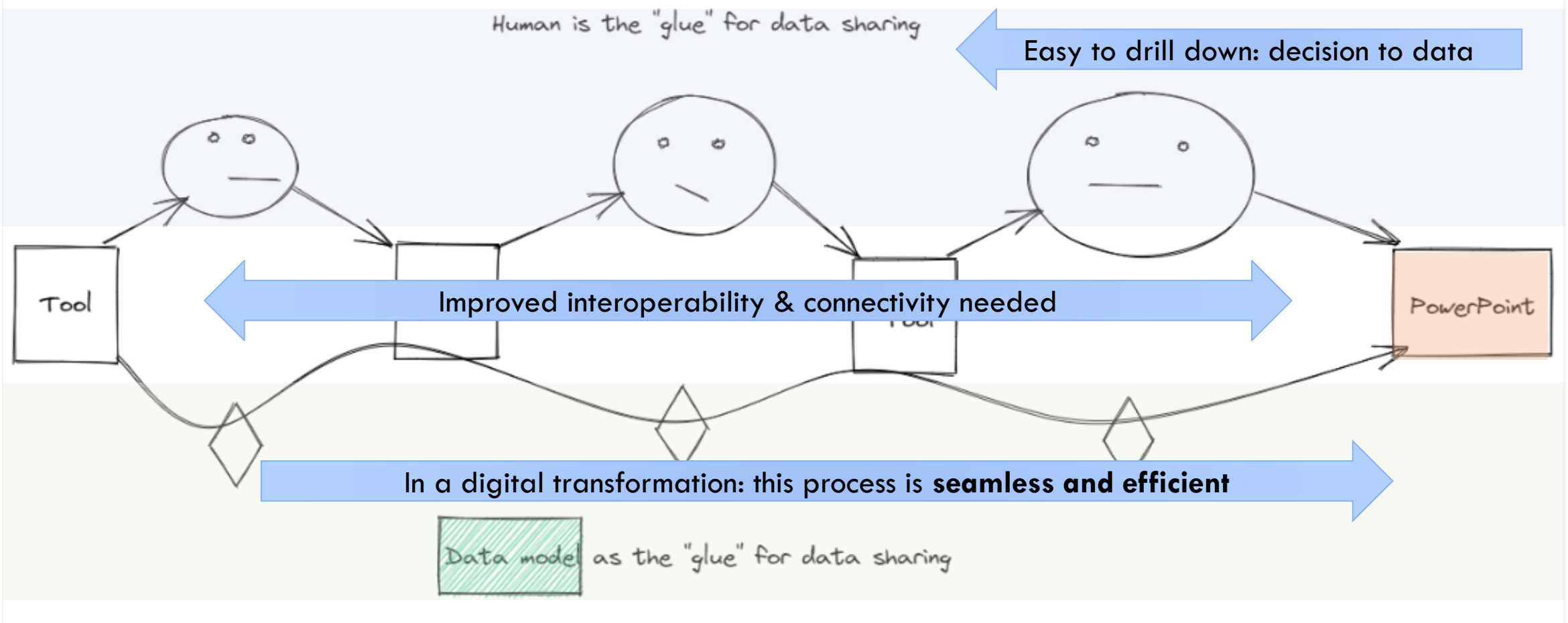
CONCEPTUAL VIEW: DIGITAL ARTIFACT DEVELOPMENT



Digital Artifact - An artifact produced within, or generated from, the engineering ecosystem. These artifacts are generated **through transformation of data and models into views** in order to visualize, communicate, and deliver data, information, and knowledge to stakeholders.

WHERE WE NEED TO BE

SEMOD evolves toward **seamless and efficient** digital flows from data to decision artifacts and from decision artifacts back to data.

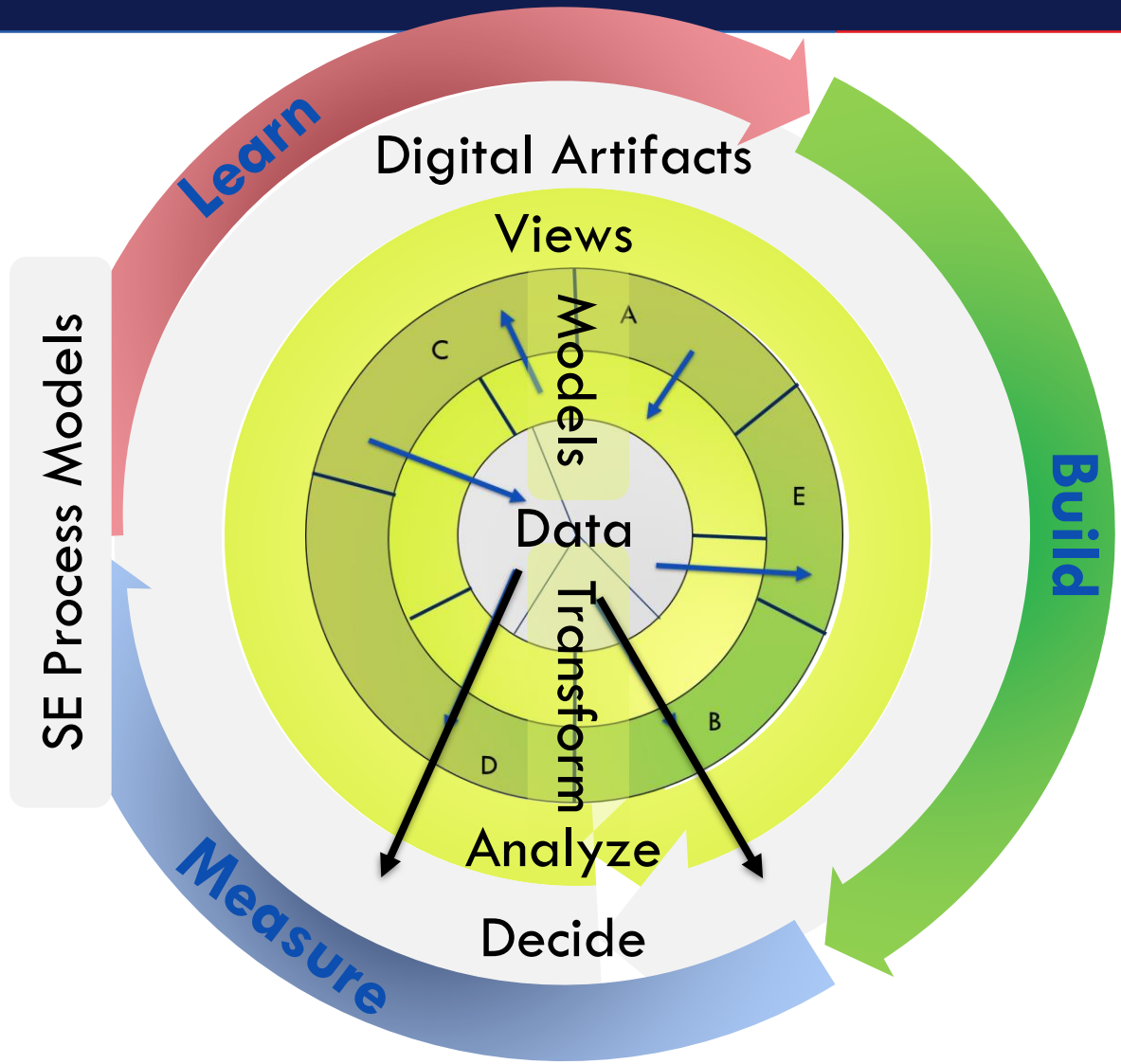


Lack of an integrated approach is creating a delay in full implementation of the Digital Transformation

A Revised Mental Model of the Systems Engineering Lifecycle

- SEMOD redraws the stages of the SE Lifecycle in a circular process to represent it as:
  1) data transformations at the core
  2) layered across disciplines & tasks
  3) continuous processes that could be entered from any point

- Data is transformed through Models into Decision Artifacts
- Data remains accessible via Decision Artifacts



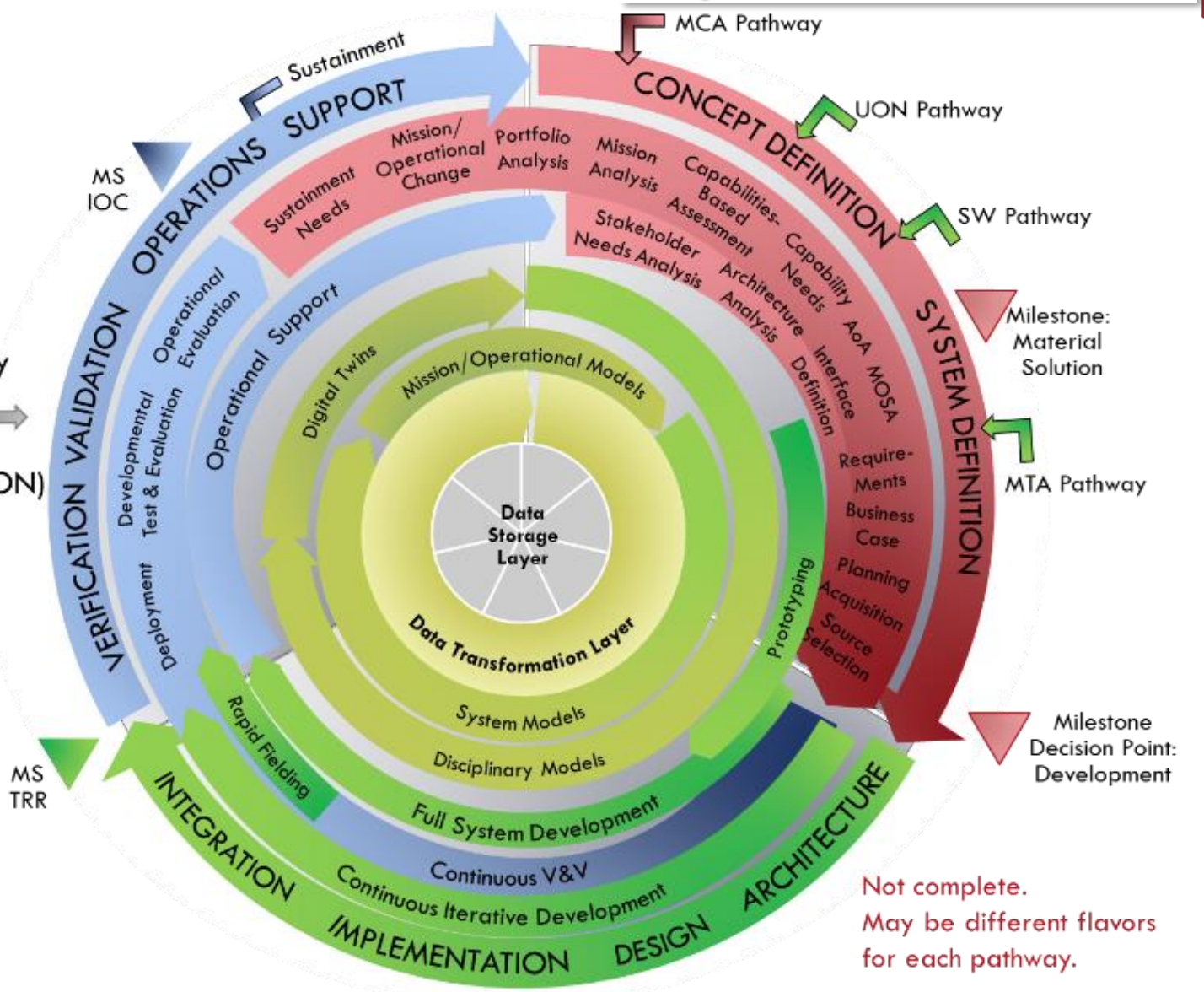
SE Modernization Mental Model

SYSTEMS ENGINEERING RESEARCH CENTER

NDIA AT THE HEART OF THE MISSION

NOTIONAL VIEW: FULL SE MODERNIZATION LIFE CYCLE

- Cyclic nature of modern SE
- Still milestone-based
- SE core principles in every Acq pathway
- Flexible system life cycle entry points:
  - Learn-Build-Measure (MCA)
  - Build-Measure-Learn (Mid-Tier, SW, UON)
  - Measure-Learn-Build (Sustainment)
- Continuous Iterative Development processes (around the circle)
- Continuous Data Management and Transformation processes (at the core)



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

15

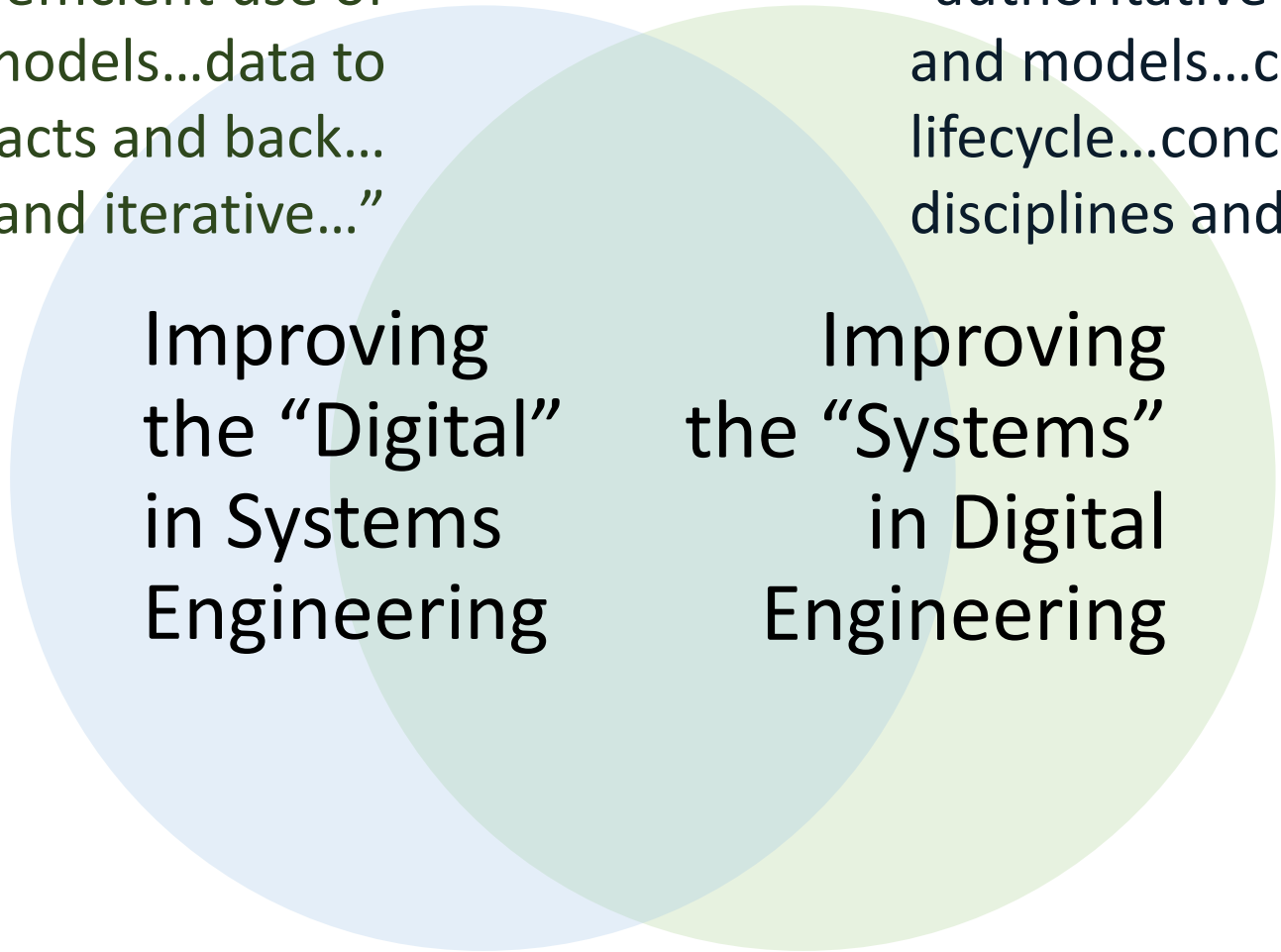
Systems Engineering Modernization and Digital Engineering

"seamless and efficient use of data and models…data to decision artifacts and back… continuous and iterative…"

SEMOD Project

"authoritative sources of data and models…continuity across lifecycle…concurrency across disciplines and domains…"

DoD DE Strategy



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SUMMARY

- SE Modernization and related focus areas represent a more significant shift in acquisition and engineering practices than envisioned by any single initiative
- The integration of these requires new mental models
  - Data at the core – many lessons learned will drive evolution
  - Seamless and efficient process integration – new exemplar standards/tools
  - All lifecycles are continuous and use appropriate iterative methods
  - But SE core lifecycle processes will remain with new practices
  - Significant workforce evolution needed
- Several SERC tasks support the community in this evolution

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Workforce Development
Planned FY22/23 SE Modernization Workshops/Webinars

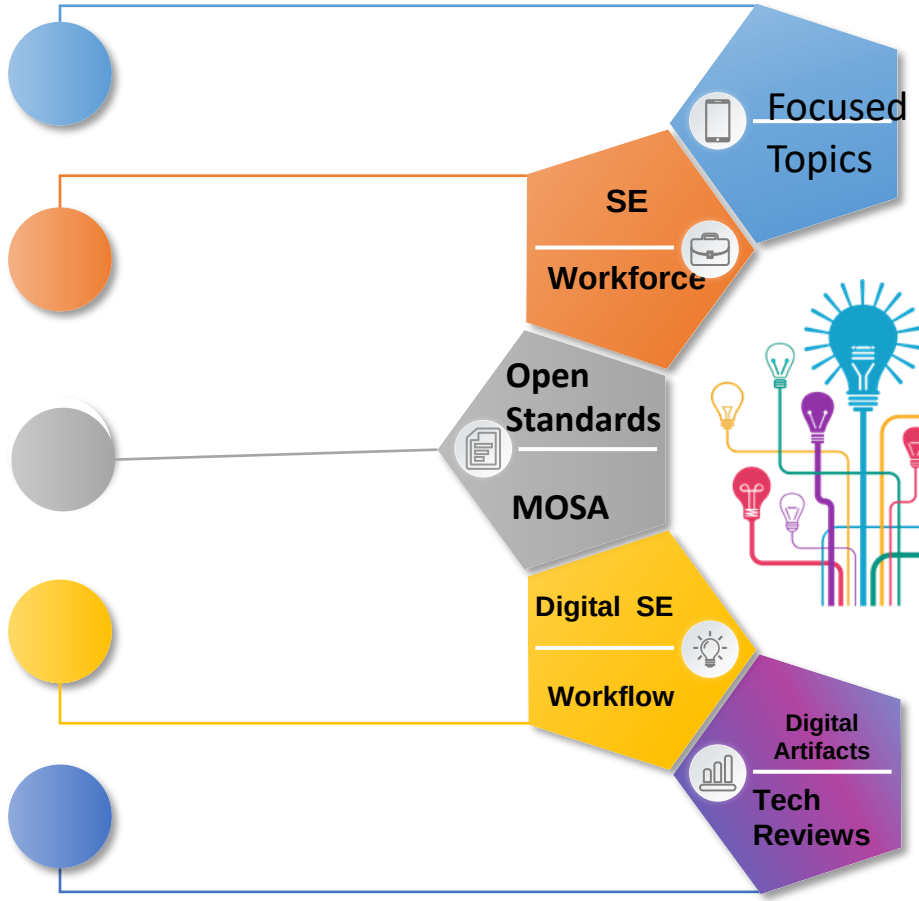
Specialty – **Focused Topics**: Digital T&E – R&M – Mission Engineering – Contracting for Digital Artifacts – Use of Reference Architecture

SE Boot Camp on Modernized SE Practices – Agile SE.

Implementing **MOSA & Open Standards in a Digital Environment**

Engineering Workflow in a Digital Environment. (DAU Acquisition Thread)

Technical Reviews & Digital SE Artifacts in a Digital Environment



Ongoing collaboration with Engineering Technical Management Functional Integration Team to develop SE Credentials

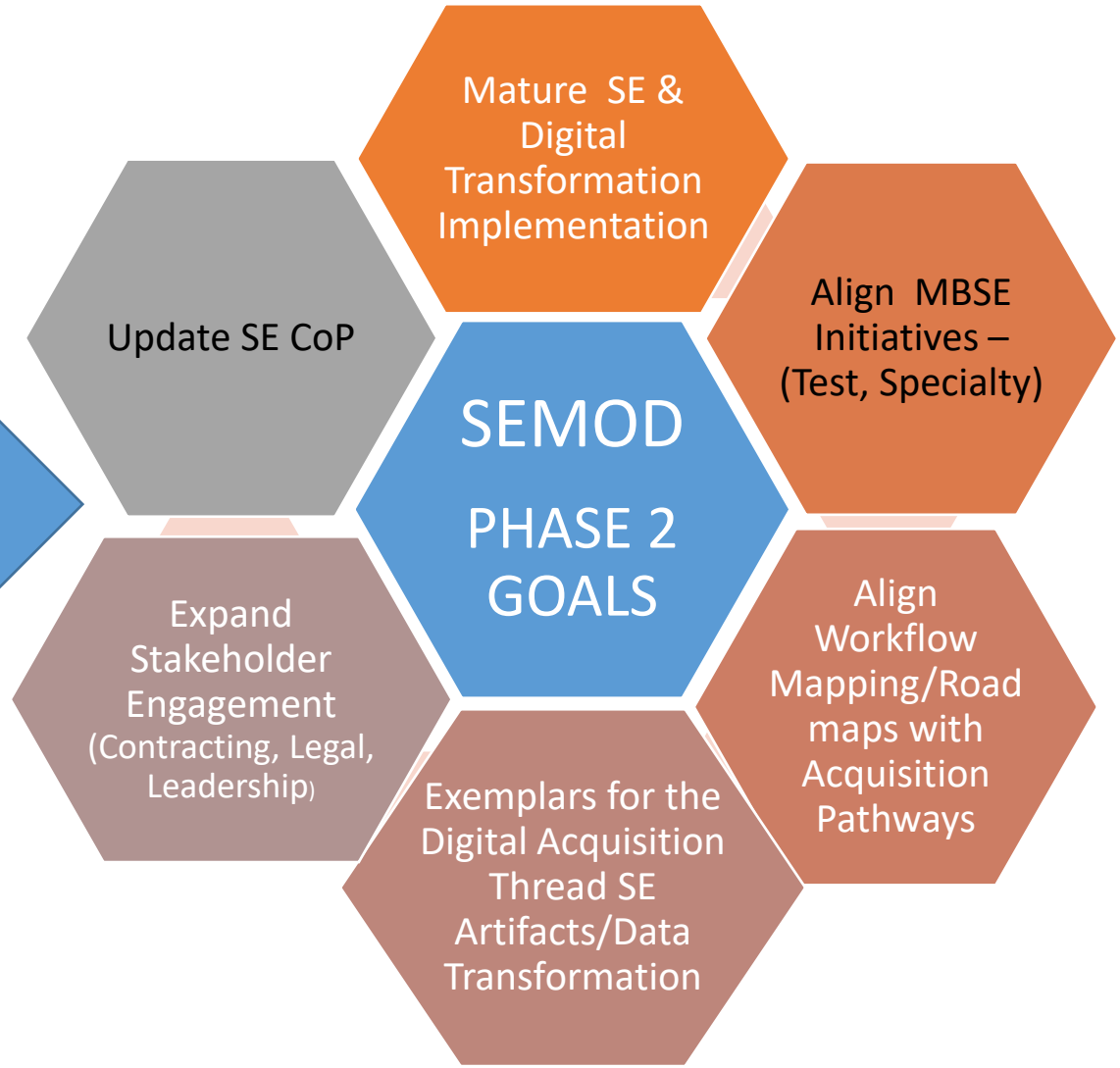
WORKSHOPS WILL INFORM BoK, UPDATES TO POLICY & WORKFORCE GUIDANCE

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

SEMOD Path Forward for Phase 2

Complete Phase 1 SERC Deliverables

- ✓ **Lessons Learned Database**
- ✓ **Ontology** guide for SEMOD policy and guidance
- ✓ **Workforce, education and training** recommendations
- ✓ Present **Policy gaps & recommendations**
- ✓ **Recommend** additional focus area integration



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Contact

Office of the Under Secretary of Defense for Research and Engineering

osd.r-e.comm@mail.mil | Attn: SE&A

https://www.cto.mil

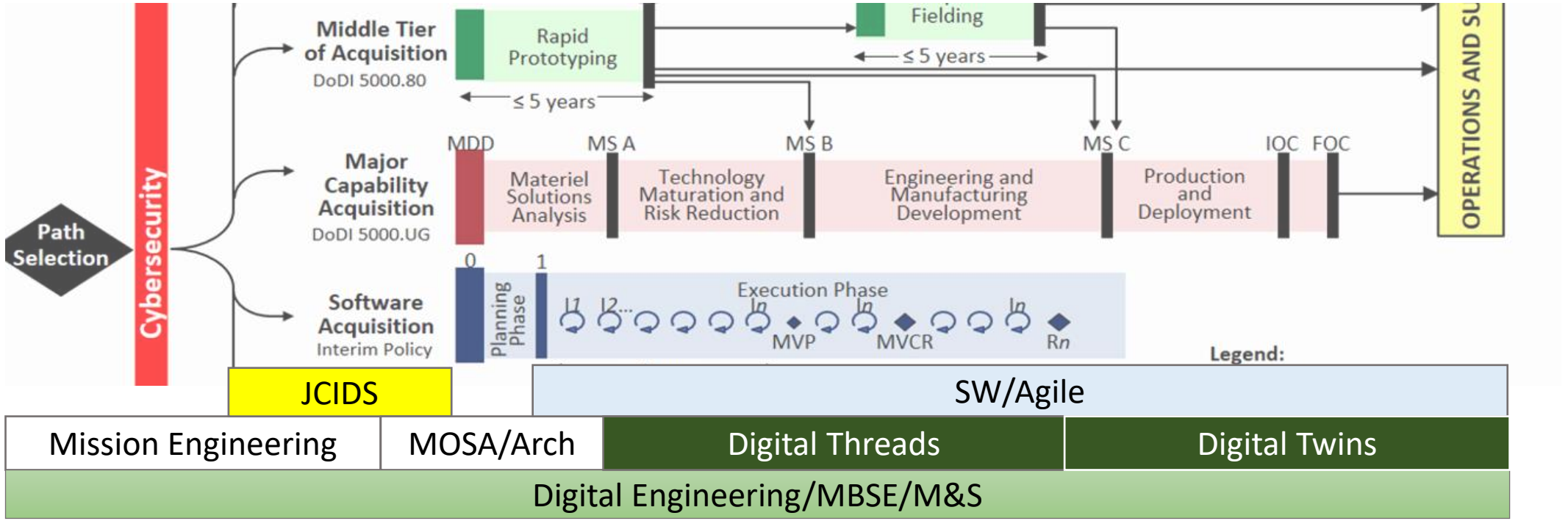
https://ac.cto.mil/engineering

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Backup charts

SEMOD Initial Framework (SERC)

- Digital Transformation introduces digital & model-based information flow into the acquisition lifecycle
- SERC is mapping information items and digital artifacts related to handoffs in 3 acquisition pathways
- Examining (1) IEEE15288/INCOSE Handbook, (2) INCOSE/NDIA SEBoK, (3) DAU guides (new), (4) NAVAIR "Skyzer" DE Pilot effort. Framework will define "What digital info/artifact might be exchanged at each decision point?"



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

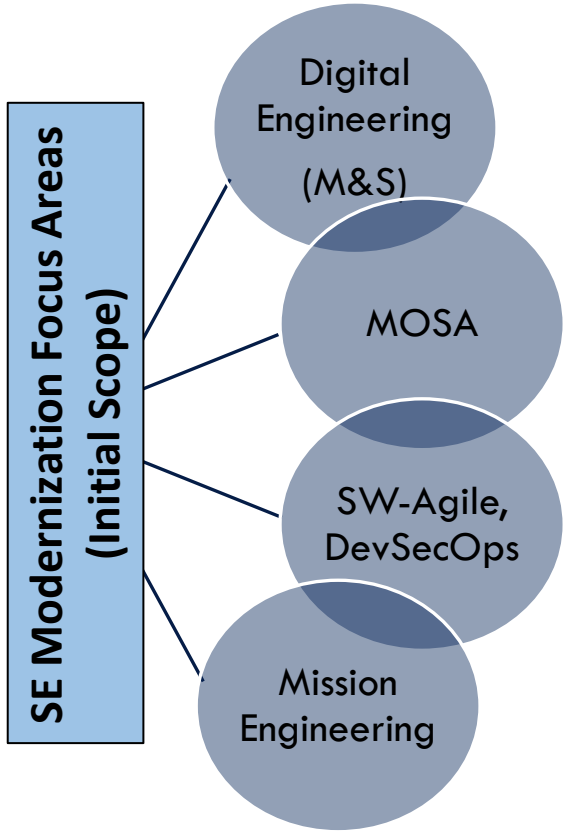
INCOSE IW 2022 Strategy Session Summary (2 Workshops)

What is the Current State?	How do we increase collaboration & knowledge sharing?	What is the Future State?
Lack integration of engineering and other competencies (science, safety, software, security, programmatics)	Leaders not managers, need to **recognize this is a digital transformation linking SE and other disciplines through data**	**Seamless interoperability and integration** of all engineering disciplines
Hard to create collaboration, continuously, in digital environments; funding is a barrier	**SE job is to communicate**! Funding allocations don't promote collaboration	**Continuous engineering** across the globe – communicating seamlessly and remotely
Lack of governance approaches for data and models, ingrained paper CM/DM mindset	**Apply automation**, remove drudge work, focus on build	**Digital twin(s)** that is holistic for a system over its entire life cycle
Historical approaches dominate**, lack change momentum**	Recognize limits of the digital technologies**, build incrementally & continuously**	**Greater (digital) integration of SE** and other disciplines including project management
Engineers lose dynamic content as the design progresses, **artifacts become more static, stale**	Leverage SW processes that could improve SE; **build iterative, collaborative teams**	The **equivalent of a DevOps revolution** cutting across disciplines & lifecycle
Need to move away from a static view of the system toward **model-based reviews; shortage of experienced practitioners**	**Training and exposure for everyone**	**"How to model" is a core competency** for more than just the engineering community
Need to know system changes are not breaking something else, not seeing full scope **Lack a digital process flow handbook(s), a digital workflow with traceability to domains**	**Interoperability standards, tools, clouds, data across boundaries**, norms for working together Recognize limits of the digital technologies, build incrementally & continuously	**Tool maturity**: more open, interoperable, usable, standardized

SEMOD Collaboration with INCOSE

- SERC led two strategy sessions to discuss:
  - Is there a strong need to “modernize”?
  - What focus areas should we tackle first?
  - How are emerging and relevant practices integrated into SE discipline?
  - How should the overall practice of systems engineering shift over time? These are all questions that must be addressed by INCOSE.
- Goals of the session:
  - Document the current state of SE with respect to evolving markets and methods,
  - Identify focus areas for INCOSE that we should address with respect to evolving practice,
  - Develop a set of prioritized actions or perhaps simple roadmaps, and
  - Recommend/Identify key enablers that are essential to a modern approach to SE (for example reference architectures, SoS collaboration environments, etc.).

SE Modernization: Broad Synergy with Other SERC/AIRC Efforts



Cross Cutting Key Enablers

- Architecture
- MBSE
- SOS/Enterprise Collaboration
- Engineering Workflow
- Workforce Culture

WRT-1036, ART-002 Model Centric Engineering – surrogate pilot project to evaluate details of DE, Navy NAVSEM process model

WRT-1040 DE Metrics – framework for quantifying DE/MBSE benefits, SE community working group

WRT-1047 Digital Data Management & Analytic Strategy – data strategies combining mission engineering, digital engineering, acquisition baseline data, etc.

ART-016 Army Common Architecture Strategy – government reference model/MOSA strategies

WRT-1041 Space Force Agile Transformation – direct experience supporting government agile transformation, metrics

WRT-1049 Agile Program & Project Management – agile processes as applied to systems and hardware intensive programs, agile training

WRT-1049 Additive Manufacturing & DE Strategy – DE supply chain strategy, analytic capabilities for acquisition program strategies

WRT-1049 Developing Capability Requirements – improving the timeliness and agility of capability requirements across acquisition pathways

WRT-1043 DAU Simulation – embedding MBSE/M&S competencies, simulations into DAU courseware\

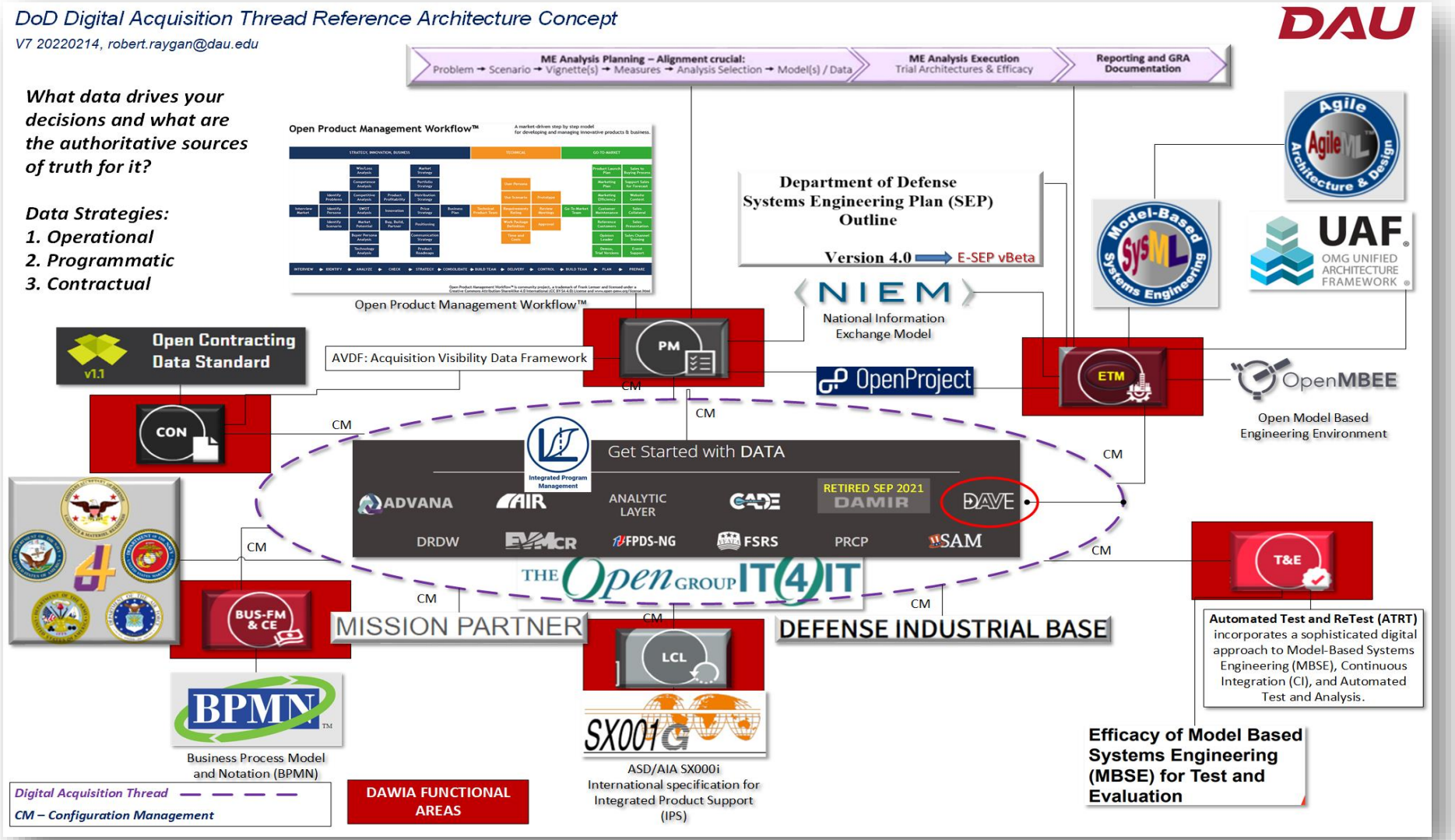
WRT-1058: Program Managers Guide To Digital And Agile Systems Engineering Process Transformation

WRT-1058 Systems Engineering Modernization Policy, Practice, And Workforce Roadmaps

A Framework to Guide Decisions for Program Managers and PEOs

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Digital Acquisition Thread (DAU Led)



Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

“Exemplar Digital Acquisition Thread” Challenges and Results

Mission and Purpose	Desired Results	Stakeholders / Sponsors / Collaborators
Why “Exemplar Digital Acquisition Thread” project? SE Modernization pain points: A. Digital Processes and Products (Digital Acquisition / E-Programs) B. Enterprise Systems Engineering approach integrating: 1. Five key areas: DE/MOSA/SWE/CID/ME 2. Collaboration and Data Sharing challenges between Government and Industry 3. Digital Tools / Methods 4. Role of Reference Architecture **Desired Result:** A Digital Acquisition Thread Reference Architecture and Examples with Digital Artifacts for each RA Element.	**GOALS:** A. Create a government reference architecture for a cross-continuum digital acquisition thread. **B. Collect exemplar reference architecture elements from mission partners, industry, and academia.** C. Share exemplar acquisition thread with the community for education, training, and re-use. **D. E-SEP: native digital systems engineering plan model with mission critical interfaces for data sharing** **SUCCESS STATEMENT:** A. Deliver a digital acquisition thread reference architecture hosed on DoD web site and incorporated into training materials and workshops for the community. B. Reference architecture element models, formats, interfaces, etc. are collected and hosted on appropriate sources of truth.	**Customer:** OUSD R&E, Nadine Geier **Who Benefits?** DoD Acquisition Teams, ASD(A), DoD CIO **Team:** OUSD R&E, SERC, DAU, NDIA SED Committees, Mission Partners, and other DoD Agencies.

Measures of Success	Accomplishments
1. **SERC SEMOD workshops established survey questions and guidance for broader audience offering and feedback** 2. DoD ASoT owners are identified with interface APIs cataloged. (NDAA21 Tasker 804.c.) 3. Digital Acquisition Thread Pilot with exemplar mission partners. 4. NDIA Project Team & OUSD R&E iteratively develops Digital Acquisition Thread Reference Architecture 5. NDIA delivers a digital acquisition thread reference architecture 6. Collected exemplar digital artifacts are hosted by DoD for education, training, and re-use. 7. 25th Annual Systems and Mission Engineering Conference (ndia.org) **Panel Discussion: Systems Engineering Modernization (SEMod) Key Enablers for System Development on DoD Programs”** on lessons learned and next steps for continuous improvement (11/3 1100-1200 Eastern)	1. **DAU** Systems Engineering Modernization (SEMod) - Defense Acquisition University (dau.edu) **Series added to DAU Events for webcasts and training reuse.** 2. **DAU SEMod Key Enabler Workshops:** WSE 028 Mission Engineering (ME) Awareness and Planning (dau.edu) and WSE 027 Modular Open Systems Approach (MOSA) Awareness and Planning Workshop (dau.edu) created in response to mission partner requests. CM workshop in development 3. Exemplar Mission Partners: AFSOC MAC, MCSC, AFC DE Cop, NAWCAD, PEO-IEWS, PEO-EIS, PEO-AVN, NAVWAR, ASA (ALT), ASN (RDA), DISA, … 4. Big challenge for DoD, work around for training provided by NPS sharing their GitLab for “DoD Reuse and Sharing Training Program Artifacts” 5. What needs work? DoD public sharing policy and process. (Update for digital artifacts) 6. OMG UAF Working Group – Model Based Acquisition - RFP and Response plus 7. NPS GitLab: To be shared – Skyzer, Silverfish, CUI WOSA.mdzip, MITRE 5000 model, DAU Bulldog 8. What needs work? NDAA21 tasker: Were interface models considered rather than “documents?

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

DAU

Deeper Learning

- Defense Acquisition University
- Tools Catalog
- SE Brainbook
- **Configuration Management**

LOG 2040 Configuration Management

MIL-HDBK-61 07APR2020

MODULAR OPEN SYSTEMS APPROACH

DEFENSE STANDARDIZATION PROGRAM
MAKING SYSTEMS WORK TOGETHER

CLE 019 Modular Open Systems Approach

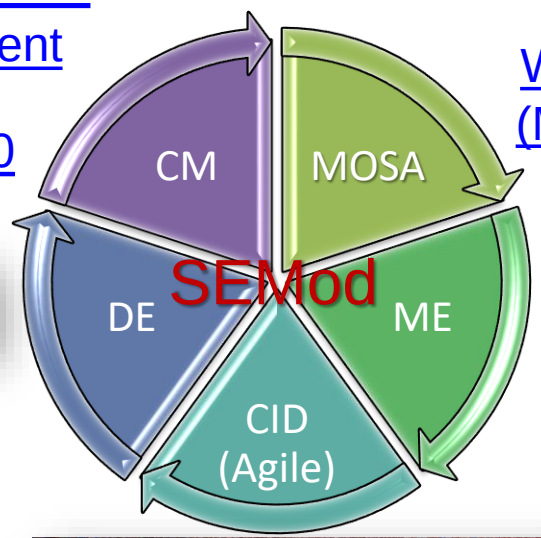
WSE 027 Modular Open Systems Approach (MOSA) Awareness and Planning Workshop

DIGITAL ENGINEERING

CLE 084 Models, Simulations, and Digital Engineering

ETM 1070 Digital Literacy Fundamentals

ETM 2070V Digital Literacy for Practitioners



DAU Agile, Cloud, Cyber and DevSecOps courses and workshops

Digital Engineering (DE) Measurement Framework

Continuous Iterative Development (*Agile*) Measurement Framework

SYSTEMS ENGINEERING MODERNIZATION
June 21, 2022

MISSION ENGINEERING

ETM 1020 Mission and Systems Thinking Fundamentals

ETM 2020V Mission and Systems Thinking for Practitioners

WSE 028 Mission Engineering (ME) Awareness and Planning (dau.edu)

Systems Engineering Modernization Workbook | Rise 360 (articulate.com)

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

DAU Events SEMod Series

Systems Engineering Modernization (SEMod) - Join this series to learn about the key enablers to modernize Systems Engineering including digital engineering, mission engineering, modular open systems approach, continuous iterative development, modern software and development methods (Agile, DevSecOps, Scrum, SAFe), and lead systems integrator. Series format is delivered live with attendee questions & answers and discussion from participants and recorded for future use.

- Established April 2022 for first SEMod key enabler, "SCRUM Implementation for Army Lessons Learned," *Linda O. Jones*, Ph.D. PM Defensive Cyber Operations (DCO) Cyber Analytics and Detection (CAD) Deputy Product Manager, CAD
- Second in series, "Government Lead Systems Integrator Benefits and Fundamentals," *Gerald Swift*, Director, AIRWorks, Naval Air Warfare Center Aircraft Division, *Christa Rodewald-Franz*, Deputy Director, AIRWorks, Naval Air Warfare Center Aircraft Division, and *Scott Hoffman*, Chief Engineer, AIRWorks, Naval Air Warfare Center Aircraft Division
- September 29th (1300-1430 Eastern) next in series, "organic Lead Systems Integrator (oLSI)," *David Hager*, Technical Director, Naval Air Warfare Center Aircraft Division Webster Outlying Field, and *Israel Jordan*, Technical Initiatives & Strategy Director, Naval Air Warfare Center Aircraft Division Webster Outlying Field https://www.dau.edu/event/organic_Lead_Systems_Integrator
- Planning: NAVWAR CM Guidance, PEO-IEWS MOSA Guidance, MCSC ME Guidance, Boeing Global Sales BD/Navy-Gov Ops, MITRE
- Contact Robert.Raygan@dau.edu to become a part of the series.
- Systems Engineering Modernization Workbook | Rise 360 (articulate.com)
  - WSE027 Modular Open Systems Approach (MOSA) Workbook | Rise 360 (articulate.com)
  - WSE 028 Mission Engineering (ME) Workbook - Overview | Rise 360 (articulate.com)
  - DAU Agile, Cloud, Cyber and DevSecOps courses and workshops - Overview | Rise 360 (articulate.com)

Distribution Statement A. Approved for public release. Distribution is unlimited. Case # 22-S-3012

Eight Components of Autonomous, Self-Healing System

Matt Kehret
Digital Technologies Chief Technology Officer
Director of Architecture and Emerging Technology

August 2022

Raytheon Missiles & Defense

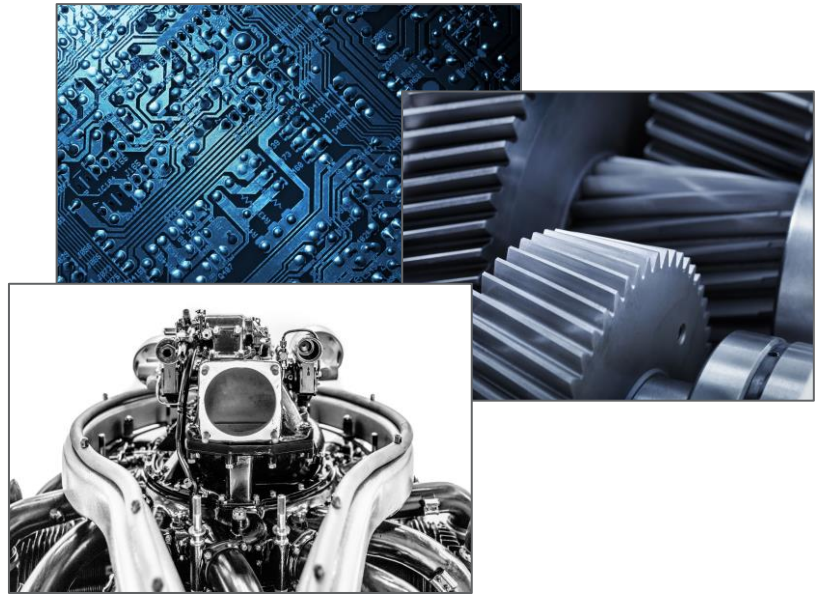
© 2022 Raytheon Technologies Corporation.
All rights reserved.

Raytheon Approved for Public Release
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.

Self-Healing Systems

- An autonomous, self-healing system can 1) detect when it is not performing as designed and 2) adjust its behavior to continue to deliver its intended value.

- Why create autonomous, self-healing systems?
  - Increase reliability and survivability; Proactive
  - Systems growing more complex
  - Failures happen
  - Required technology exists today



The pump is primed to deliver self-healing systems!

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

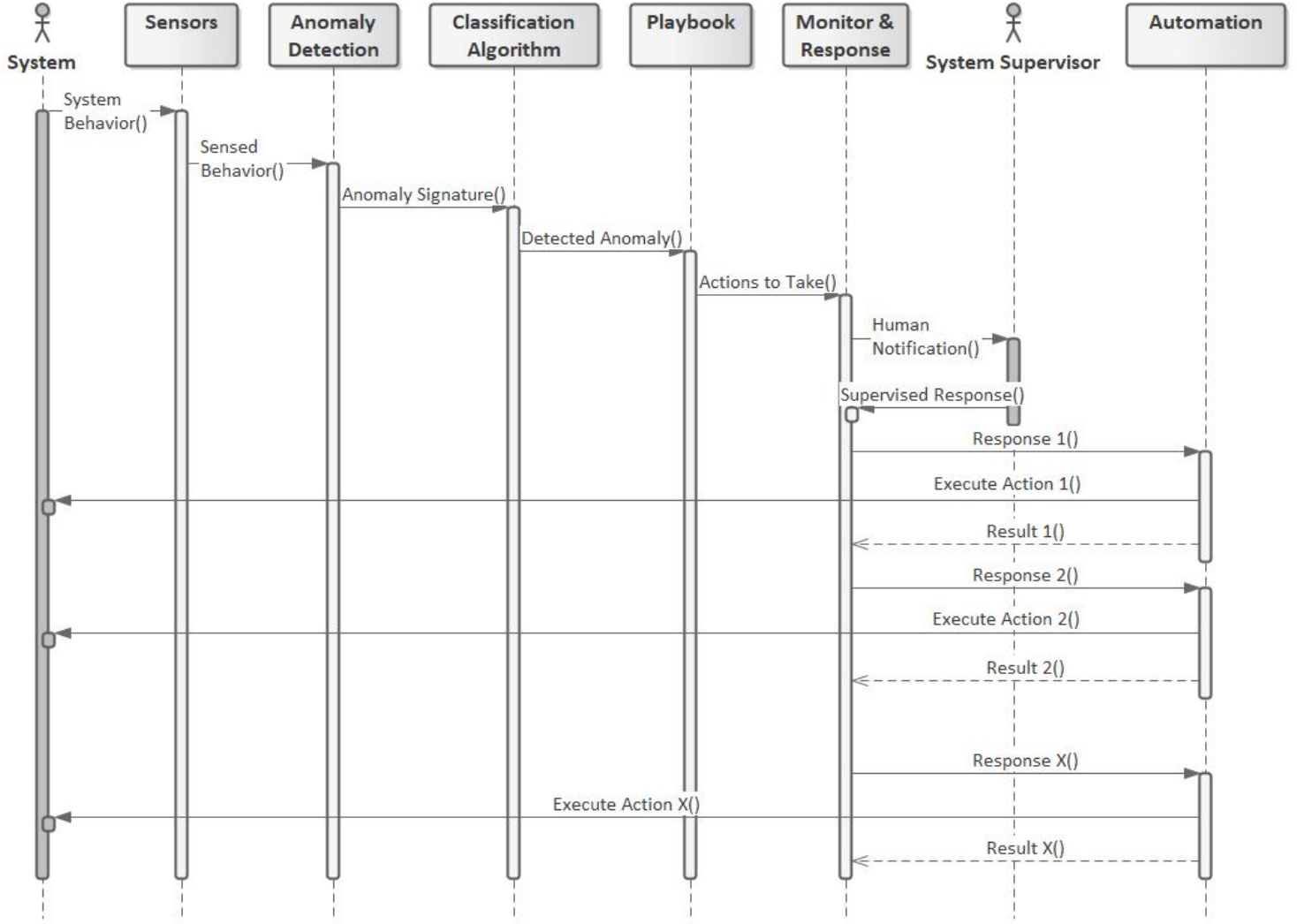
Companies with Self-Healing Systems

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Components of an Autonomous, Self-Healing System

1. Sensors
2. Anomaly Detection
3. Classification Algorithms
4. Playbooks
5. Monitoring & Response
6. Automation
7. Engineered Chaos
8. Logging & Reporting



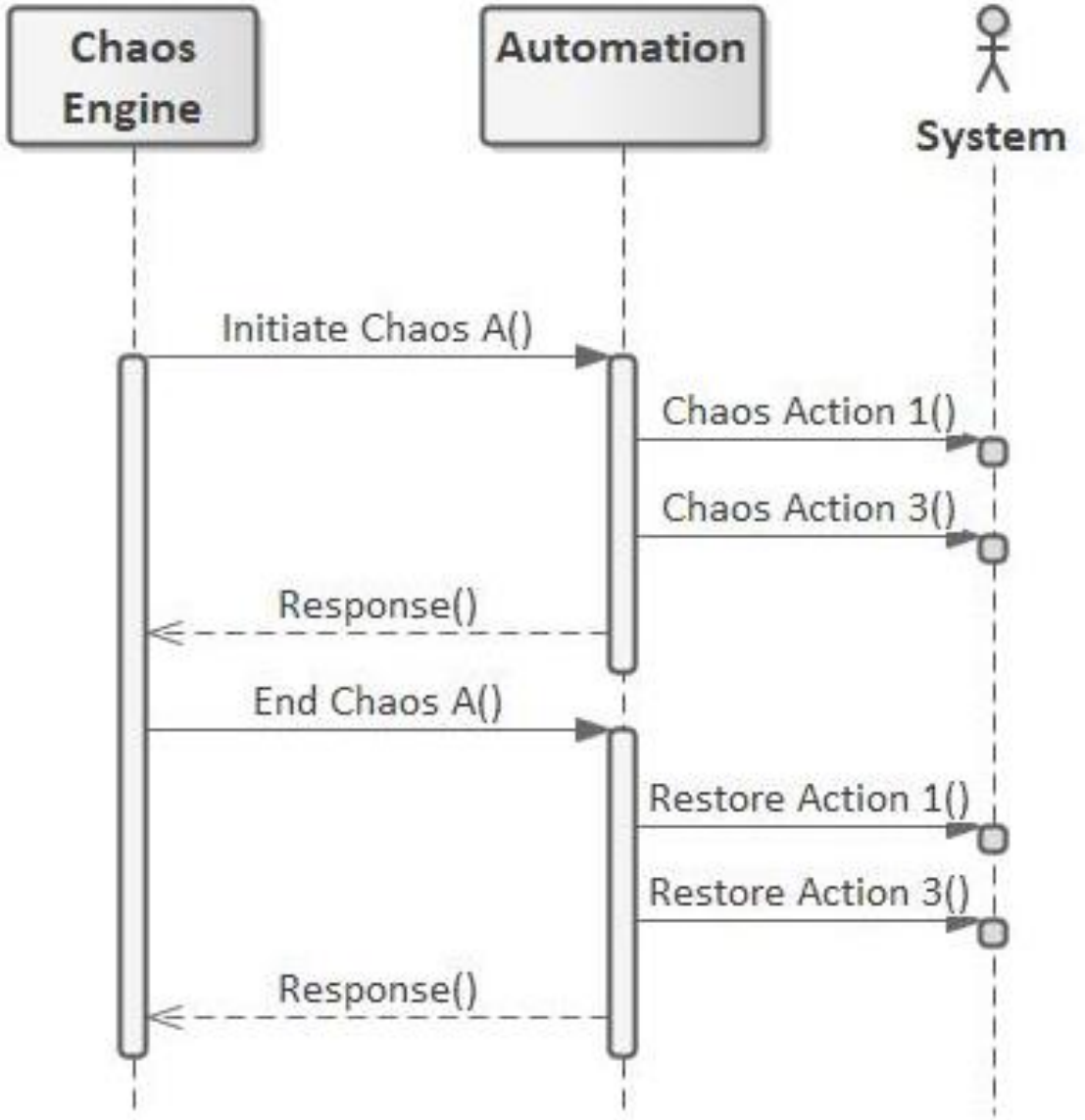
Known Technologies and Processes Exist to Create Each Component

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Engineered Chaos

1. Sensors
2. Anomaly Detection
3. Classification Algorithms
4. Playbooks
5. Monitoring & Response
6. Automation
7. **Engineered Chaos**
8. Logging & Reporting

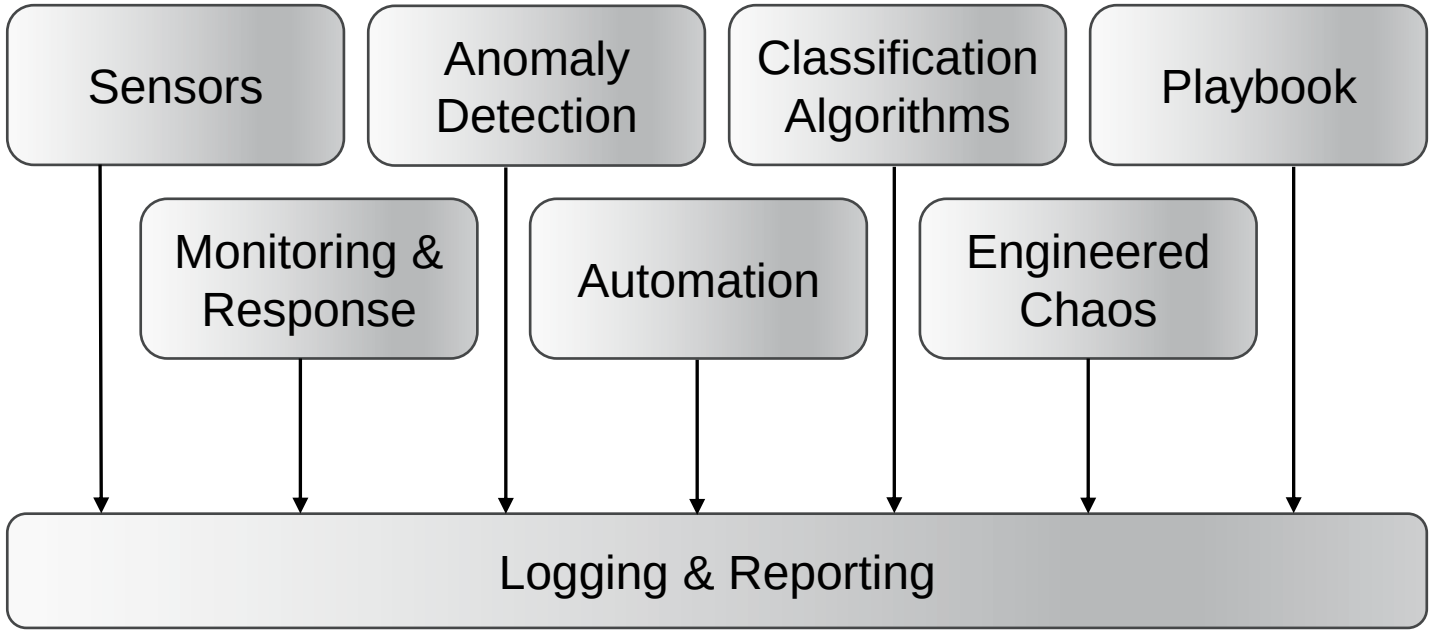


Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Transparent Decisions and Actions

1. Sensors
2. Anomaly Detection
3. Classification Algorithms
4. Playbooks
5. Monitoring & Response
6. Automation
7. Engineered Chaos
8. Logging and Reporting



Raytheon Missiles & Defense
Raytheon Approved for Public Release
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.

BONUS: Collaborative Communication

1. Sensors
2. Anomaly Detection
3. Classification Algorithms
4. Playbooks
5. Monitoring & Response
6. Automation
7. Engineered Chaos
8. Logging and Reporting

- Share environment and failures across system of systems
  - Swarm peers may be about to experience similar conditions
  - System of system peers may experience environment in different ways
  - Collaboration will help system to adapt and respond

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Conclusion & Questions

- Logical Architectural Framework for building autonomous systems
- 8 key elements

1. Sensors
2. Anomaly Detection
3. Classification Algorithms
4. Playbooks
5. Monitoring & Response
6. Automation
7. Engineered Chaos
8. Logging & Reporting

- Questions?

We can make our products and systems more intelligent and autonomous today!

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 1: Sensors

- Purpose
  - Capture data regarding the current behavior of the system.
- Technology
  - Digital, mechanical, hydraulic, etc devices capture system data
- Challenges
  - Anticipating reasonable failure points to detect
  - Balancing costs, both financial and computational, to capture system data

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 2: Anomaly Detection

- Purpose
  - Process data captured by the sensors to determine if the system is operating within design tolerances. When system is outside of expected tolerances, send pertinent data to classification algorithms.
- Technology
  - Machine Learning algorithms are a prime way to detect anomalous behavior
- Challenges
  - Developing/training effective algorithms
  - Allocating sufficient processor cycles to perform calculations
- Examples
  - Unsupervised Machine Learning Algorithms
  - Statistical Approach

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 3: Classification Algorithms

- Purpose
  - Process anomalous data provided by the anomaly detection algorithm and determine or classify the environmental challenge and/or failure. Pass the classification and pertinent data to the Playbook.
- Technology
  - Logistic Regression, Naïve Bayes, Decision Tree, Stochastic Gradient Decent, etc
- Challenges
  - Developing/training effective algorithms with proper detail
  - Allocating sufficient processor cycles to perform calculations
- Example Implementation
  - Yelp uses classification algorithms to compile, categorize, and label images

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 4: Playbook

- Purpose
  - Take the identified failure condition and associated data and use it to determine the best course of action to respond.
- Technology
  - Lookup table, decision tree, machine learning algorithm
- Challenges
  - Anticipating failure states and determining best action for response
  - Developing sufficient data to train algorithms
  - Selecting appropriate responses to take given failure condition

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 5: Monitoring and Response

- Purpose
  - When applicable, communicates with human in the loop to show diagnosed state and proposed response
  - Launches series of automated activities to carry out the desired actions to improve system performance in current environment. Monitors automation.
  - Tracks current health of system, performs system health assessments
  - Provides failure notification to system owners
- Technology
  - Software system and database
- Challenges
  - Effective interaction with human partner
  - Handling automation failures

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 6: Automation

- Purpose
  - Enable the change of system behavior in response to anomalous behavior
- Technology
  - Alternative software, hardware, switches, etc
- Challenges
  - Anticipating useful automation
  - Avoiding over automation
  - Designing robust, redundant automation that works while parts of the system are failing
- Example Vendors
  - Chef, Puppet, Ansible

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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.

Component 7: Engineered Chaos

- Purpose
  - Intentionally introduces failures into production and development system. Encourages architects, designers, and builders to create autonomous systems. Enables the generation of data that represents failures.
- Technology
  - Software and hardware
- Challenges
  - Scoping the effort to include reasonable system failures
- Example Implementation
  - Netflix Chaos Monkey

Raytheon Missiles & Defense

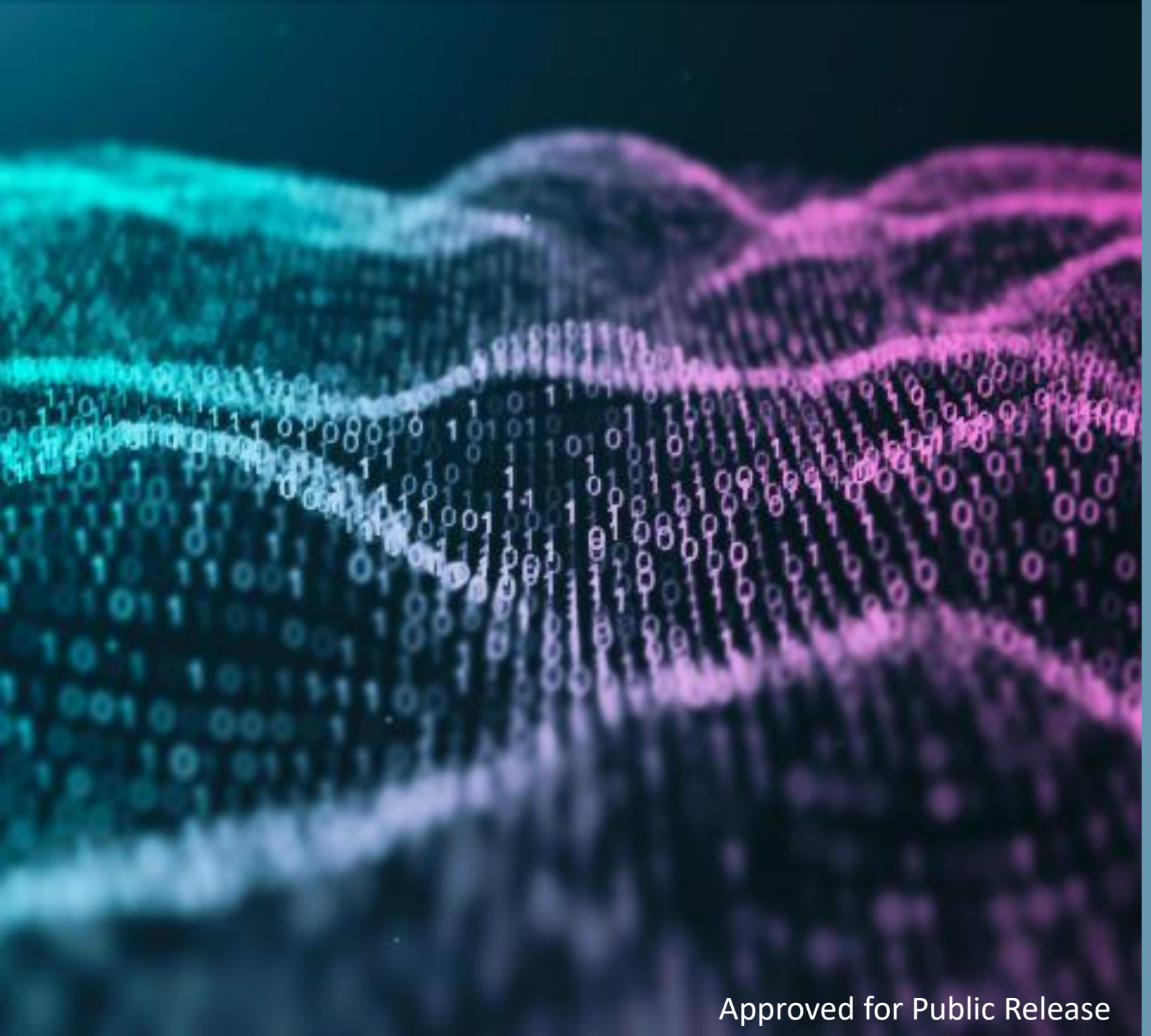
Raytheon Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Component 8: Logging & Reporting

- Purpose
  - Record all events taking place in the system to enable future analysis. Enables transparent system behavior and increases the understanding of the decisions made by the autonomous system. Provide the ability to report on the logged data in a way that users to connect events from the system components.
- Technology
  - Files, databases, software
- Challenges
  - Minimizing storage and processing requirements
  - Anticipating value added reporting needs
  - Capturing data from fielded systems
- Example Vendor
  - Splunk

Raytheon Missiles & Defense

Raytheon Approved for Public Release
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 and Complexity

DAVE CHESEBROUGH

Approved for Public Release

Agenda

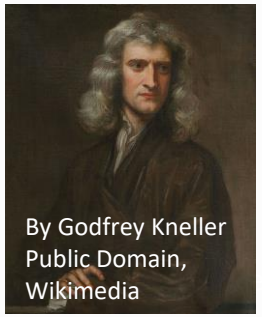
- Complexity Theory – Background and Applications
- Mission Engineering Context
- Relationship to Systems Engineering
- A Look Ahead
- Conclusion

Complexity Sciences

Driven by computational science

Branched into five distinct lines of research

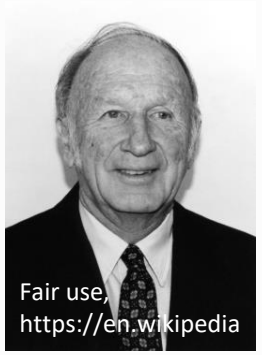
17th Century **Science of Dynamics**



Isaac Newton

Ability to predict motion based on Newtonian mechanics

20th Century **Chaos**



Edward Lorenz, MIT

Computer Weather Modeling

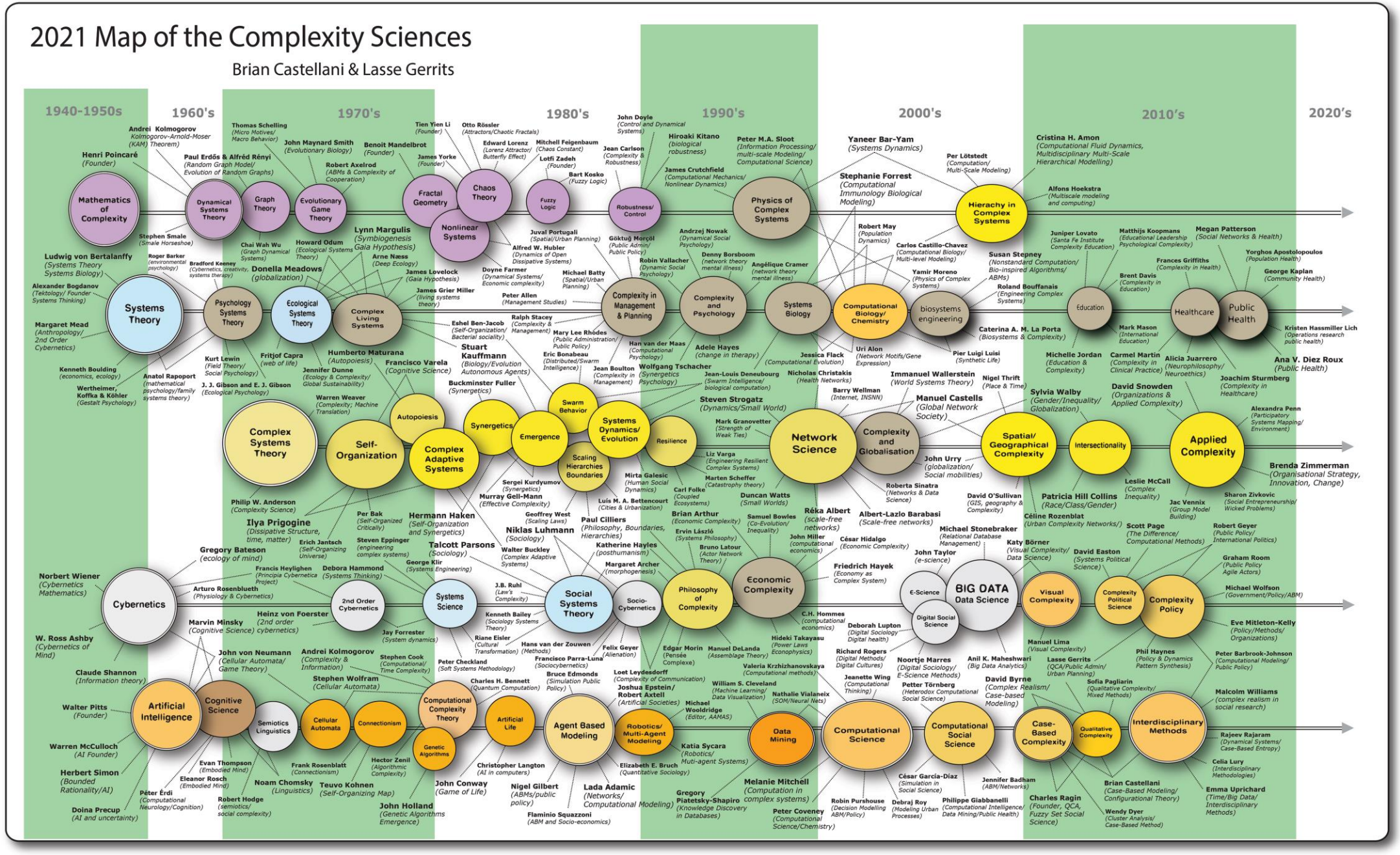
- deterministic nonlinear systems
- Butterfly effect
- deterministic nature of these systems does not make them predictable

Complexity

Theoretical Computer Science and Information Theory

- Nonlinear
- Emergent, non-predictable behavior
- Transitions between order and disorder

Chaos and Complexity both feature non-linearity



Castellani, B. (2018) Map of the Complexity Sciences. Art & Science Factory. https://www.art-sciencefactory.com/complexity-map_feb09.html

Complicated Systems

- Engineered and Deterministic
- Many interacting components
- Dependencies
- Predictable, known, planned and linear behavior

THESE

must function within

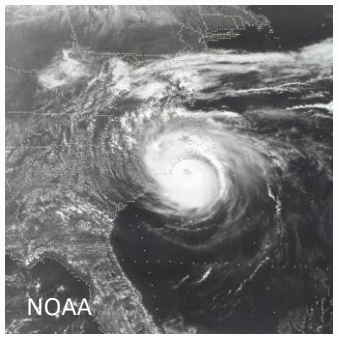
Complex Systems

- Unordered and Stochastic
- Many interacting components
- Dependencies, competitions, relationships
- Exhibit nonlinearity, emergence, self-organization, adaptation

THESE

Photo by Ralph Chang

Photo by Michał Ludwiczak



NOAA

Systems Thinking

Focus on structure, relationships, interdependence

Thinking systematically about the properties of the whole being different from the parts

Define the end-state and work to fill the gaps

Complexity Theory

- the study of complex dynamic, non-linear, self-organizing, open, emergent, sometimes chaotic and adaptive systems (Larsen-Freeman, 1997)
- There are limits to what can be anticipated given current knowledge
- We don't know what we don't know (COVID-19 results if chip shortage)

The search for simple – if not simpleminded – solutions to complex problems is a consequence of the inability to deal with complexity

- Russell L. Ackoff, Wharton School

“There are known knowns — there are things we know we know. We also know there are known unknowns — that is to say, we know there are some things we do not know. But there are also unknown unknowns, the ones we don’t know we don’t know.”

- Donald Rumsfled, Secretary of Defense, February 2002

“The absence of evidence is not evidence of absence”

Complexity Theory – Current

Santa Fe Institute

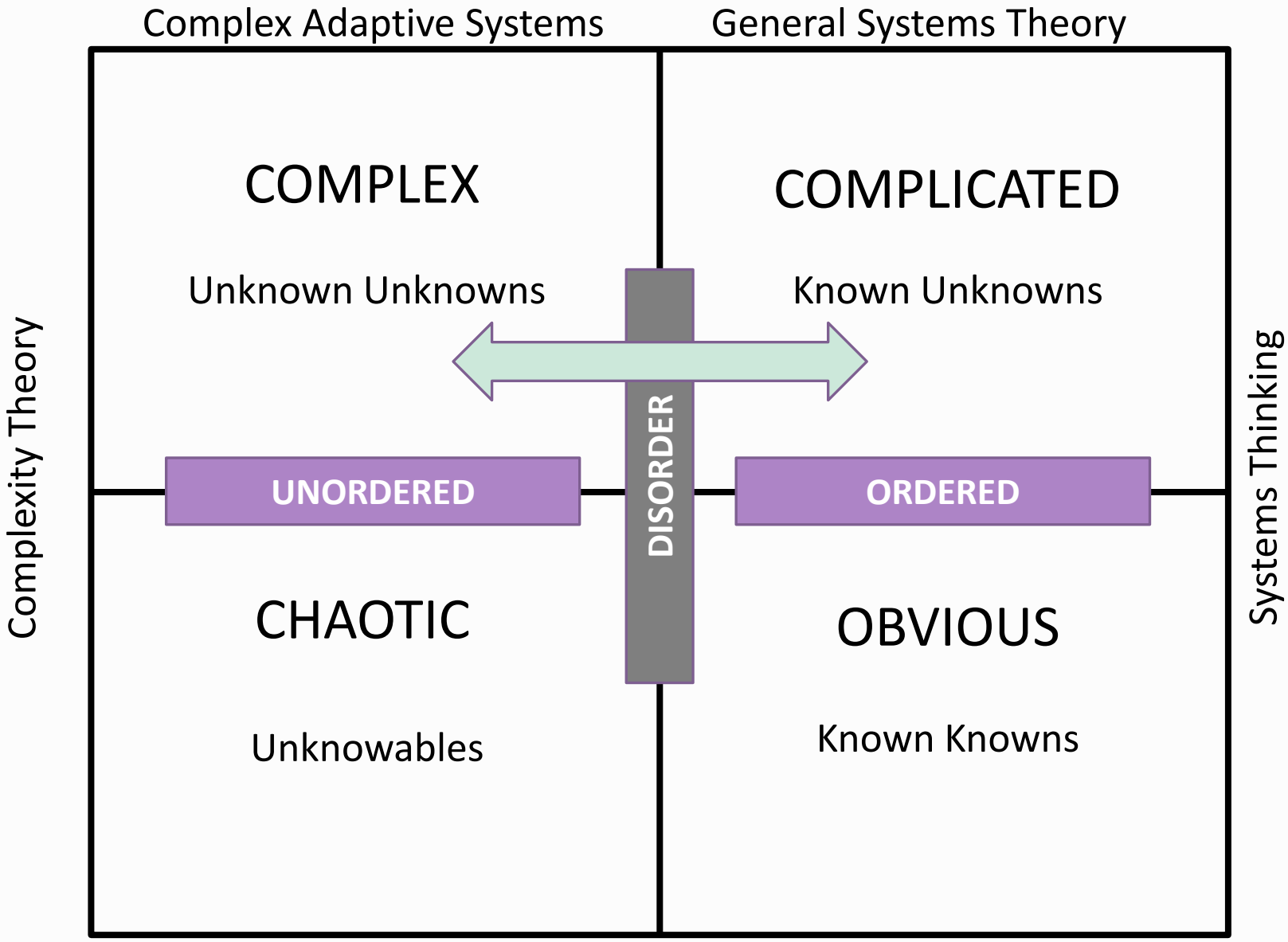
- Founded 1984
- First research institute dedicated to the study of complex adaptive systems
- Focus on complex physical, biological, social, cultural, technological areas

Cynefin Framework

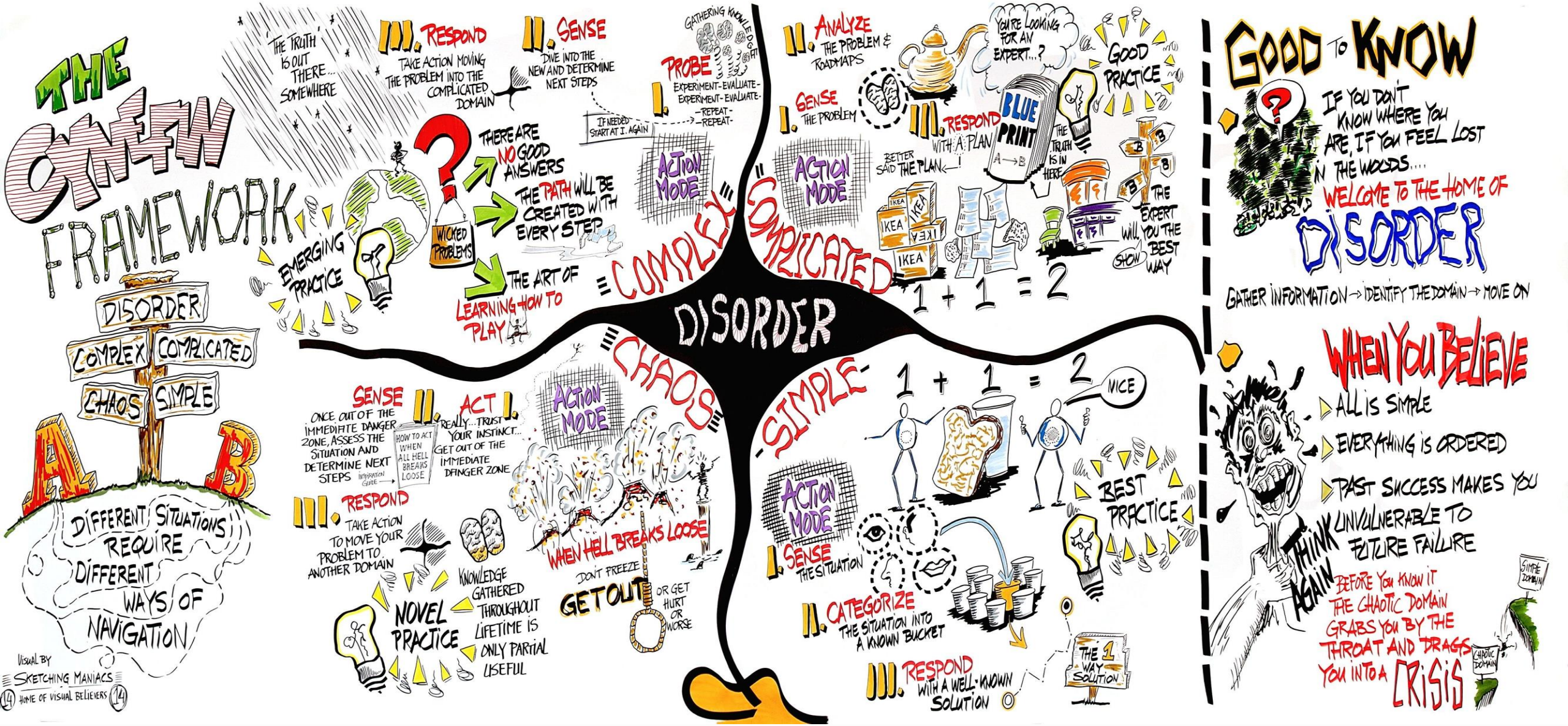
- Developed in 1999 by Dave Snowden, IBM Global Services
- Draws on research into systems theory, complexity theory, network theory and learning theories
- Conceptual framework to aid in decision-making

Cynefin Framework

- Started in Knowledge Management
- Framework for contextualization
- Used to frame multiple perspectives around a specific event
- Scenario planning and wargaming



Kurtz and Snowden, IBM, **2003**



By Edwin Stoop (User:Marillion!!62) - [1], CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=53810658

Mission

a duty assigned to an individual or unit

Mission Integration Management

the synchronization, management, and coordination of concepts, activities, technologies, requirements, programs, and budget plans to guide key decisions focused on the end-to-end mission.

MISSION ENGINEERING CONSUMERS

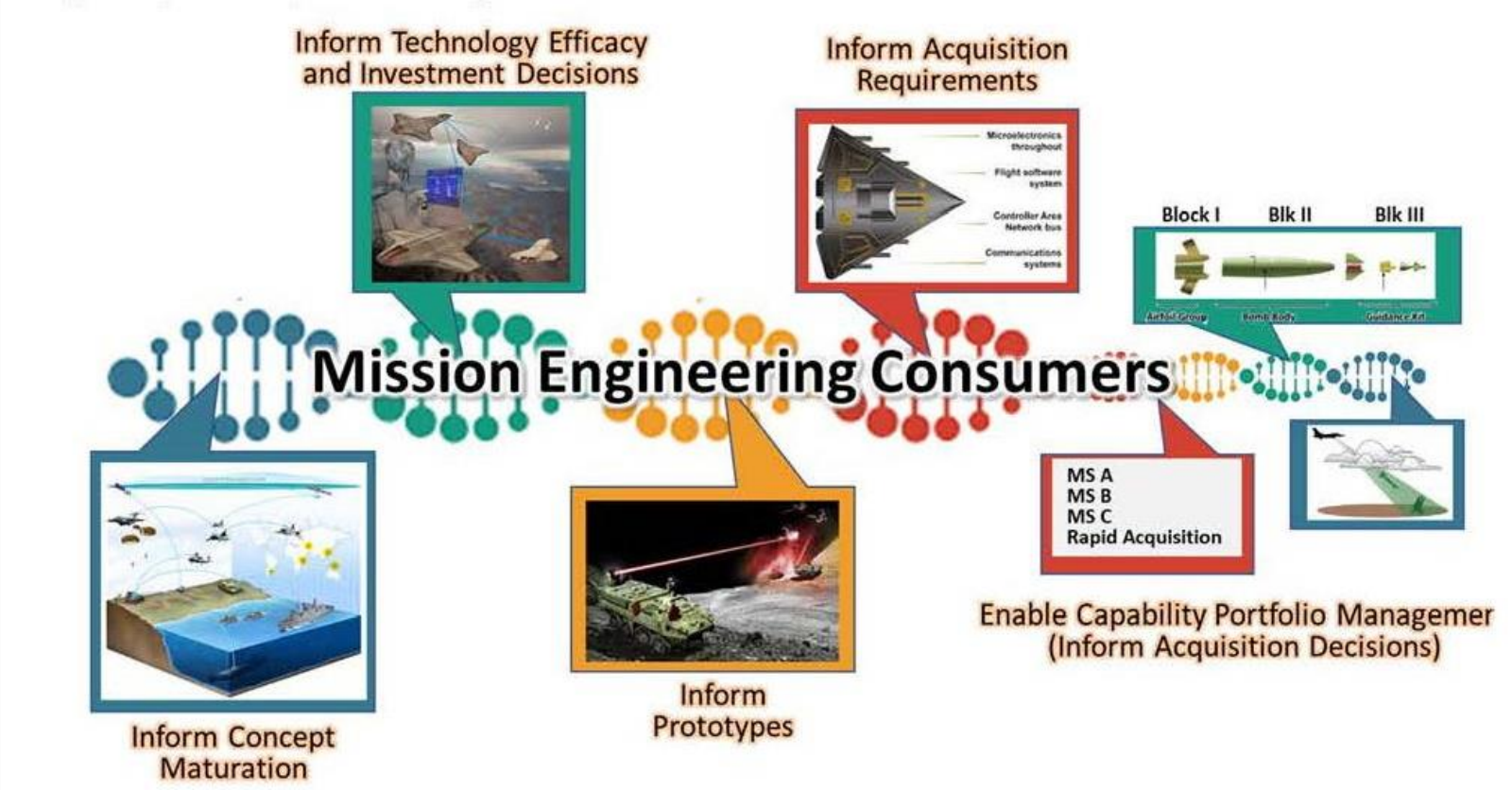


Figure 1-1. Consumers of Mission Engineering Outputs

Mission Engineering

the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects

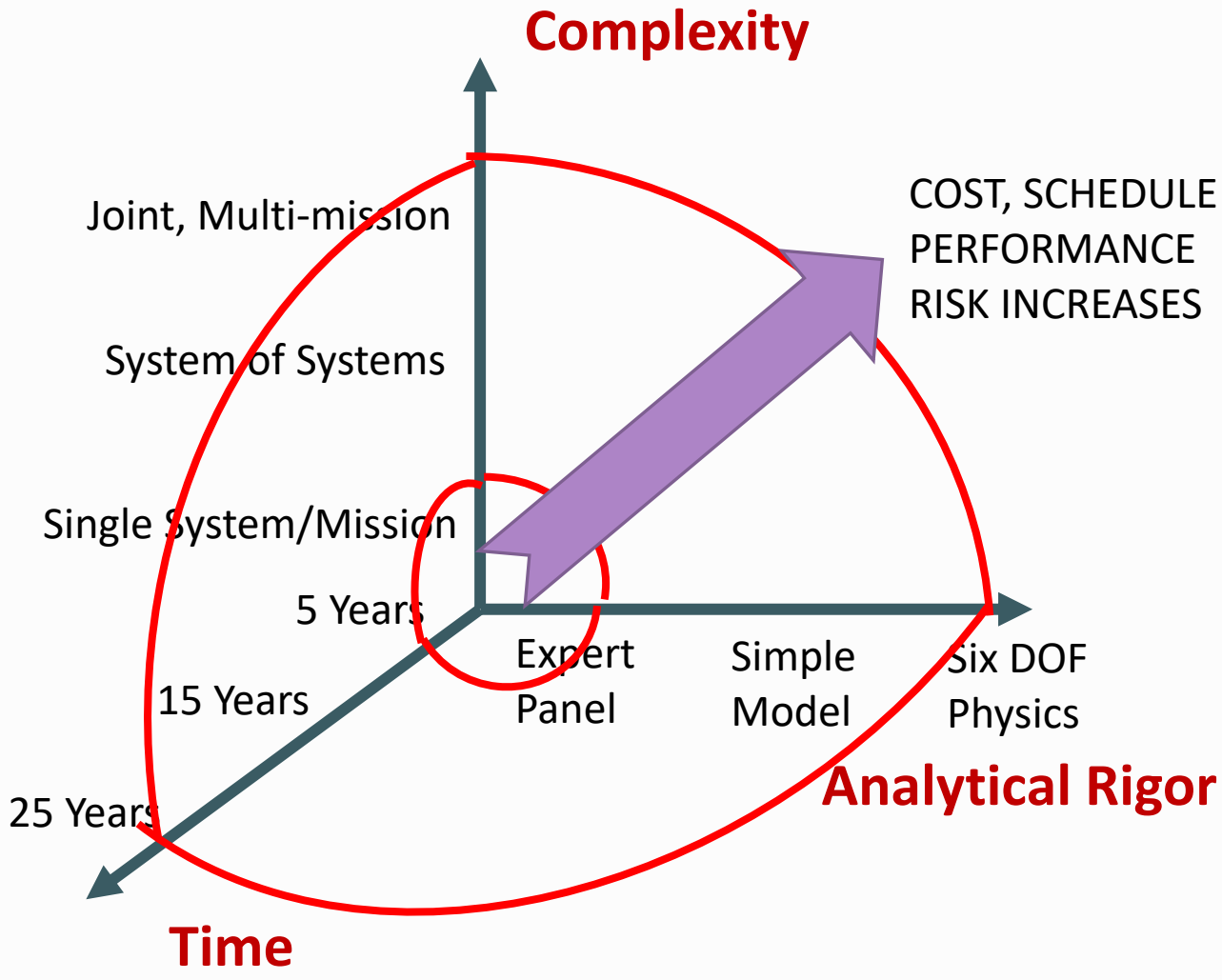
The right thing, at the right place, at the right time

Mission Engineering Balance

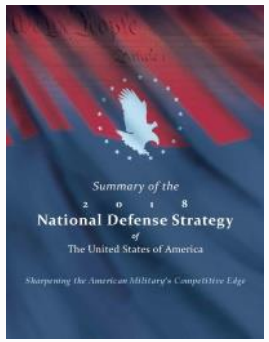
Overreach on any axis will impact

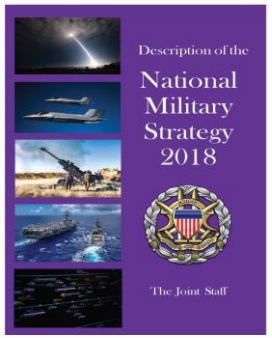
- Confidence in ME products
- Validity of analysis
- Availability of data

Three Axes of Mission Engineering

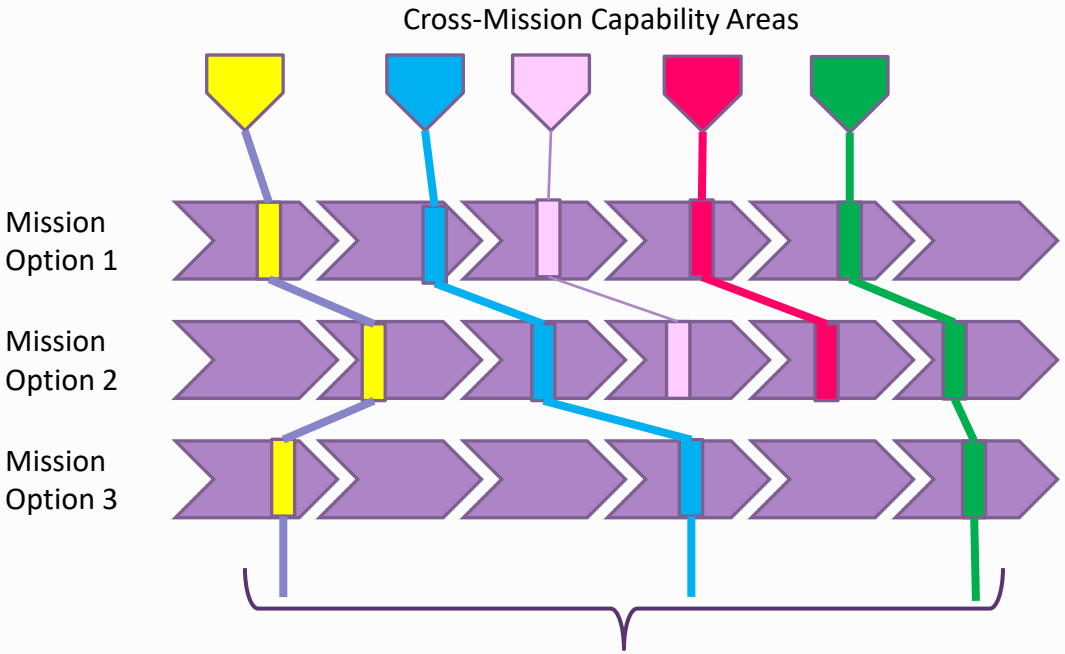


Strategy & Guidance





Mission Engineering Analysis



Mission Reference Architectures

Capability Reference Architectures

Investment Decisions and Programmatic Guidance

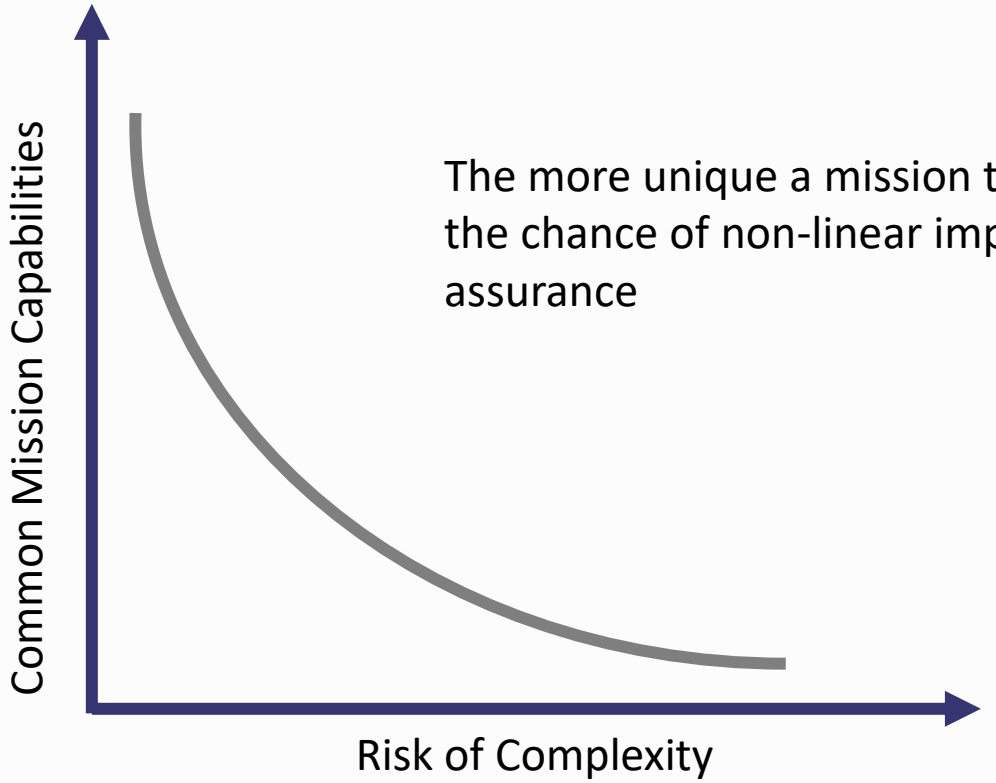
Trade studies between mission effectiveness and common capabilities

The Non-linearity Effect

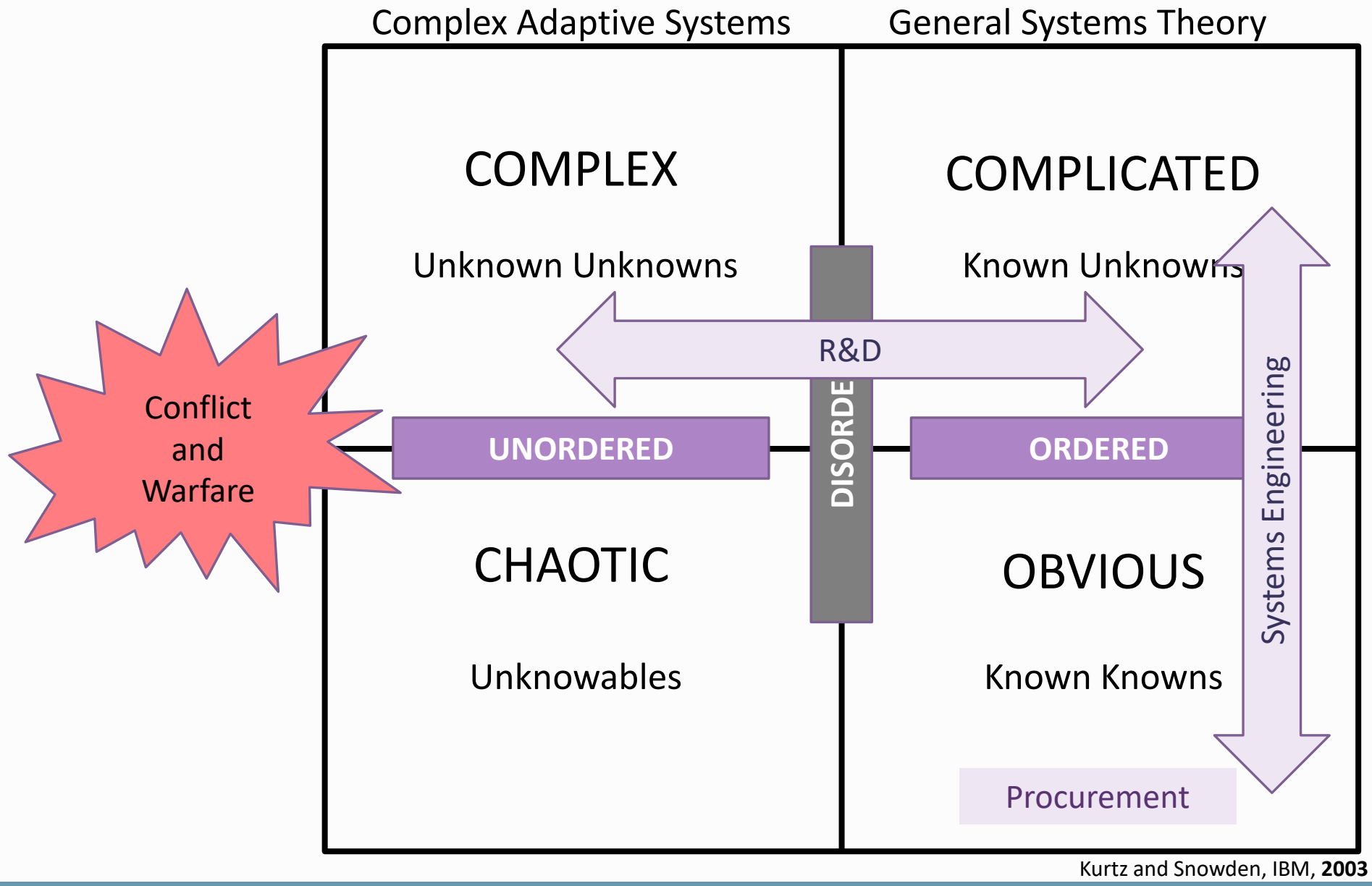
For want of a nail the shoe was lost. For want of a shoe the horse was lost. For want of a horse the rider was lost. For want of a rider the battle was lost. For want of a battle the kingdom was lost.

- A Proverb

- Something minor has a disproportionate effect on outcomes
- Complexity increases the possibility of having non-linear interdependencies
- Standardization of capabilities across missions provides a measure of assurance



The more unique a mission thread is the greater the chance of non-linear impacts on mission assurance



Kurtz and Snowden, IBM, **2003**

What Do We Know?

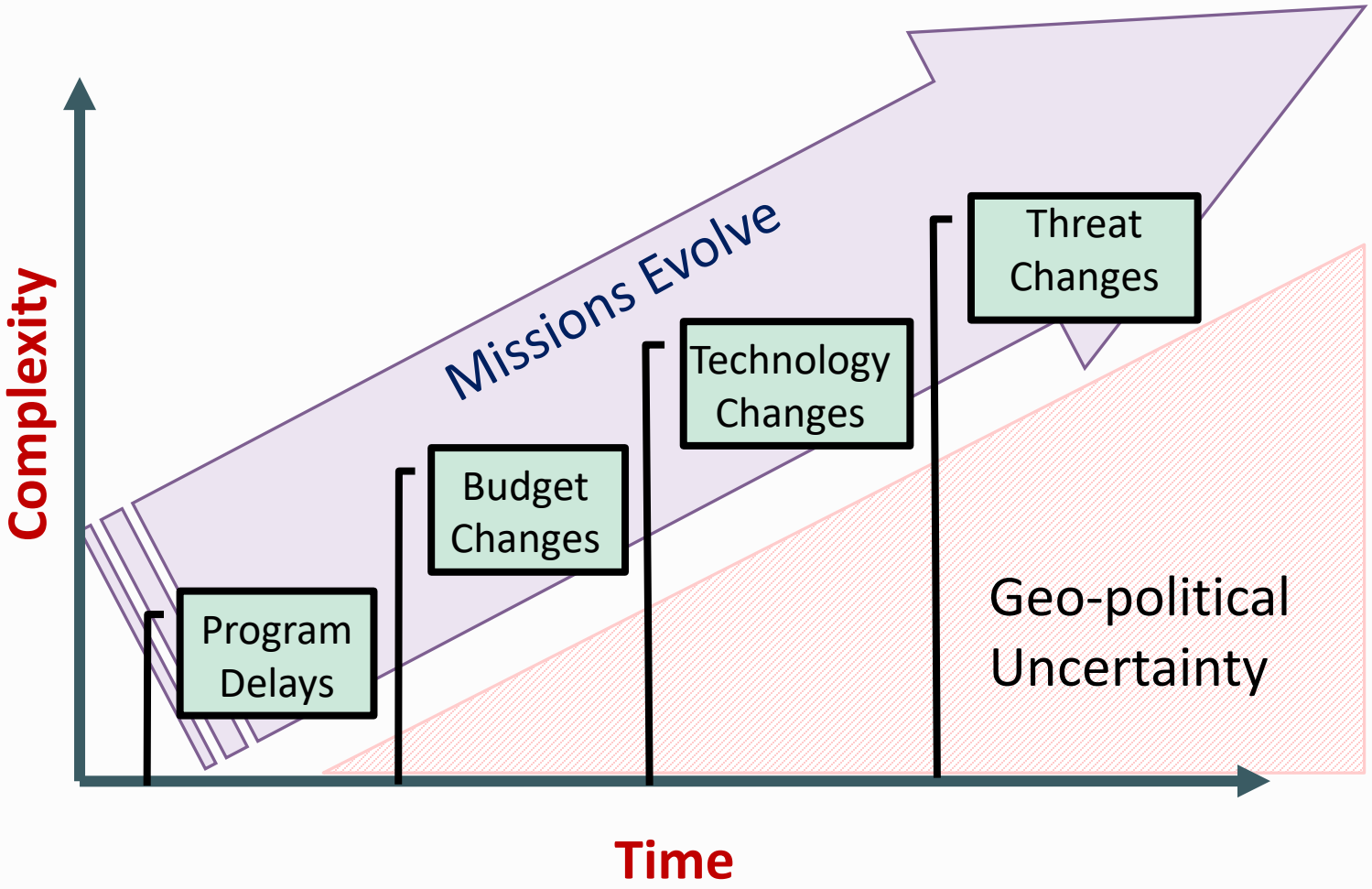
Change is constant and unpredictable

Systems must adapt

Real-world complexity always creeps in

Present imperative is to move faster, innovate quicker

Three Axes of Mission Engineering



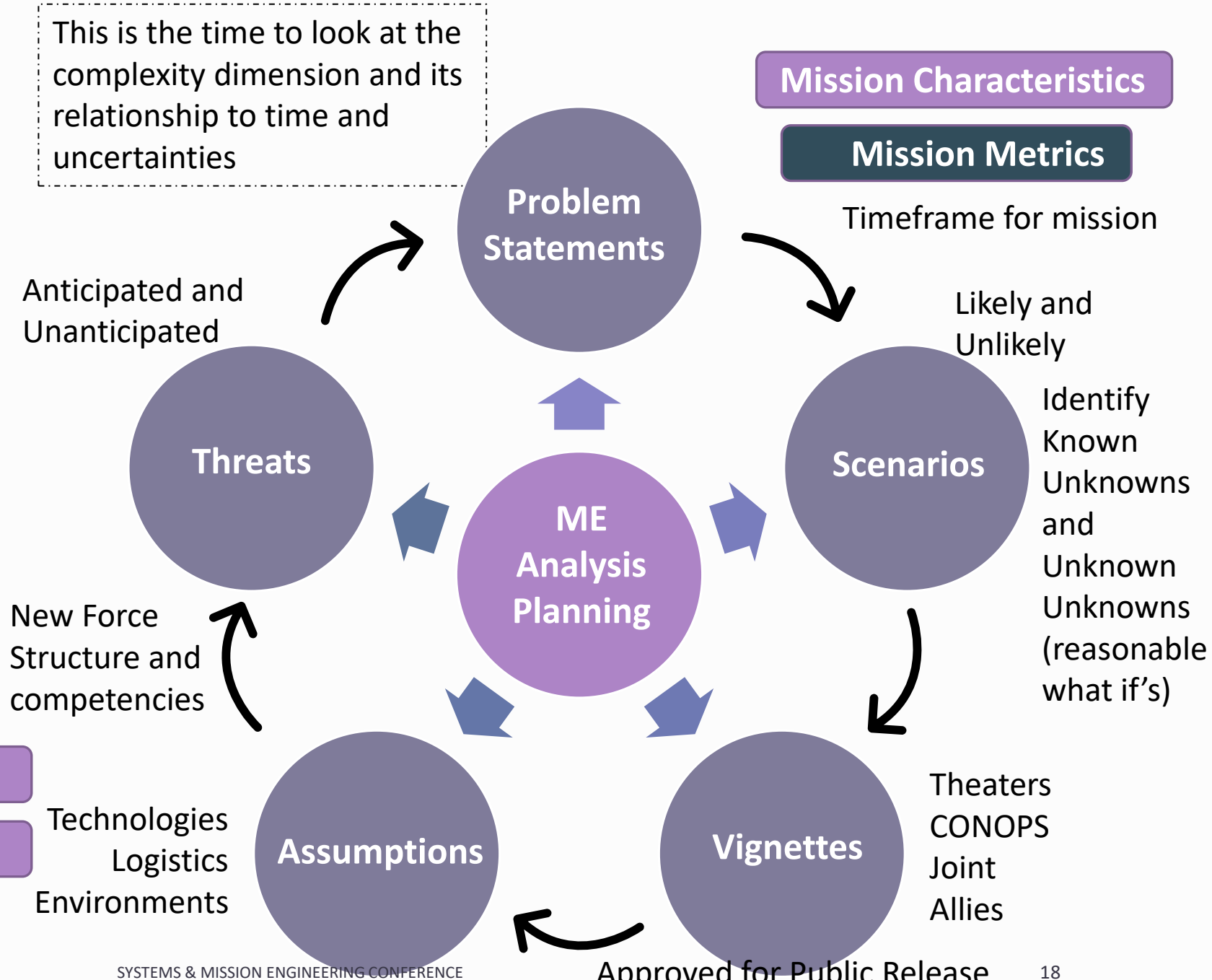
How does ME Deal with Complexity

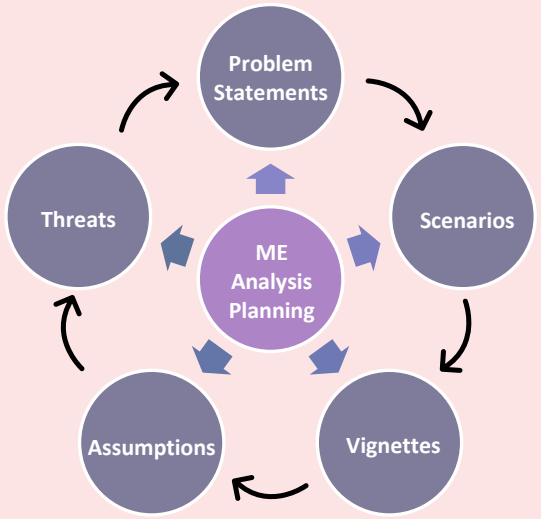
By addressing questions that impact mission architectures while planning the analysis

- What are we trying to do?
- Who should be doing it?
- What is the context?
- What is the timeframe?

Relationships

Dependencies



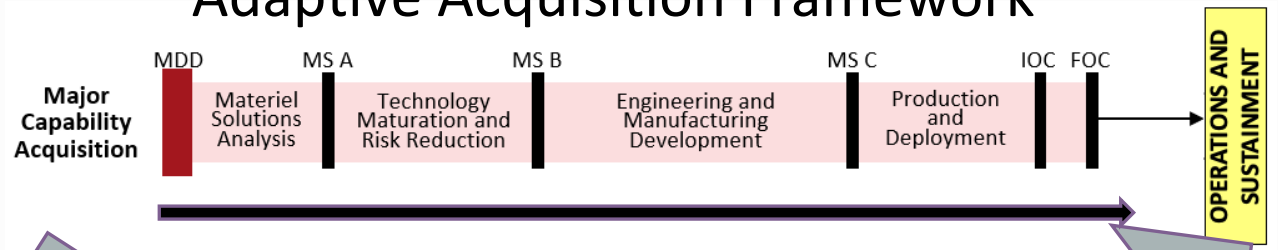


GMRA/GCRA

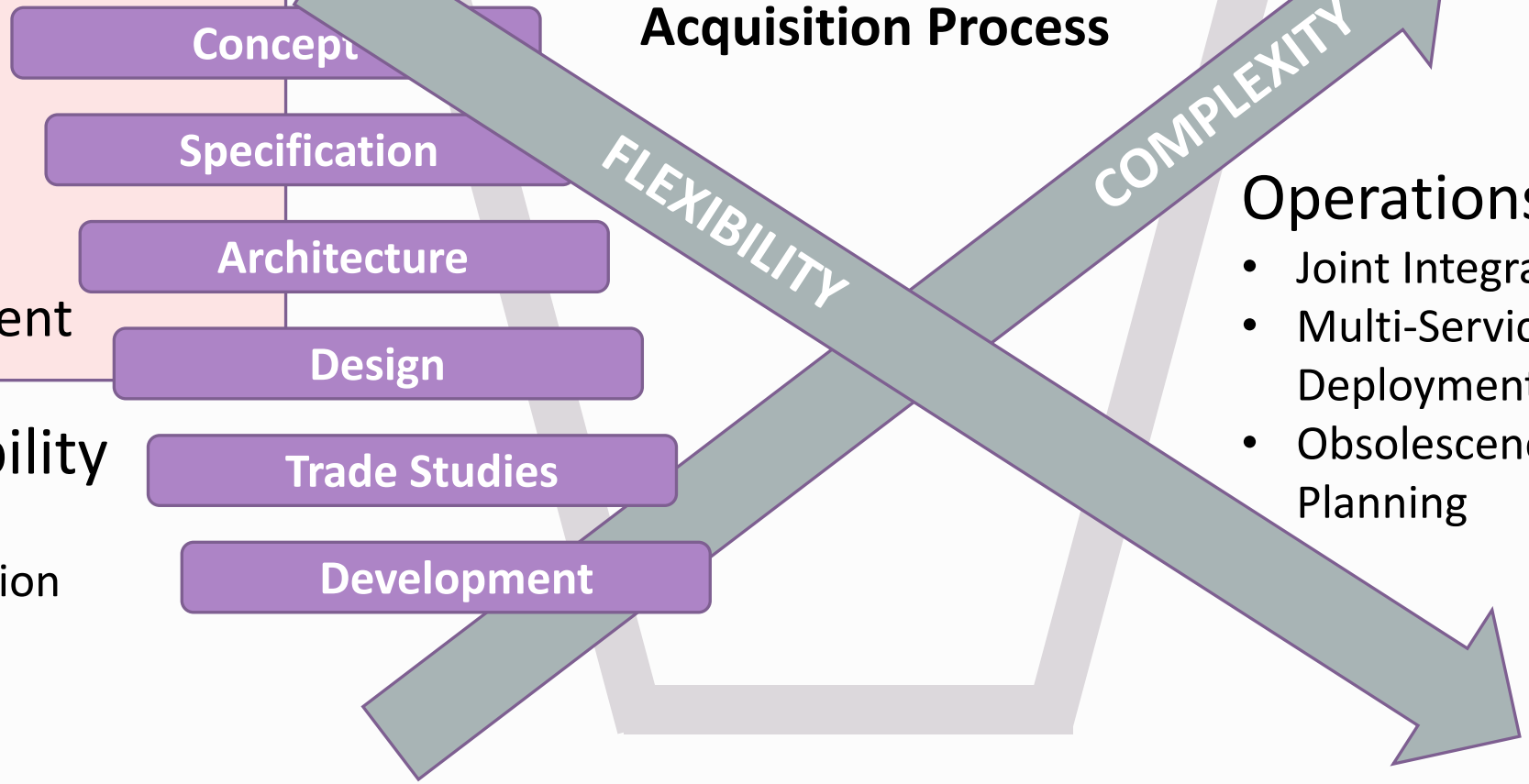
Mission Engineering

Capability Assessment

Adaptive Acquisition Framework



Acquisition Process



Design for Flexibility

- Digital Engineering
- Modeling & Simulation
- MOSA
- SOS Interoperability

Operations

- Joint Integrated Ops
- Multi-Service Force Deployment
- Obsolescence Planning

Summary

- Mission Engineering addresses complexity
  - Problem Statements, Scenarios, Assumptions
- Systems Engineering Provides Flexibilities
  - Modeling and simulation
  - MOSA
  - SOS Interoperability
- Over time the ability to deal with complexity shifts from design to operations – plan on it!

Thank You

Dave Chesebrough

dchesebrough@definedbusiness.com

National Defense Industrial Association Systems and Mission Engineering Conference

November 2022

Applying Mission Engineering to the U.S. Department of Defense Rapid Defense Experimentation Reserve

Mr. Elmer Roman
Director, Mission Integration
OUSD (R&E), Mission Capabilities

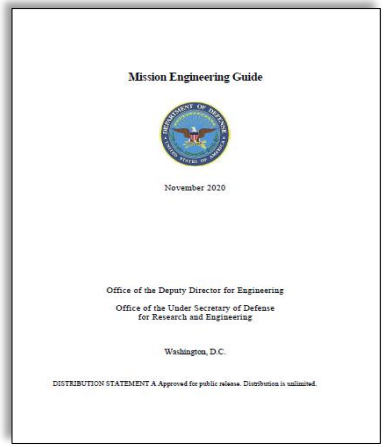
Dr. Judith Dahmann
OUSD R&E, Mission Capabilities, Mission Integration
Technical Fellow
MITRE Corporation

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

Mission Engineering

ME Guide

https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf


Mission Engineering Guide

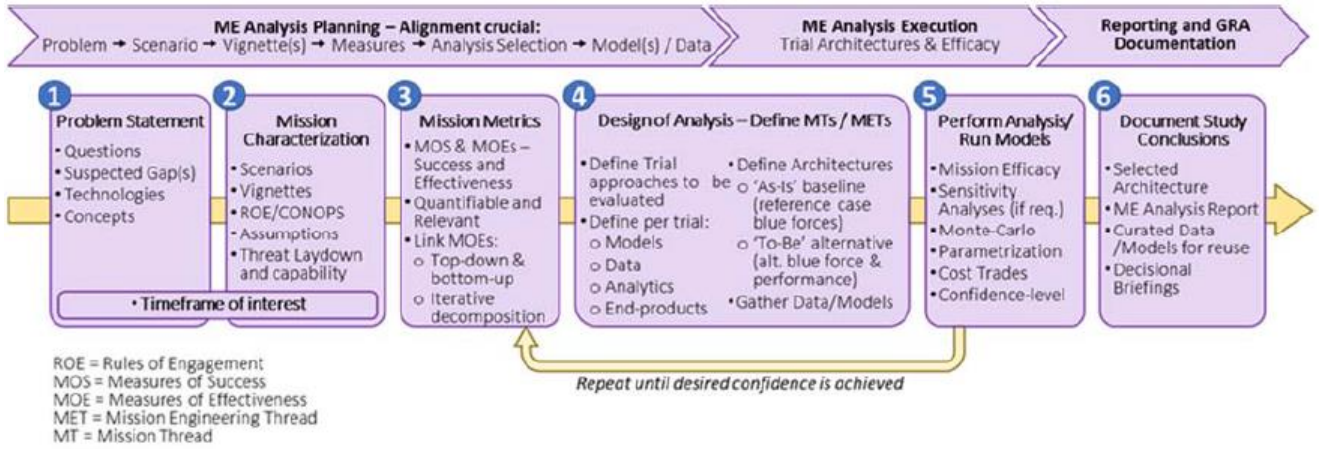
November 2020

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

Washington, D.C.

DISTRIBUTION STATEMENT A Approved for public release. Distribution is unlimited.

Mission Engineering (ME) Methodology



The ME process begins with the end in mind, a carefully articulated problem statement, the characterization of the mission and identification of metrics, and working through the collection of data and models needed to analyze the mission and document the output results.

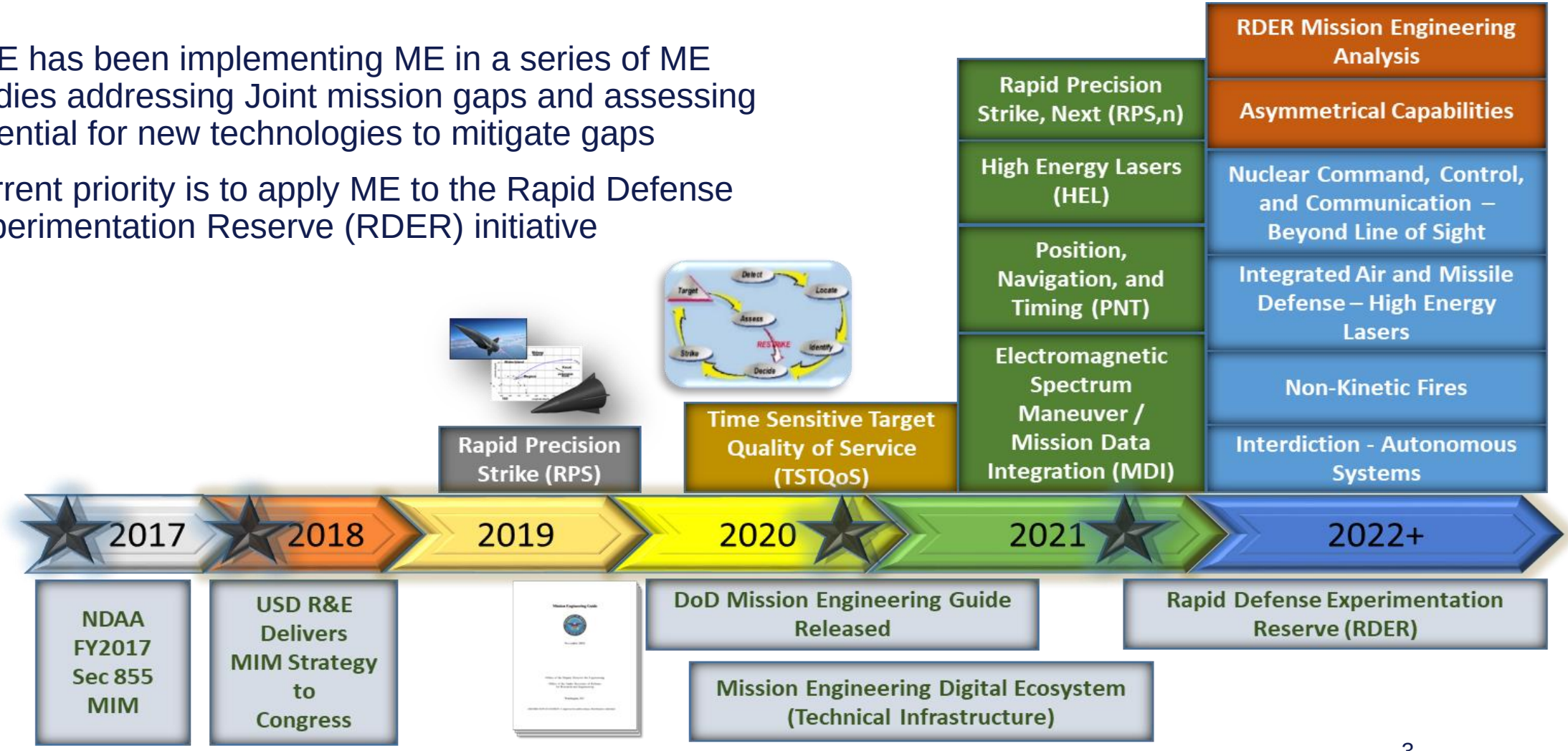
DoD ME Guide, 2020, p5

ME provides consistent methodology to deliver analytically and data-driven, mission-focused, threat-informed outputs to help guide future mission superiority

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

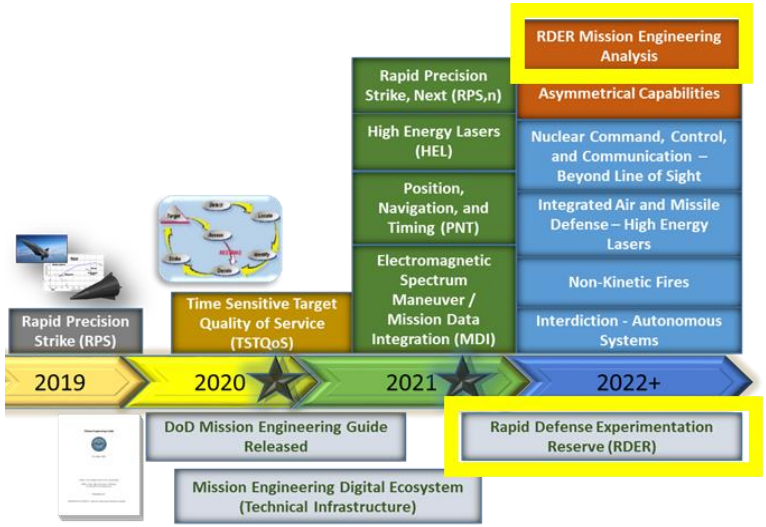
R&E Mission Engineering Implementation Based on Experience With FY20-22 Studies

- R&E has been implementing ME in a series of ME studies addressing Joint mission gaps and assessing potential for new technologies to mitigate gaps
- Current priority is to apply ME to the Rapid Defense Experimentation Reserve (RDER) initiative



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

Rapid Defense Experimentation Reserve (RDER)



The Secretary of Defense established RDER to:

- Focus multi-Component experimentation in a structured, multi-year campaign of learning.
- Proposed experiments based on alignment to Joint missions and potential to yield demonstrable warfighting utility in the near-term.
- Demonstrations and experiments will be conducted at key exercise venues (INDOPACOM Focused).
- Successful demonstrations and experiments can be quickly transitioned to the Components for fielding as new systems or approaches.

"RDER will drive efforts to compete with peer and near-peer adversaries through the development of capabilities that support the Joint Warfighting Concept (JWC) including, but not limited to, fires, command and control, logistics, and capabilities that will drive information advantage." – Deputy Secretary of Defense Dr. Kathleen Hicks

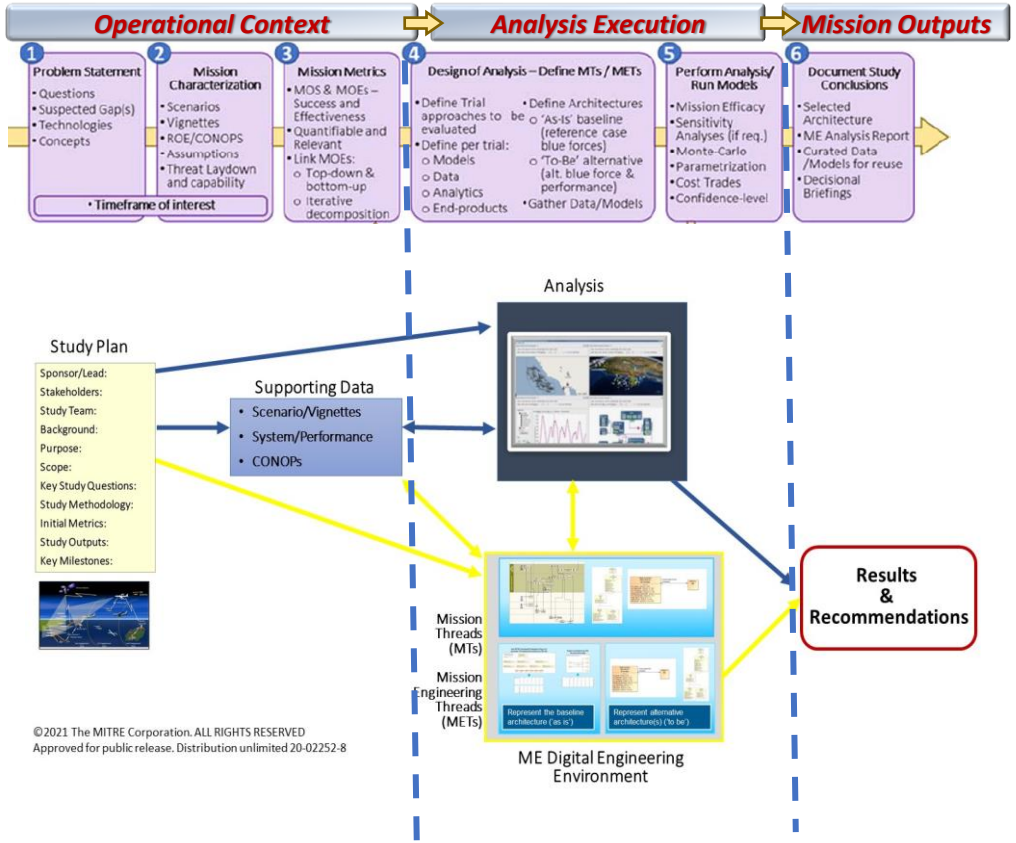
RDER will bring five benefits to DoD:

1. Accelerate Joint Warfighting Capability
2. Expand International Partnerships and Multi-lateral engagement
3. Focus Service experimentation to enable the JWC
4. Quickly demonstrate and assess innovative ideas
5. Provide feedback to future Warfighting concept development

Apply *Mission Engineering* across RDER → utilize mission context products and artifacts to make mission-focused decisions

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

R&E ME Studies implementation of the ME Methodology Provides Foundation for ME for RDER



ME Implementation Applied Across R&E ME Studies

Study Plan (Terms of Reference)

- The scope: stakeholders, background, problem statement, key questions, hypothesis, methodology/approach, mission context, products/deliverables

Supporting Data

- Mission Characterization: Detailed data on the mission scenario and vignette (context for the analysis), threat, systems and their role in execution the mission, etc., assumptions

ME Digital Engineering Environment

- Digital representation of the mission architecture (Mission Threads (MT), Mission Engineering Threads (MET)) for baseline and the alternatives

Mission Analysis

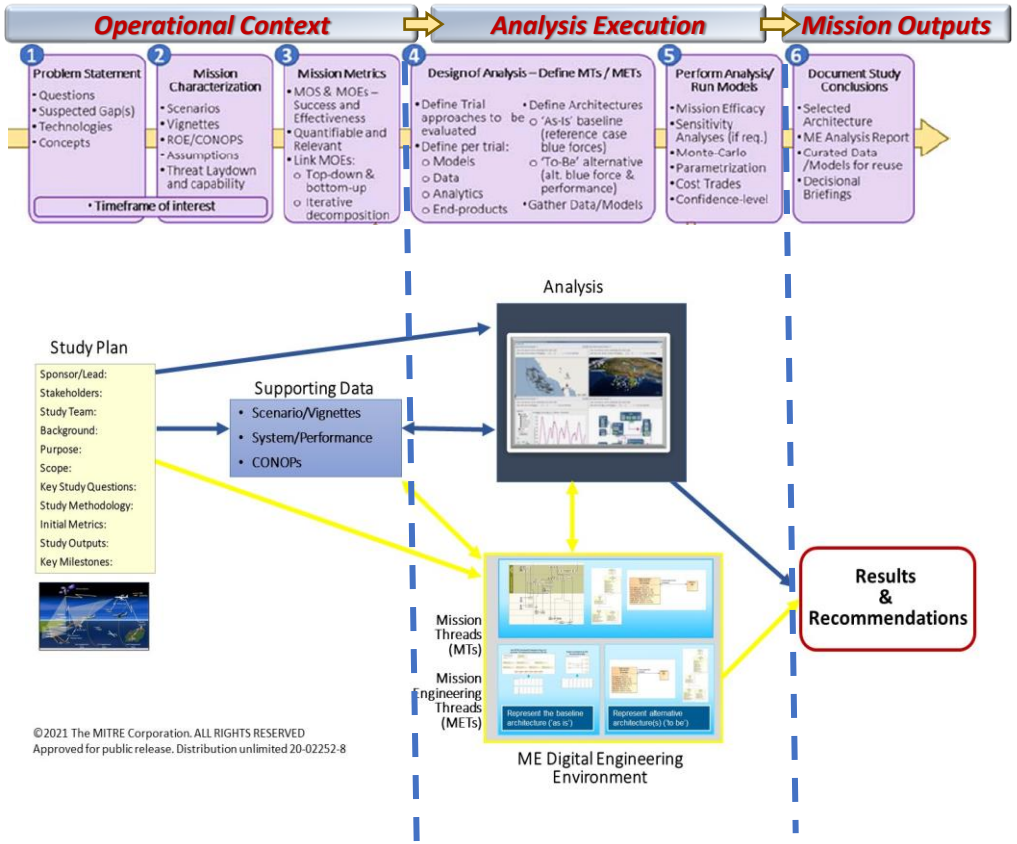
- Implementation of the scenario, systems and activities in operational analysis tool(s)
- Simulation runs for baseline and alternatives; outputs quantitative metrics

Results

- Outputs, trends, observations, and recommendations based on mission analysis

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

RDER Applies and Extends the ME Approach



RDER ME Implementation Builds on the ME Experience

RDER Sprint Focus / Plans (Terms of Reference)

- Mission Scenario/Vignette
- RDER Proposal Concepts

Supporting Data

- Scenario documentation (i.e, JFOS)
- Kill Chain data (i.e., Long Range Fires)
- Data on RDER Concepts

ME Digital Engineering Environment (DEE)

- Extend Reusable DEE for ME for digital representation of the mission architecture (MTs, METs) for baseline and the concepts

Mission Analysis

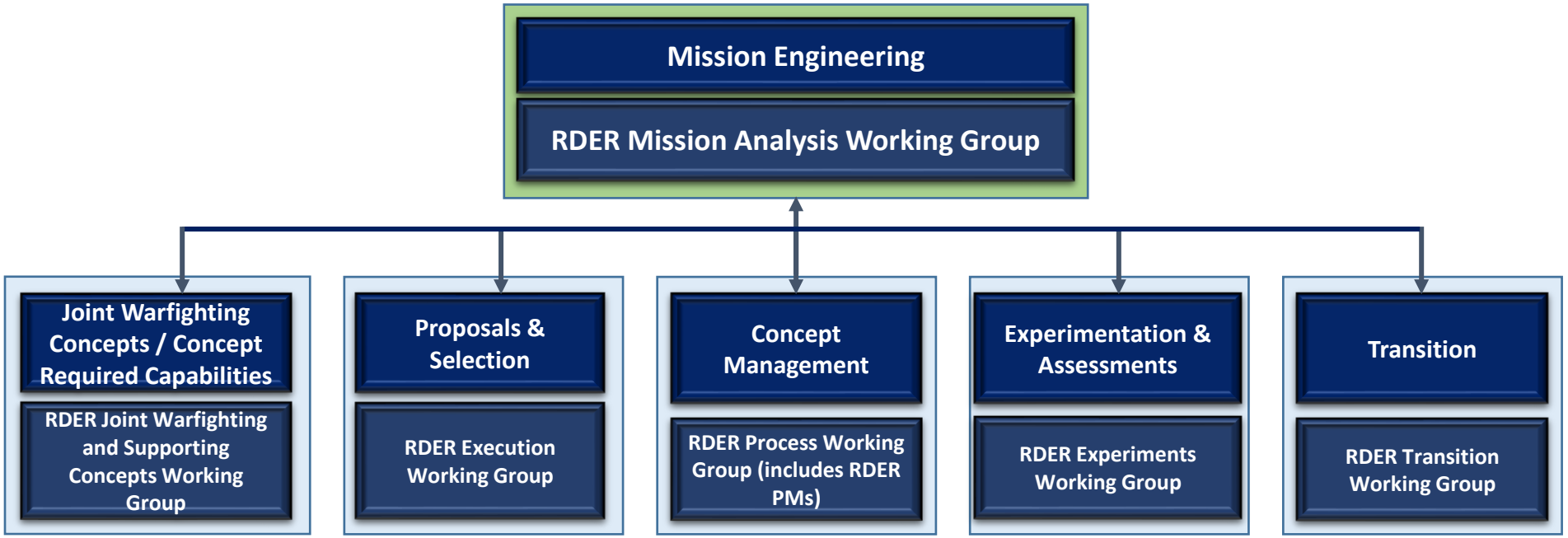
- Implementation of scenario, systems and activities in operational analysis tool(s) in AFSIM
- Simulation runs for baseline and concepts; outputs quantitative metrics

Results

- Results, trends, observations, and recommendations based on mission analysis provided to Concept leads, RDER Proposal managers, Experimentation Leads

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

Mission Engineering Across RDER



- Tracks Concept Required Capabilities (CRC) Alignment of RDER Proposals

- Provides scenario and baseline MTs/METs to inform proposals
- Maps alignment of selected proposals to METs for mission analysis

- Models how RDER concepts will be implemented in the mission
- Analyzes impact of RDER concepts on mission outcomes

- Supports experiment planning (i.e., "kill web" design) and execution of experimentation
- Projects potential benefit of full concept development on mission

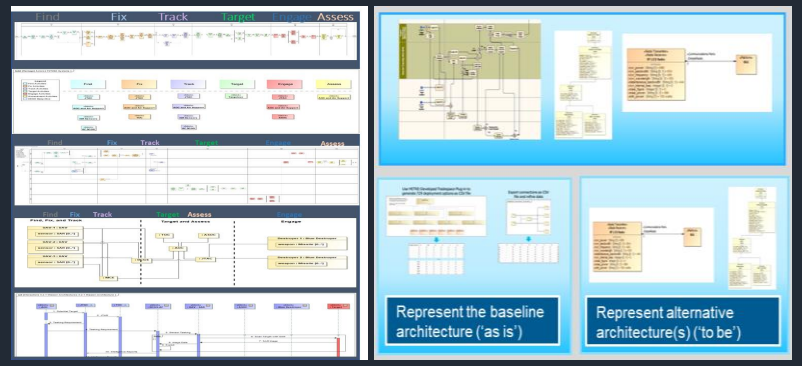
- Supports transition with digital mission architectures of concepts to support System of Systems engineering

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

RDER R&E Mission Engineering Activities and Products

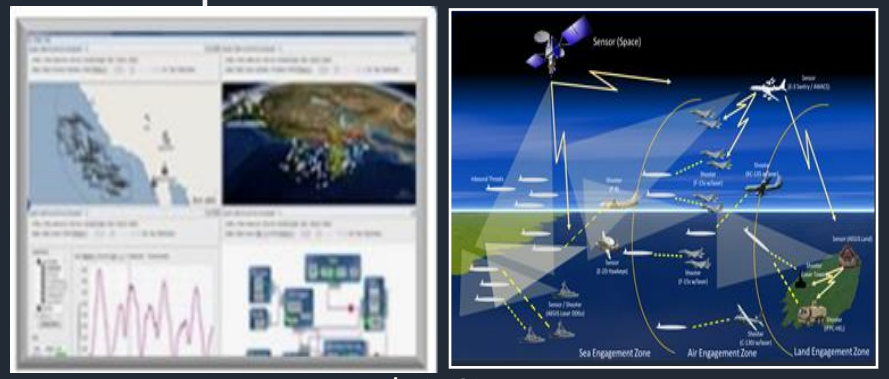
Lines of Effort

Mission Models



Tool: CAMEO/SysML

Operational Simulation



Tool: AFSIM

Baseline

- Digital representation of the baseline Mission Threads (MTs) scenario independent activities and Mission Engineering Threads (METs) adding scenario specific organizations and activities
- Representation of the baseline MTs/METs within scenario including threat, systems' attributes and behaviors – conduct baseline analysis of mission metrics

Alternatives

- Updated MTs and METs to include RDER Concepts with associated changes
- Update the systems' attributes and behaviors as specified in RDER concepts and assess impact on mission metrics

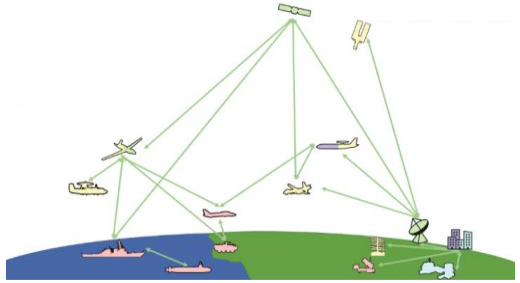
MISSION THREAD ALIGNMENT [TRACEABILITY]

QUANTIATIVE ANALYSIS [MISSION METRICS – OUTPUTS]

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

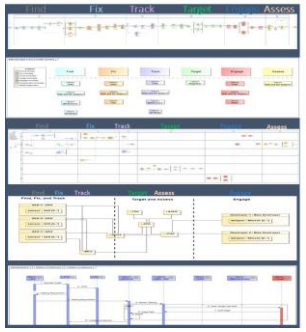
Mission Engineering Modeling Workflow

Obtain Kill Chain Source Information



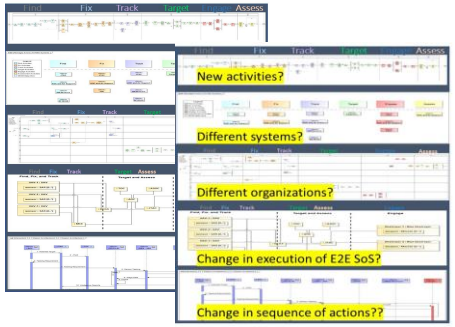
informs

Baseline MTs/METS



Provides basis for

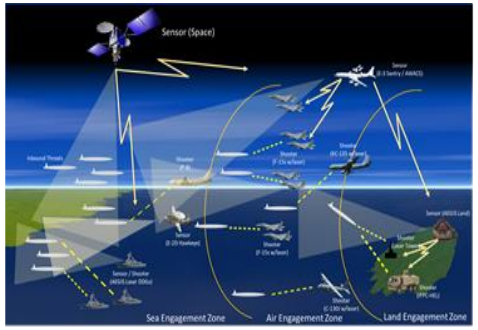
RDER Concepts - Represented as changes in the MT/METs



Represented in AFSIM

Represented in AFSIM

Alignment with Scenario Documentation (i.e., JFOS)



informs

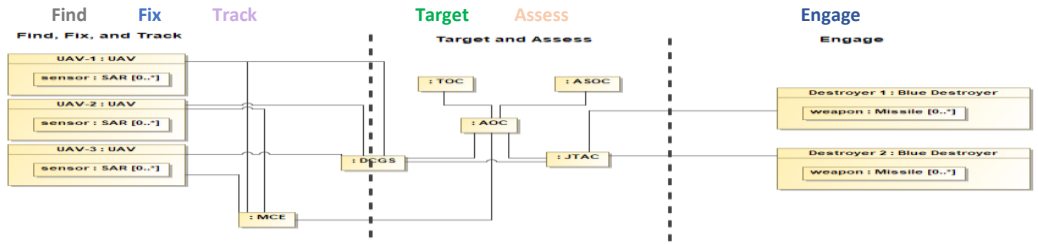
Analysis of Baseline Compared to Concept on Mission Outcome Metrics In Selected RDER Scenario

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

Mission Models
Mission Threads (MTs) and Mission Engineering Threads (METs)

Mission Thread (MT): An end-to-end sequence of tasks, activities and events to execute a mission.

Mission Engineering Thread (MET): Mission threads that include technical details of the capabilities and systems required and utilized to execute the tasks and activities for a mission.



In executing ME

- MTs define the essential sequence of activities in the execution of the mission

  key elements of the *operational mission architecture*

- METs are used to define the systems / SoS in the execution of the mission activities

  key elements of the *systems of systems architecture*

MTs and METs provide an organizing construct across RDER proposal selection, concept maturation, experimentation, and transition

Distribution Statement A. Approved for public release. Distribution is unlimited. (pending)

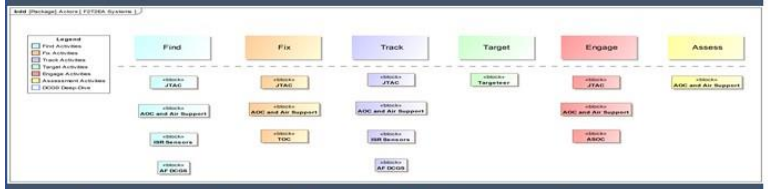
ME Digital Mission Models

- How would BLUE fight in this scenario (independent of RDER)?
  - Identify BLUE kill chains – develop BLUE mission engineering threads (Baseline METs)
- How will these change when we introduce the concepts in the RDER 23-1 proposals?
  - Update the baseline METs to add concepts (RDER METs)

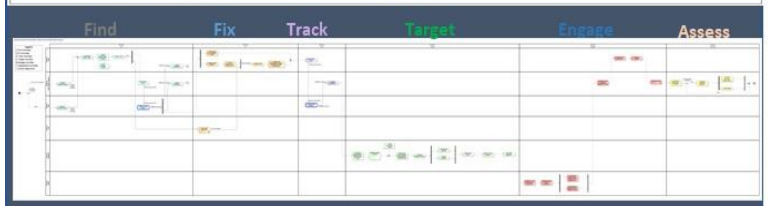
Baseline MT and MET Models

Activities

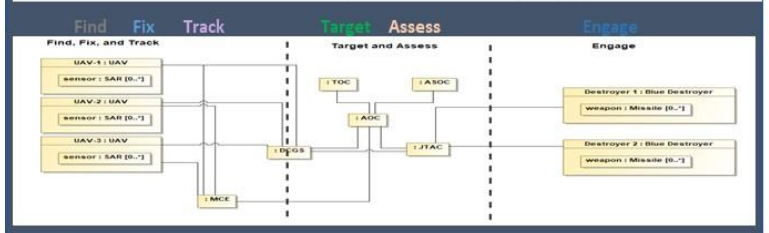
Systems supporting Activities



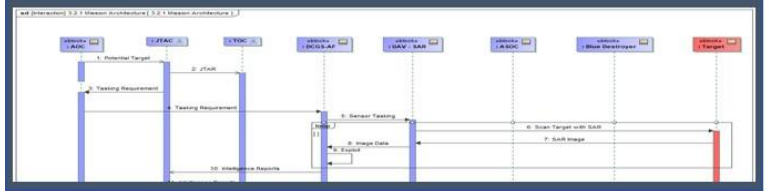
Organizations executing activities



End-to-end flow of SoS



Sequence of actions



RDER Concepts

What new activities are now needed to execute the mission?

What new systems does the concept require?

What different organizations are now part of mission execution? Which activities do they execute?

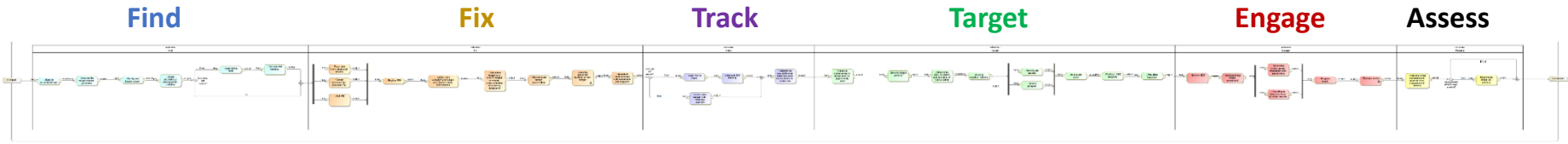
How does this change the execution of the End-to-end (E2E) SoS?

How does this change the sequence of actions?

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

Baseline Mission Thread – Joint Targeting

Mission Thread – lays out the set of actions needed to accomplish the mission



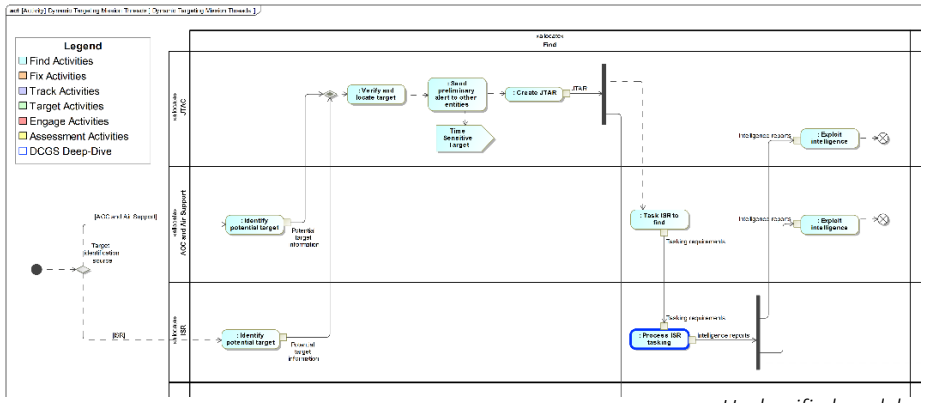
Unclassified model

- This core RDER mission thread provides context for representing the activities and systems
  - Found in the baseline RDER scenario
  - Changes in the baseline activities and systems when the concept is introduced into the scenario

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

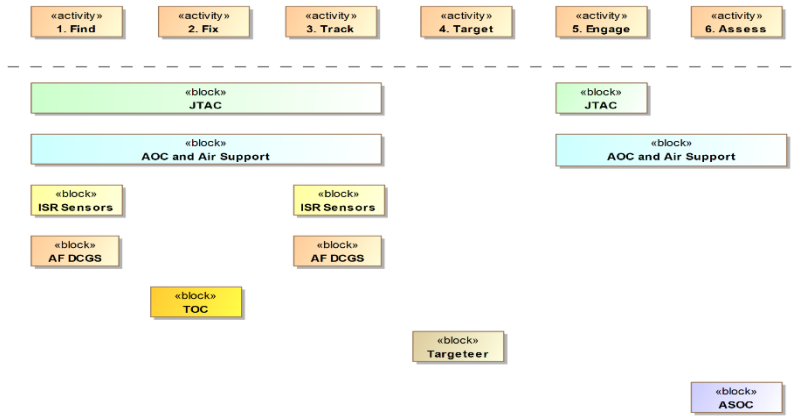
Views of Digital Mission Models

Baseline Scenario & Concepts As Implemented in Scenario

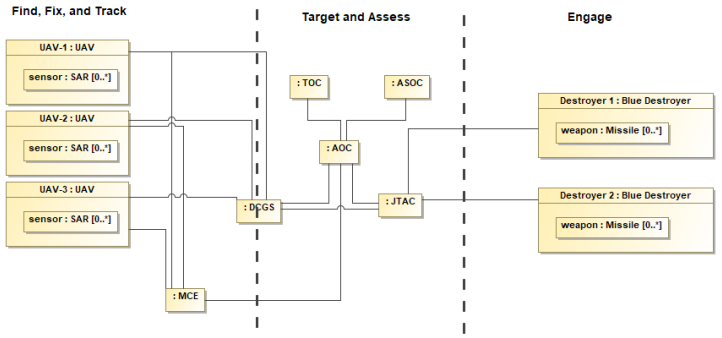


Unclassified model

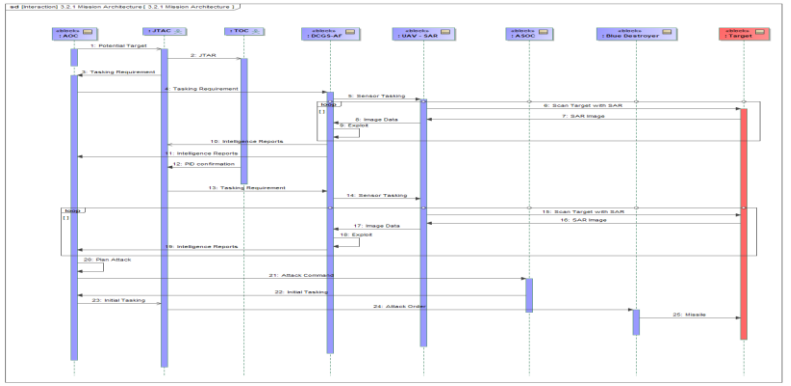
Apply systems and organizations to base mission thread



Systems employed to execute MT activities



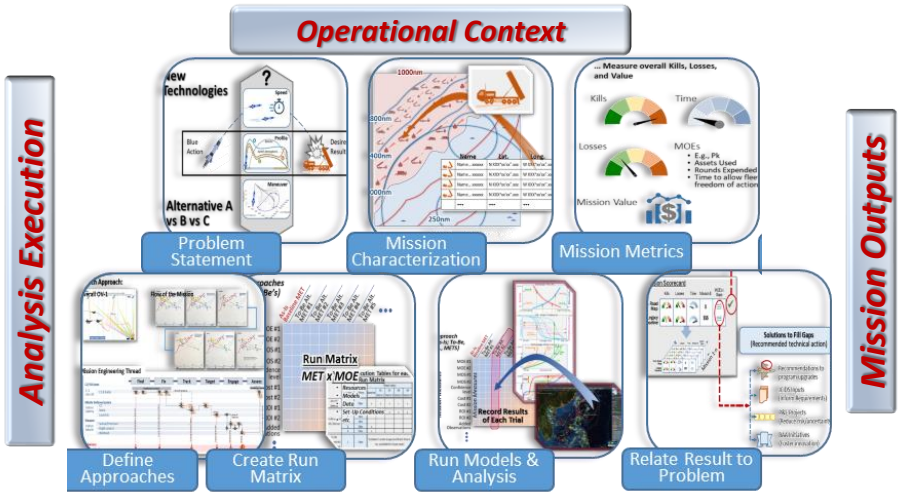
End-to-end flow of systems interaction

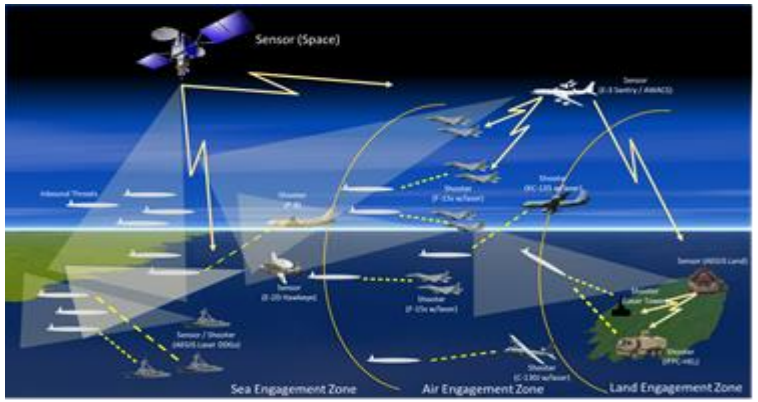


Sequence of system to system interactions

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

Overview of RDER AFSIM





- Represent baseline in the operational context for analysis and generate the baseline mission metrics
- Represent the changes made in the baseline to represent each concept to:
  - Compute the impact on mission metrics of the concept
  - Compute metrics on the performance of the particular concept as represented in the scenario and analysis
    - Calibrate the inputs the concepts have on the outcomes
    - Drive the metrics prototyping & experimentation
    - Support transition

Distribution Statement A. Approved for public release. Distribution is unlimited. (pending)

RDER R&E ME Analytical Approach

(U) Mission Engineering Analysis will be:

- An agile and iterative approach;
- Conducted on:
  - Each individual RDER Concept; and
  - Combinations of RDER Concepts

(U) ME Analysis Approach:

- How is the RDER Concept to be implemented in the scenario (across METs)?
- What is the objective of the concept (e.g., increased ISR coverage, increased weapons platform survivability)? How is this measured?
- Under what conditions do we expect the concept to impact mission outcomes (e.g., day without space)?
- What are the concept dependencies on baseline (organic) systems?
- What is the performance of each element in the concept?

Drive the run matrix

Example Run Matrix
(Tailored For each RDER Concept)

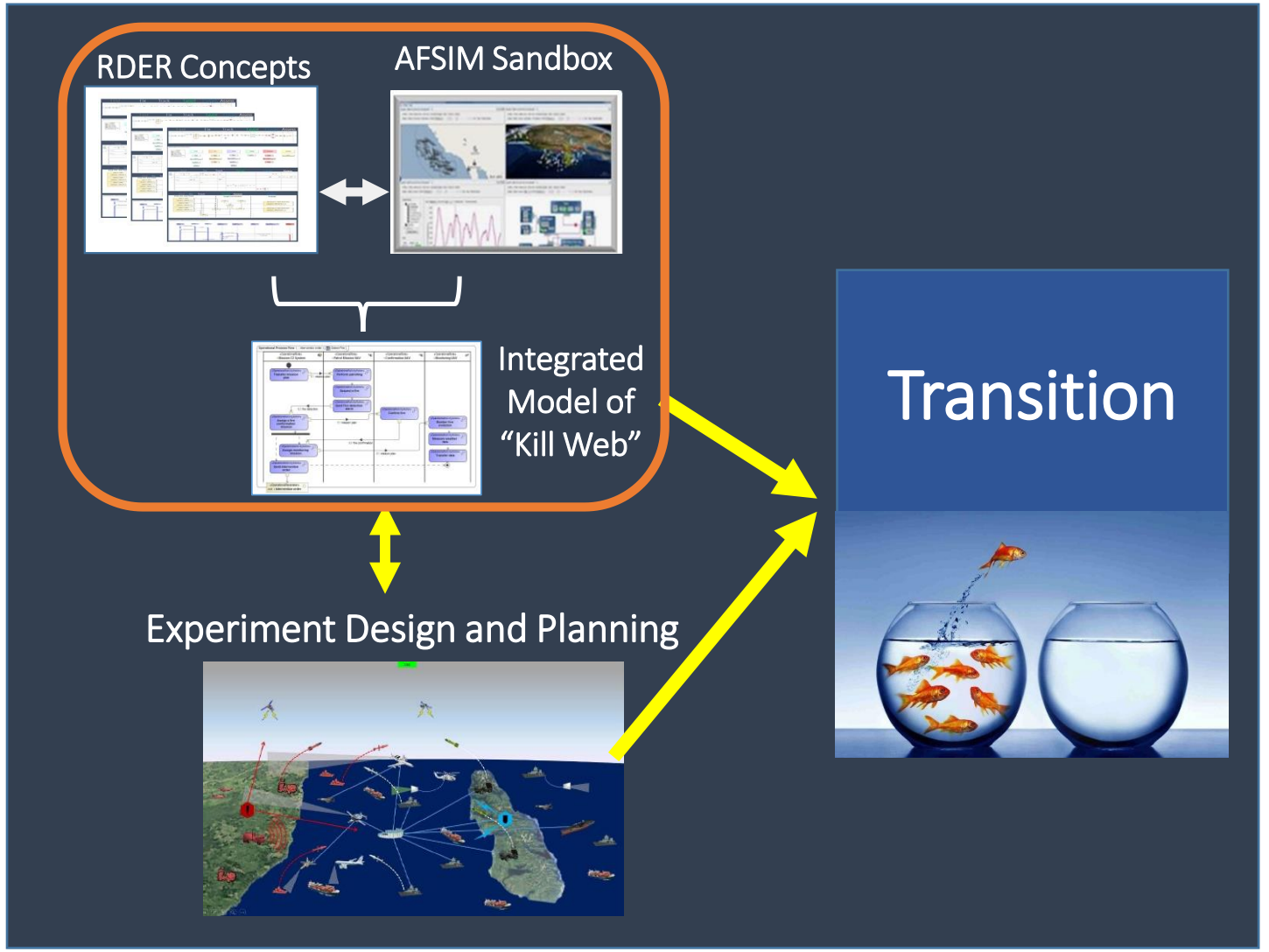
Case	
Baseline A - Uncontested (run once)	Do nothing to respond to adversary *(Green only)*
Baseline B - Baseline Scenario (run once)	Implement the baselines METS
Baseline C - Tailored Scenario (each concept)	Conditions addressed by concept (e.g., no space)
Alternative 1 - Baseline Scenario (B) with RDER Concept Excursions to explore tradespace	RDER Concept implemented in updated METs (specific for each RDER Concept)
Alternative 2 - Tailored Scenario (C) with RDER Concept Excursions to explore tradespace	

Similar agile and iterative approach will be applied to individual or combined RDER Concepts

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

ME Products and Results Support Experimentation and Transition

- Digital mission models support experimentation planning (design of “kill web”)
- Results of AFSIM operational simulation support:
  - Selection of RDER Concepts
  - Drive metrics for experiment data collection
  - Inform transition activities
- Experiment results may lead to added ME analysis



Distribution Statement A. Approved for public release. Distribution is unlimited. (pending)

Summary

- Digital Mission Threads and Mission Engineering Threads are developed for each scenario/vignette and submitted as part of the Call for Proposals
- MTs/METs align the RDER concepts and put the concepts into a mission context
- Mission Engineering analysis will model the concepts into an operational environment (AFSIM) to assess and evaluate the mission effectiveness of concepts (excursions from the as-is mission architecture)
- ME analysis outputs quantitative results in terms of mission metrics
- Results will support selection, prioritization and development of RDER Concepts; and shape future RDER call for proposals
- Leverage data and lessons learned from experiments to discover and mature future Warfighting Concepts

This is an Iterative and repeatable process to support continuous evaluation and assessment of JWC CRCs through RDER experimentation in a mission context

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

Authors / Points of Contact

Marc Goldenberg
Technical Director
OUSD R&E/Mission Capabilities/Mission Integration
Phone: 703-692-6551
Email: marc.j.goldenberg.civ@mail.mil

Dr. Judith Dahmann
Technical Fellow, MITRE Corporation
Phone: 703-298-6694
Email: jdahmann@mitre.org

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

An Enterprise Portfolio Management Framework for Mission Planning, Engineering, and Acquisition

Presented to

NDIA Systems & Mission Engineering Conference

1-3 November 2022

Dr. Warren Vaneman, ESEP wvaneman@nps.edu
Prof. Ron Carlson rrcarlso@nps.edu
Prof. Corina White corina.white@nps.edu
Mr. Raymond "Joe" Stone Raymond.stone@nps.edu

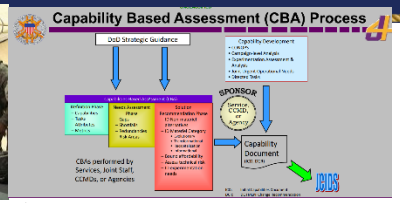
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

Background

- Mission success requires a careful orchestration between mission planning, engineering, and analysis of the mission, and an acquisition strategy that acquires systems, and assembles system of systems for mission-capability satisfaction.
- The challenge is to develop a mission architecture that demonstrates continuity of mission capabilities from the Strategic Objectives and Policies to the individual platforms.

This paper develops a mission framework that defines the structure that provides traceability from the policy and operational drivers of the mission, to the system of systems that satisfy the mission capabilities, and finally to the individual system's hardware and software.

Intersection of Mission-Based Disciplines



Mission Planning
- Identify mission capabilities
- Develops Concepts of Operations(scenarios)
- Capability-Based Planning
- Assess risk

Mission Capabilities Defined

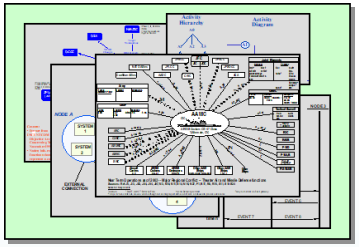
Mission Capabilities Provided

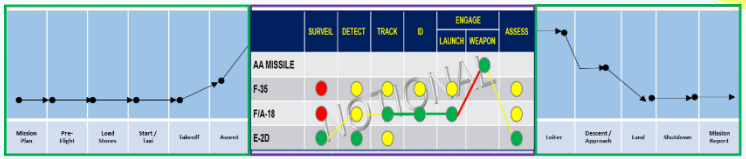
Operational Plans

Initial Capabilities Description

Mission Engineering
- Evaluates mission capabilities
- Analyzes Concepts of Operations(scenarios)
- Defines the mission (capability) architecture

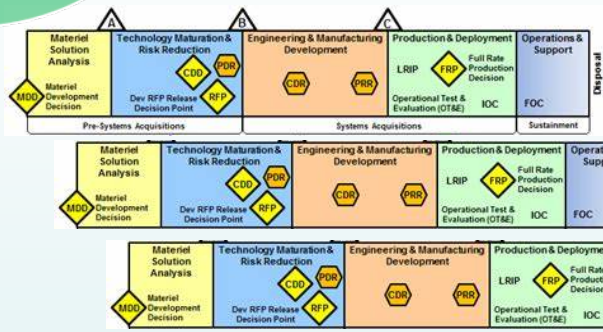
Lead Systems Integration
- Develops System of Systems Architecture
- Engineers and manages capabilities and interdependencies among constituent systems





Prepare/Config | Effects Chain | Post Mission Tasks

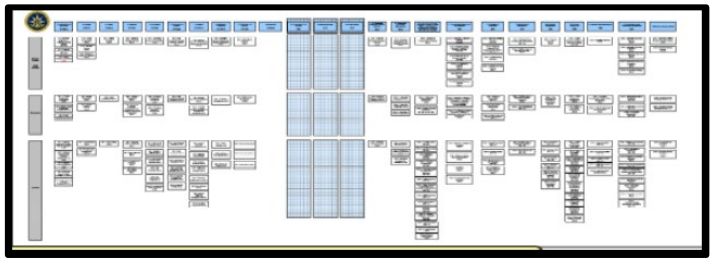
Mission Capabilities Specified

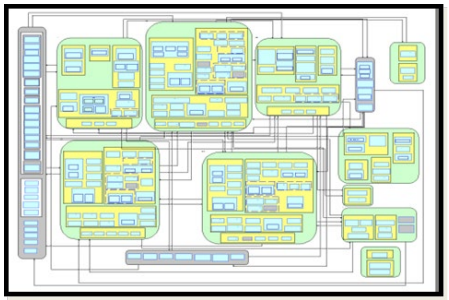


SoS Capability Development Document

Mission Architecture Levels

Enterprise Architecture-The process of translating vision and strategy into an effective and cohesive enterprise by communicating and improving the key requirements, principles and models that describe the enterprise's future state and enable its evolution.





SoS Architecture-The process of describing the structure of a SoS, its decomposition into constituent systems, the relationship between this systems, and the relationship with the external environment.

Systems Architecture-The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

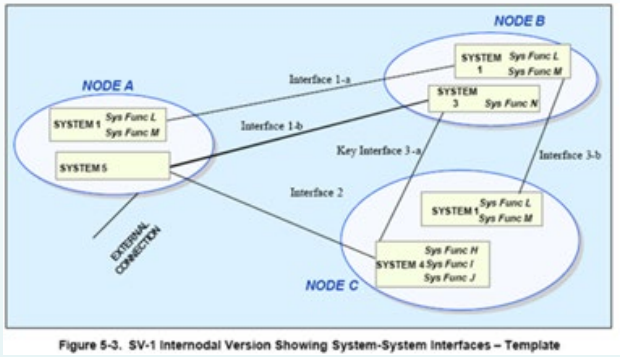


Figure 5-3. SV-1 Internodal Version Showing System-System Interfaces – Template

10-Layers within the Mission Architecture

10. Strategic Objectives and Policies
- Top-level strategic guidance

9. Enterprise Mission Area
- Mission Areas

8. Enterprise Mission Threads
- Mission scenarios

7. Enterprise Mission Tasks
- Universal Tasks required to accomplish the mission

6. SoS Mission Operations
- System of Systems Concept of Employment

5. SoS Mission Structures
- Structure of platforms and systems that comprise the SoS

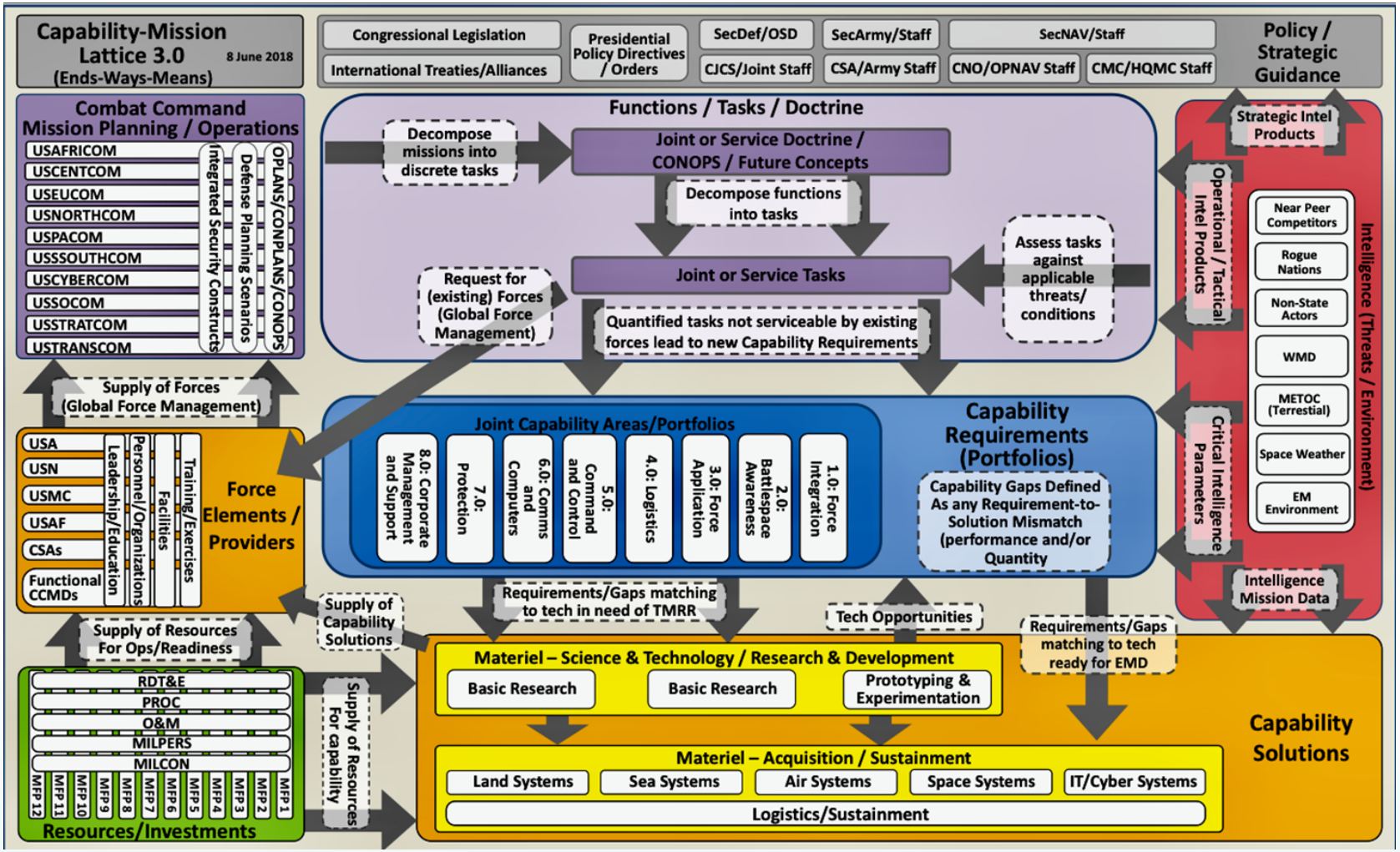
4. Platforms

3. Systems

2. Sub-Systems

1. Assemblies and Components

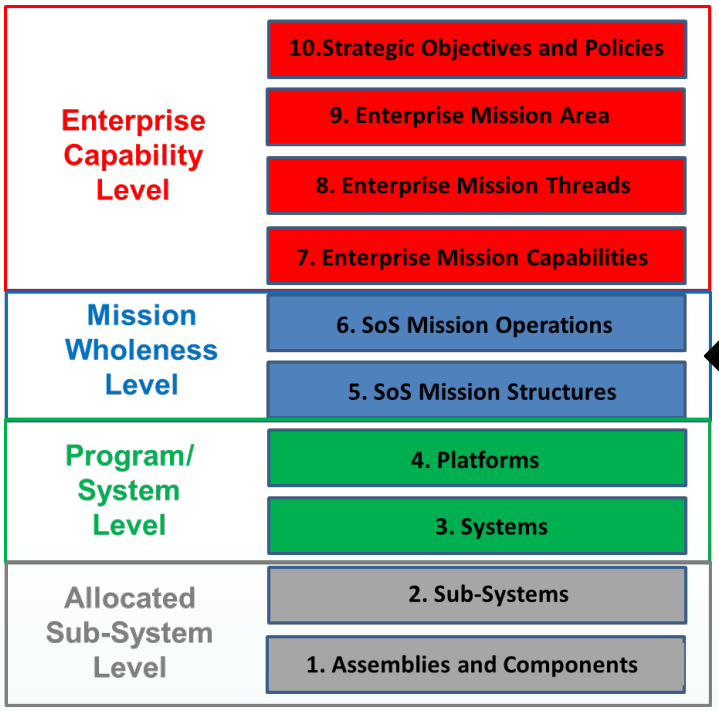
Capability-Mission Lattice

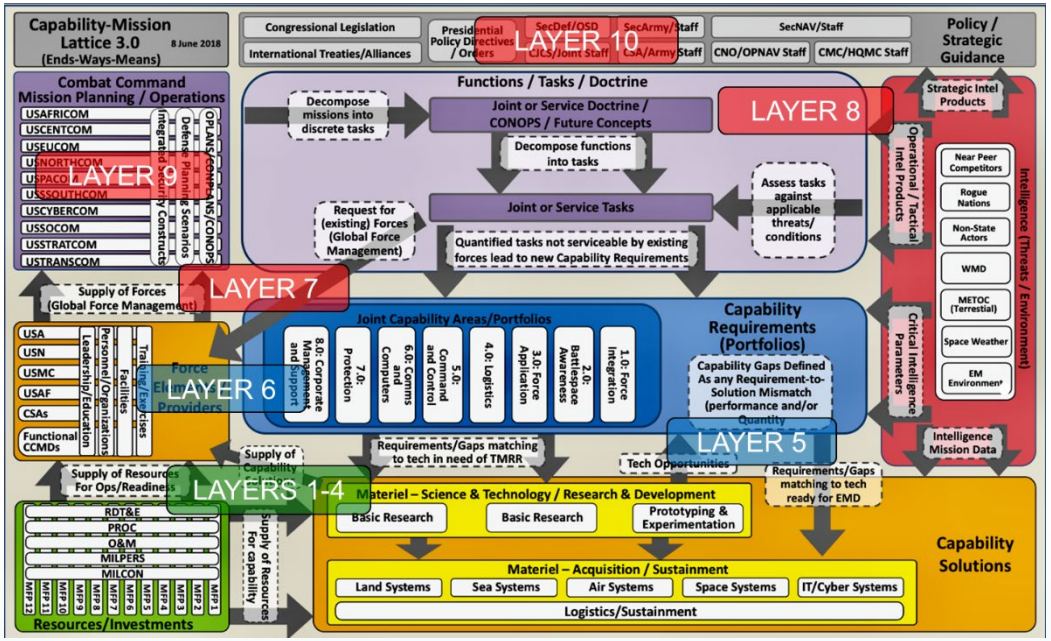


The **Capability-Mission Lattice** is used as an integrating construct for identification of capability requirements and the development of capability solutions.

Mission Architecture + Capability-Mission Lattice

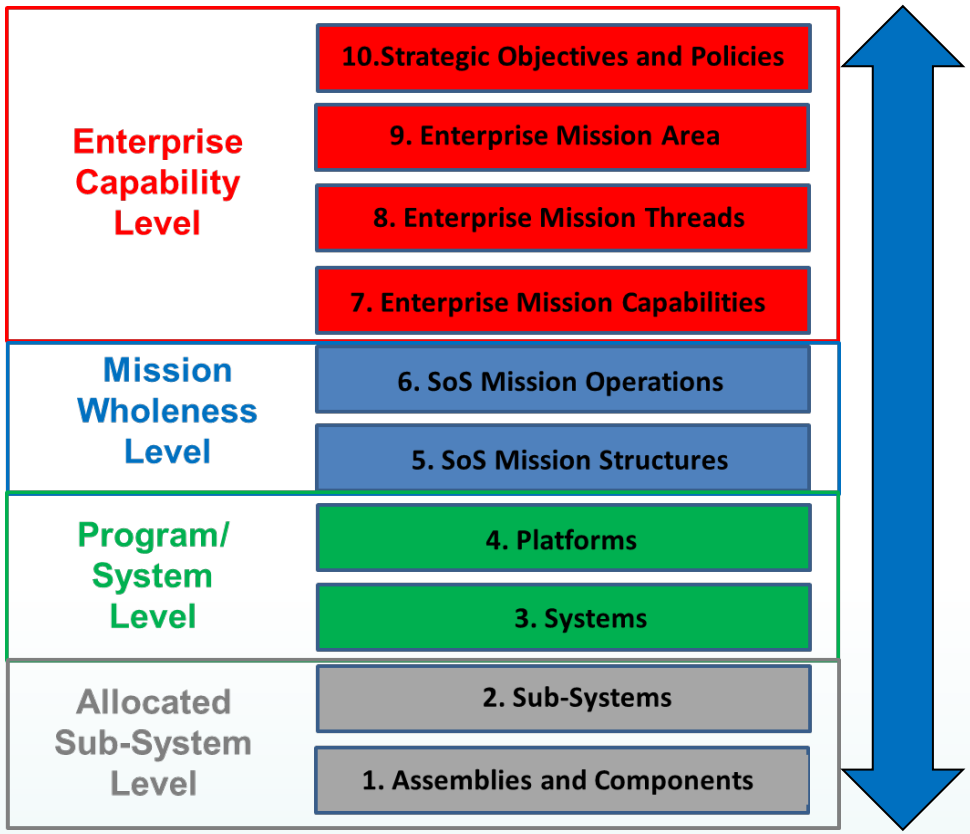
The 10-Layer Mission Architecture is correlated with and implements the JCIDS Capability-Mission Lattice within a modeling environment.





The combination of the Mission Architecture and the Capability-Mission Lattice provides a roadmap of how mission strategies can be implemented.

The Mission Architecture Purposes



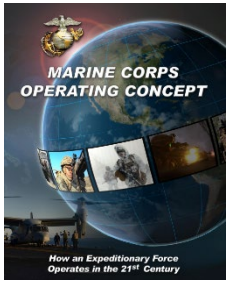
- Assists in making prioritization and budget decisions based on mission capabilities that are not being addressed or are being overly addressed.
- Provides a framework for insight and discovery of functions, systems, and services that exists with the mission architecture.
- Provides traceability of mission-capabilities from strategic objectives to individual systems.

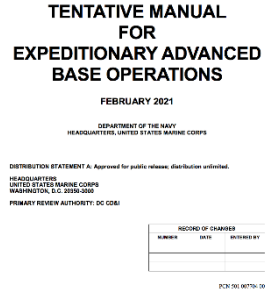
Force Design 2030 Use Case

"War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously."

-MCDP-1

Force Design 2030
March 2020

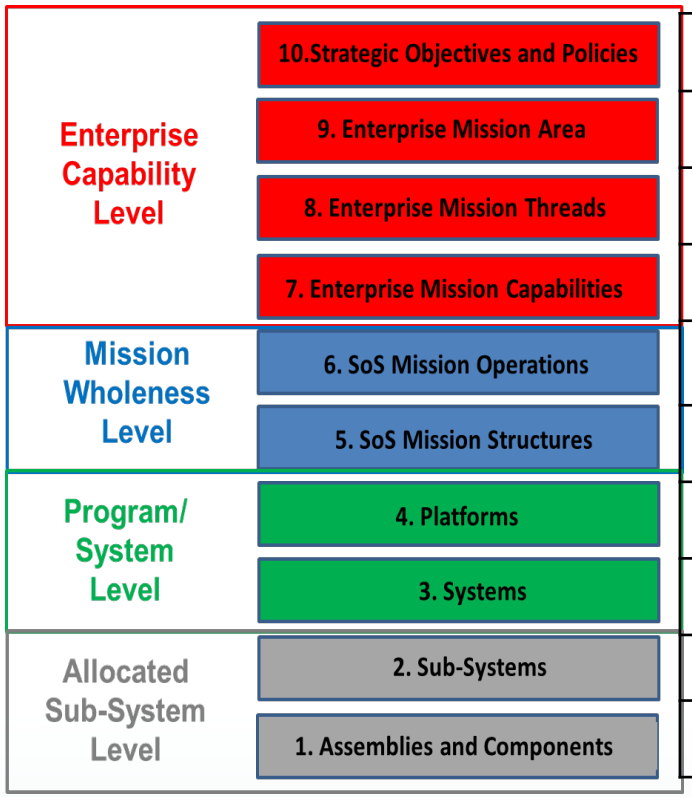




- Establish a focus area for force development pertinent to National and Naval Strategy.
  - Operational Employment of USMC Forces consistently retains the **FLEXIBILITY** to conduct a wide variety of missions to meet National objectives.

- Focused on:
  - **Littoral Maneuver and Sustainment**
  - **Maritime Reconnaissance/Counter Reconnaissance**
  - **Long-Range Precision Fires**
  - **Operations in the Information Environment**

Using the 10-Layer Mission Architecture



Commandant's Planning Guidance
Expeditionary Advanced Base Operations (EABO)
Coordinate Air and Missile Defense
Conduct Short Range Ground Based Air Defense
Deny hostile UAS from targeting Expeditionary Forces
Ground Base Air Defense (GBAD)
Joint Light Tactile Vehicle (JLTV)
Marine Air Defense Integrated System (MADIS)
MK 2 Radar / C2 Systems
Receiver / Transmitter / Display Panel

Marine Corps Force Design 2030

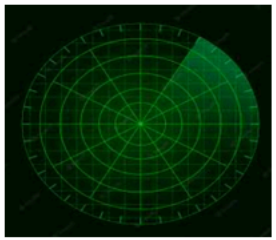
The 10-Layer mission architecture can help determine the required mix of force structure and essential equipment needed to fulfill the USMC desired missions and adapt to changes. This application will show areas that must grow and be equipped to support the missions as well as forces and equipment that may not be required to adapt to the changing USMC missions.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

Using the 10-Layer Mission Architecture

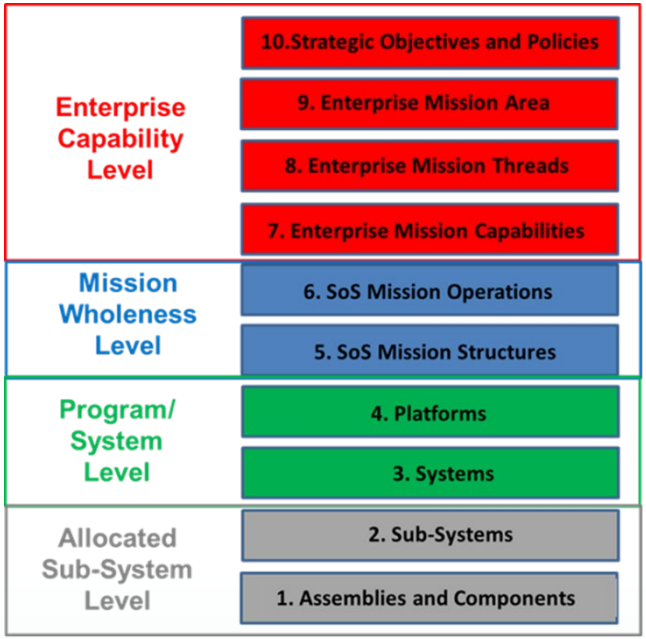
Strategic Objectives & Policies (Layer 10)	Enterprise Mission Areas (Layer 9)	Enterprise Mission Threads (Layer 8)	Enterprise Mission Capabilities (Layer 7)	SoS Mission Operations (Layer 6)
Strategic Objective: Provide U.S.Indo-Pacific Command (U.S. INDOPACOM) and the Commander, 7th Fleet with a fight-tonight, stand-in force capability to persist inside an adversary's weapon systems threat range, create a mutually contested space, and facilitate the larger naval campaign. 	Mission Areas: • Distributed Maritime Operations (DMO) • Littoral Operations in a Contested Environment • **Expeditionary Advanced Base Operations (EABO)** 	Mission Threads for EABO: • **Coordinate Air and Missile Defense Actions** • Support Maritime Domain Awareness • Support Operations in the Information Environment • Conduct Expeditionary Strike • Attack Enemy Maritime Targets 	Support Coordinated Air & Missile Defense: • Conducts fires • Conduct reconnaissance • Conduct counter-reconnaissance • Conduct anti-air warfare • Conduct air control • Conduct airspace surveillance • **Conduct short range ground based air defense** • Provide forward arming and refueling points 	SoS Mission Operations for conducting Short-Range Ground Based Air Defense: • Enable joint kill chains through multi-domain C5ISR • Secure key maritime terrain • Provide ground based naval strike missiles • Support AAW and ASUW kill webs • **Deny hostile UAS and loitering munitions from targeting Expeditionary Forces**

Using the 10-Layer Mission Architecture

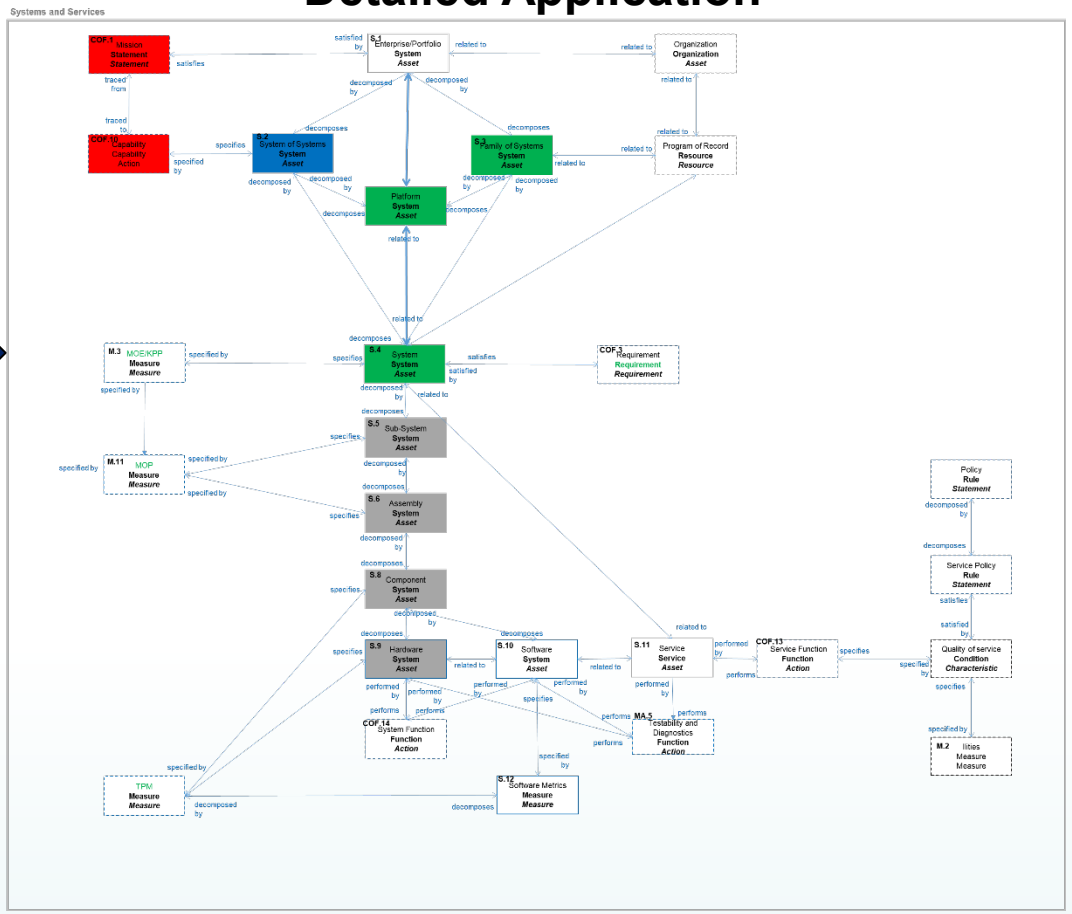
SoS Mission Structures (Layer 5)	Platform (Layer 4)	System (Layer 3)	Sub-Systems (Layer 2)	Assemblies & Components (Layer 1)
Deny hostile UAS and loitering munitions from targeting Expeditionary Forces: **GBAD** • C2 Nodes • Ground radars • Marine Air Defense Integrated System (MADIS) • Target tracking 	• **Joint Light Tactical Vehicle (JLTV)** 	• **Marine Air Defense Integrated System (MADIS)** 	• MK1 turret launched sparrow missiles • **MK2 360 radar and C2 system** 	• **Radar Receiver** • **Radar Transmitter** • Power • **Display Panel** • Control Panel • Etc. 

10-Layer Mission Architecture Related to a Conceptual Data Model

High-Level Description



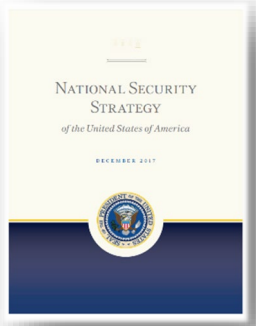
Detailed Application

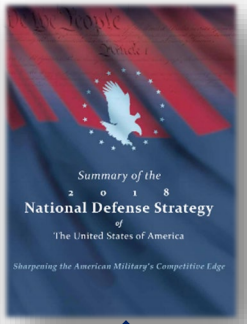


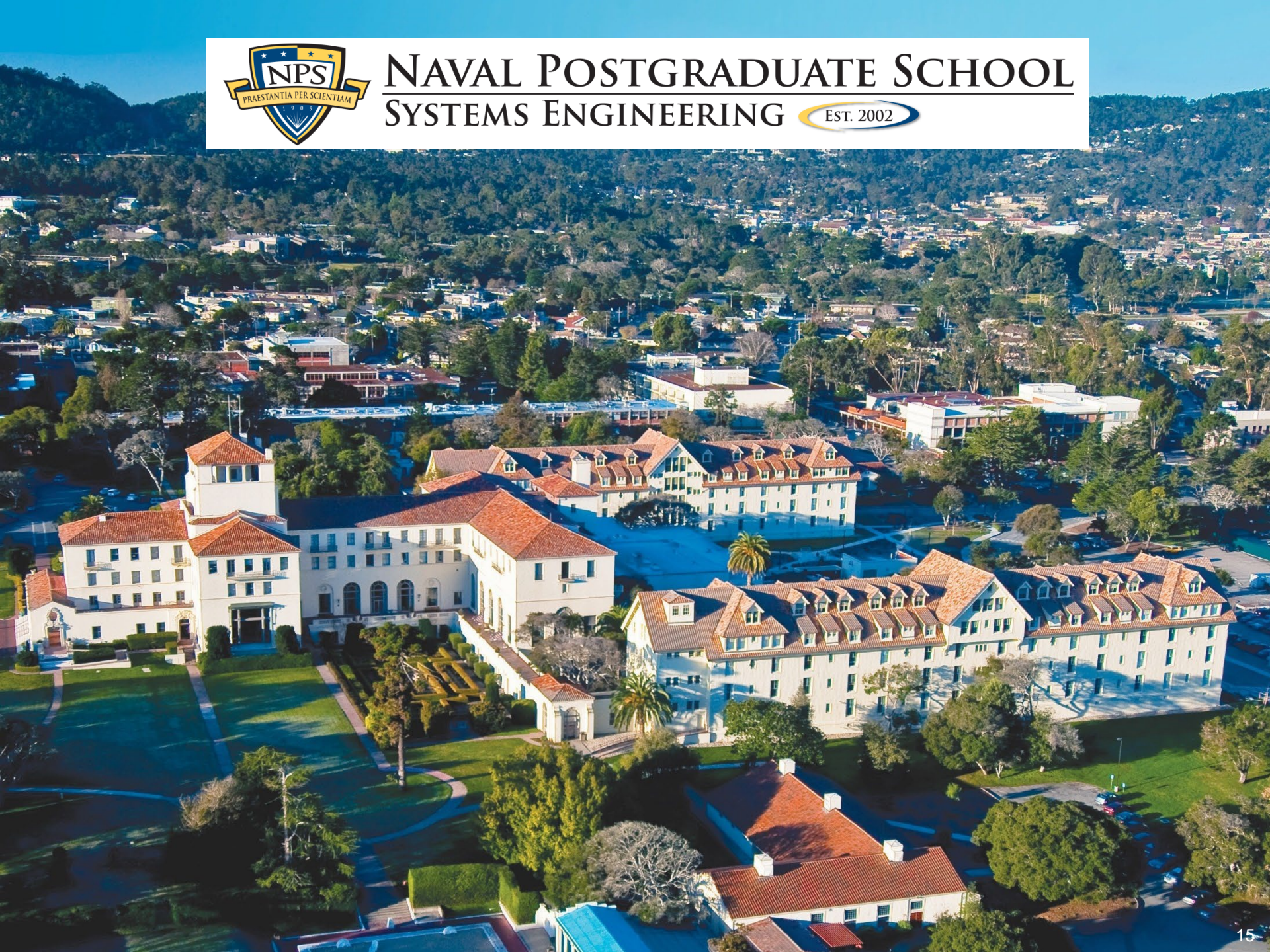
Please Join Us on Thursday for a Follow-on Discussion in the 3D1-DE track
Abstract 24642 – A Common Ontology: The Rosetta Stone for Exchanging Data between Different Digital Engineering Tools, Languages, and Frameworks

Summary

- The 10-Layer Mission Architecture:
  - Shows the continuity of mission-capabilities from strategic objectives to individual systems.
  - Assists in making prioritization and budget decisions based on mission capabilities that are not being addressed or are being overly addressed.
  - Provides a framework for insight and discovery of functions, systems, and services that exists with the mission architecture.
- The 10-Layer Mission Architecture depicts mission data as an “Executive Summary” for detailed analysis performed at lower-levels.






NPS
PRAESTANTIA PER SCIENTIAM
1909
NAVAL POSTGRADUATE SCHOOL
SYSTEMS ENGINEERING
EST. 2002

Operationally Responsive Mission Engineering (ORME)

NDIA

25th Annual Systems and Mission Engineering Conference

November 3, 2022

Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

Operationally Responsive Mission Engineering

The application of

Digital Mission Engineering methods

to current and emerging

US, Allied, threat and commercial systems

operating in designated

areas of interest.

Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

System Digital Twin Ancestry

No Digital Twin

Fleet Enterprise Twin

Classified

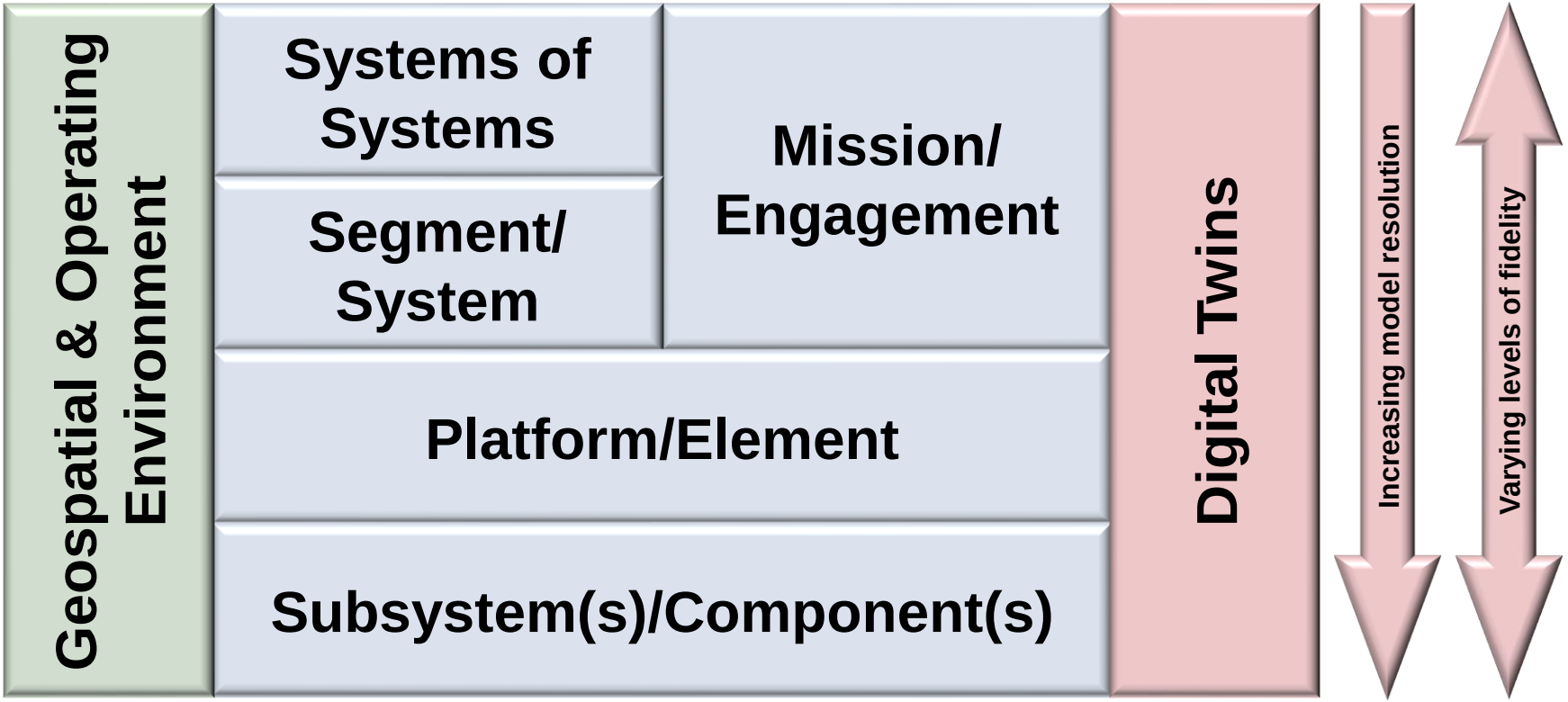
Open Source

Proprietary

Approved for Public Release

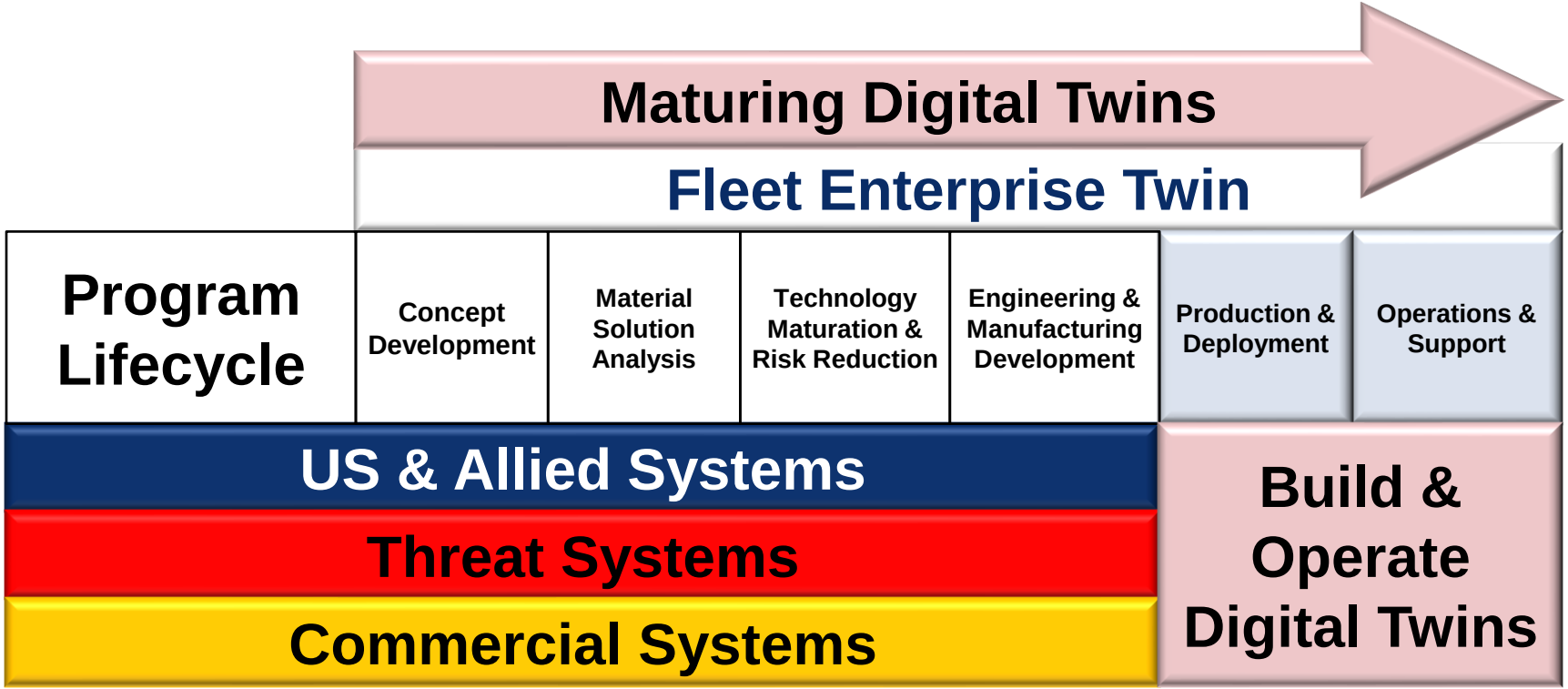
Copyright © 2022 TerraConcepts. All rights reserved.

Mission Model Hierarchy (MMH)



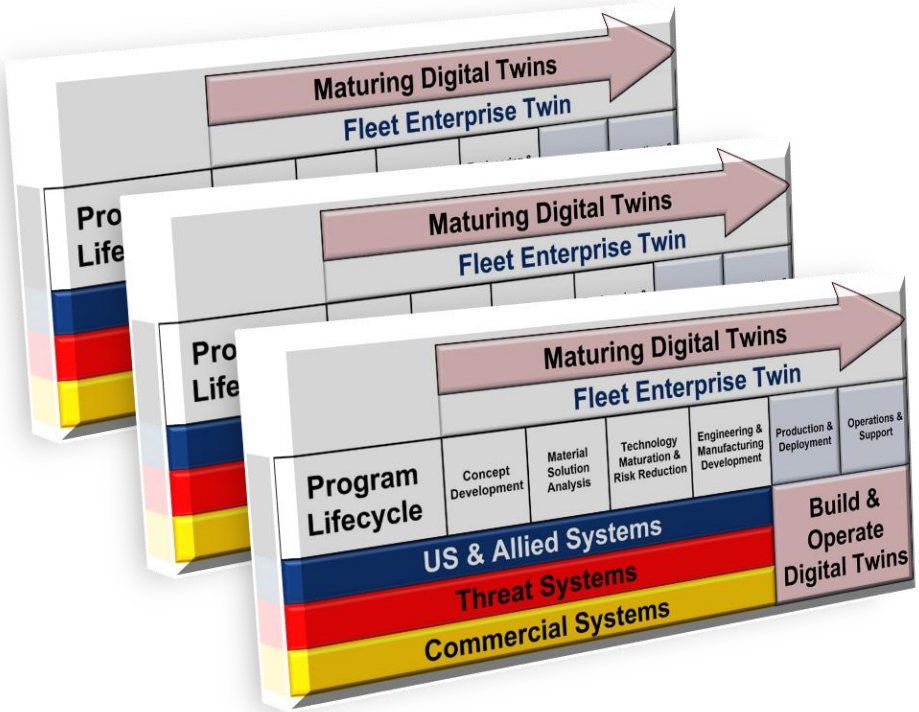
Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

Cradle-to-Grave Digital Mission Engineering



Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

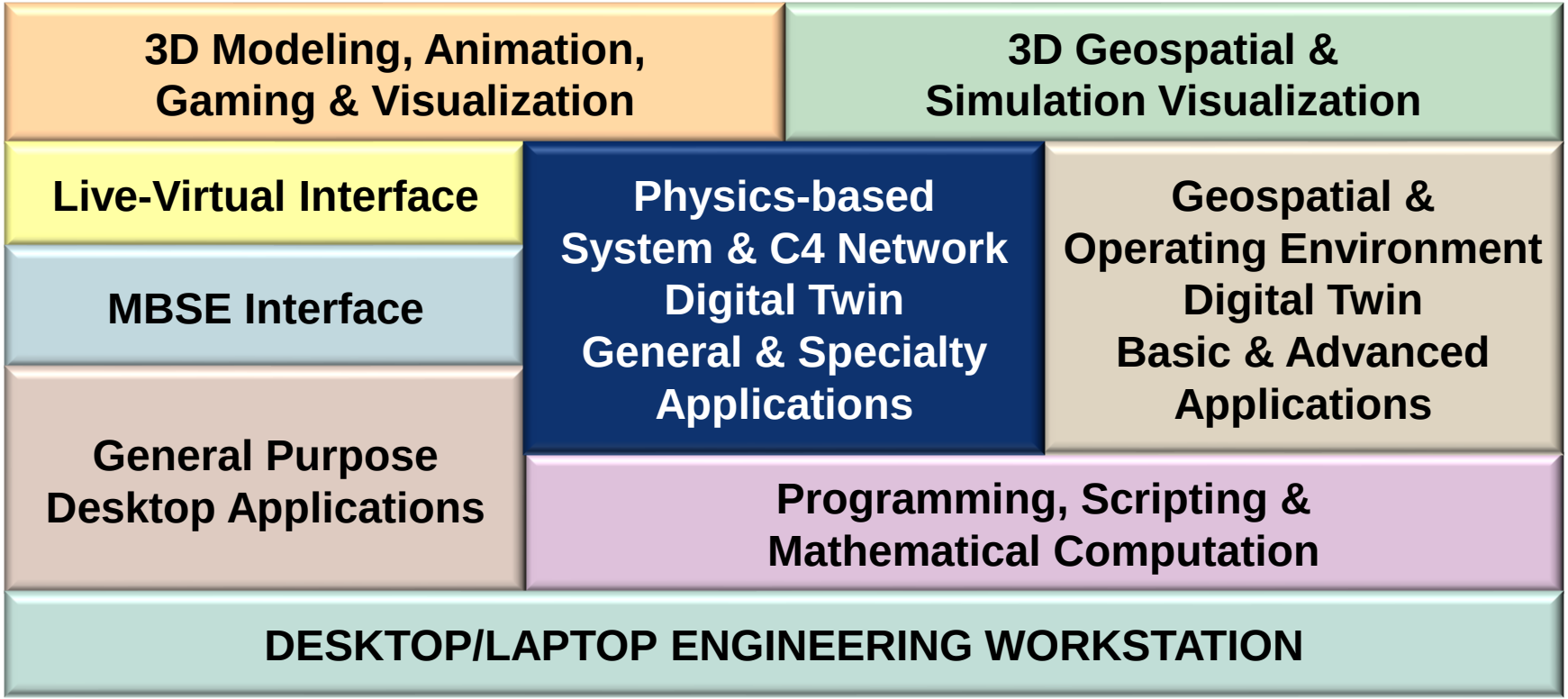
Operationally Responsive Mission Engineering



Approved for Public Release

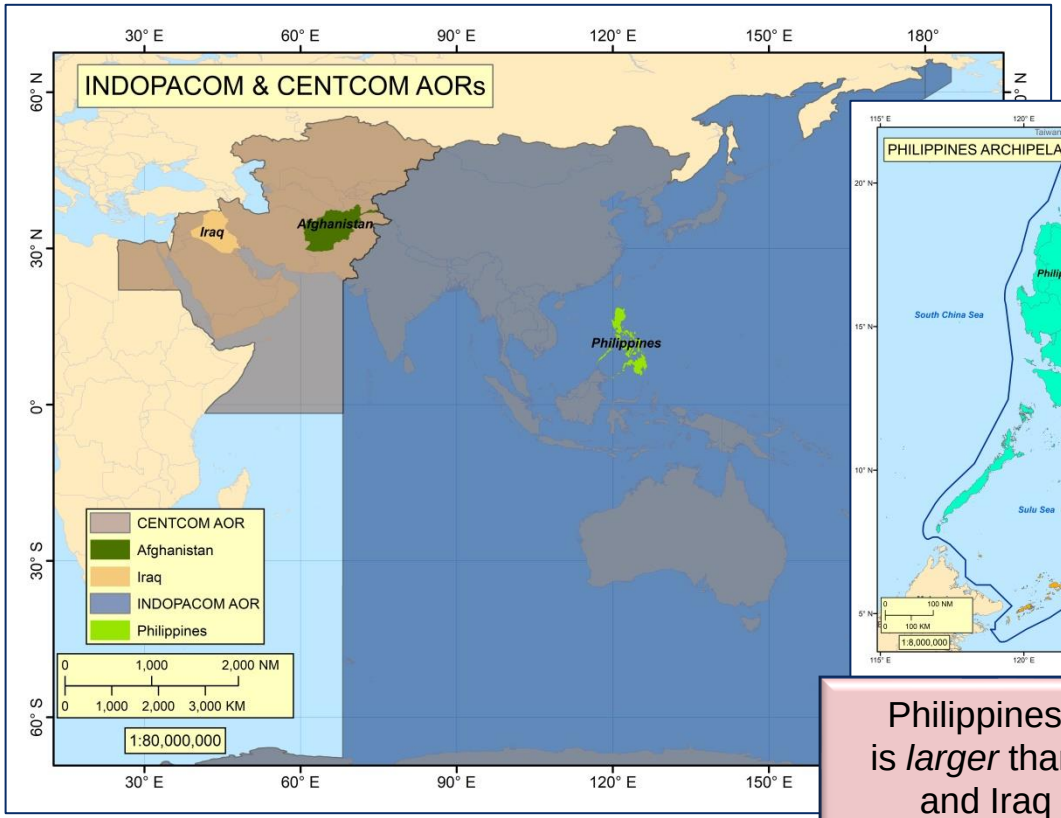
Copyright © 2022 TerraConcepts. All rights reserved.

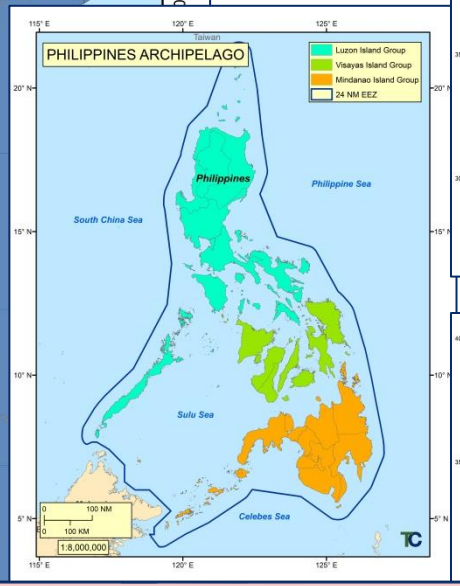
Digital Mission Engineering Environment (DMEE™)

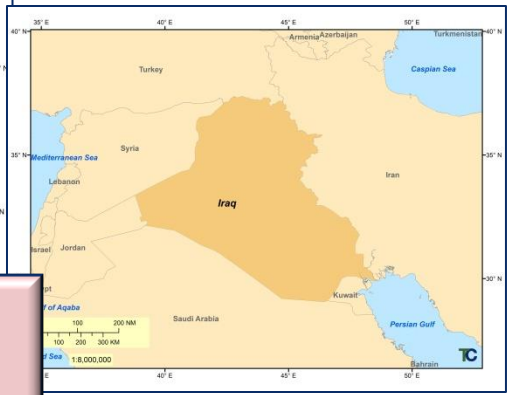


Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

Geospatial Digital Twins: Custom Maps



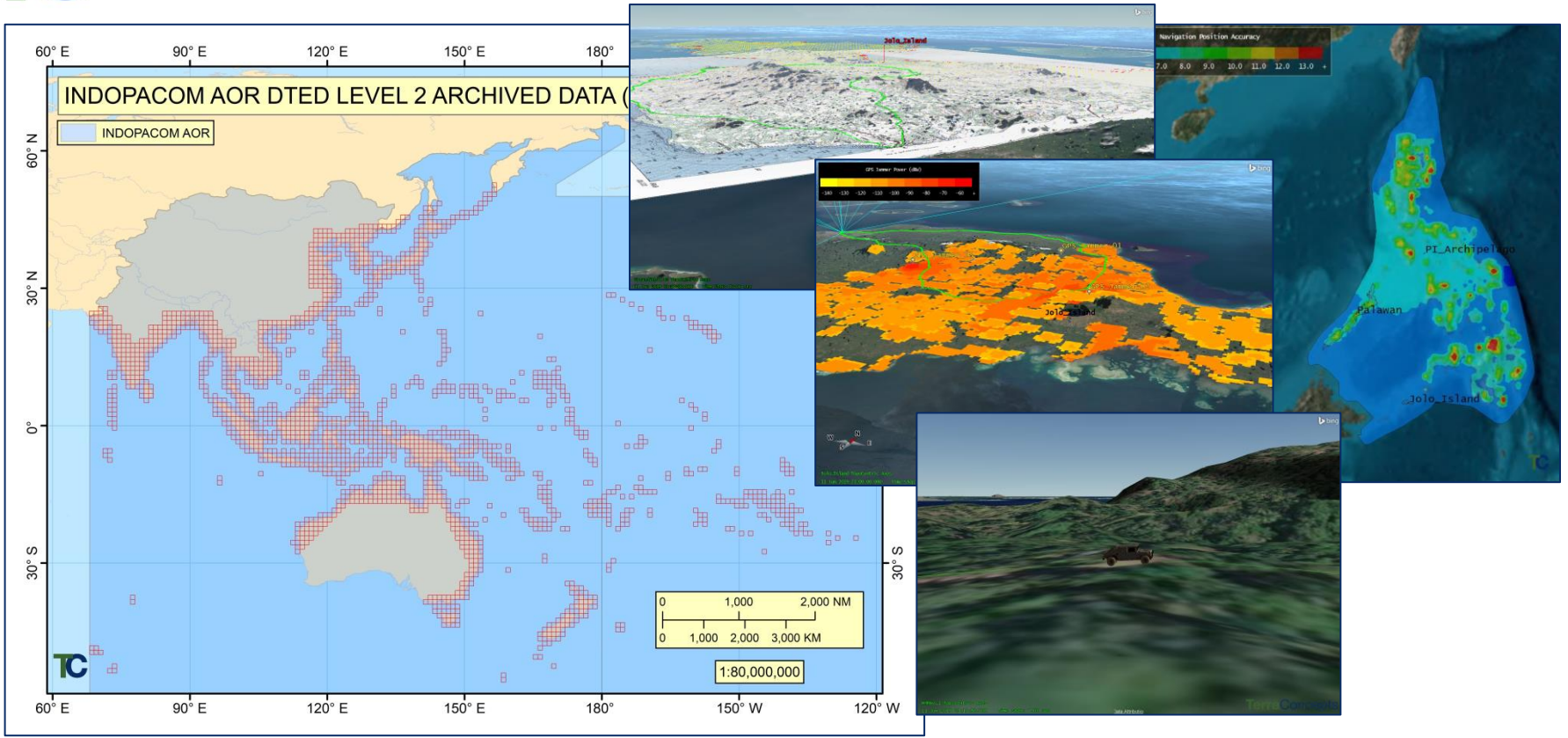




Philippines Archipelago is *larger* than Afghanistan and Iraq *combined*.

Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

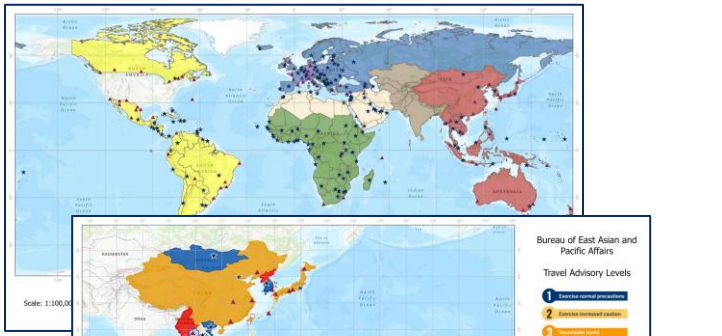
Geospatial Digital Twins: Digital Terrain Data

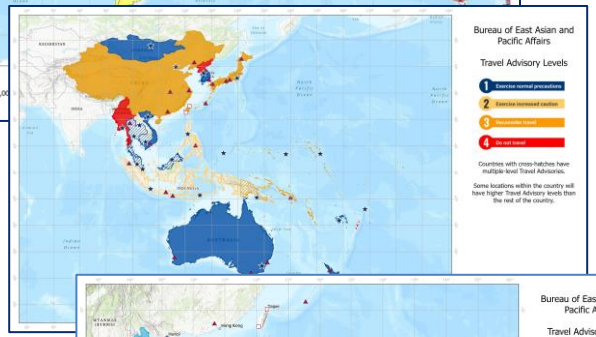


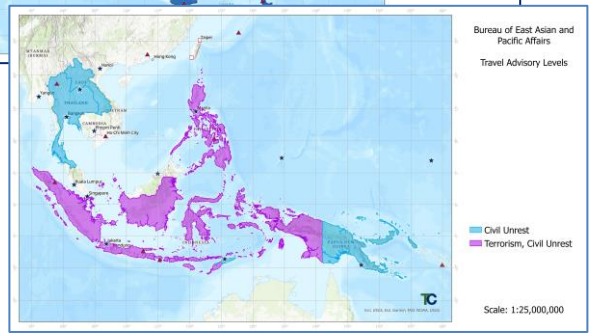
Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

Geospatial Digital Twins: Geospatial Databases







Approved for Public Release

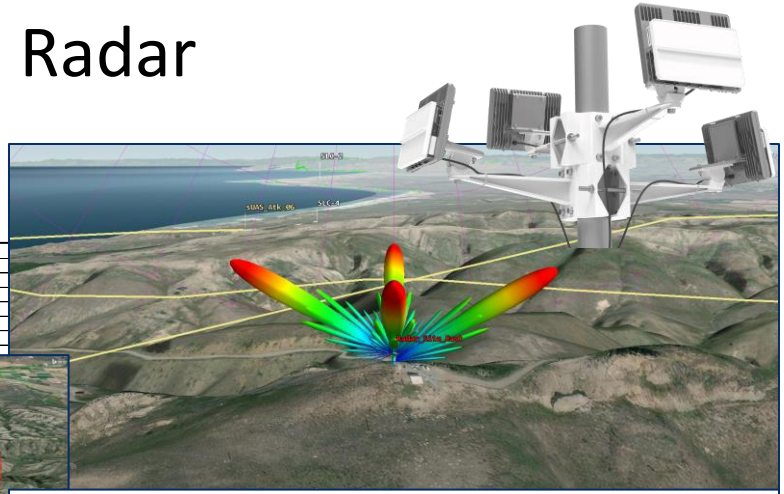
Copyright © 2022 TerraConcepts. All rights reserved.

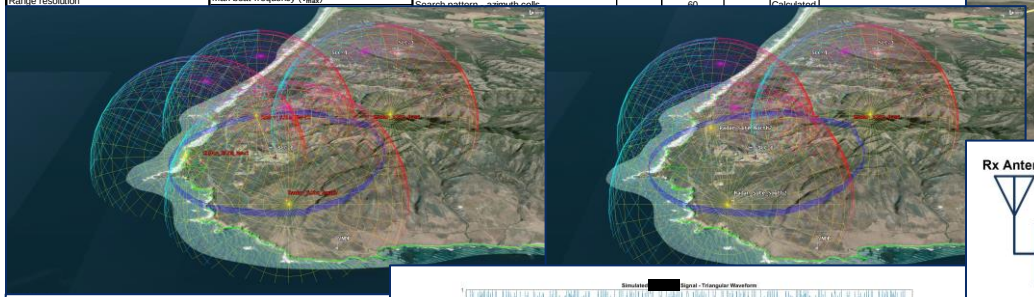
System Digital Twins: FMCW Radar

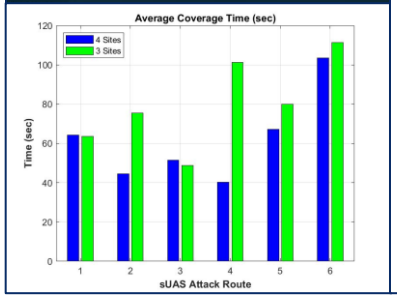
RADAR PARAMETER	SYMBOL	VALUE	UNITS	SOURCE/COMMENTS	
RF band		K		Given	Spec sheet
RF lower end frequency	f_1	24.05	GHz	Given	Spec sheet
RF upper end frequency	$f_$	24.25	GHz	Given	Spec sheet
RF center frequency					
RF Bandwidth					
RF wavelength at center frequency					
FMCW waveform					
Max (Instrumented) range					
Pulse round trip time					
FM bandwidth sweep					
Range resolution					

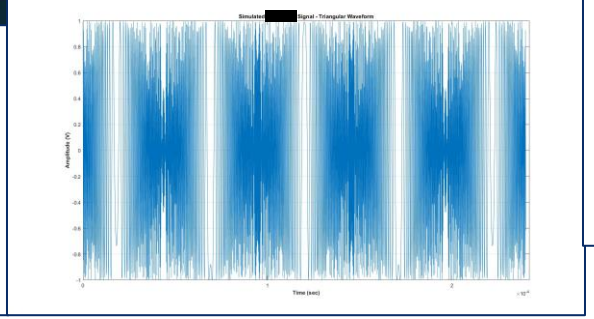
RADAR PARAMETER	SYMBOL	VALUE	UNITS	SOURCE/COMMENTS
Beat frequency max (instrumented) range	$f_{bmax\,rng}$	7.850	MHz	Calculated
Beat frequency/range ratio		1.31	kHz/m	Calculated
Range/beat frequency ratio		0.76	m/kHz	Calculated
Min beat frequency interval				
Target spectral width				
Range resolution limit				
Maximum target speed				
Doppler shift (v_{max})				
Max beat frequency (v_{max})				

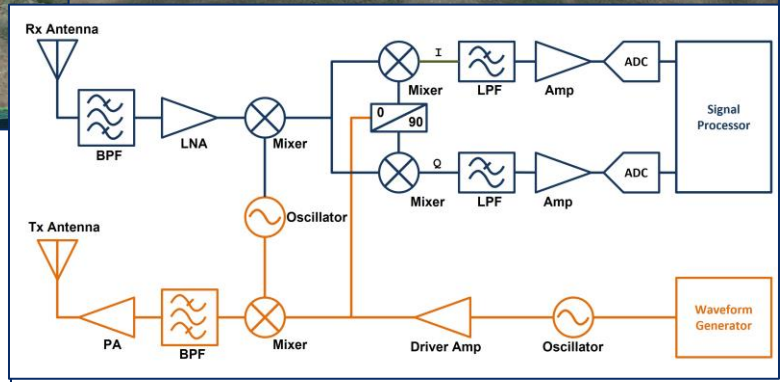
RADAR PARAMETER	SYMBOL	VALUE	UNITS	SOURCE	
Window range resolution (6 dB)		5.76	m	Calculated	
Search update (scan) rate		1	Hz	Given	Spec sheet
Search volume - azimuth		120	deg	Given	Spec sheet
Search volume - elevation		60	deg	Given	Spec sheet
Angular resolution - azimuth		2	deg	Given	Spec sheet
Angular resolution - elevation		6	deg	Given	Spec sheet
Search pattern - azimuth cells		60		Calculated	







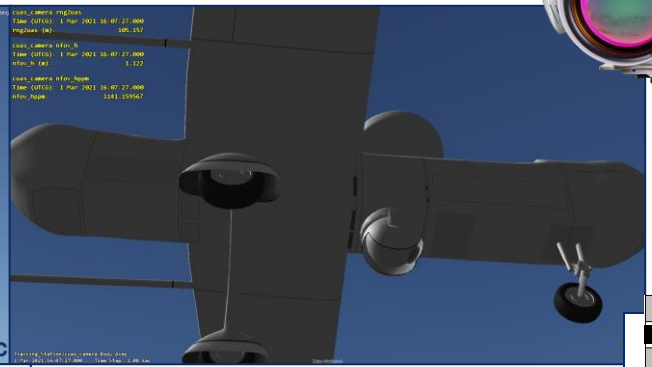


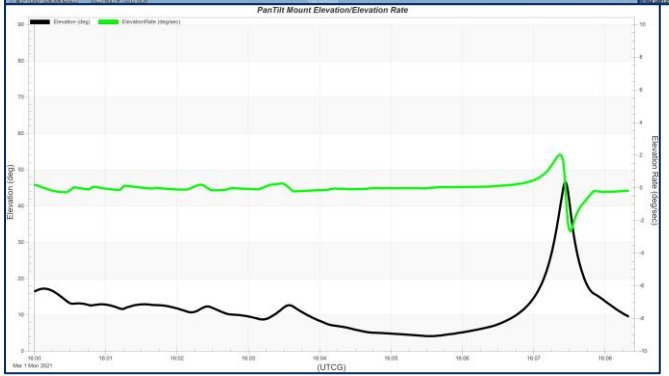


Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

System Digital Twins: EOIR Cameras

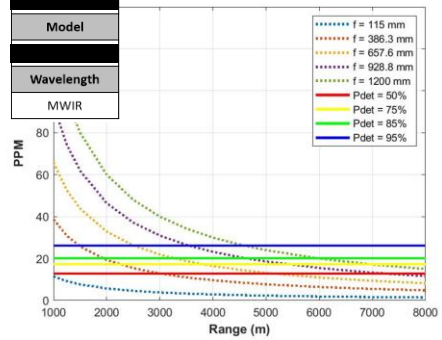




Vendor	[redacted]	Wavelength	Visible/NIR
Model	[redacted]	Sensor	1/2.8" CMOS
Resolution	1920 x 1080	Pixel Pitch	2.9 µm

		FOCAL LENGTH (mm)																								
	PPM_rms	15.4	50.0	137.0	239.0	341.0	443.0	545.0	647.0	749.0	851.0	953.0	1055.0	1157.0	1259.0	1361.0	1463.0	1565.0	1667.0	1769.0	1871.0	1973.0	2075.0	2177.0	2279.0	2381.0	2483.0
RANGE (m)	50	107	346	948	1653	2359	3064	3770	4476	5181	5887	6592	7298	8003	8709	9414	10120	10825	11531	12236	12942	13647	14353	15058	15764	16469
	100	54	173	474	827	1179	1532	1885	2238	2591	2943	3296	3649	4002	4354	4707	5060	5412	5765	6118	6470	6823	7176	7528	7881	8234
	200	27	87	237	413	590	766	942	1119	1295	1472	1648	1824	2001	2177	2353	2530	2706	2883	3059	3236	3412	3589	3765	3941	4118
	300	18	58	158	276	393	511	628	746	864	981	1099	1216	1334	1451	1569	1686	1804	1922	2039	2157	2274	2392	2510	2627	2745
	400	13	43	118	207	295	383	471	559	648	736	824	912	1000	1089	1177	1265	1353	1441	1530	1618	1706	1794	1882	1971	2059
	500	11	35	95	165	236	306	377	448	518	589	659	730	800	871	941	1012	1083	1153	1224	1294	1365	1435	1506	1577	1647
	1000	5	17	47	83	118	153	188	224	259	294	330	365	400	435	471	506	541	577	612	647	682	718	753	788	824
	1250	4	14	38	66	94	123	151	179	207	235	264	292	320	348	377	405	433	461	489	518	546	574	602	630	659
	1500	4	12	32	55	79	102	126	149	173	196	220	243	267	290	314	337	361	384	408	431	455	478	502	525	549
	2000	3	9	24	41	59	77	94	112	130	147	165	182	200	218	235	253	271	288	306	324	341	359	377	394	412
	2500	2	7	19	33	47	61	75	90	104	118	132	146	160	174	188	202	217	231	245	259	273	287	301	315	329
	3000	2	6	16	28	39	51	63	75	86	98	110	122	133	145	157	169	180	192	204	216	227	239	251	263	274
	3500	2	5	14	24	34	44	54	64	74	84	94	104	114	124	134	145	155	165	175	185	195	205	215	225	235
	4000	1	4	12	21	29	38	47	56	65	74	82	91	100	109	118	127	135	144	153	162	171	179	188	197	206

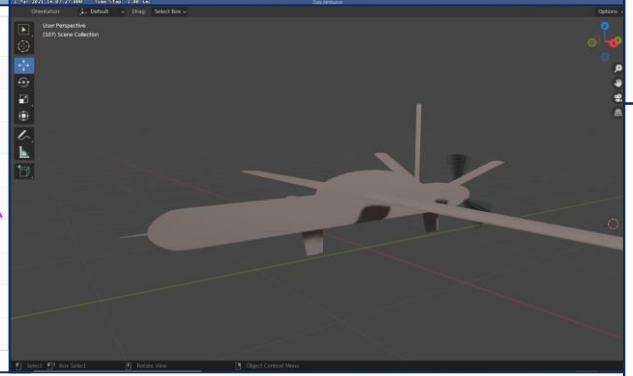
Vendor	[redacted]
Model	[redacted]
Wavelength	MWIR



Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

System Digital Twins: Threat Systems



SCIENCE & GLOBAL SECURITY
https://doi.org/10.1080/08929882.2020.1846279

Routledge
Taylor & Francis Group

Check for updates

Flight Performance Analysis of the Samad Attack Drones Operated by Houthi Armed Forces

Mark Voskuijl, Thomas Dekkers, and Ralph Savelsberg

Faculty of Military Sciences, Netherlands Defence Academy, Den Helder, The Netherlands

ABSTRACT

In recent years, there has been a large increase in the use of

Figure 1. Reconstruction of Samad-2, length of 2.80 m (left); Samad-1 including details of the airfoil shape at the wing root (right).[15]

Figure 2. Motor and propeller (left); Samad-3 (front) and Samad-1 (back) on a display in Sana'a Yemen (right).[16]

170 engine. The Samad-3, with an external fuel tank mounted on top of fuselage, can be seen in Figure 2

Figure 3. Close-up of Samad-1 (in Figure 1) showing the wing root airfoil (left); NACA 23018 airfoil and NACA 23009 (right).

Figure 4. Schematic representation of the Samad-2 and Samad-3. The external fuel tank on the Samad-3 is indicated with a dashed line. The dash-dotted line in the front view on the top left

Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

Takeaways

- ORME
  - Multi-domain, multi-functional
  - US, Allied, threat & commercial systems
  - Deployment, Operations & Support
- ORME Team
  - Task organized around core team of engineers, analysts, modelers, and operators
- Analysis & visualization work products driven by requirements
  - CONOPS
  - Trade Studies
  - Test & Evaluation
  - Site Surveys
  - Wargaming & Exercises
- Geospatial digital twins essential to ORME

Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

Questions?

Approved for Public Release

Copyright © 2022 TerraConcepts. All rights reserved.

Definitions

- Mission Engineering: the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects (Defense Acquisition Guidebook)
- Digital Mission Engineering (DME): a Digital Engineering approach using digital modeling, simulation, analysis and visualization (MSAV) to create physics-based system, geospatial and operating environment digital twins
- System Digital Twin: a virtual representation of a [connected] physical asset (AIAA/AIA White Paper)
- Geospatial Digital Twin: a virtual representation of the natural and built environments (ESRI)
- Operationally Responsive Mission Engineering (ORME): the application of DME methods to current and emerging US, Allied, threat and commercial systems operating in designated areas of interest (AOI)

Approved for Public Release
Copyright © 2022 TerraConcepts. All rights reserved.

USD(R&E)

Software Assurance Roadmap

Mr. Steve Grice
Technical Director, Software Assurance

Mr. Bradley Lanford
SAIC Contractor Support

Science and Technology Program Protection
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Software Assurance

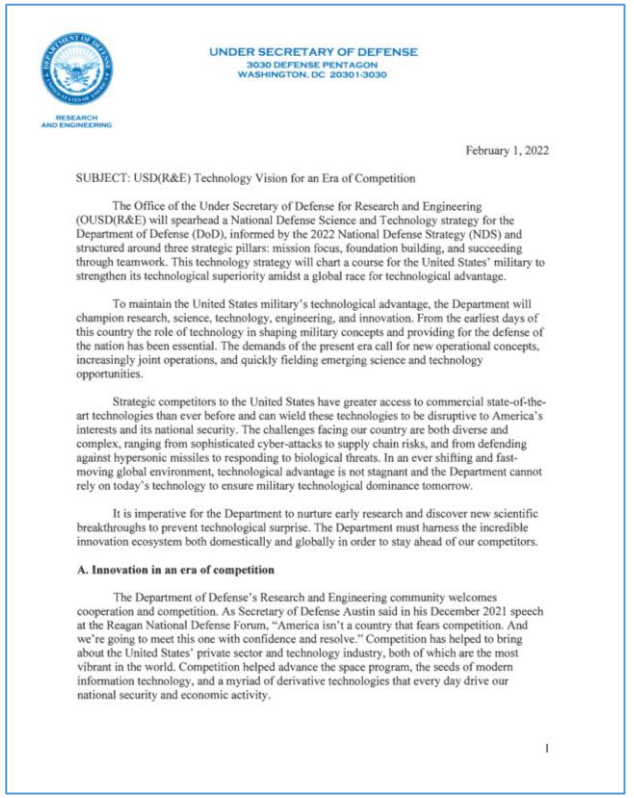
- **Software Assurance (SwA):**
  - *The level of confidence that software functions only as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle*
    - PL112–239, JAN. 2, 2013, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, Section 933

- **Activities to Date**
  - Development of policies, instructions, guides, and standards to promote best practices
  - Joint Federated Assurance Center (JFAC)
  - JFAC Technical Working Group Community
  - DoD/National Nuclear Security Administration (NNSA) Software Assurance Community of Practice
  - Partnerships with Department of Homeland Security, NNSA, National Security Agency, and Industry thru NDIA

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Strategic Vision

Ms. Heidi Shyu, Under Secretary of Defense for Research and Engineering, released *"Technology Vision for an Era of Competition,"* (dated February 1, 2022) to provide guidance on those areas needing further technology investments.



UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH AND ENGINEERING

February 1, 2022

SUBJECT: USD(R&E) Technology Vision for an Era of Competition

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E) will spearhead a National Defense Science and Technology strategy for the Department of Defense (DoD), informed by the 2022 National Defense Strategy (NDS) and structured around three strategic pillars: mission focus, foundation building, and succeeding through teamwork. This technology strategy will chart a course for the United States' military to strengthen its technological superiority amidst a global race for technological advantage.

To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities.

Strategic competitors to the United States have greater access to commercial state-of-the-art technologies than ever before and can wield these technologies to be disruptive to America's interests and its national security. The challenges facing our country are both diverse and complex, ranging from sophisticated cyber-attacks to supply chain risks, and from defending against hypersonic missiles to responding to biological threats. In an ever shifting and fast-moving global environment, technological advantage is not stagnant and the Department cannot rely on today's technology to ensure military technological dominance tomorrow.

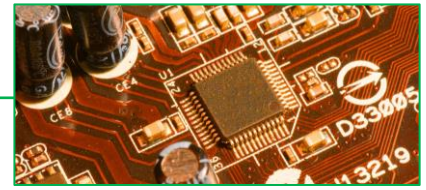
It is imperative for the Department to nurture early research and discover new scientific breakthroughs to prevent technological surprise. The Department must harness the incredible innovation ecosystem both domestically and globally in order to stay ahead of our competitors.

A. Innovation in an era of competition

The Department of Defense's Research and Engineering community welcomes cooperation and competition. As Secretary of Defense Austin said in his December 2021 speech at the Reagan National Defense Forum, "America isn't a country that fears competition. And we're going to meet this one with confidence and resolve." Competition has helped to bring about the United States' private sector and technology industry, both of which are the most vibrant in the world. Competition helped advance the space program, the seeds of modern information technology, and a myriad of derivative technologies that every day drive our national security and economic activity.

Strategic Vision *(continued)*

- **Critical Technology Areas**
  - Effective Adoption Areas
    - Trusted AI and Autonomy
    - Integrated Network Systems-of-Systems
    - Microelectronics
    - Space Technology
    - Renewable Energy Generation and Storage
    - Advance Computing and Software
    - Human-Machine Interfaces
  - Seed Areas of Emerging Opportunity
    - Biotechnology
    - Quantum Science
    - Future Generation Wireless Technology (FutureG)
    - Advance Materials
  - Defense-Specific Areas
    - Directed Energy
    - Hypersonics
    - Integrated Sensing and Cyber



Strategic Vision *(continued)*

- **Current, Ongoing, and Relevant Topics**
  - Software Bill of Materials (SBOM)
    - Executive Order 14028, “Improving the Nation’s Cybersecurity”
    - FY19 NDAA Section 1655: Mitigation of risks from disclosure to foreign adversaries
    - Enduring Security Framework, Securing the Software Supply Chain
  - DevSecOps
    - DoD Instruction 5000.83, Technology and Program Protection, Program Protection Planning Outline and Guidance alignment with software modernization efforts
    - Identifying best practice for automation of SwA methods and practices
  - Existing Tool Maturation
    - Coordination with vendors, S&T organizations, and Service labs
    - PD Cyber and LLNL collaboration to evaluate tool landscape
  - Software Assurance Metrics
    - Development of metrics to support policy and guidance implementation
    - Nuclear Enterprise Assurance Workshop Metrics Track

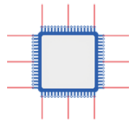
Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Software Assurance Roadmap

SwA Gap Areas FY2022	Focus Areas FY 2023 – 2025			Outcomes 2026 - 2030
Protecting Emerging Technologies	Embedded SW	AI & Autonomy	Quantum	Perform research, develop SwA guidance, and identify gaps for emerging technology areas
Maturing Existing Capabilities	SwA Toolset	Workforce	Metrics	Advance SwA tools, workforce, and performance metrics within DoD programs
Securing SW Development	SBOM	DevSecOps	Open Source	Promote SwA best practice and provide guidance for DoD SW modernization areas
Advancing the State of Practice	Partnerships	SwA Platform	S&T Innovation	Achieve state of the art capabilities through partnerships and investment in S&T
Policy, Guidance & Standards				

Software Assurance Roadmap
Emerging Technologies

Emerging Technology	Current Efforts	Short Term	Future
Embedded SW 	**Gap: Limited Capability to analyze embedded SW** NSA leading Hardware / Software Assurance Pilot	Identify capability gaps in labs ability to analyze embedded SW Document existing SW analysis and mitigation capabilities	**Goal: Alignment of HW/SW protections for critical microelectronics**
AI & Autonomy	**Gap: Limited understanding of SwA impacts and protections for AI & autonomy**	Research and whitepapers on SW protections for AI/autonomy SwA for AI / Autonomy Pilot Program	Updates to AI /autonomy whitepapers based on Pilot **Goal: Define SwA best practice for AI and autonomy**
Quantum	**Gap: Limited understanding of SwA impacts and protections for quantum**	Research and whitepapers on SW protections for quantum	SwA for Quantum Pilot Program **Goal: Define SwA best practice for quantum**
Additional technologies added as prioritized by USD(R&E)			

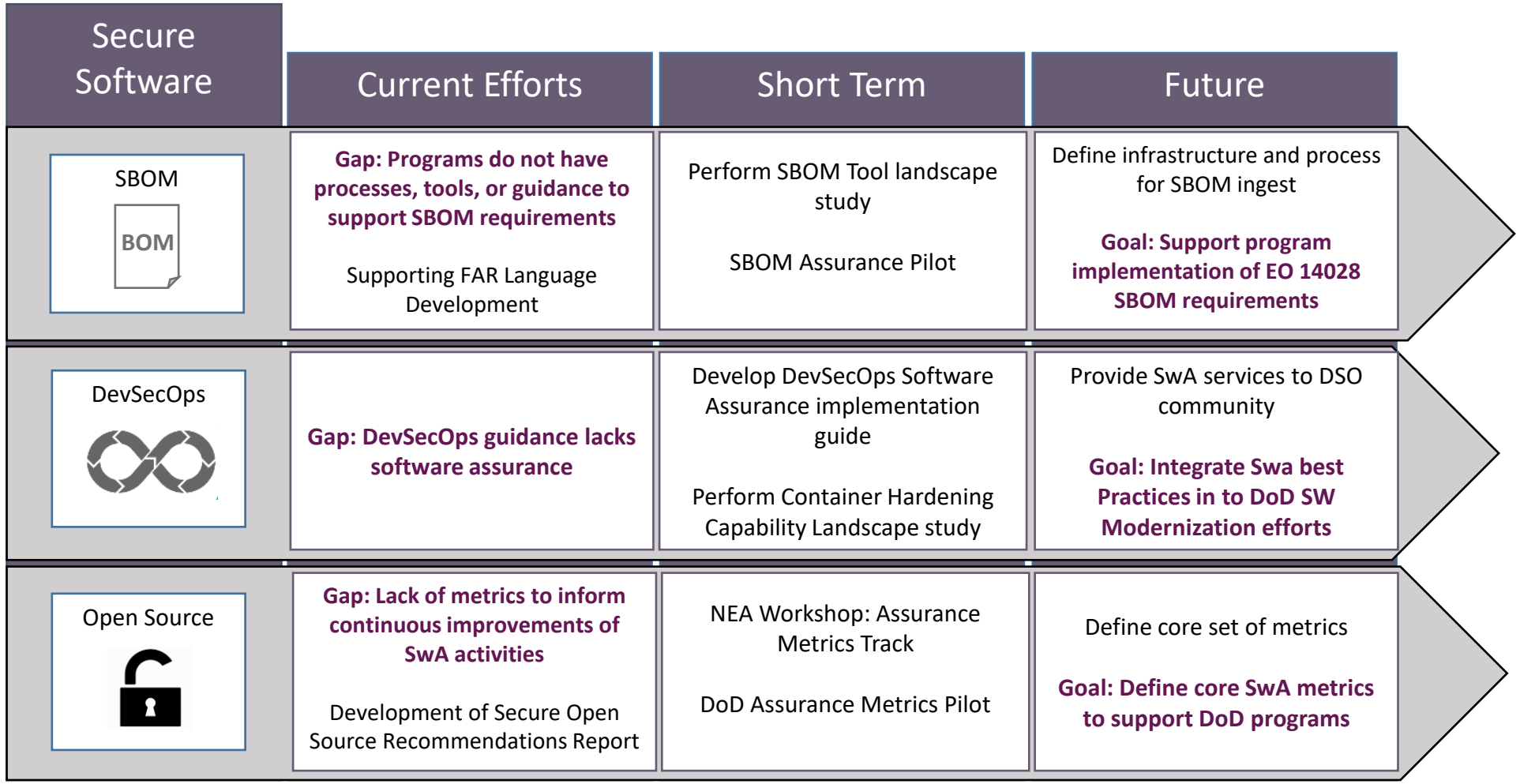
Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Software Assurance Roadmap
Maturing Existing Capabilities

Capability Elements	Current Efforts	Short Term	Future
SwA Toolset	**Gap: Programs do not have access to SwA tools to inform decision making and support analysis**	Perform SwA tool and capability landscape study Define process for SwA tool selection and assessment process	Recommend and implement plan to make identified SwA tools accessible **Goal: Inform program tool selection**
Workforce	**Gap: Existing SwA expertise is limited and DoD lacks training for future growth**	Develop DAU SwA Credential	Inclusion of SwA best practices in SW and cyber training **Goal: Grow SwA expertise to support program needs**
Metrics	**Gap: Lack of metrics to inform continuous improvements of SwA activities**	NEA Workshop: Assurance Metrics Track DoD Assurance Metrics Pilot	Define core set of metrics **Goal: Define core SwA metrics to support DoD programs**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Software Assurance Roadmap
Securing Software Development



Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Software Assurance Roadmap
Advancing the State of Practice

Advancement Opportunities	Current Efforts	Short Term	Future
Partnerships	**Gap: DoD is not fully aligned with UGA on assurance approach and sharing** NEW Workshop & DoD/NNSA SwA CoP	Develop Joint SwA Roadmap with DHS S&T, NSA, & NNSA	**Goal: Align DHS S&T, NSA, & NNSA Assurance efforts to raise assurance posture across departments**
SwA Platform	**Gap: SwA Resources have limited access to expertise and tools required to support programs** Developing AoA for hosting of JFAC infrastructure	Deploy MVP of JFAC Infrastructure to support SwA analysis and tools Prioritize SwA tool offerings and develop timeline	**Goal: Provide comprehensive SwA services to DoD programs**
S&T Innovation	**Gap: DoD lacks awareness of and infrastructure to transition assurance S&T** Coordination with DoD Assurance S&T organizations	Complete Assurance S&T Landscape Study Develop Investment Recommendations Report	Pilot assurance S&T transition **Goal: Make S&T assurance capabilities available early to programs**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Summary

- **Ms. Shyu's memo, "Technology Vision for an Era of Competition," provides clarity, intention, and direction for the future of the Office of the Secretary of Defense for Research and Engineering.**

- **DoD has seen great success with SwA tools, policies, instructions, and guidelines developed and provided to our community. However, the landscape is always changing:**
  - Introduction of new development techniques and tools
  - Discovery of new vulnerabilities
  - Maturing S&T capabilities

- **DoD is looking for input and feedback from NDIA and Industry on how to best address the tools of today and emerging technologies to ensure the U.S. warfighter's ability to counter threats both today and into the future.**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

Questions

Steven Grice

Technical Director, Software Assurance

Office of the Under Secretary of Defense
for Research and Engineering

steven.a.grice.civ@mail.mil

Bradley Lanford

SAIC Contractor Support

Office of the Under Secretary of Defense
for Research and Engineering

bradley.p.lanford.ctr@mail.mil

Distribution Statement A: Approved for public release. DOPSR case #23-S-0065 applies. Distribution is unlimited.

USD(R&E)

Software Assurance through DevSecOps

Mr. Bradley Lanford
SAIC Contractor Support
Science and Technology Program Protection
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Software Assurance in DevSecOps

- **The DoD has rapidly transitioned to DevSecOps (DSO) in an effort to deliver software at the speed of relevance. Software modernization efforts include:**
  - Standup of approximately 30 organizations providing infrastructure and platform services to programs
  - Updates to Adaptive Acquisition Framework (AAF) policy and supporting guidance
  - Issued DoD Instruction 5000.87 Operation of the Software Acquisition Pathway supporting DoD adoption of DSO
  - Publication of standards and best practices to support program implementation

- **The DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," requires programs to employ system security engineering methods and practices, including software assurance (SwA), commensurate with technology, program, system, and mission objectives**
  - OUSD(R&E) STPP is currently updating the Program Protection Planning Outline and Guidance (PPP O&G) to reflect changes to the 5000.83 and support software modernization objectives
  - The automation of manual assurance processes and standardization of risks processes continue to challenge the effectiveness of SwA implementation

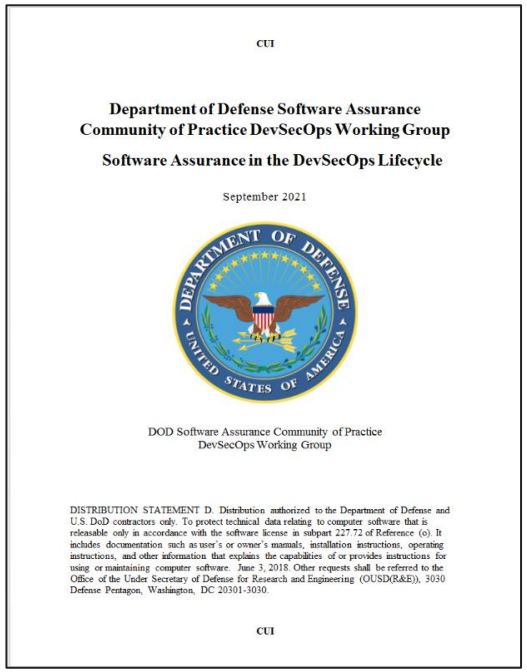
- **As DevSecOps capabilities mature, the Department and industry partners must ensure the implementation of DevSecOps supports both the broad application of SwA practices and can be tailored to protect critical software**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

SwA in DevSecOps

Completion of SwA in DevSecOps whitepaper with DoD/NNSA Software Assurance Community of Practice

Alignment of software assurance practices with the DevSecOps lifecycle and generation of artifacts to support decisions



CUI

Department of Defense Software Assurance Community of Practice DevSecOps Working Group

Software Assurance in the DevSecOps Lifecycle

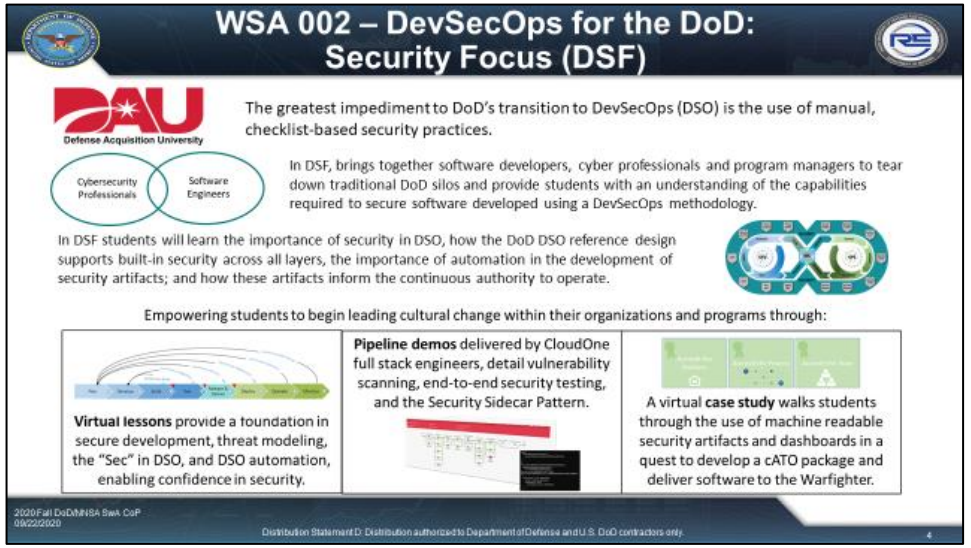
September 2021

DOD Software Assurance Community of Practice
DevSecOps Working Group

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only. To protect technical data relating to computer software that is releasable only in accordance with the software license in subpart 227.72 of Reference (o). It includes documentation such as user's or owner's manuals, installation instructions, operating instructions, and other information that explains the capabilities of or provides instructions for using or maintaining computer software. June 3, 2018. Other requests shall be referred to the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), 3030 Defense Pentagon, Washington, DC 20301-3030.

CUI

Development of DAU WSA 002 – DevSecOps for the DoD: Security Focus (DSF)



WSA 002 – DevSecOps for the DoD: Security Focus (DSF)

Defense Acquisition University

The greatest impediment to DoD's transition to DevSecOps (DSO) is the use of manual, checklist-based security practices.

Cybersecurity Professionals | Software Engineers

In DSF, brings together software developers, cyber professionals and program managers to tear down traditional DoD silos and provide students with an understanding of the capabilities required to secure software developed using a DevSecOps methodology.

In DSF students will learn the importance of security in DSO, how the DoD DSO reference design supports built-in security across all layers, the importance of automation in the development of security artifacts; and how these artifacts inform the continuous authority to operate.

Empowering students to begin leading cultural change within their organizations and programs through:

Virtual lessons provide a foundation in secure development, threat modeling, the "Sec" in DSO, and DSO automation, enabling confidence in security.

Pipeline demos delivered by CloudOne full stack engineers, detail vulnerability scanning, end-to-end security testing, and the Security Sidecar Pattern.

A virtual **case study** walks students through the use of machine readable security artifacts and dashboards in a quest to develop a cATO package and deliver software to the Warfighter.

2020 Fall DoD/NNSA SwA CoP
09/22/2020

Distribution Statement D: Distribution authorized to Department of Defense and U.S. DoD contractors only.

Software Assurance Gaps 2020

Hardened Container SRG

Existing DevSecOps service provider capabilities use automated scanning (OpenSCAP, Anchor, Twistlock) focusing on cybersecurity STIG and known vulnerability assessments. Opportunity for enhanced assurance capabilities.

Assurance Baseline and critical function assessments

Pipeline adoption continues to utilize a small subset of assurance tools and lacks consideration of raised assurance level for critical components.

Software Threat Modeling

Iterative threat modeling established through development process and cadence. Limited automation and MBSE maturity to support CI/CD.

Analysis Data Strategy

Correlation of analysis findings and data strategy for pipeline data artifacts impact programs ability to effectively use assurance tools.

Risk Categorization/Tolerance

Standard process for risk categorization and process to establish risk tolerance based on assurance level does not exist. Does not support

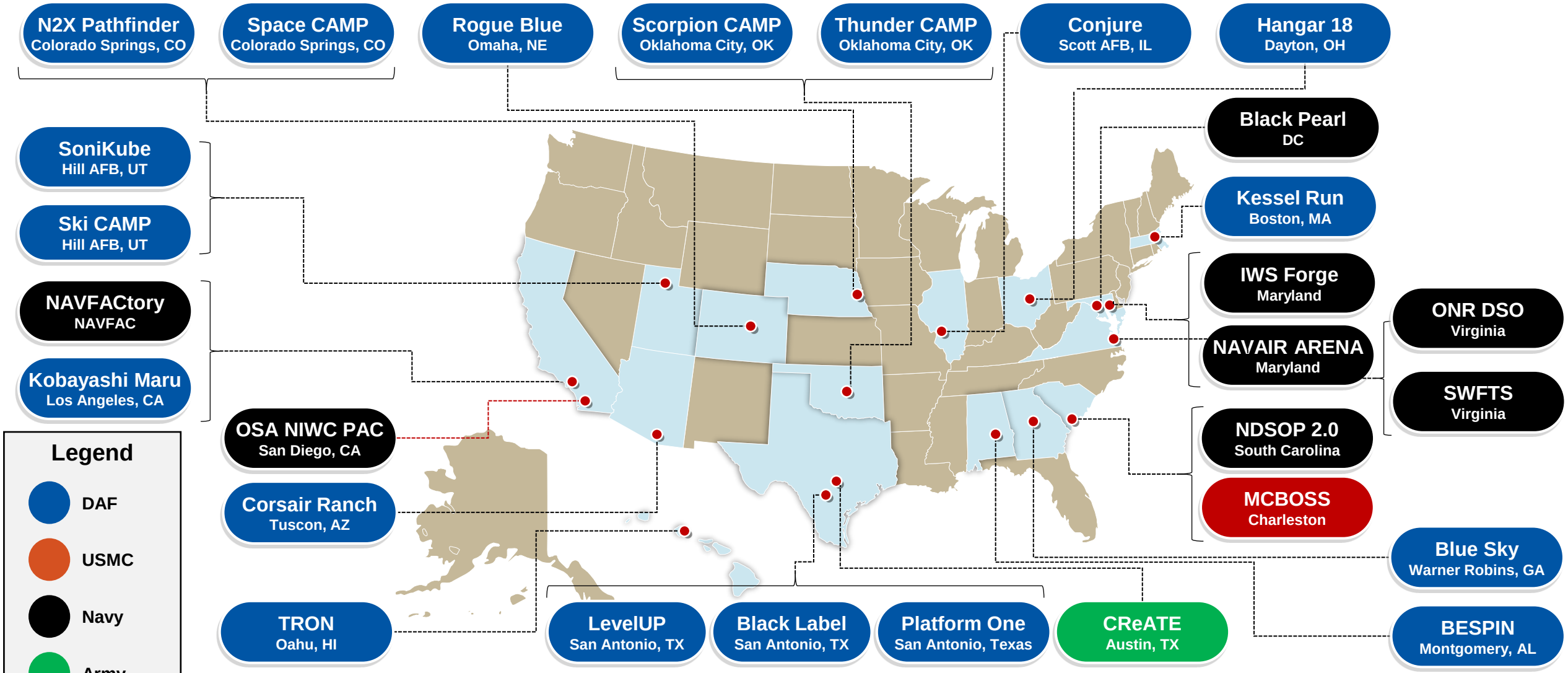
Open Source Assurance

Limited understanding of Software Supply Chain for Open Source and COTS continues to be a source of risk.

The automation of manual assurance processes and standardization of risks processes impede SwA adoption for DSO

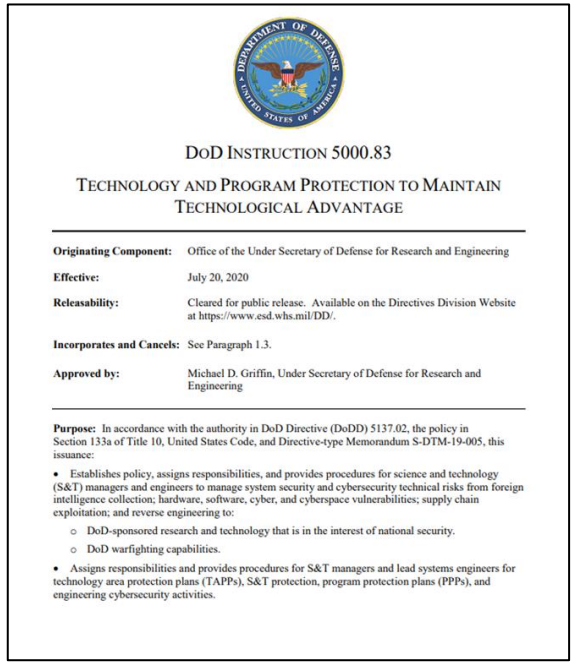
Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Scope of DevSecOps in the DoD



Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

DoDI 5000.83 Technology and Program Protection



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

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

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- 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 to:
  - 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.

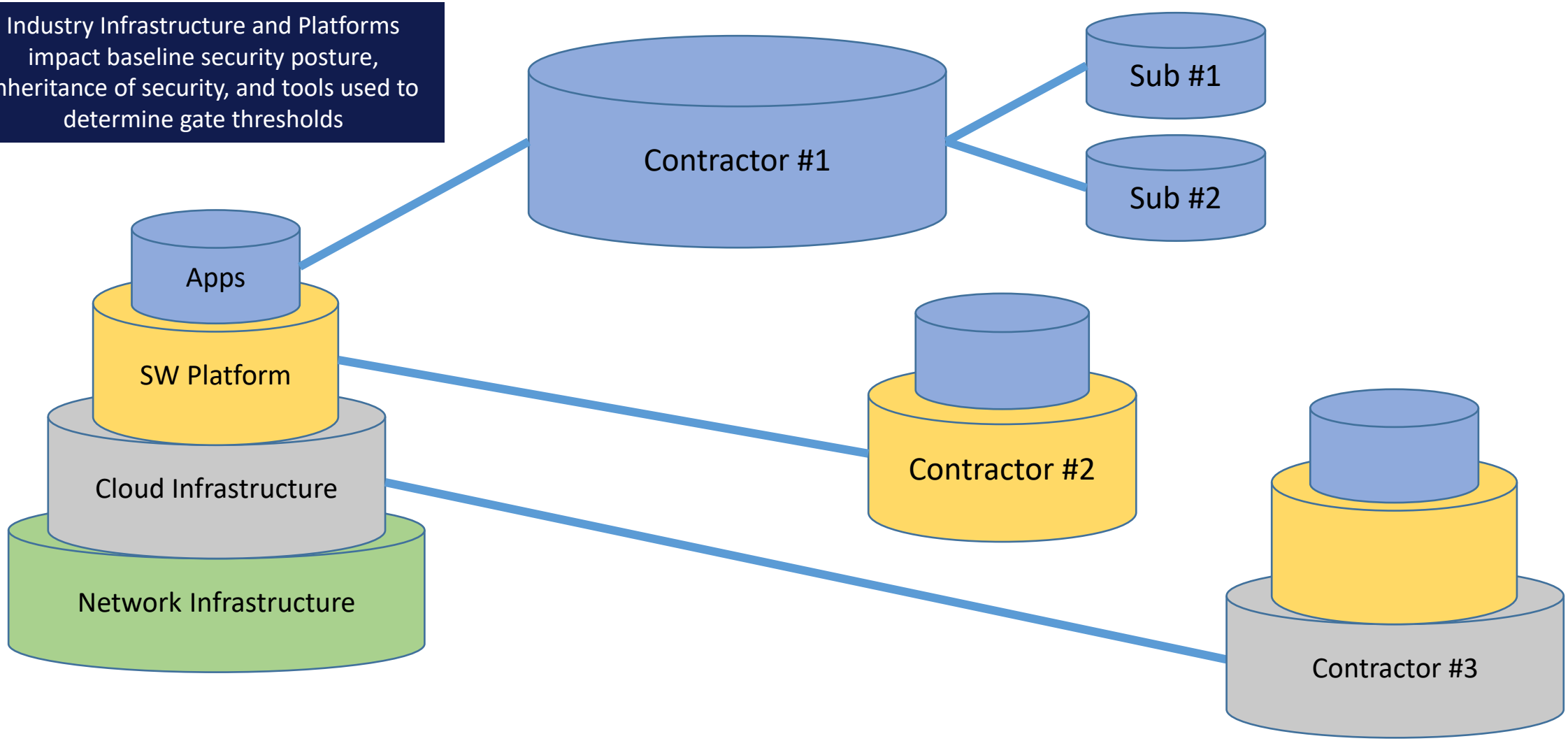
DoDI 5000.83, “Technology and Program Protection to Maintain Technological Advantage”

Programs will employ **system security engineering methods and practices**, including cybersecurity, cyber resilience, and cyber survivability in design, test, manufacture, and sustainment. Such methods and practices will ensure that systems function as intended, mitigating risks associated with **known and exploitable vulnerabilities** to provide a **level of assurance** commensurate with technology, program, system, and mission objectives.

Selection of DevSecOps tools supporting program protection must be informed by technology, program, system, and mission objectives

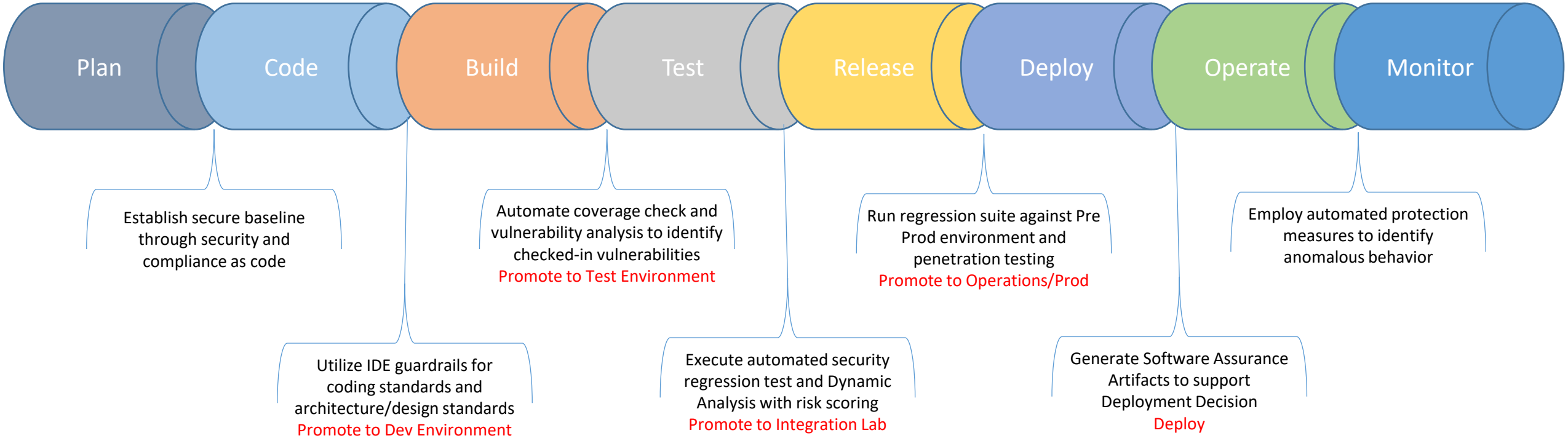
Relationship to Industry Partners (Infrastructure and Platform)

Industry Infrastructure and Platforms impact baseline security posture, inheritance of security, and tools used to determine gate thresholds



Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

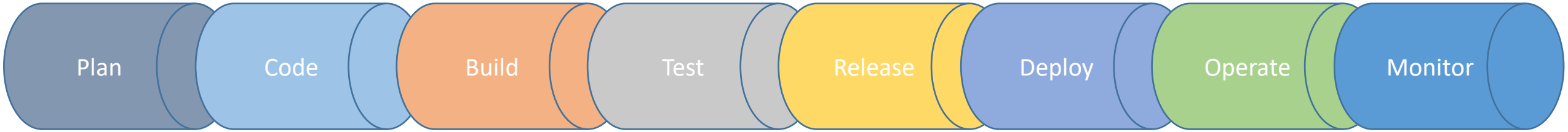
SwA in the CI/CD pipeline



CI/CD automation establishes gates where assurance thresholds can be evaluated prior to promotion of software builds. Vulnerabilities can delay deployment, or risk can be accepted and tracked.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

SwA Tool Mapping to DSO



FOSSID
JUnit 5
IDA Pro
splunk>
JIRA
ANSIBLE
Cucumber
Supported by SMARTBEAR
DEPENDENCY-CHECK
clair
sonarqube
Flawfinder
terrascan by tenable
Kibana
GitLab
GO Vet
JFrog
SPDX
pytest
VERACODE
aqua
CodeDx
Grafana
IJ
APACHE ANT
Visual Studio
FORTIFY
COVERITY
AdaCore
Twistlock

Security tools and capabilities integrated into common DevSecOps tools provide assurance across the DSO lifecycle

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

SwA Tool Story

What is Software Assurance?

Vulnerability Analysis
Configuration Check
Fuzzing
Compliance Verification
Source Code Analysis
Malware Detection
Reverse Engineering
Software Composition Analysis
Web Scanner

SymfonyInsight
Scrutinizer
Code Inspector
Contemplate - ThreadSafe
Gimpel - PC-lint
Axivion - Bauhaus Suite
SourceMeter
Codacy
Bug Scout (SAST)
BlueClosure Javascript Security
Puma Scan
Semantic Designs - CheckPointer
Semmle - LGTM
DefenseCode - Thunderscan (SAST)
SmartDec Scanner
Software Secured - reshift
Positive Technologies: Application Inspector (SAST, DAST, IAST, and SCA)
Mathworks - Polyspace Code Prover
Mathworks - Polyspace Bug Finder
Green Hils Software - DoubleCheck
ICS Motif - CodeCenter
Google - Closure Compiler
AttackFlow
Absint's - Astree
Rips
Exakat
LDRA - Testbed
CodePeer (formerly known as AdaCore and as SofCheck)
Viva 64 - PVS-Studio
NCC Group - DAST and SAST Tools
Perforce - Klocwork
Kiuwan - Insights (SCA)
Kiuwan - Code Security (SAST)
ForAllSecure's Mayhem
Contrast Security - Contrast Community Edition
Contrast Security - Contrast Assess Interactive Application Security Testing (IAST) Solution
CAST Software Composition Analysis
Snyk Open Source
Micro Focus - Fortify Static Code Analyzer (SCA)
Whitehat Security - Scout
Whitehat Security - Sentinel Source (SAST)
HCL Technologies - AppScan Source (formerly IBM)
SonarQube
Veracode Software Composition Analysis
Veracode Static Analysis - (SAST)
Veracode Greenlight
Synopsys Static Analysis Security Testing (SAST)- Coverity
Synopsys Software Composition Analysis - Black Duck
GrammaTech CodeSonar (Members of the Darpa TECHx team)
CheckMarx CxSAST
CheckMarx CxOSA
Micro Focus - DevPartner
Fuzzbuzz
aDolus
Ion Channel
Embold
FOSSA
GitLab
Sigrid
Resharper
StepSecurity Harden-Runner

~400 SwA Tools

137 Vulnerability Scanning Tools

Static/Java/OSS
10 Tools

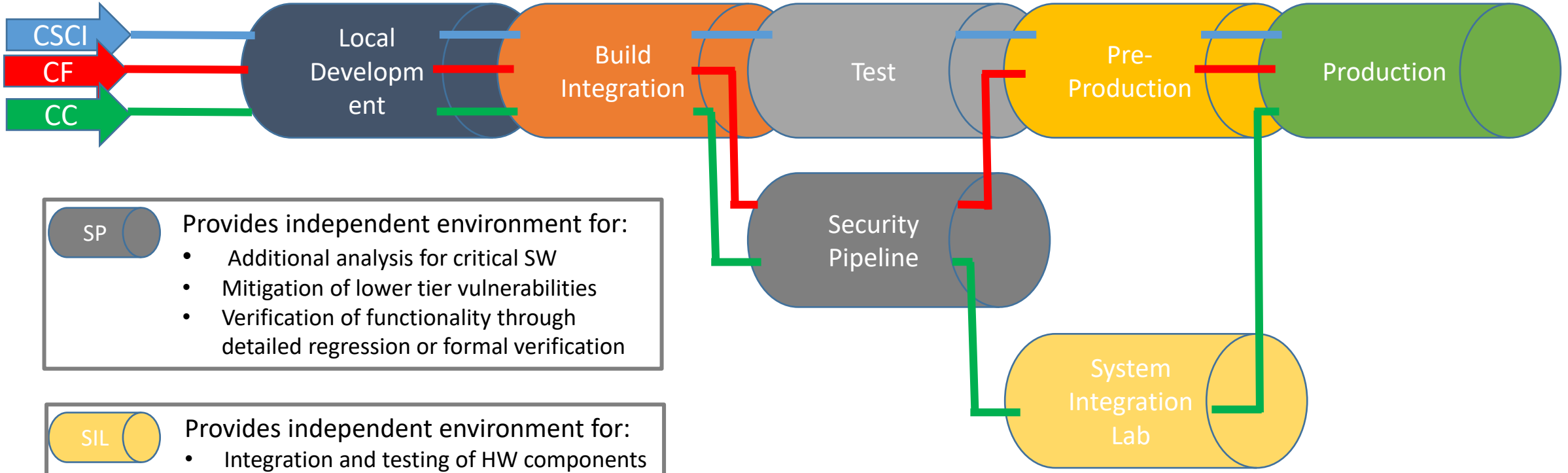
RE/Vulnerabilities
6 Tools

Static/Go/COTS
10 Tools

Ada / Vulnerabilities
5 Tools

Source: Software Assurance Tools Landscape – Levi Lloyd, 2020

Level of Assurance



SP

Provides independent environment for:

- Additional analysis for critical SW
- Mitigation of lower tier vulnerabilities
- Verification of functionality through detailed regression or formal verification

SIL

Provides independent environment for:

- Integration and testing of HW components
- Mocking of services for regression testing
- Execution of misuse and abuse cases based on threat informed senarios

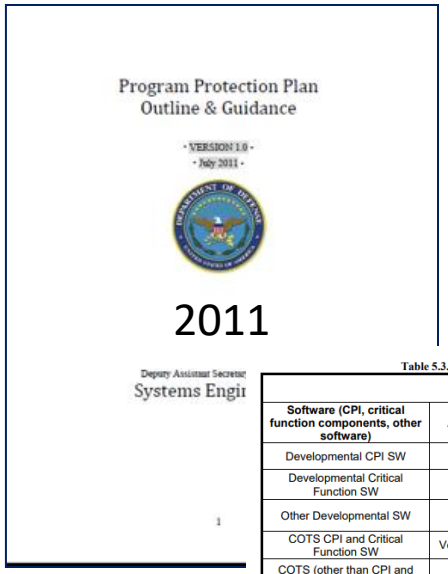
Increased levels of assurance in DSO requires programs to establish more rigorous testing and pre-production environments, ensuring assurance is commensurate with technology, program, system, and mission objectives

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

PPP O&G SwA Table Mapping to DSO

PPP O&G 2011 SwA Section



Program Protection Plan
Outline & Guidance

- VERSION 1.0 -
- July 2011 -

2011

Deputy Assistant Secretary
Systems Engi

1

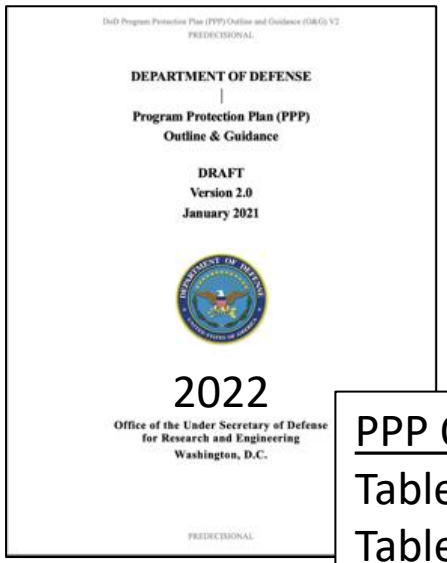
Table 5.3.3-1: Application of Software Assurance Countermeasures (sample)

Development Process								
Software (CPI, critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW	100/80	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK

Operational System						
	Failover Multiple Supplier Redundancy (%)	Fault Isolation	Least Privilege	System Element Isolation	Input checking / validation	SW load key
Developmental CPI SW	30	All	all	yes	All	All
Developmental Critical Function SW	50	All	All	yes	All	all
Other Developmental SW	none	Partial	none	None	all	all
COTS (CPI and CF) and NDI SW	none	Partial	All	None	Wrappers/ all	all

Development Environment								
SW Product	Source	Release testing	Generated code inspection p/a (%)					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment	Controlled access; Cleared personnel only							

PPP O&G 2022 SwA Section



DoD Program Protection Plan (PPP) Outline and Guidance (O&G) V2
PREDECISIONAL

DEPARTMENT OF DEFENSE

Program Protection Plan (PPP)
Outline & Guidance

DRAFT
Version 2.0
January 2021

2022

Office of the Under Secretary of Defense
for Research and Engineering
Washington, D.C.

PREDECISIONAL

PPP O&G SwA Sections

- Table 2-12 SW Infrastructure
- Table 2-13 Software Scope
- Table 2-14 Software Process
- Table 2-15 SW Methods Practices and Tools
- Table 2-16 SW Environments Summary
- Table 2-17 SW Weaknesses and vulnerabilities
- Table 2-18 SW Protections
- Table 2-21 SW Procurement

Updated PPP O&G tables support tracking of assurance methods, practices and protections for infrastructure, environments, and assurance tools

Transparency, Data, and Confidence

Plan
SwA Requirements
Secure Design Considerations
Threat Model

Test
Static Dynamic Analysis Results
Prioritized Vulnerabilities

Operate
Verification of user behavior
SW updates

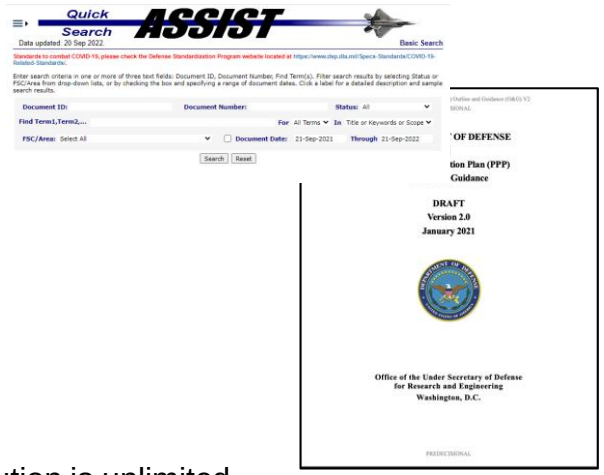
Code
Coding Standards
IDE configurations
Unit Test Cases

Release
Pre-production regression results
Penetration Testing Findings

Monitor
Anomalous Behavior Response
Alerts

Build
Static Analysis Findings
Software composition
Security & Configuration as Code

Deploy
Software Bill of Materials
Residual Risks
Deviation from gate thresholds



Data Item Descriptions should include artifacts that provide decision makers with confidence that software is adequately protected and that protection measures have been employed to mitigate risks

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

PPP O&G SwA Table Mapping to DSO

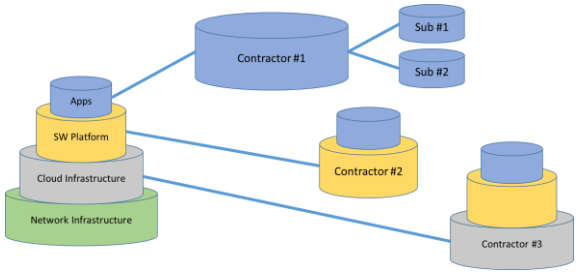


Table 2-12
Software Infrastructure

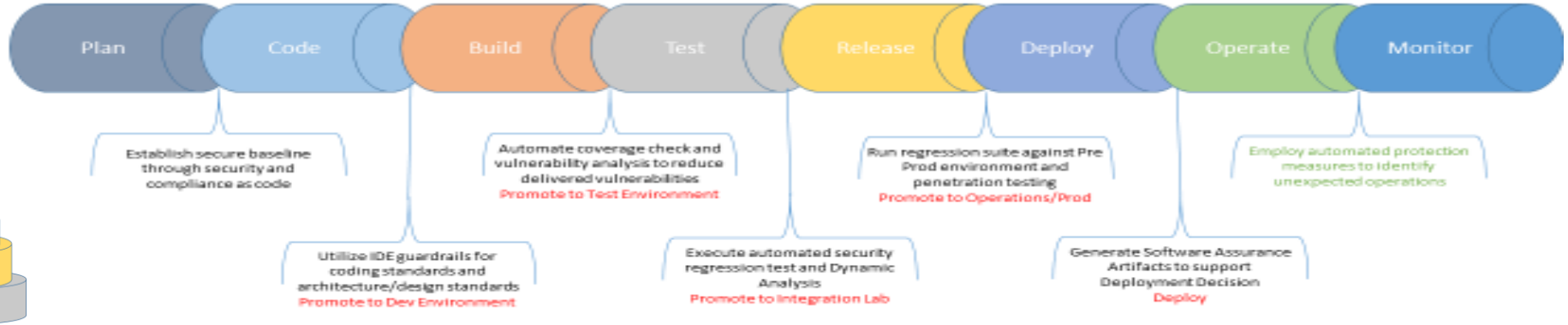


Table 2-13
Software Scope

Table 2-14
Software Process

Table 2-15
SW Methods
Practices and Tools

Table 2-17
SW Weaknesses and vulnerabilities

Table 2-16
SW Environments Summary

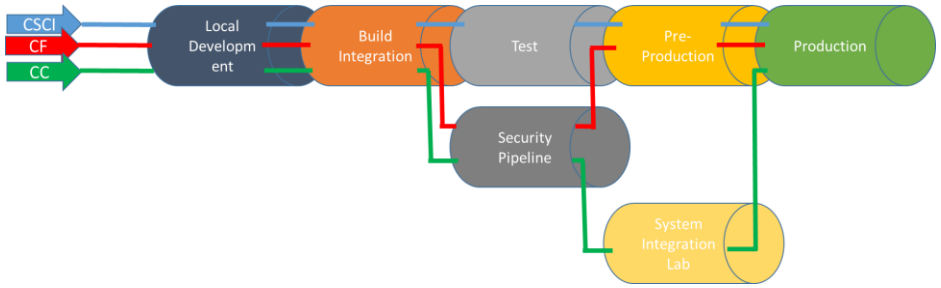


Table 2-18 SW Protections
Operating Systems
Language Selection
Standards
Security Sidecar

Table 2-21
Software Procurement
Vendor SwA Process
SW Bill of Materials
Protection Measures

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Summary

- **DoD Adoption of DevSecOps and the availability of automated tools are enhancing program's ability to implement software assurance**

- **Acquisition processes and the contractual relationship to industry partners create boundaries not present in commercial software development. These boundaries also impact program confidence in the systems assurance including:**
  - Security and Configuration across PaaS and IaaS solutions
  - Tool customization to support technology, program, system, and mission objectives
  - Design of integration and test environments to mirror operations
  - Delivery of assurance artifacts to support risk decisions

- **OUSD(R&E) STPP (Systems Security directorate) updates to the PPP O&G and supporting DIDs will enable the planning and execution of software assurance in a DevSecOps ecosystem**

- **Industry support, review, and feedback on Software Assurance DID is welcomed and appreciated**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Questions?

Bradley Lanford

SAIC Contractor Support

Office of the Under Secretary of Defense
for Research and Engineering

bradley.p.lanford.ctr@mail.mil

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

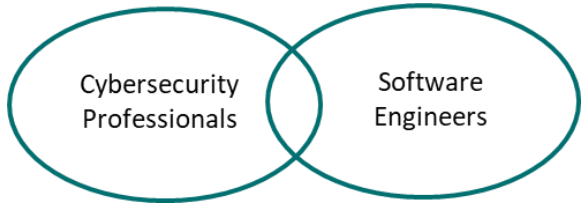
Backup Slides

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

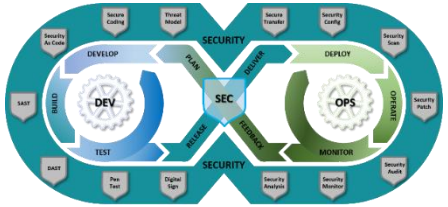
WSA 002 – DevSecOps for the DoD: Security Focus (DSF)

Defense Acquisition University

The greatest impediment to DoD's transition to DevSecOps (DSO) is the use of manual, checklist-based security practices.

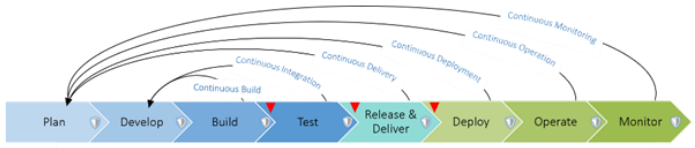


In DSF, brings together software developers, cyber professionals and program managers to tear down traditional DoD silos and provide students with an understanding of the capabilities required to secure software developed using a DevSecOps methodology.



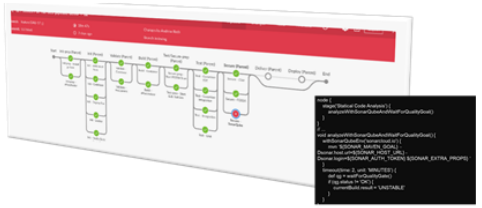
In DSF students will learn the importance of security in DSO, how the DoD DSO reference design supports built-in security across all layers, the importance of automation in the development of security artifacts; and how these artifacts inform the continuous authority to operate.

Empowering students to begin leading cultural change within their organizations and programs through:



Virtual lessons provide a foundation in secure development, threat modeling, the "Sec" in DSO, and DSO automation, enabling confidence in security.

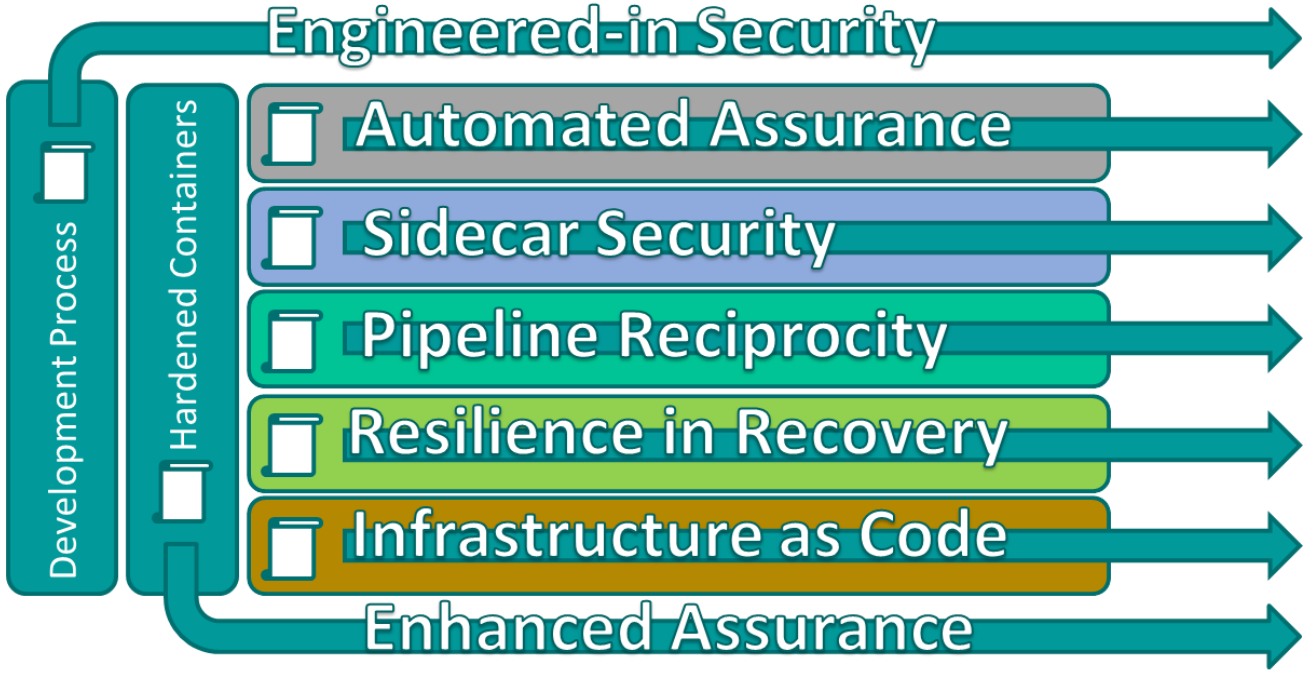
Pipeline demos delivered by CloudOne full stack engineers, detail vulnerability scanning, end-to-end security testing, and the Security Sidecar Pattern.

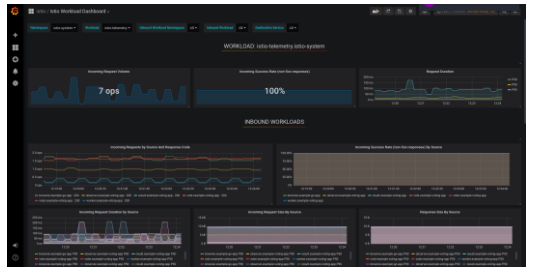


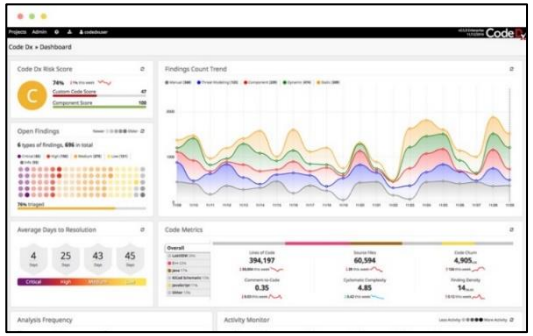
A virtual **case study** walks students through the use of machine readable security artifacts and dashboards in a quest to develop a cATO package and deliver software to the Warfighter.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Continuous Verification of Assurance







USD(R&E)

Design Code Basis for Secure Cyber Resilient Engineering

Foundation for a Secure System

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for
Research and Engineering
Science and Technology Program Protection

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Agenda

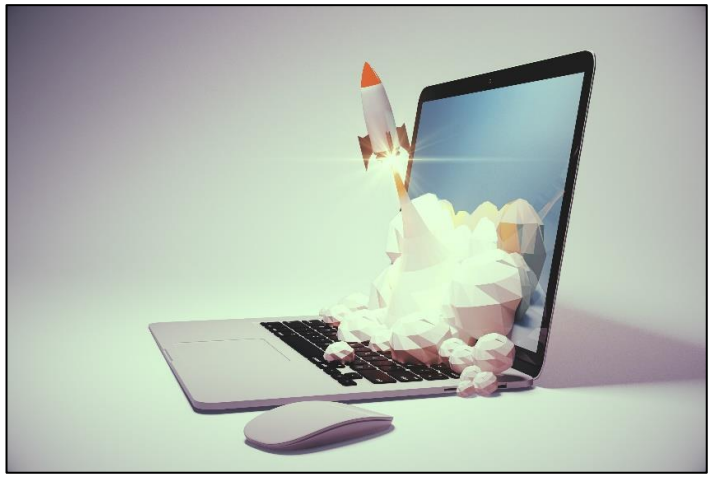
- **The Need**
- **The Concept**
- **History – Trusted Computer Security Evaluation Criteria (TCSEC)**
- **Design Code Basis for Secure Cyber Resilient Engineering (SCRE)**
- **Production Nucleus**
- **What the Design Code Will Establish**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

The Need for Design Code

- **Design code: *criteria* to guide activities to establish and mature the design of trustworthy, secure, and resilient weapon systems**

- **The criteria is targeted for use by system engineers, architects, designers, and developers for activities such as:**
  - System requirements derivation and decomposition
  - System architecture development
  - System design definition
  - System analysis
  - Requirements analysis

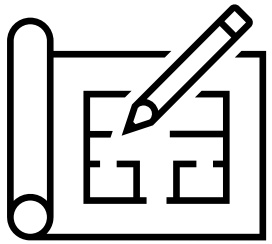


- **Design code will assist in developing and executing SCRE practice activities and tasks**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

The “Code” Concept

- ***Code* is a form of expression to a specific audience.**
- **Code addresses:**
  - Capability, performance, and constraints.
  - Verification methods and overview acceptable solutions.
- **Code is structured and phrased specifically to facilitate its use within the scope of control or authority of its intended audience.**



- **Code continuously evolves to reflect need changes, technology evolution, practitioners’ experience growth, and research and development.**
- **Examples in other domains:**
  - Building Code: A set of rules specifying standards for constructed objects. Its main purpose is to protect public health, safety, and general welfare.
  - Electrical Code: A set of regulations for the design and installation of electrical wiring in a building. The intention of a code is to provide standards to ensure electrical wiring systems that are safe for people and property.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

History of Design Code: Trusted Computer Security Evaluation Criteria

- **The Trusted Computer Security Evaluation Criteria (TCSEC) was the first instance of design code for trustworthy secure design.**
  - It served as the basis for the design, development, and evaluation of trusted operating systems.
  - The design code basis for the TCSEC was the seminal work that established the principles, concepts, objectives, and capabilities of an inherently secure system.
- **TCSEC motivated efforts to refine and extend aspects of design code criteria and its representation.**
- **However, none of these efforts established a principled design code suitable for use in the engineering of trustworthy secure systems.**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Design Code Basis for SCRE (Concept)

- **The capabilities, properties, and characteristics that are necessary and inherent to any trustworthy secure and resilient system**
- **Design code basis**
  - Enables the system to satisfy stakeholder expectations but is not dependent on any specific protection requirements
  - Encompasses
    - The core security protection mechanisms for the system to function security
    - The capability of the system to protect itself
  - Enables
    - The system to deliver the protection capability that fulfills the stakeholder's protection needs

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

SCRE Design Code (Principled Basis)

- ***Design for Security and Cyber Resiliency* expectations (DoD Instruction 5000.83)**
  - Manage access to, and use of, the system and system resources
  - Be structured to protect and preserve system functions or resources
  - Maintain priority system functions under adverse conditions
  - Interfaces with the DoD Information Network or other external services
  - Monitor, detect, and respond to security anomalies
  - Be configurable to minimize exposure of vulnerabilities
- **Transforming these expectations led to further characterization of the *protection nucleus* for secure cyber resilient systems**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Protection Nucleus

- **The concept of protection capabilities and characteristics that are necessarily an inherent part of any secure system (Anderson Report*) expands to be the *protection nucleus***
- **Key protection functions**
  - Protect what the system does functionally
  - Protect the interfaces necessary to provide functionality
  - Protect the configuration that determines the functionality
  - Protect the data associated with all the above

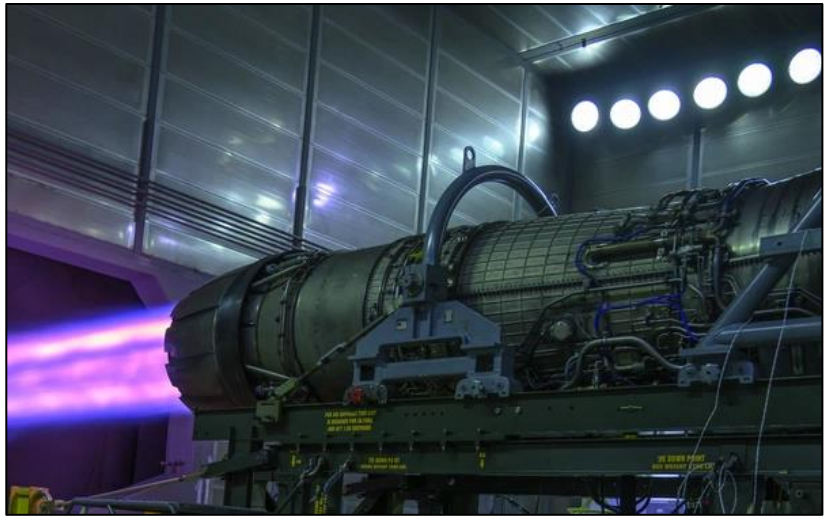
- **Core capabilities for the protection nucleus**
  - *Mediated Access*: enforce authorizations for all system interactions (internal and with external)
  - *System Control*: achieve only the intended system behaviors and outcomes associated with the authorization enforced by mediated access, and prevent and limit loss

*J. P. Anderson, "Computer Security Technology Planning Study, ESD-TR-73-51 Volume 1, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC)," 1972. AKA The Anderson Report

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Design Code Criteria Development

- **Criteria for the *protection nucleus functions, capability, and its mechanisms***
- **Criteria for the *system***
  - To enable success of the nucleus
  - To not interfere with nucleus function
- **Criteria for *related engineering activities*, including verification**



Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Next Steps

- **Work with industry for inputs**

- **Continue activities to standardize SCRE practice to inform specific needs in design code**

- **Pull applicable criteria from existing documents and build additional candidate criteria for comment**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

Questions?

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

References

- J. P. Anderson, "Computer Security Technology Planning Study, ESD-TR-73-51 Volume 1, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC)." 1972. AKA The Anderson Report.

- Department of Defense, “DoD Instruction 5000.83: Technology and Program Protection to Maintain Technological Advantage.” July 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

- National Research Council, “Computers at Risk: Safe Computing in the Information Age.” 1991. https://doi.org/10.17226/1581

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

USD(R&E)

Application of Marking and Distribution Statements on Controlled Technical Information (CTI)

Tabletop Exercise Summary

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for
Research and Engineering
Science and Technology Program Protection

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Purpose/Objective

Identification, Marking, and Flow Down of Unclassified Controlled Technical Information (CTI) Tabletop Exercise:

- **Overview of technical information requiring protection**
- **Overview of procedures to identify, mark, and disseminate technical information requiring protection**
- **Opportunity to explore lessons learned, hands-on experience, and working knowledge of procedures to identify and mark technical information and how it flows through the supply chain**
- **Opportunity to identify gaps surrounding government implementation of requirements that apply to technical information**
- **Opportunity to illuminate process gaps**
- **Opportunity to identify next steps for continued improvement**

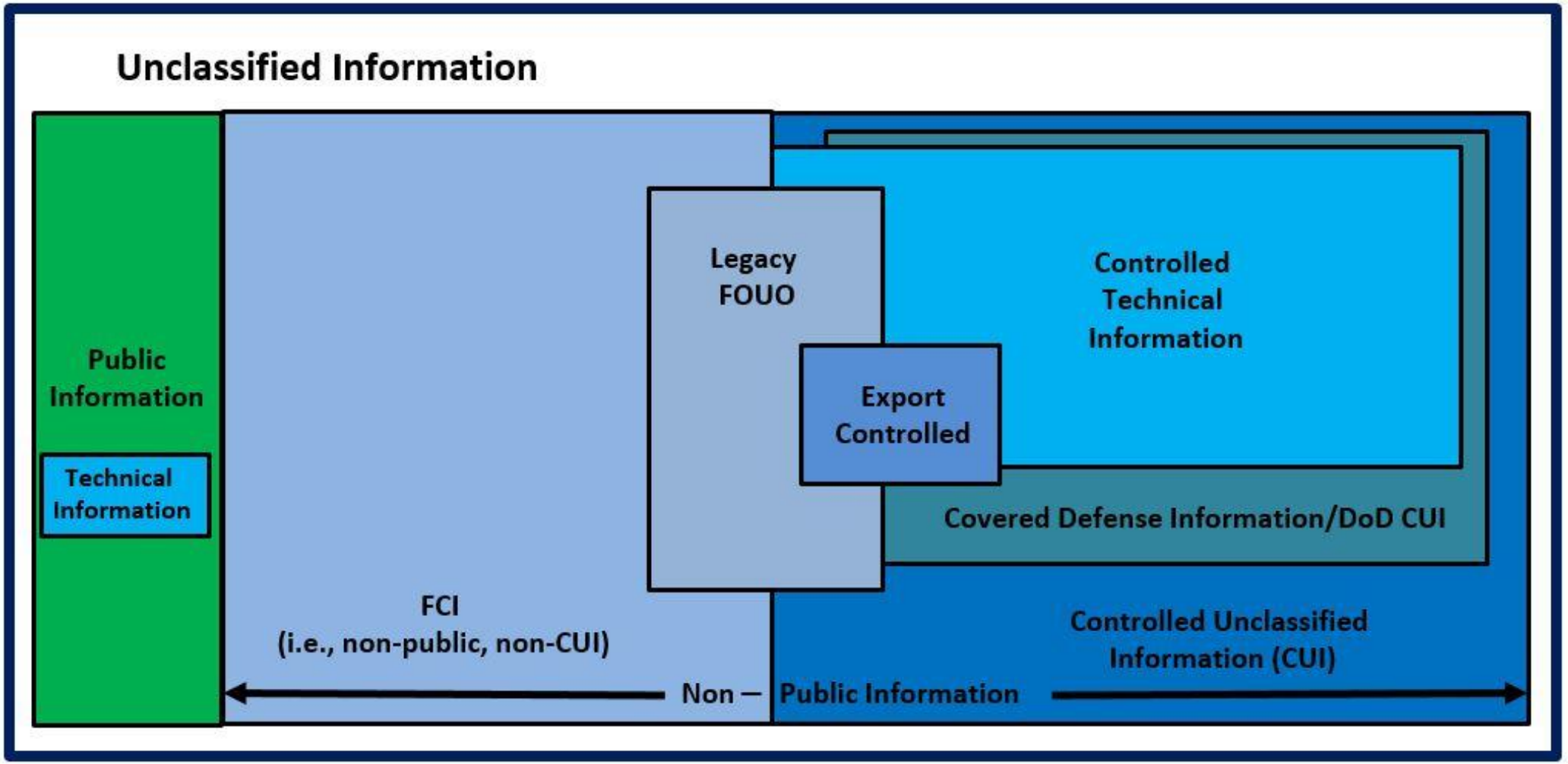
Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Agenda

- **Unclassified Technical Information Requiring Protection**
- **Overview of Protection Requirements**
- **Overview of Identification, Marking, and Dissemination Requirements**
- **Identifying, Marking, and Disseminating Technical Information**
- **Bulldog Exercise / Scenarios**
- **Identification of Lessons Learned**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Notional Unclassified Information Universe



Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Controlled Technical Information (CTI)

The authoritative source for technical information is DoD Instruction (DoDI) 5230.24, Distribution Statements on Technical Documents:

Technical information is technical data or computer software, as defined in DFARS 252.227-7013. Examples include:

- Research and engineering data
- Engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information
- Computer software executable code and source code

Controlled Technical Information (CTI) is technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

- If disseminated - meets the criteria for distribution statements B through F as set forth in DoDI 5230.24
- Does *not* include information that is lawfully publicly available without restrictions

When providing CTI to the contractor in support of the performance of the contract, CTI must be marked or otherwise identified in the contract, task order, or delivery order

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Protection Requirements Codified in the FAR and DFARS

Information	Coverage in the FAR and DFARS	Req'ts for Protection
Federal Contract Information (FCI) (i.e., non-public, non-CUI)	**FAR 52.204-21, Basic Safeguarding of Contractor Info Systems** *(Requires contractor to **apply basic safeguarding requirements to information systems** that process, store, or transmit FCI)*	**FAR contains subset of NIST SP 800-171** ***(as documented in 8582.01)***
Controlled Technical Information (CTI) **Covered Defense Information (includes CTI)** **Controlled Unclassified Information (CUI) (includes covered defense information and CTI)**	**DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting** *(Requires contractor to implement NIST SP 800-171 **to safeguard covered defense information - to include unclassified CTI –** on the contractor's unclassified information system)*	**NIST SP 800-171** ***(as documented in 8582.01)*** **NIST SP 800-172** ***(DoD implementation pending)***
	FAR Case 2017-016, Controlled Unclassified Information *(Proposed Rule – pending publication)* *Implements NARA CUI program which provides regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI*	
Controlled Unclassified Information (CUI) (includes covered defense information and CTI)	**DFARS 252.204-7019/7020, Assessing Contractor Implementation of Cybersecurity Requirements** *Requires contractor to have a current NIST SP 800-171 DoD Assessment (and refers to NIST SP 800-171A) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.*	**NIST SP 800-171**

When a contract includes these provisions/clauses – you should not duplicate the protection/assessment requirements elsewhere in the contract

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Overview of Relevant Policy/Guidance

- **DoDI 5000.83,Technology & Program Protection to Maintain Technological Advantage**
  - Reinforces responsibilities for S&T managers and engineers to manage and control the breadth of technical information to include the identification, marking, and dissemination of CTI
- **DoDI 3200.12, DoD Scientific and Technical Information Program (STIP)**
  - Establishes a coordinated program to manage scientific and technical information created or acquired in the execution of science and technology programs consisting of basic research, applied research, and advanced technology development programs
- **DoDI 5230.24, Distribution Statements on Technical Documents**
  - Establishes procedures for marking CTI and assigning distribution statements and warning labels
- **DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure**
  - Assigns responsibilities for the dissemination/withholding of technical data that discloses critical technology (export controlled) with military or space application
- **DoDI 2040.02 International Transfers of Technology, Articles, and Services**
  - Assigns responsibilities, and prescribes procedures for the international transfer of dual-use and defense-related technology, articles, and services
- **ITAR (22 CFR Sections 120-130) and EAR (15 CFR Sections 730-774)**
- **DoDI 5200.48, Controlled Unclassified Information (CUI)**
  - Assigns responsibilities, and prescribes procedures for CUI throughout DoD in accordance with Executive Order (EO) 13556 and other authorities

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

ITAR vs. EAR – Which Applies?

Regulation	Regulates	Governing Agency	Documentation
ITAR	Defense articles and defense services	U.S. Dept of State, Directorate of Defense Trade Controls (DDTC)	United States Munitions List (USML)
EAR	Commercial/dual-use items and technology	U.S. Department of Commerce Bureau of Industry & Security (BIS)	Commerce Control List (CCL)

If you are unsure whether your item is controlled by ITAR or EAR, contact your International Program Office for assistance with the following:

- Determine what governing agency is responsible for the jurisdiction, licensing, policy and enforcement of your items.
- Conduct a thorough review of the USML. Your customer may be able to provide you with information about the item and its end-use that can be helpful/
- Obtain a Commodity Jurisdiction (CJ) from DDTC to understand which regulation applies.

Although different in terms of structure, administration, and items controlled, both the ITAR and EAR seek to protect U.S. national security by preventing the unauthorized export of controlled items

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Identification and Marking of CTI

DoDI 5230.24 – Distribution Statements on Technical Documents

Dissemination Limitation

Distribution A: Public Release*
Distribution B: U.S. Govt Only
Distribution C: U.S. Govt & Contractors
Distribution D: DoD & US DoD Contractors
Distribution E: DoD only
Distribution F: Further dissemination only as directed by controlling office

**** For CUI developed by or for the government apply Distro A: Public Release – NO Dissemination limitation***

Category / Reason

Administrative or Operational Use
Contractor Performance Evaluation
Critical Technology
Direct Military Support
Export Controlled
Foreign Government Information
Operations Security
Premature Dissemination
Proprietary Information
Software Documentation
Specific Authority
Test and Evaluation
Vulnerability Information

Date

Note: Reason Determination Date

Controlling Org

Note: Controlling Org can be different than the Authoring Org

DoD Policy was established in 1965

Example of Marking for Distribution Statement E

Distribution authorized to DoD only; Proprietary Information; 15 Apr 2017. Other requests for this document shall be referred to AFRL/VSSE, 3550 Aberdeen Ave. SE, Kirtland AFB, NM 87117-5776. REL TO UK

Example of Marking for Export Control Warning (Also requires separate distribution statement)

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Control Reform Act of 2018 (Title 50, U.S.C., Chapter 58, Sec. 4801-4852). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Marking and Identifying CTI

S&T Managers/Engineers/Program Offices/Requiring Activities must:

- Mark or otherwise identify Controlled Technical Information (CTI) provided to the Contractor as Government Furnished Information (GFI)
- Direct appropriate marking and dissemination requirements for CTI in the contract when CTI is to be acquired

Contractor requirements to safeguard CTI in accordance with DFARS 252.204-7012 apply *only when* CTI is marked or otherwise identified in the contract

The Contractor must follow the terms of the contract, to include:

- Implementing the marking and dissemination requirements contained on GFI
- Marking CTI that is collected, developed, received, transmitted, used or stored in support of the performance of the contract
- Determining if information provided to subcontractors retains identify as CTI (consult with contracting office if/as required)
- Include DFARS Clause 252.204-7012 in subcontracts that require CTI for subcontractor performance

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Marking and Dissemination Guidance

The Contract

- Guidance may be found in Statement of Work, Contract Clauses, CDRLs, DIDs, SCGs, etc.

DoDI 5230.24, Distribution Statements on Technical Documents

- Establishes markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law
- Provides Distribution Statements for Use on Technical Documents

CTI must be marked with distribution statements in accordance with DoDI 5230.24

DD Form 254, DoD Contract Security Classification Specification

- Provides Contractors/Subcontractors with security requirements and classification guidance in contracts involving access to classified information
- Guidance for CUI can be found here if the program also includes classified information

DoDI 5200.48, CUI

- Establish policy for designation/safeguarding/decontrolling CUI; establish DoD CUI Registry
- Provides marking guidelines for unclassified and classified documents containing CUI

Program offices/requiring activities are not required to modify existing contracts solely to comply with DoDI 5200.48 or to address updates to the DoD CUI Registry

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Defense Categories / "Reasons" to Assign Distribution Statement B-E (DoDI 5230.24)

Reason	B	C	D	E
Administrative or Operational Use	X	X	X	X
Contractor Performance Evaluation	X			X
Critical Technology *	X	X	X	X
Direct Military Support *				X
Export Controlled *	X	X	X	X
Foreign Government Information	X	X	X	X
Operations Security	X			X
Premature Dissemination	X			X
Proprietary Information	X			X
Test and Evaluation	X			X
Software Documentation	X	X	X	X
Specific Authority	X	X	X	X
Vulnerability Information	X	X	X	X

*** Indicates information will be marked with an Export Control Warning**

Frequently used reasons highlighted in blue – in depth discussion to follow

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Marking and Identifying CTI

Distribution Statements A – F

DISTRIBUTION STATEMENT A	Approved for public release: distribution unlimited.
DISTRIBUTION STATEMENT B	Distribution authorized to U.S. Government agencies (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION STATEMENT C	Distribution authorized to U.S. Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION STATEMENT D	Distribution authorized to DoD and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION STATEMENT E	Distribution authorized to DoD Components only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).
DISTRIBUTION STATEMENT F	Further dissemination only as directed by (controlling office) (date of determination) or higher DoD authority.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Example* of Marking Directions for Controlled Technical Information

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE
A012	SOFTWARE REQUIREMENTS SPECIFICATION (SRS)/ INTERFACE REQUIREMENTS SPECIFICATION (IRS)	

4. AUTHORITY (Data Acquisition Doc. No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-IPSC-81433A	SOW Paragraphs A.2.1, A.6.3, B.2.1, D.3.2,F.8	PMS425

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMSSN	14. DISTRIBUTION
LT	D (SEE BLK 16)	ASREQ	SEE BLOCK 16	

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQ SUBMSSN
A	N/A	SEE BLOCK 16

16. REMARKS

BLOCK 4: DI-IPSC-81434A contains the IRS requirements to be included in the SRS.

BLOCK 9: DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD Contractors only for Administrative or Operational use, 5 July 2017. Other requests shall be referred to Program Executive Office, Submarines, PMS 425.

Release to Australia authorized under the BYG-1 Armament Cooperative Program.

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Control Reform Act of 2018 (Title 50, U.S.C., Chapter 58, Sec. 4801-4852). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

The information is furnished upon the condition that it or knowledge of its possession will not be released to another nation without specific authority from the Department of the Navy of the U.S.; that it will not be used for other than military purposes; that individual or corporate rights originating in the information, whether patented or not, will be respected and; that the information will be provided the same degree of security afforded it by the Department of Defense of the U.S. Regardless of any other markings on this document, it may not be declassified or downgraded without the written approval of the originating U.S. agency.

BLOCKS 10, 12 and 13: Draft submittal fifteen (15) days prior to PDR. Final submittal at CDR closure.

a. ADDRESSEE	b. COPIES		
	Draft	Final Reg	Final Repro
PMS425	1	1	0
NUWC DMO	1	1	0
PMS425DMO	1	1	0
PCO026	1	1	0
ACO	1	1	0

* Contained in publicly released solicitation

A Cooperative Program Example

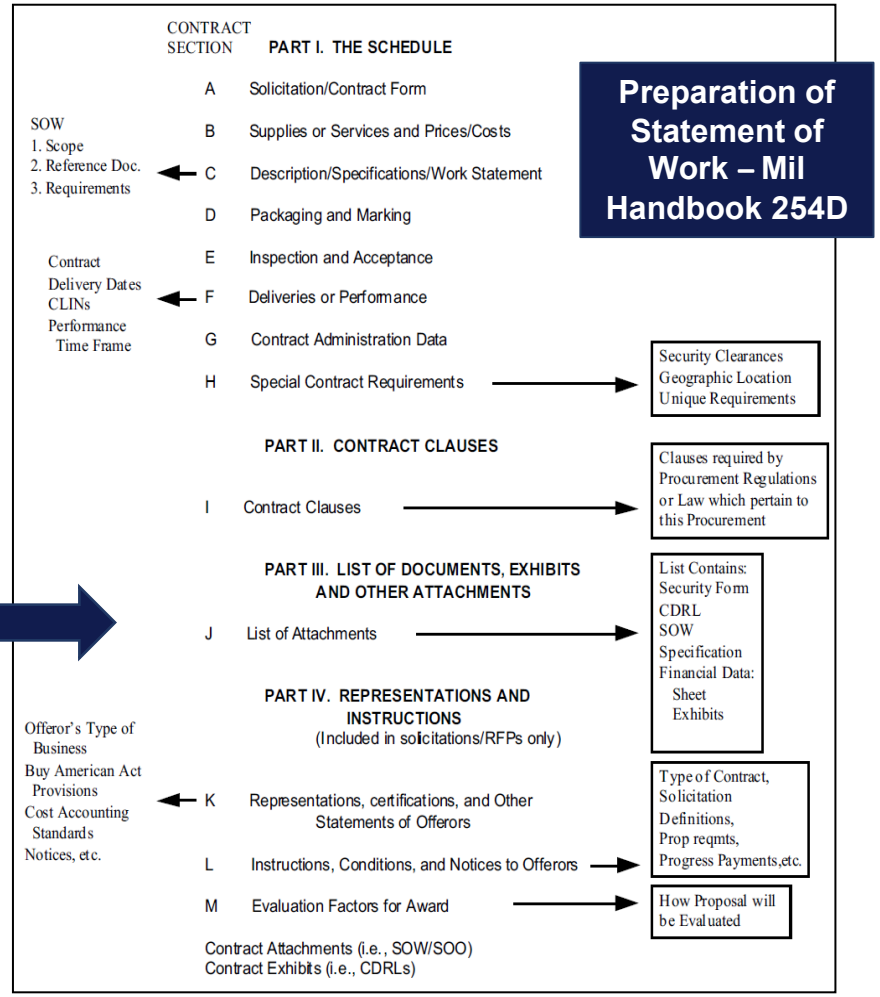
- **Information can be shared with:**
  - DoD and DoD contractors
  - Australia, in accordance with the PMO agreement
- **Information has export control requirements**
- **International markings are currently not consistent with U.S. markings**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

CTI in Solicitations and Contracts

- **Statement of Work (Section C)**
  - Prepared by Program Office (PM)/ Requiring Activity (RA)

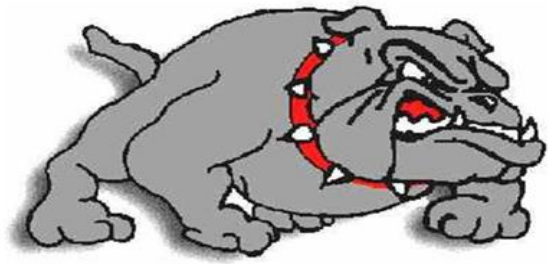
- **List of Attachments (Section J)**
  - Attachments collected by Program Office
  - Data deliverables as identified in CDRL: Prepared by PM/RA
  - Security Classification Guides
  - Specifications: Prepared by PMO/RA
  - Other GFI: Various



Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Bulldog Exercise / Scenarios

- **Exercise Instructions**
- **Scenarios to Determine, Identify and Mark CTI**
  1. Initial Capabilities Document (ICD)
  2. System Performance Specification
  3. Systems Engineering Plan (SEP) and Systems Engineering Management Plan (SEMP)
  4. Use of Capability Development Document (CDD)
  5. CTI Provided to Contractor by DoD
  6. CTI Created by the Contractor



Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Exercise Instructions

- **Identify reasons to control technical information *(i.e., Administrative or Operational Use, Critical Technology, Export Controlled, Foreign Government Information, Operations Security, Proprietary Information, Vulnerability Information)***
- **Identify marking requirements for DoD, prime, subcontractors, suppliers**
- **Identify distribution statements to apply to CTI (*i.e., B, C, D, E, or F*)**
- **Determine types of technical information included in flow down *(i.e., public information or CTI)***
- **Track identified program data as it flows from DoD, to prime, to subcontractors**
- **Break out CUI categories in the data flow descriptions for tracking purposes (*i.e., reasons and distribution statement*)**
- **Identify best practices for limiting flow of information**

Assumption: For the purposes of this exercise – all technical information has been determined to be 'unclassified'

It is the objective of this exercise to identify appropriate markings for controlled technical information

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 1: Initial Capabilities Document (ICD)

- **Unmanned Ground Vehicle (UGV) Systems must:**
  - Be expeditionary with lethal and non-lethal capabilities that are versatile, agile, sustainable, survivable, and *capable to transition across the spectrum of operations.*

    C | **U.S. Government agencies and their contractors (Reason: Critical Technology)**

  - Provide *persistent surveillance for situational awareness*. Can provide *force application*, including targeting, lethal fires, and non-lethal effects, *while protecting the force through standoff from threat capabilities.*

    E | **DoD Components only (Reason: Operational Security)**

  - *Utilize distributed network control-communication architecture* which allows for flexible integration/operation of multiple remote sensor systems/control stations. Architecture must provide flexibility in future integration with *evolving military digital radio networks* (i.e. Army's Tactical Internet/DARPA's Warfighter Internet).

    C | **U.S. Government agencies and their contractors (Reason: Critical Technology)**

  - Provide *options not available to meet an urgent need*. Needed *operational capabilities are not provided* in any near term integrated combat system, *putting soldiers, airmen, and marines in inordinately high-risk situations.*

    D | **DoD and U.S. DoD contractors only (Reason: Critical Technology)**

  - Capable of conducting operations in *all operational environments, including hot/basic/cold.*

    C | **U.S. Government agencies and their contractors (Reason: Critical Technology)**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 1: Initial Capabilities Document (ICD)

- ***Potential for allied cooperation*** **deemed high due to** ***multi-mission/multi-role nature*** **of UGVs, i.e., Export Controlled or Federal Government Information**

  C | U.S. Government agencies and their contractors (Reason: Foreign Government Information)

- **Potential alternatives limited to UGV Systems, components, and technologies already fielded and/or in production,** ***technologies in advanced development (e.g., Joint Capability Technology Demonstration (JCTD)),*** **and those slated for production within 3-4 years.** ***Emerging and later maturing technologies*** **may be considered for future insertion to meet objective system requirements.**

  D | DoD and U.S. DoD contractors only (Reason: Critical Technology)

- **Standardization/Interoperability: The UGV System must have appropriate levels of** ***standardization and interoperability*** **with the** ***other Services, allies, and coalition partners.***

  C | U.S. Government agencies and their contractors (Reason: Foreign Government Information)

- **Infrastructure Support: The UGV System must be supportable by current and projected combat support and service support assets. They must be** ***transportable in an operational configuration in strategic and tactical air transportation aircraft.*** **UGV Systems** ***must also be capable of transport on unrestricted highway, rail, maritime*** **prepositioned ships, amphibious ships, amphibious landing craft, and** ***other marine transport worldwide.***

  C | U.S. Government agencies and their contractors (Reason: Vulnerability Information)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 2: System Performance Specification

The Bull Dog UGV System will be *used in a variety of critical, high risk warfighting situations requiring an integrated suite of unmanned air and ground vehicles across the spectrum of conflict*.

C | U.S. Government agencies and their contractors (Reason: Critical Technology)

Capable of independent operations, … will carry onboard weapons *with the capacity to destroy fixed and mobile targets.*

D | DoD Components only (Reason: Critical Technology)

The UGV System will also be *capable of line-of-sight (LOS) remote control from the Joint Command and Control System (JCCS) and non-LOS (NLOS) control via relay using participating UAV assets.*

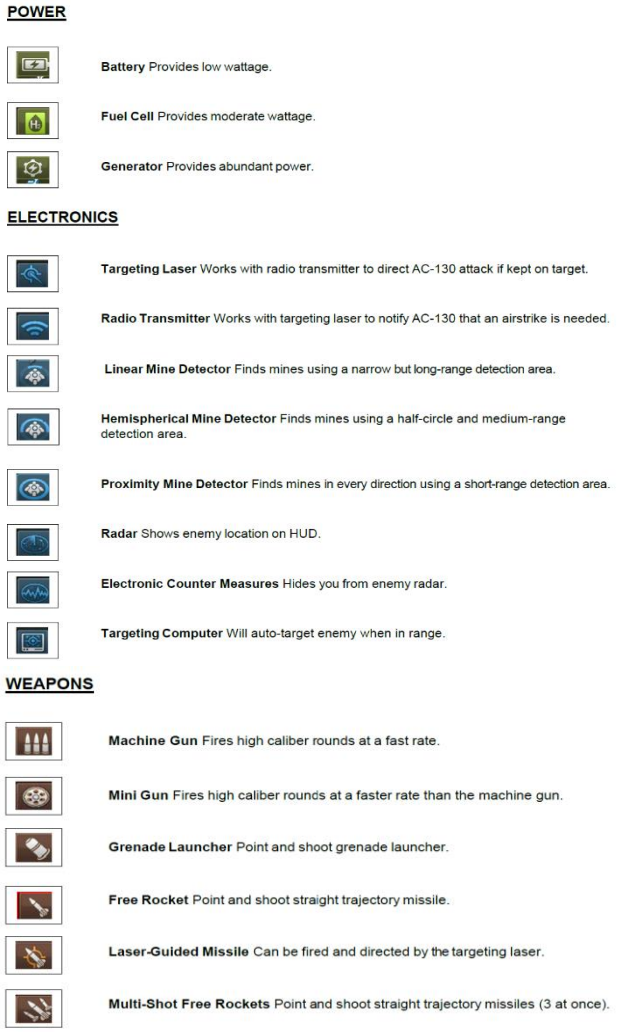
D | DoD Components only (Reason: Critical Technology)

Missions include: *intelligence; RSTA; mine detection; direct and indirect fire support; attack of moving targets; reduction of bunkers and other strong point defenses; and communication of target locations to indirect fire and command and control systems …*

D | DoD Components only (Reason: Critical Technology)

These missions will be *performed predominately in areas too hazardous to send humans or manned vehicles*. The Bull Dog UGV will be *capable of operating in Biological/Chemical (BC) contaminated environments.*

D | DoD Components only (Reason: Critical Technology)



Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 4: Capability Development Document (CDD)

Joint Capability Areas (JCAs) - Description, Metrics, Minimum values

- Force application – Engagement
- Protect – Prevent – Mitigate
- Command and Control – Understand

D **DoD and U.S. DoD contractors only (Reason: Critical Technology)**

CDD Requirements

- Dissemination of Target Data

D **DoD and U.S. DoD contractors only (Reason: Critical Technology)**

- **Probability of Detect (Pd) for Mines**

D **DoD and U.S. DoD contractors only (Reason: Critical Technology)**

- **Unrefueled Range (i.e., Mission range from Operator Control Unit (OCU) unrefueled)**

C **U.S. Government agencies and their contractors (Reason: Critical Technology)**

- **Minimum Top Speed**

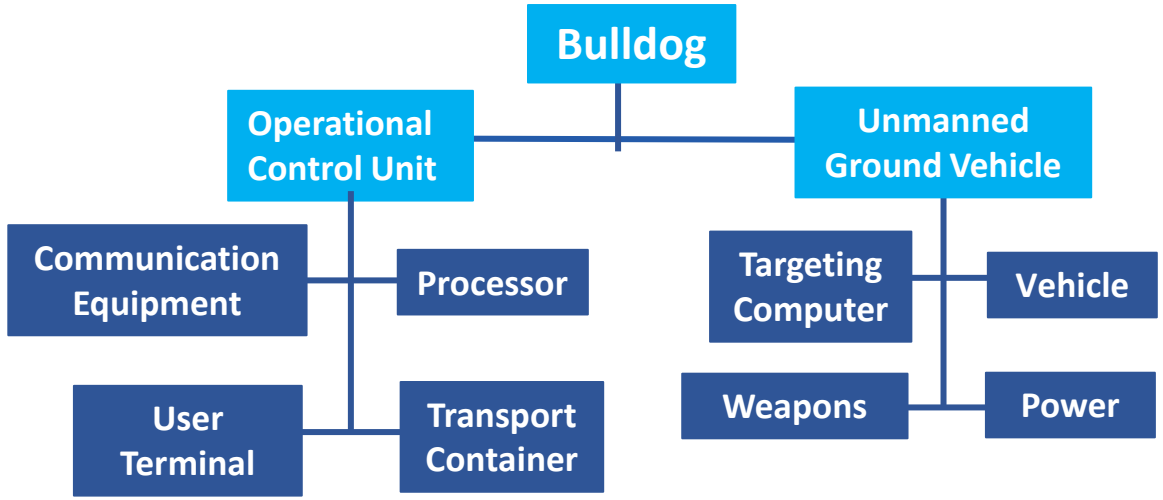
D **DoD and U.S. DoD contractors only (Reason: Critical Technology)**

- **Probability of Kill (Pk) in Autonomously Targeting and Launching One or More Weapons**

C **U.S. Government agencies and their contractors (Reason: Critical Technology)**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 5: CTI Provided to Contractor by DoD



System: Bulldog

Tasks:

- Support Program Mgt Office with competition, logistics support, etc.
- System/subsystem design, development, integration, and verification; production/ final assembly

Data flow from DoD to Prime (Bulldog) — **Distribution/Reason =**

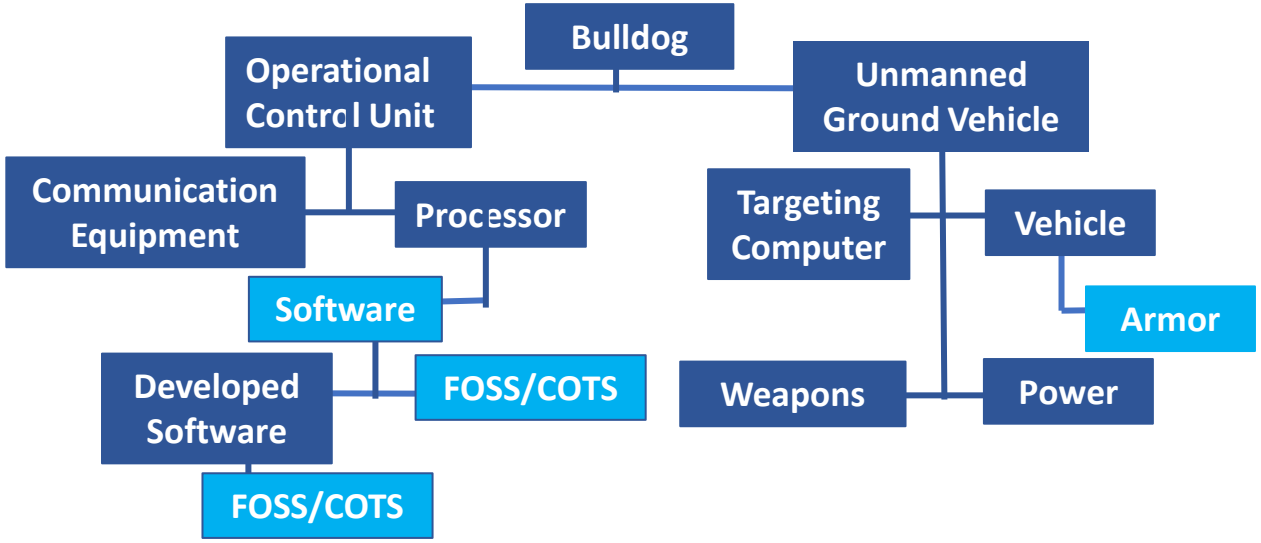
- **Systems Engineering Plan (SEP)** — D: DoD and U.S. DoD contractors only (Reason: Critical Technology)
- **Program planning information** — D: DoD and U.S. DoD contractors only (Reason: Administrative or Operational Use)
- **Interface Control Documents** — D: DoD and U.S. DoD contractors only (Reason: Critical Technology)
- **Technical Manuals** — C: U.S. Government agencies and their contractors (Reason: Administrative or Operational Use)

Data flow from Prime (Bulldog) to Subs — **Distribution/Reason =**

- **Subsystem specification and ICDs** — D: DoD and U.S. DoD contractors only (Reason: Critical Technology)
- **Subcontractor SOW** — D: DoD and U.S. DoD contractors only (Reason: Critical Technology)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 5: CTI Provided to Contractor by DoD



System: Armor

Task: Armor design, development, and production

System: Radar Real Time Operating System

Task: Supply COTS Operating System

NOTE: COTS items could also be wing nuts, O-rings, etc.

Data flow from USG to Prime (Bulldog) — **Distribution/Reason =**

- **Armor Requirements/Performance Specification** — D — DoD and U.S. DoD contractors only (Reason: Critical Technology)
- **Software Source Code, SBOM** — E — DoD Components only (Reason: Software Documentation, Proprietary)
- **Commercial (modified COTS) & COTS SW Executables** — E — DoD Components only (Reason: Software Documentation)
- **Non-commercial Software Executables (GFE)** — D — DoD and U.S. DoD contractors only (Reason: Critical Technology)

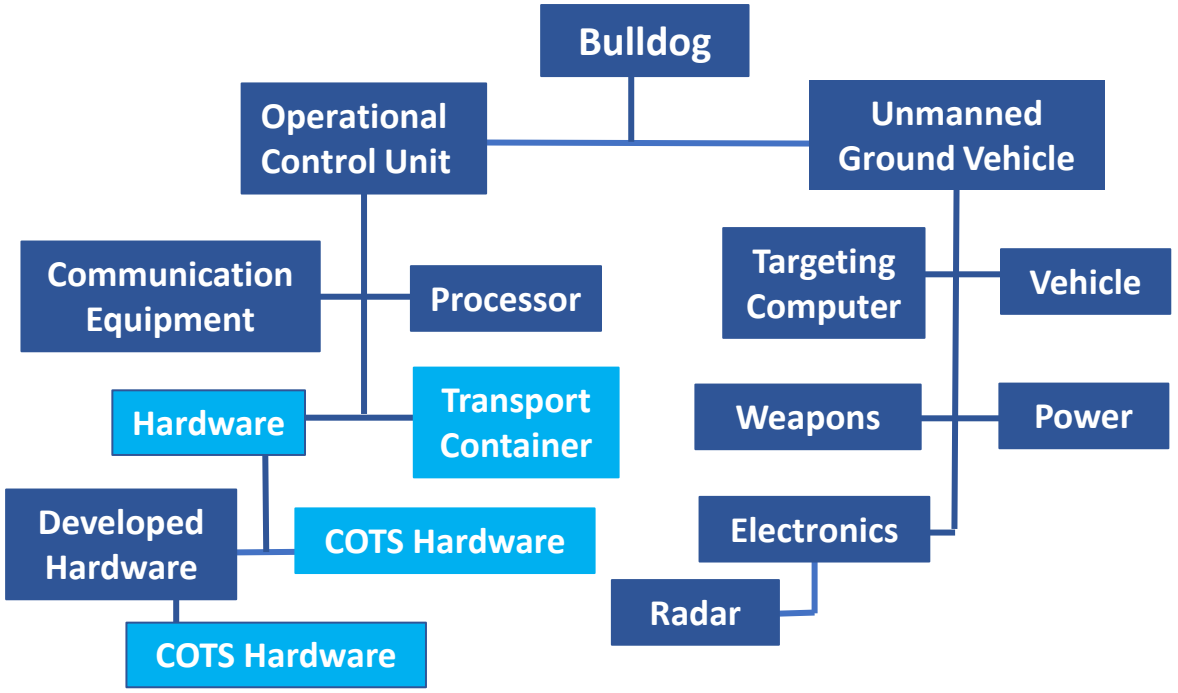
Data flow from Prime (Bulldog) to Subs — **Distribution/Reason =**

- **Proc Spec, SSOW for prod spt, License requests** — D — DoD and U.S. DoD contractors only (Reason: Critical Technology)

Goal would be to only flow down public data when purchasing COTS

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 6: CTI Created by the Contractor



System: Transport Container

Task: Container design, development, and verification; production/container assembly

System: Radar Processor Hardware

Task: Supply COTS motherboard

NOTE: COTS items could also be wing nuts, O-rings, etc.

Data flow from Prime (Bulldog) to DoD — **Distribution/Reason =**

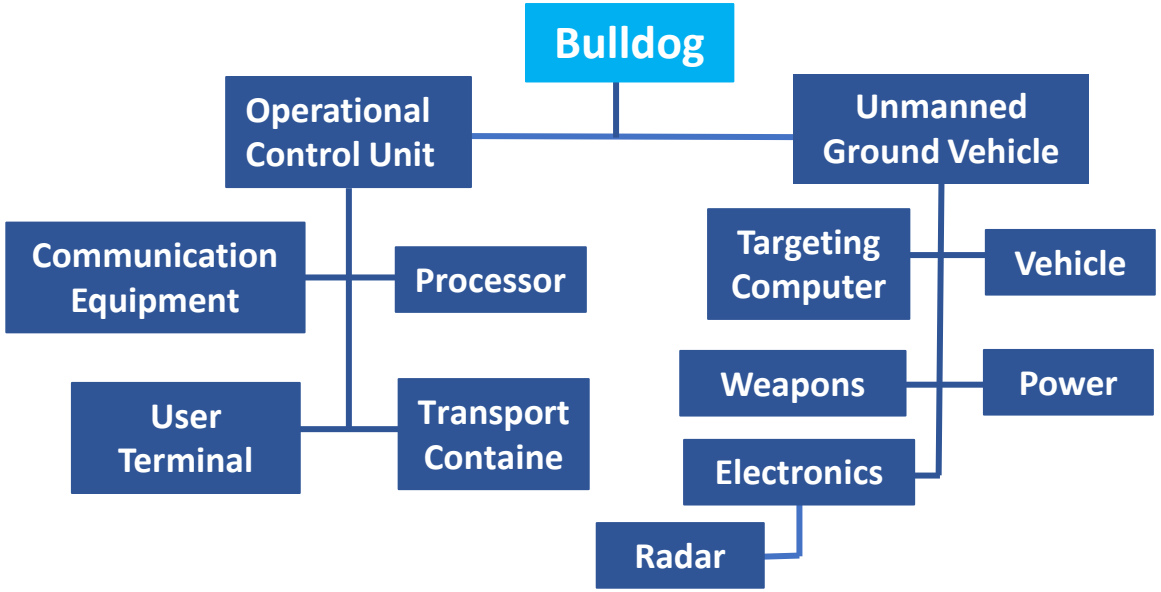
- **Transport container design drawings, dimensions, tech specs, user manual** — **D** DoD and U.S. DoD contractors only (Reason: Administrative/Operational Use)

Data flow from Sub to Prime — **Distribution/Reason =**

- **COTS Motherboard component requirements** — **D** DoD and U.S. DoD contractors only (Reason: Software Documentation)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Scenario 6: CTI Created by the Contractor



System: Bulldog

Task:

- **Manage program cost, schedule, and performance**

Data flow from Prime (Bulldog) to DoD — **Distribution/Reason =**

- **Systems Engineering Management Plan (SEMP)** — E DoD and U.S. DoD contractors only (Reason: Proprietary)
- **Program management planning, financials, schedules, technical risk** — E DoD and U.S. DoD contractors only (Reason: Proprietary)

Data flow from Subs to Prime (Bulldog) — **Distribution/Reason =**

- **Financials, schedules, technical risk** — E DoD and U.S. DoD contractors only (Reason: Proprietary)
- **Test results, post-test equip changes** — E DoD and U.S. DoD contractors only (Reason: Proprietary)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

Next Steps

- **Provide Exercise through Defense Acquisition University (DAU) webinar that steps through Bulldog scenarios**
- **Use feedback to refine the training**
- **Work with DAU to integrate training into their curriculum**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0111 applies. Distribution is unlimited.

USD(R&E)

Risk and Issue Revisited in Systems Security Engineering

Dr. Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Summary

- Much of what some security/cybersecurity/resilience communities refer to as “risk” deal more with operational rather than engineering risk.
- The subsequent approaches may cause dissonance with systems engineering efforts, leading to misapplication of resources and efforts.
- This presentation provides an examination of technical protection risks and issues and the opportunity presented to better align with systems engineering needs and equities by adopting different approaches.
- These possible alignments are reflective of how safety risk aligns with systems in communities with similar objectives due to the catastrophic consequences associated with system failure.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Some Systems Engineering Definitions

- **Risk:**
  - Effect of uncertainty on objectives – ISO 73
  - Effect: deviation from the expected
- **Technical risk:**
  - Potential for performance deficiencies (NASA Systems Engineering Handbook, adapted)
- **Technical protection risk:**
  - Potential for protection performance deficiencies (as informed by protection expectations /requirements)
- **Issue:**
  - Event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (probability = 1) – DoD Risk, Issue, and Opportunity Guide
  - Systems Engineering Body of Knowledge definition refers to types of issues: A problem that exists, a risk certain to occur, and a lack of information

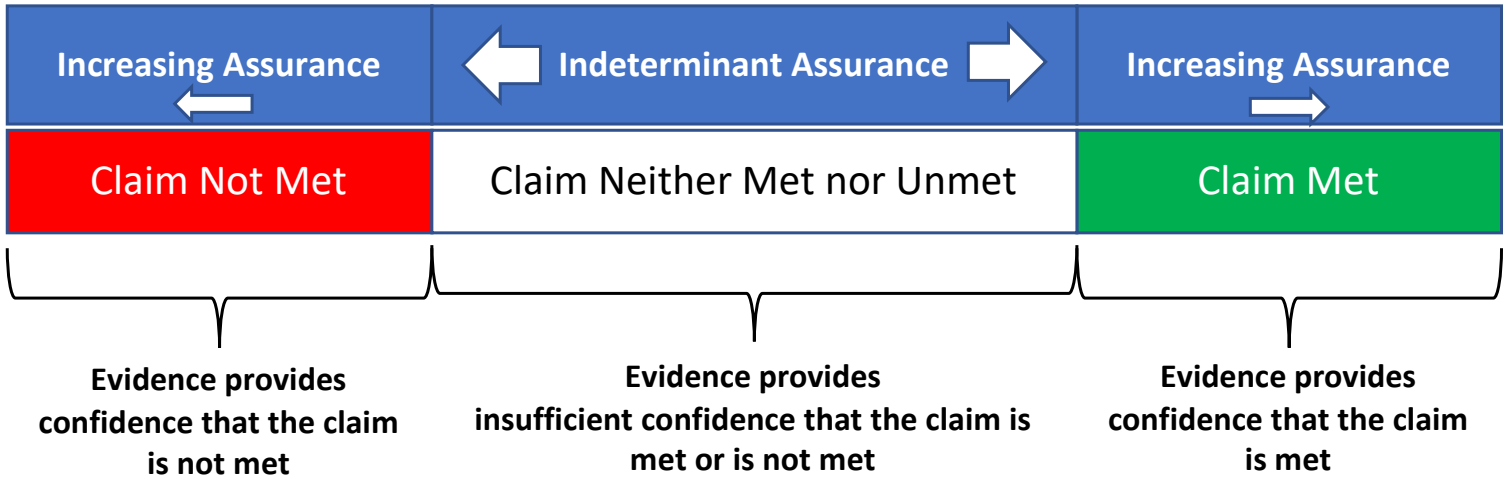
Definitions of the terms we use are necessary for effective communications. There is no right or wrong definition, only the one we choose to use. … Limited definitions, however, may also limit potential solutions to the problems. If we start from more inclusive and practical definitions, then overlap and common approaches to achieving the properties are possible.

- Nancy Leveson, "Safety and Security are Two Sides of the Same Coin," **The Coupling of Safety and Security**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Assurance

- **Assurance is grounds for justified confidence a claim has been or will be achieved [IEEE 15026]**
  - Assurance – certainty
  - Lack of assurance – uncertainty
- **Three possibilities**
  - Sufficient grounds that a claim is achieved
  - Sufficient grounds that a claim is not achieved
  - Insufficient grounds to support any conclusion about a claim
- **Claims of concern for this presentation**
  - "Required performance will be delivered"
  - "Required protection performance will be delivered"

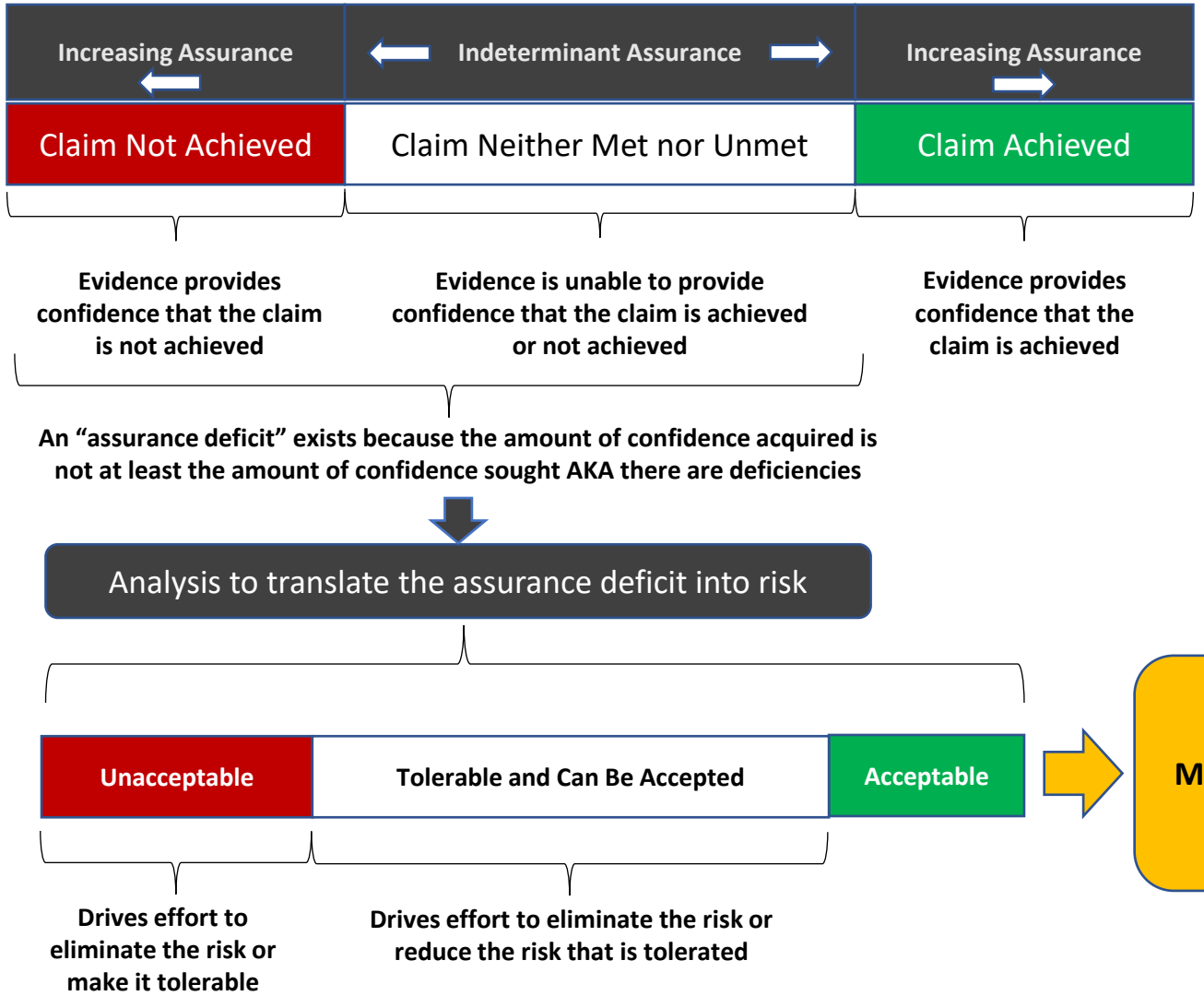


Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Deficiencies and Risk

ASSURANCE

RISK



Assurance Activities

For risk driven by confidence derived from evidence-based judgments

1. Determine how much confidence is needed
2. Acquire the confidence

If

(a) The confidence needed is met by the confidence acquired – good!

(b) The confidence needed is not met by the confidence acquired – take action!

Risk Management Activities

1. Translate the deficit in confidence into the associated risk(s)
2. Determine if the associated risk is
   - Unacceptable
   - Tolerable and acceptable
   - Non-existent
3. Conduct the appropriate risk management activities to identify, assess, and accept or mitigate the identified risks

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Technical Protection Information Deficiencies Are Critical Issues

- **Information often used/discussed includes threat, vulnerability, and undesired effects (undesired losses and consequences)**
- **Deficiencies exist in threat information**
  - Timeliness, accuracy, completeness, actionability, etc.
- **Deficiencies exist in vulnerability information**
  - Supply chain insight gaps (e.g., use of Commercial Off-The-Shelf)
  - Deficiencies in engineering rigor result in vulnerability information deficiencies
- **Deficiencies exist in undesired losses and consequences information**
  - Typically, a result of deficiencies in engineering process and rigor

Which deficiencies are easier to address? Harder to address?

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Threat, Vulnerability, and Effect Information Deficiency Handling

- **Threat and vulnerability are intractable; undesirable consequences of effects bounded**
- **Through rigor in engineering efforts, it is possible to sufficiently close effect information deficiencies**

Threat and Vulnerability

What might/has happened?

- Incomplete data on threat and vulnerability make this always incomplete
- A constant chase of the OODA loop

Effects

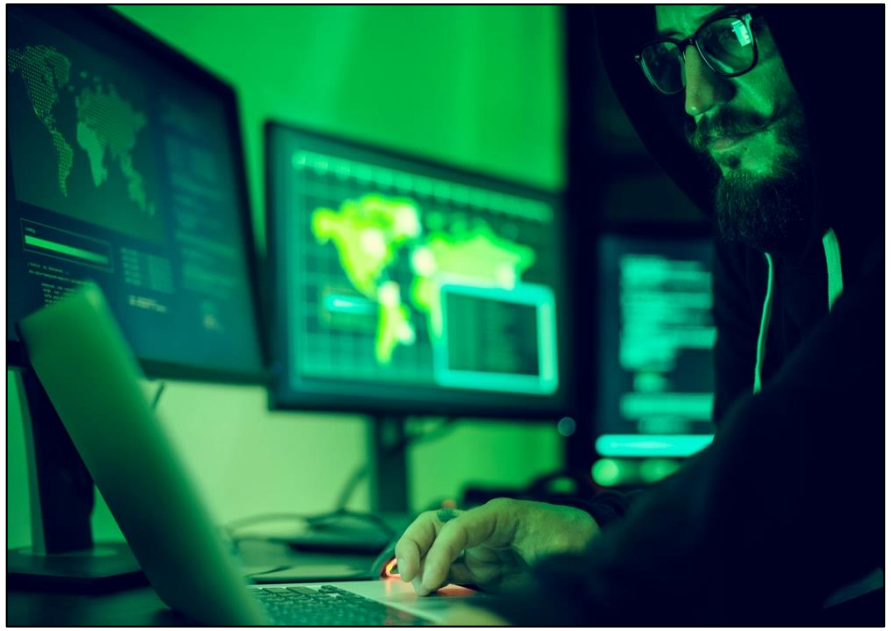
What is our confidence in addressing what might be or is?

- Ensuring function
- Effective means to verify action to control loss and loss effects

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Addressing Effects (Expanded)

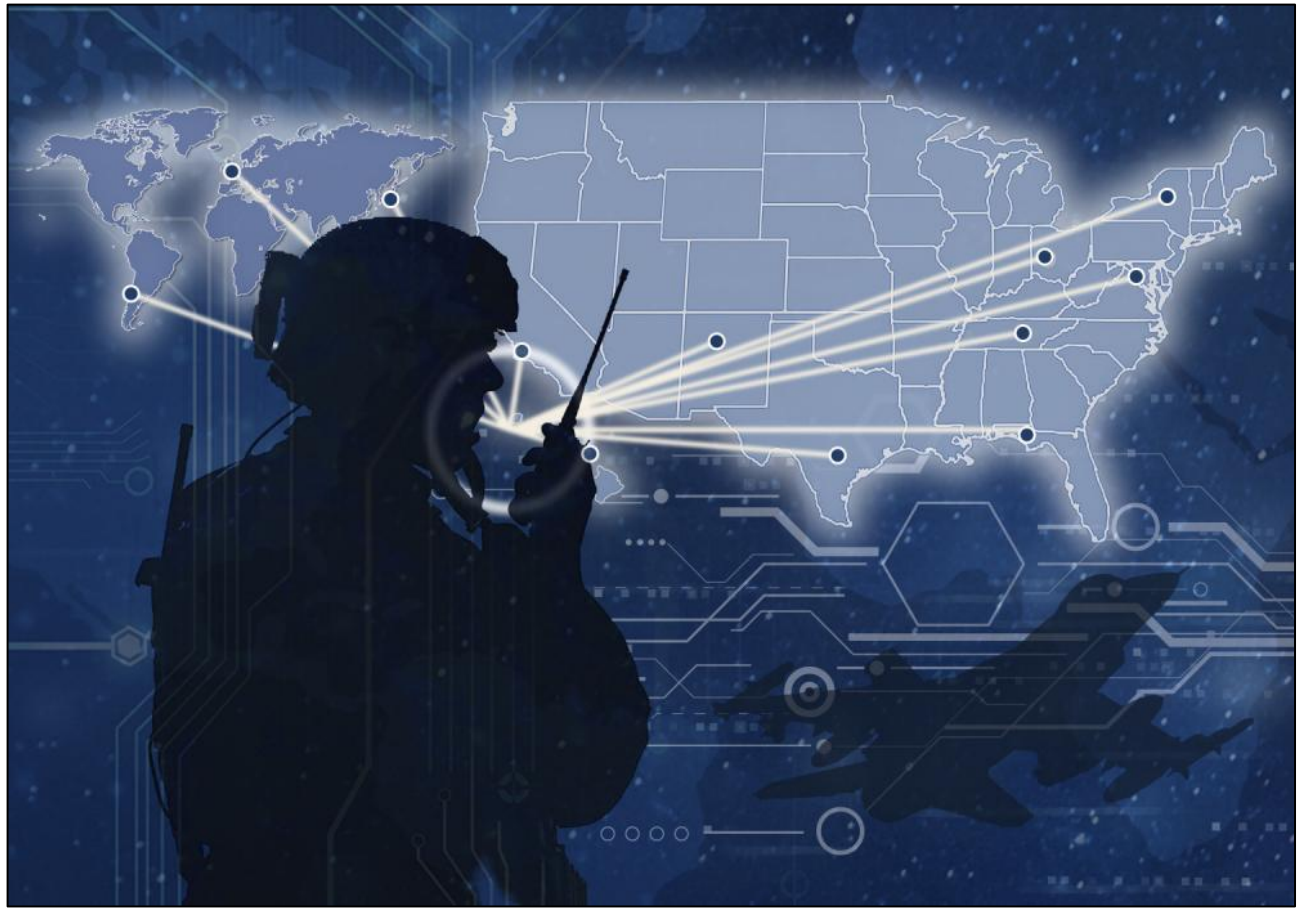
- **Identify constraints needed to address effects**
  - Constraints to avoid effects
  - Constraints to limit effects including duration
- **Enforce constraints**
- **Ensure enforcement (i.e., assurance of the constraint enforcement)**



Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

What's Next

- **Articulate clearly protection as capability and functional driven**
- **Standardize practice with assurance deficit risk thinking**



Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

Questions?

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

References

- Bider and Gould, editors, “The Coupling of Safety and Security.” https://doi.org/10.1007/978-3-030-47229-0
- National Aeronautics and Space Administration, “NASA Systems Engineering Handbook.” https://www.nasa.gov/connect/ebooks/nasa-systems-engineering-handbook
- Department of Defense, “Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.” January 2017. https://www.dau.edu/tools/Lists/DAUTools/Attachments/140/RIO-Guide-January2017.pdf
- Department of Defense, “Technology and Program Protection to Maintain Technological Advantage.” 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf
- ISO, “ISO Guide 73:2009 – Risk Management Vocabulary.” 2009. https://www.iso.org/standard/44651.html
- “Systems Engineering Body of Knowledge.” 2022. https://www.sebokwiki.org/

Distribution Statement A: Approved for public release. DOPSR case #23-S-0023 applies. Distribution is unlimited.

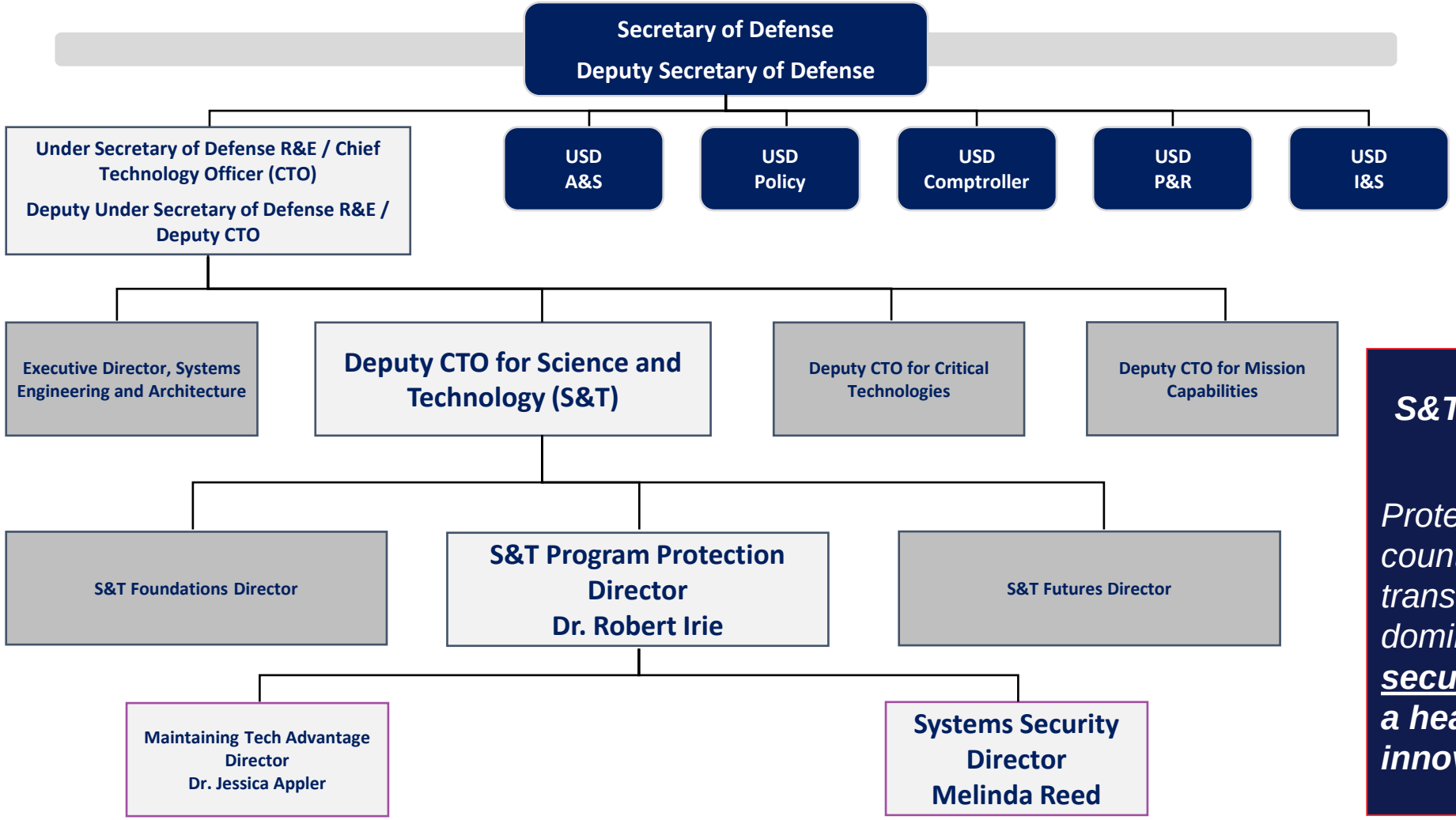
USD(R&E)

Critical Program Information Identification

Mr. Randy Woods
Director, Systems Security Engineering and Anti-Tamper
Office of the Under Secretary of Defense for Research and Engineering
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

OUSD(R&E) Organization



S&T Program Protection (STPP) MISSION:

Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through ***assured, secure and resilient systems*** *and a healthy, viable national security innovation base.*

Three Pillars of Robust Program Protection: Critical Program Information Protection with an Overall Approach to Program Protection

Systems Security Engineering Design and Tradeoffs

Information / Data	Technology	Mission Components
What to Protect: Information and data on the system and about the research and or acquisition program.	**What to Protect:** A U.S. capability element that contributes to the warfighter's technical advantage.	**What to Protect:** Mission critical functions and components.
Protection Activities: • Classification • Information security • Cybersecurity protections and technology solutions • Joint Acquisition Protection and Exploitation Cell (JAPEC) • Damage Assessment Management Office (DAMO)	**Protection Activities:** • Export control • Anti-tamper (AT) • Defense Exportability Features • DoD Horizontal Protection Guide • Acquisition Security Database (ASDB)	**Protection Activities:** • Software assurance (SwA) • Hardware assurance (HwA) • Trusted/assured microelectronics • Supply Chain Risk Management (SCRM) • Anti-counterfeit • Joint Federated Assurance Center (JFAC)
Goal: Safeguard research and / or program information and technical data from adversary collection and disruption.	**Goal:** Prevent compromise or loss of critical technology.	**Goal:** Protect mission-critical components (hardware, software, firmware) from malicious exploitation.

Protecting Warfighting Capability throughout the Lifecycle

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Identification of Critical Program Information (CPI) as Part of Technology and Program Protection

- **Technology and Program Protection (T&PP) responsibilities are assigned in the DoD Instruction (DoDI) 5000.83, Technology and Program Protection to Maintain Technological Advantage" for program managers and lead systems engineers:**
  - Hardware and software assurance
  - Cyber and cyberspace
  - Supply chain exploitation
  - Reverse engineering
- **Additional T&PP policy and responsibilities for anti-tamper are further refined in specific policies such as:**
  - DoD Directive (DoDD) 5200.47E: "Anti-Tamper"
  - DoDI 5200.39: "CPI Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)"
  - DoDI 5230.28: "Policy for Low Observable (LO) and Counter Low Observable (CLO) Programs"
- **Critical Program Information (CPI) elements are identified utilizing sources such as:**
  - Acquisition Security Database (ASDB)
  - CPI Horizontal Protection Guidance
  - Expert questions
  - Program-specific and anti-tamper Security Classification Guides (SCG)

Updated guidance is available in the newly published T&PP Guidebook

Guidebook accessible at: https://rt.cto.mil/wp-content/uploads/TPP_Guidebook_Jul2022_cleared.pdf

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Industry Perspective on DoD Challenges to CPI Identification

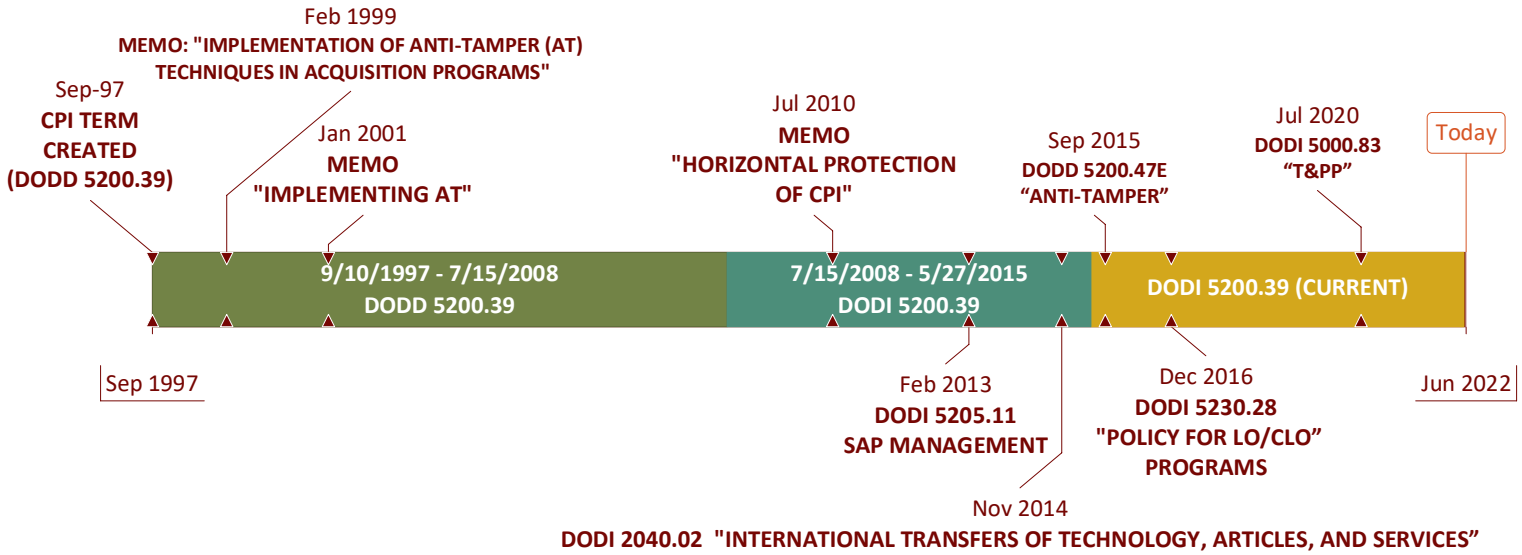
- **The National Defense Industrial Association (NDIA) provided a briefing regarding CPI Identification Challenges to Offices of the Under Secretary of Defense (OUSD):**
  - OUSD for Acquisition and Sustainment
  - OUSD for Intelligence and Security
  - OUSD for Research and Engineering
- **DoD's senior leadership has also expressed an interest in streamlining the CPI Identification and protection process for programs**

- **Challenges (as provided by NDIA):**
  1. DoD has multiple CPI definitions
     a. How to constrain the expanding definition of CPI (as it relates to AT)
  2. Differing chains of command use different CPI processes
     a. Inconsistent policy, understanding, and education undermine horizontal protection
     b. CPI identification is often not accurate, consistent, or repeatable
  3. Lack of CPI-focused intelligence support

Every dollar spent on protecting old technology robs the warfighter of new and necessary capability – unnecessary anti-tamper hurts the warfighter

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Challenge 1: DoD Has Multiple CPI Definitions – Deviation in the CPI Definition



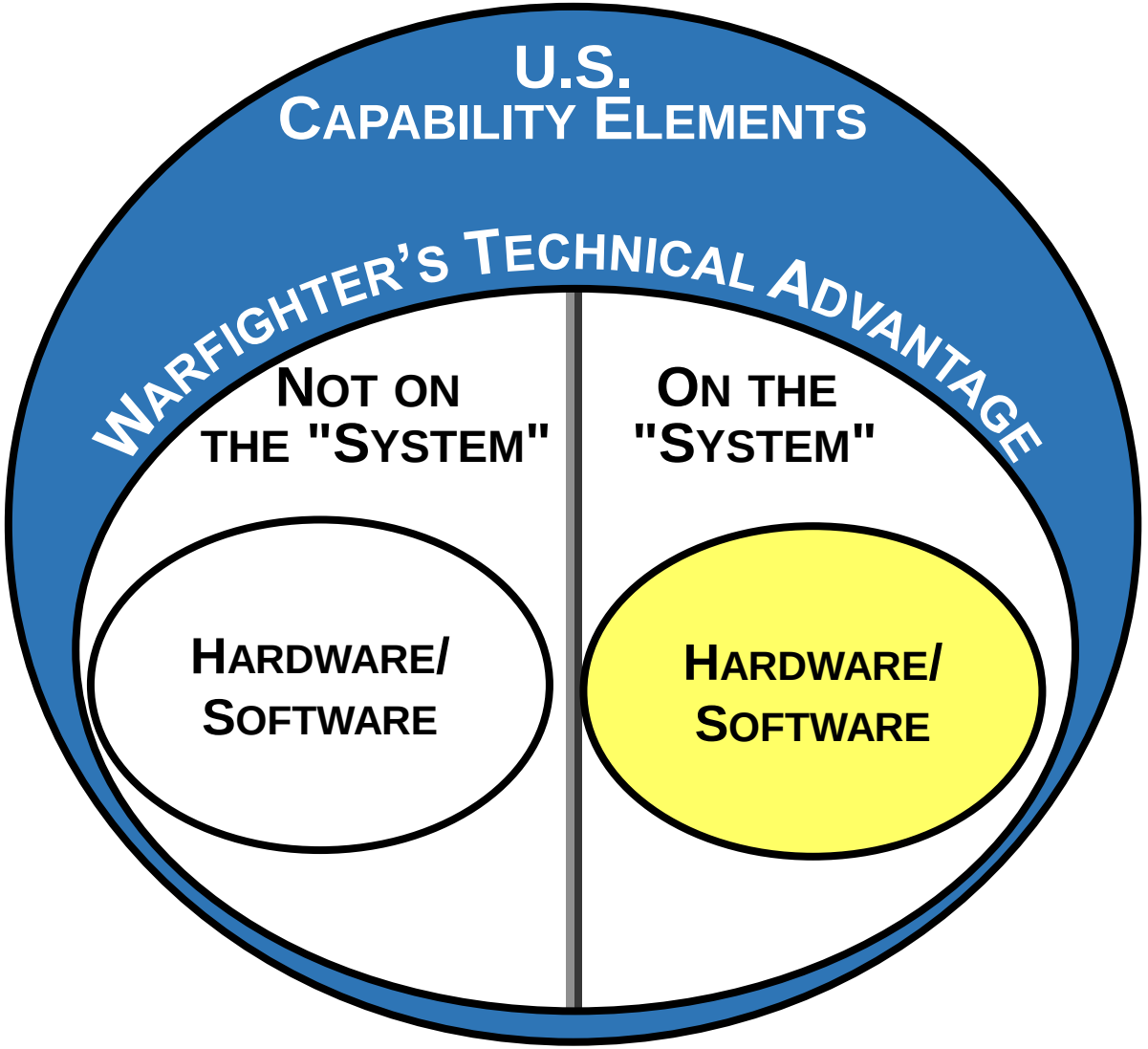
- **1997: CPI term was created as part of the DoDD 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection"**
- **2008 – 2015: CPI definition included "elements or components of a Research, Design, or Acquisition (RDA) Program"**
  - DoDI 2040.02 (2014) "International Transfers of Technology, Articles, and Services"
  - DoDI 5205.11 (2013) "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)"
- **2015 – Current: CPI definition aligned to "warfighter's technical advantage" that may include but is not limited to specific software and hardware "residing on the system"**
  - DoDD 5200.47E (2015) "Anti-Tamper" (utilizes 2015 DoDI 5200.39 definition)
  - DoDI 5230.28 (2016) "Policy for LO/CLO Programs" (utilizes 2015 DoDI 5200.39 definition)

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

DoD CPI Definitions

- **DoDI 5200.39, *"CPI Identification and Protection within RDT&E" (issued 2015)* and DoDI 5230.28 *"Policy for LO/CLO Programs" (published 2016; defines CPI and ref. to 5200.39)***
  - U.S. capability elements that contribute to the **warfighter's technical advantage**, which if compromised, undermines U.S. military preeminence. U.S. capability elements **may include, but are not limited to**, software algorithms and specific hardware **residing on the system,** its training equipment, or maintenance support equipment.
- **DoDI 5205.11, *"Management, Administration, and Oversight of DoD SAPs" (issued 2013; almost identical to the first part of DoDI 5200.39 2008 definition)***
  - **Elements or components of a SAP** that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage, significantly alter program direction, or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.
- **DoDI 2040.02, "International Transfers of Technology, Articles, and Services" *(issued 2014; identical to the first part of DoDI 5200.39 2008 definition)***
  - **Elements or components of a RDA program** that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage, significantly alter program direction, or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. This includes information about applications, capabilities, processes, and end-items, elements or components critical to a military system or network mission effectiveness, and technology that would reduce the U.S. technological advantage if it came under foreign control.

DoDI 5200.39 (2015) Definition of CPI



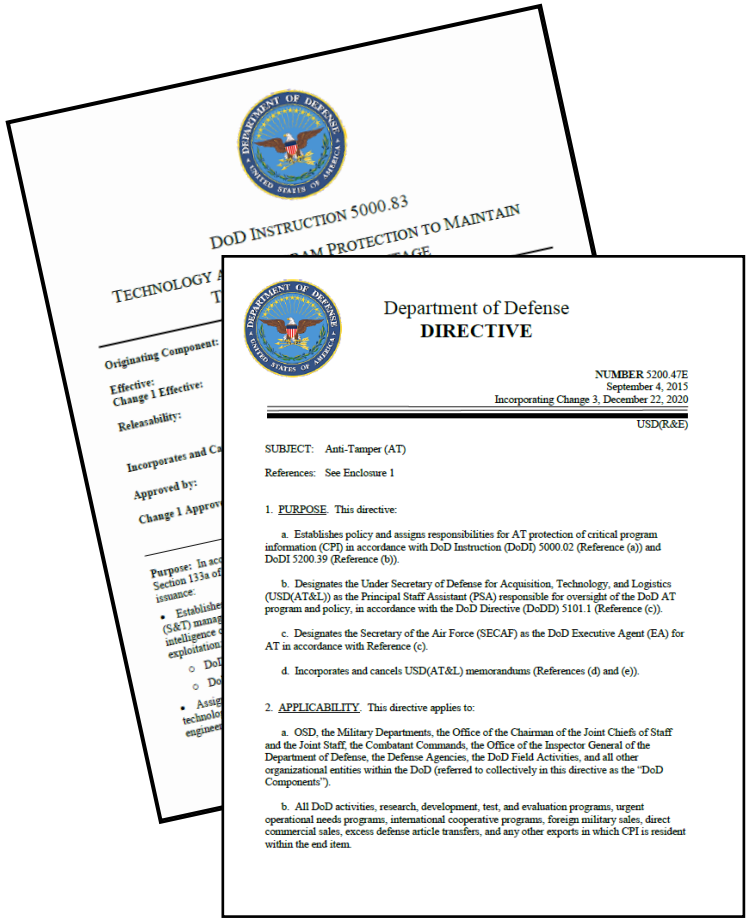
- **CPI definition in DoDI 5200.39 uses and defines "U.S. capability elements":**

  CPI - U.S. capability elements that contribute to the warfighter's technical advantage, which if compromised, undermines U.S. military preeminence. U.S. Capability Elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment

- **Objective (highlighted): Create a specific term for the warfighter's technical advantage when the capability is "on the system" and subject to reverse engineering attacks**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

DoDD 5200.47E: Anti-Tamper



DoD INSTRUCTION 5000.83

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).

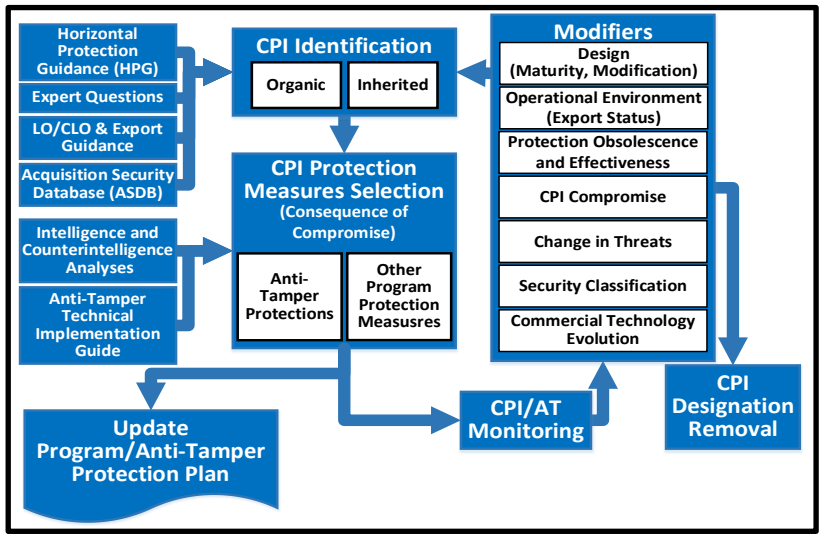
d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

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, excess defense article transfers, and any other exports in which CPI is resident within the end item.

- **Establishes AT Program:**
  - Designates Secretary of the Air Force as the DoD Executive Agent for AT
  - Requires DoD Component heads to establish Offices of Primary Responsibility for AT
- **Requires DoD Component heads in alignment with guidance from the DoD Executive Agent for AT to:**
  - Conduct AT planning
  - Implementation
  - Evaluations
- **Uses DoDI 5200.39, CPI Identification and Protection within Research, Development, Test and Evaluation (RDT&E), to identify CPI**



Provides policy for AT activities for the end item, to include identification of the end item; requires identification of Critical Program Information

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

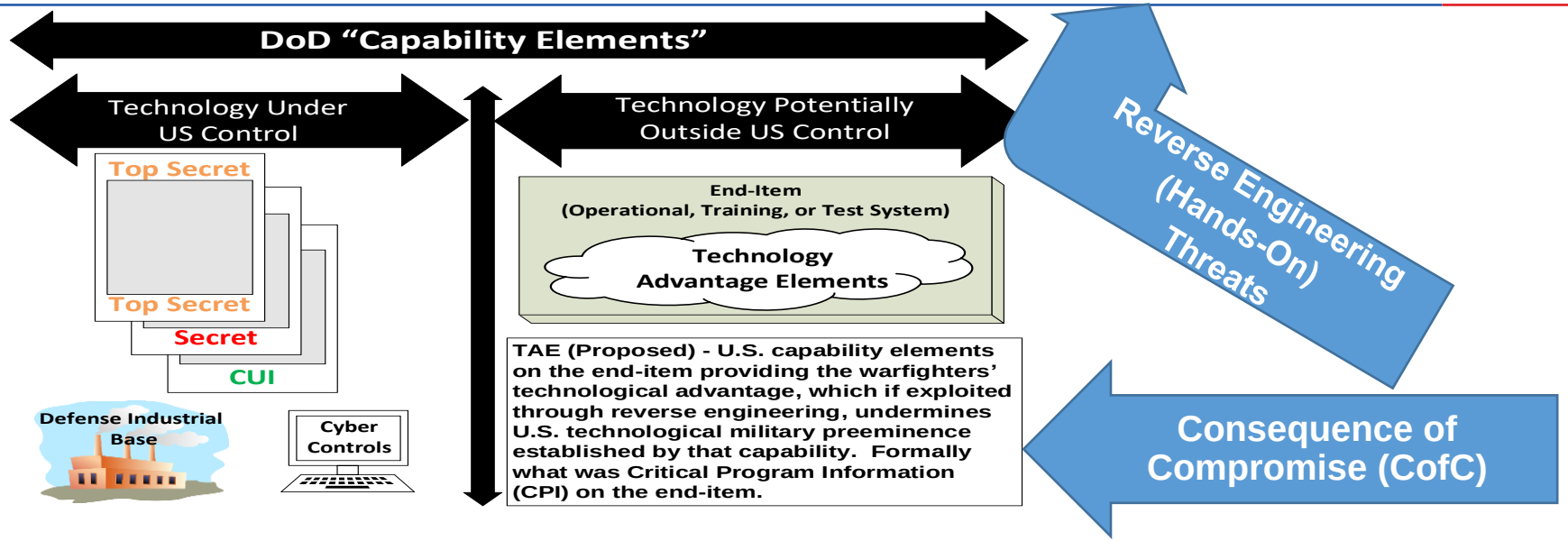
Current Alignment of CPI with Anti-Tamper

DoD Instruction 5200.39	CPI	DoD Directive 5200.47E
"CPI Identification and Protection within RDT&E"		*"Anti-Tamper"*
Establishes policy and assigns responsibilities for the **identification** and **protection** of **CPI**	(DoDD 5200.47E utilizes CPI definition from current 5200.39)	Establishes policy and assigns responsibilities for **Anti-Tamper (AT) protection** of **CPI**

- **2015 updates of DoDI 5200.39 and DoDD 5200.47E definitions and responsibilities are complementary and were synchronized:**
  - DoDI 5200.39 - CPI: Hardware and software algorithms that **may be** residing on the system
  - DoDD 5200.47E - AT: Systems engineering activities to prevent or delay exploitation, alteration, or countermeasure development of (or to) CPI in U.S. defense systems due to reverse engineering
- **Other communities utilize CPI definitions other than the DoDI 5200.39 CPI definition**
  - DoDI 2040.02 (2014) "International Transfers of Technology, Articles, and Services"
  - DoDI 5205.11 (2013) "Management, Administration, and Oversight of DoD SAPs"

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Potential Solution 1: Create Different Definition for the Anti-Tamper Community



- **DoD's technical advantage needs protection across the development and operational lifecycle. However, systems exposed to reverse engineering attacks exhibit unique vulnerabilities that need to be protected utilizing AT techniques**
- **DoDD 5200.47E is being updated to clarify AT responsibilities for reverse engineering (hands-on) threats encountered when the end-item (system, maintenance, and test equipment) may be outside of U.S. control**
- **Technology Advantage Elements (TAE): A proposed term to identify specific warfighter advantages on the end-item eligible for AT protections from the unique vulnerabilities presented from reverse engineering**

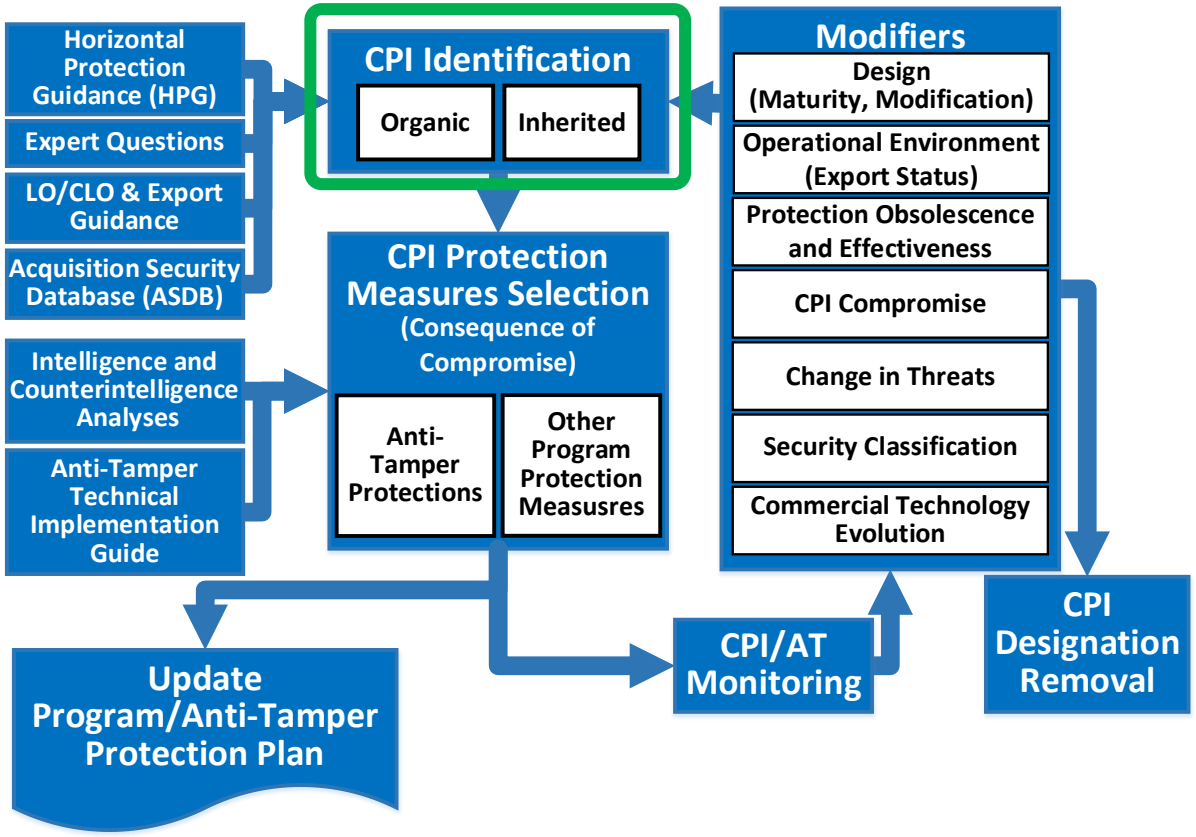
Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Challenge 2: Differing Chains of Command Use Different CPI Processes

- **The OUSD for Research and Engineering (OUSD(R&E)) is running a working group to clarify the CPI processes**
  - Goals:
    - Align AT as a technology protection activity
    - Clarify AT processes
    - Clarify identification (and removal) criteria for CPI
  - Completed:
    - Mapping and identification of working group members
    - Mapping of the CPI identification process

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

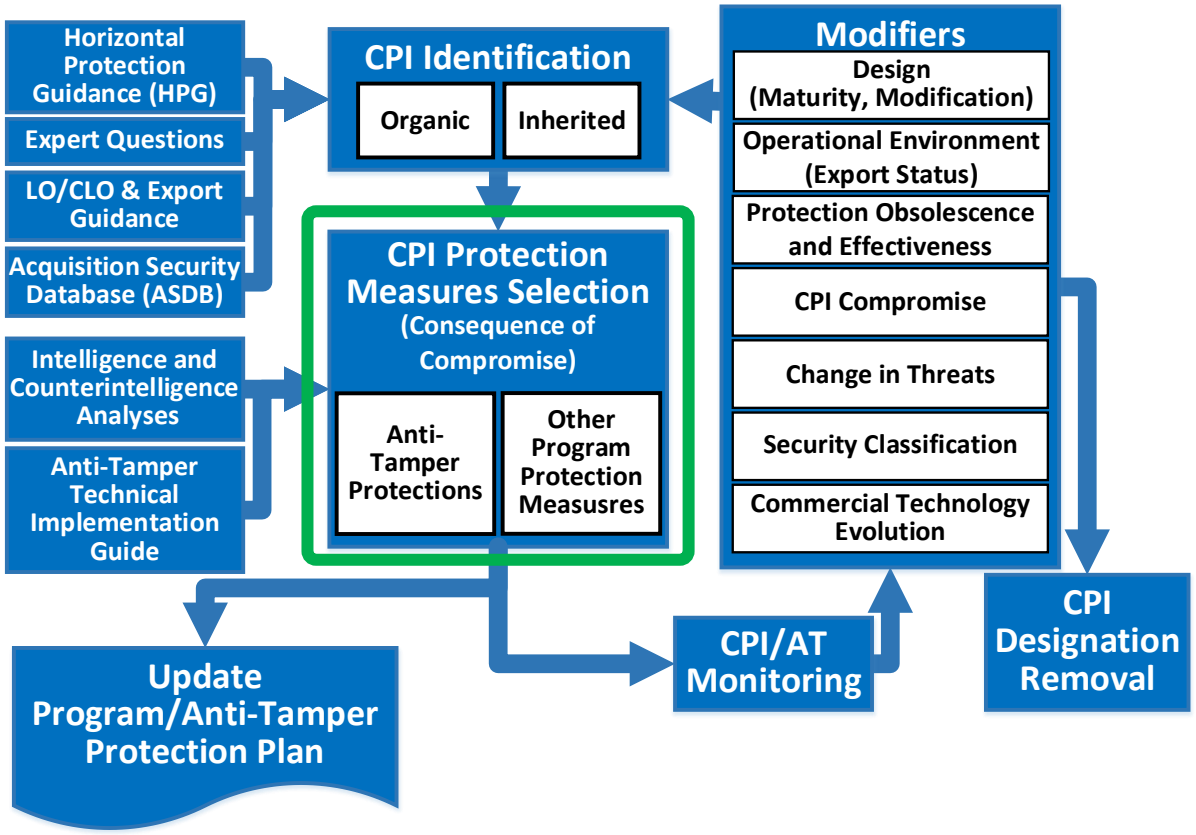
CPI Process: CPI Identification



- **Stakeholders should:**
  - Identify CPI to determine if it is:
    - Organic CPI (developed by the program), and/or
    - Inherited CPI (developed by another program but incorporated into the program/system) exists or will exist in the operational, deployed system
  - Identify technology that DoD no longer considers to provide a U.S. technological advantage to the warfighter
- **S&T managers and engineers should identify CPI early and reassess the CPI throughout the lifecycle of the program, to include:**
  - Prior to:
    - Each acquisition milestone, or
    - Systems Engineering Technical Review;
  - Operations and sustainment; and
  - Software/hardware technology updates

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

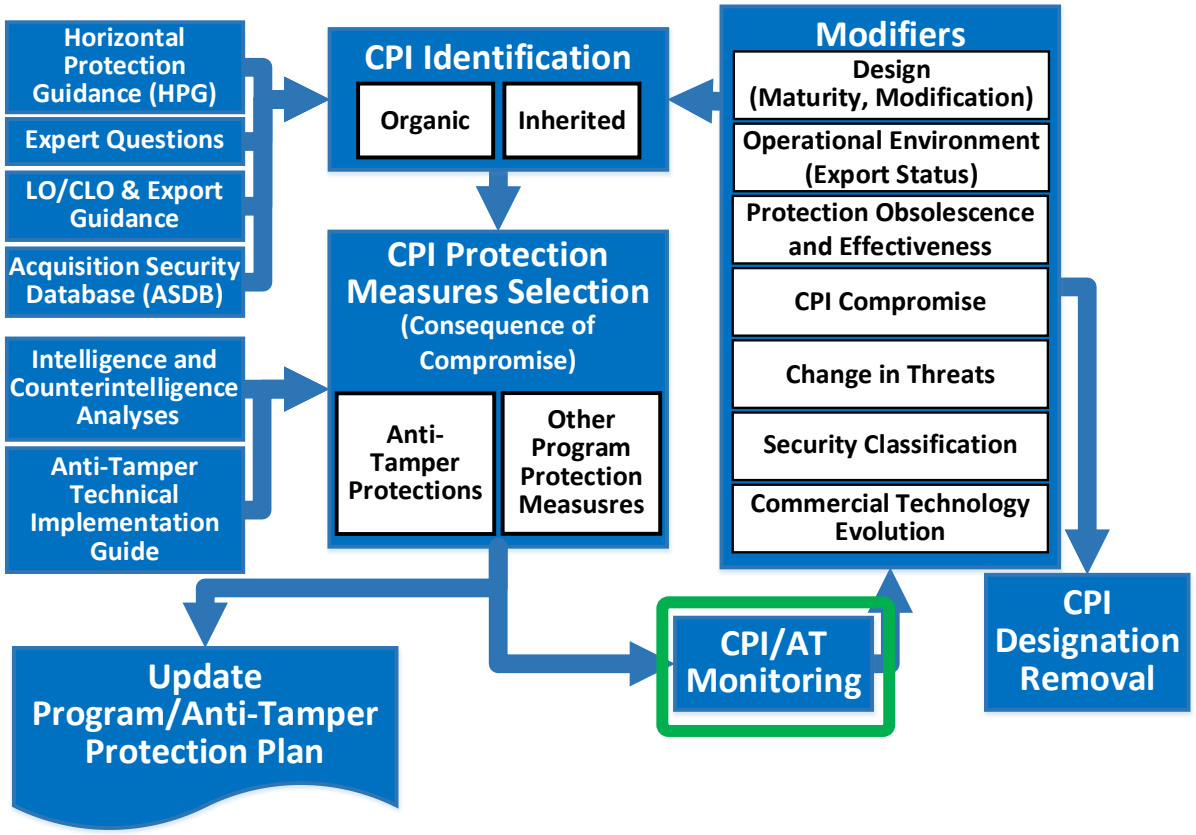
CPI Process: CPI Protection Measure Selection



- **Stakeholders should:**
  - Select CPI protection measures soon after identification of the CPI
- **Protection measures seek to protect the warfighter's technical advantage by deterring, delaying, detecting, or reacting to:**
  - Reverse engineering attempts, or
  - Other attacks on the warfighter's technical advantage
- **Other protection measures, listed under other systems security engineering specialties and other security specialties, may also contribute to the protection of CPI**
  - Design and manufacturing know-how is protected in accordance with the classification guidance and protection mechanisms
  - When manufacturing information is considered unclassified controlled technical information (CTI), a Component would protect it in accordance with the protections for CTI

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

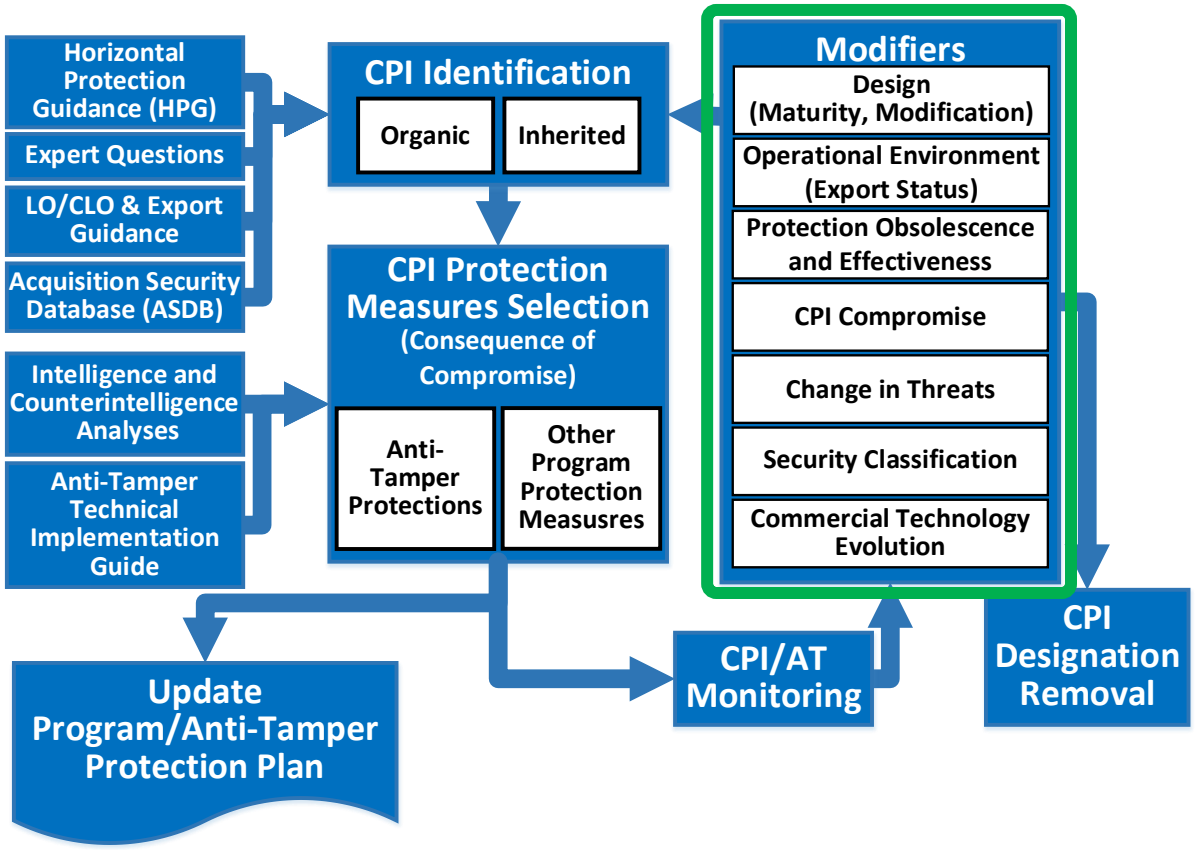
CPI Process: Monitoring



- **Stakeholders should:**
  - Commence CPI monitoring soon after identifying the CPI
  - Continue this monitoring throughout the lifecycle of the program
- **CPI monitoring determines:**
  - If an event has occurred that requires a reassessment of the CPI or its protection measures
  - Removal of the CPI designation
- **If (or when) these events occur, programs should reassess the CPI and protection measures to determine if they can or need to make changes to the CPI's associated protection measures**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

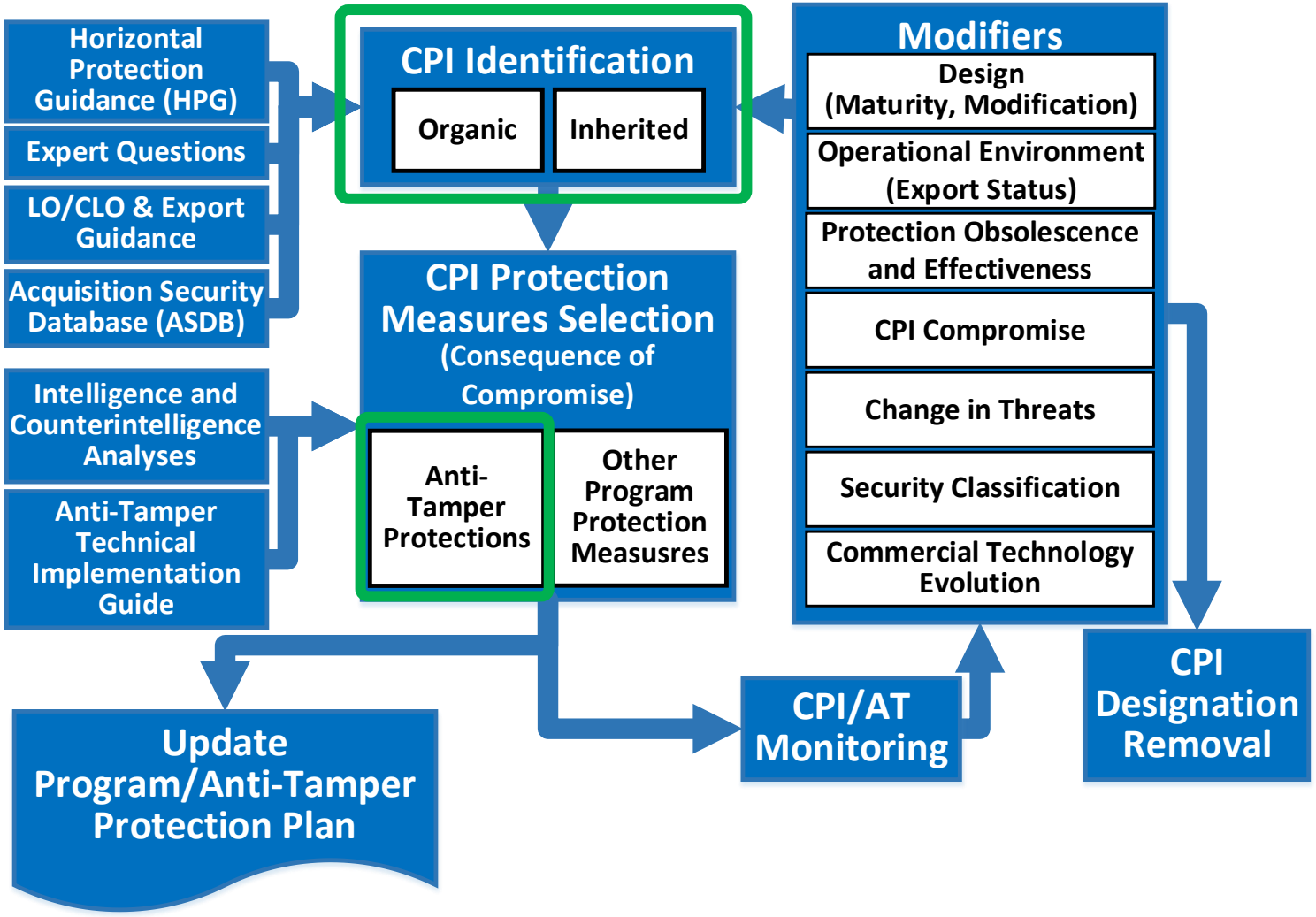
CPI Process: Modifiers



- **Design:**
  - **Capability maturation**: A change in the state-of-the-art for a particular capability and thus the thresholds used for CPI identification
  - **System modification**: A change to the system architecture and/or designs
- **Operational Environment**: A change in the physical location of the system with CPI other than that for which it was originally designed
  - **Export status:** Current or future plans for the system to be available to allies or partners through Direct Military Sales or other export programs
- **Protection Obsolescence or Effectiveness**: A change in the ability of the CPI protections to deter, delay, detect, and respond to attempts to compromise CPI
- **CPI Compromise:** A known loss of the capability can result in a change in the need to protect the capability
- **Change in Threats**: A change in foreign adversary interest and skill in obtaining CPI
- **Security Classification:** A change to a relevant SCG
- **Commercial Technology Evolution:** Improvements in the state-of-the-art can erode technical advantage over time

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Ongoing CPI Process Improvement Working Groups



CPI Identification Working Group

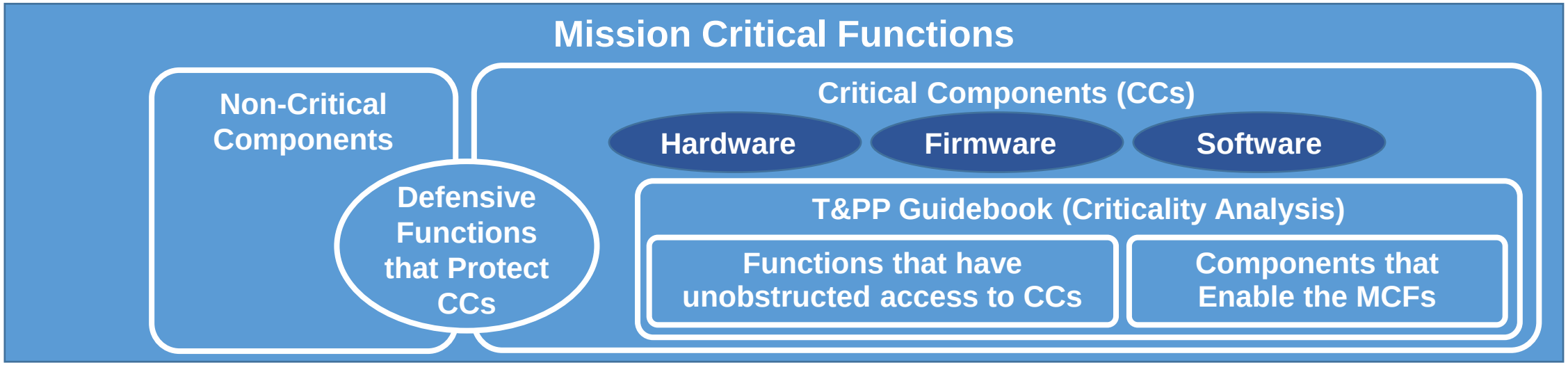
- **Working within the larger DoD Community:**
  - Clarify and refine the identification process
  - Discuss and develop criteria for CPI designation removal

AT Processes Tiger Team

- **Working within the AT community:**
  - Identify potential efficiencies in applying AT to identified technologies

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

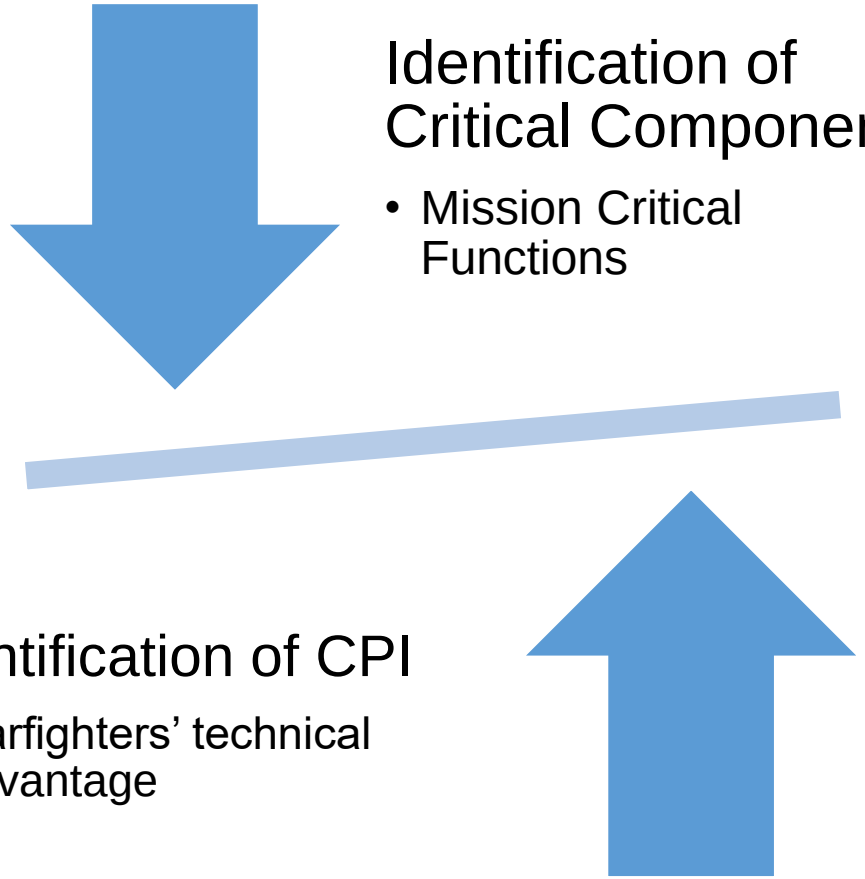
DoDI 5200.44 and T&PP Guidebook: Mission Critical Functions and Components



- **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 #23-S-0021 applies. Distribution is unlimited.

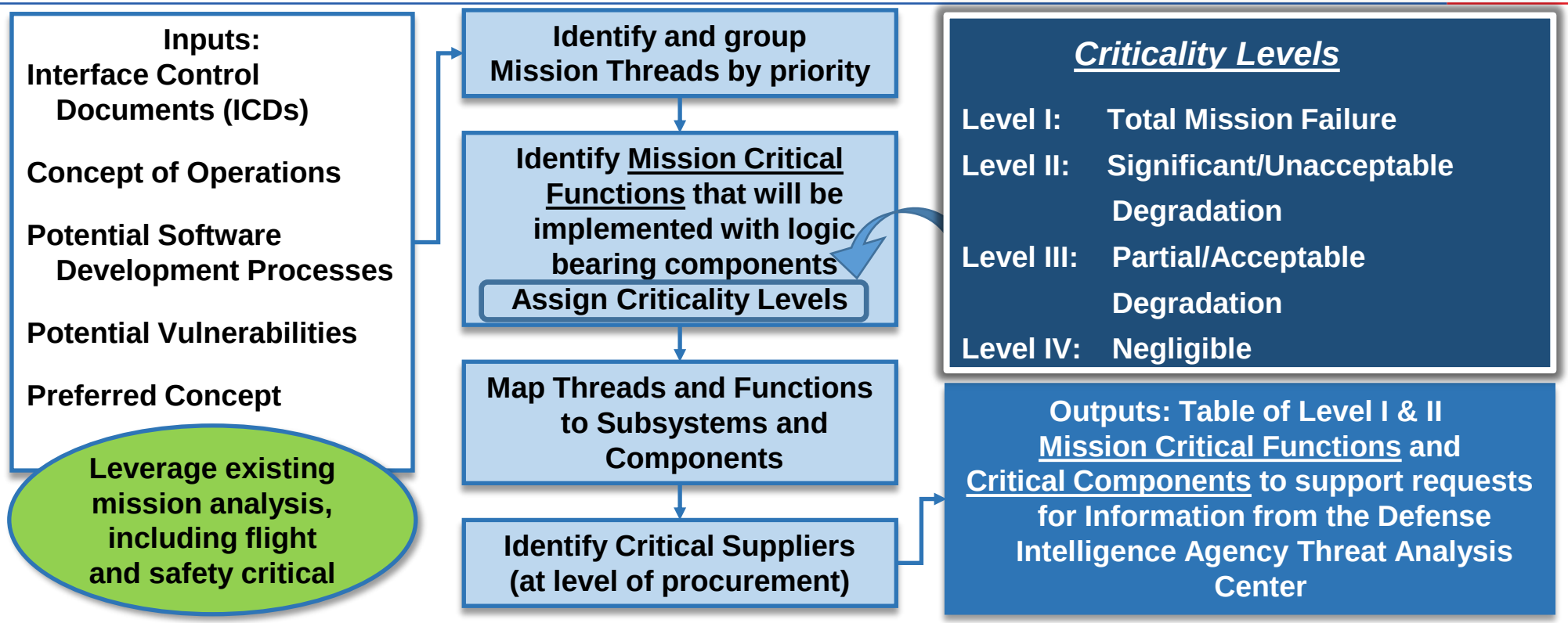
Critical Components and CPI Identification



- **Identification of Critical Components (CCs) supports the system's ability to complete the assigned mission if that component is lost due to sabotage**
- **Identification of CPI supports the DoD's ability to protect the warfighter's technical advantage from loss**
  - Components that protect Mission Critical Functions become CCs too
- **While there is overlap in the components and technologies identified, there are enough unique properties to each process that they should be evaluated separately**
  - CPI Process may identify components and technologies that are not critical to the mission (training and maintenance)
  - Mission Critical Function Process may identify components that don't directly contribute to the warfighter's technical advantage

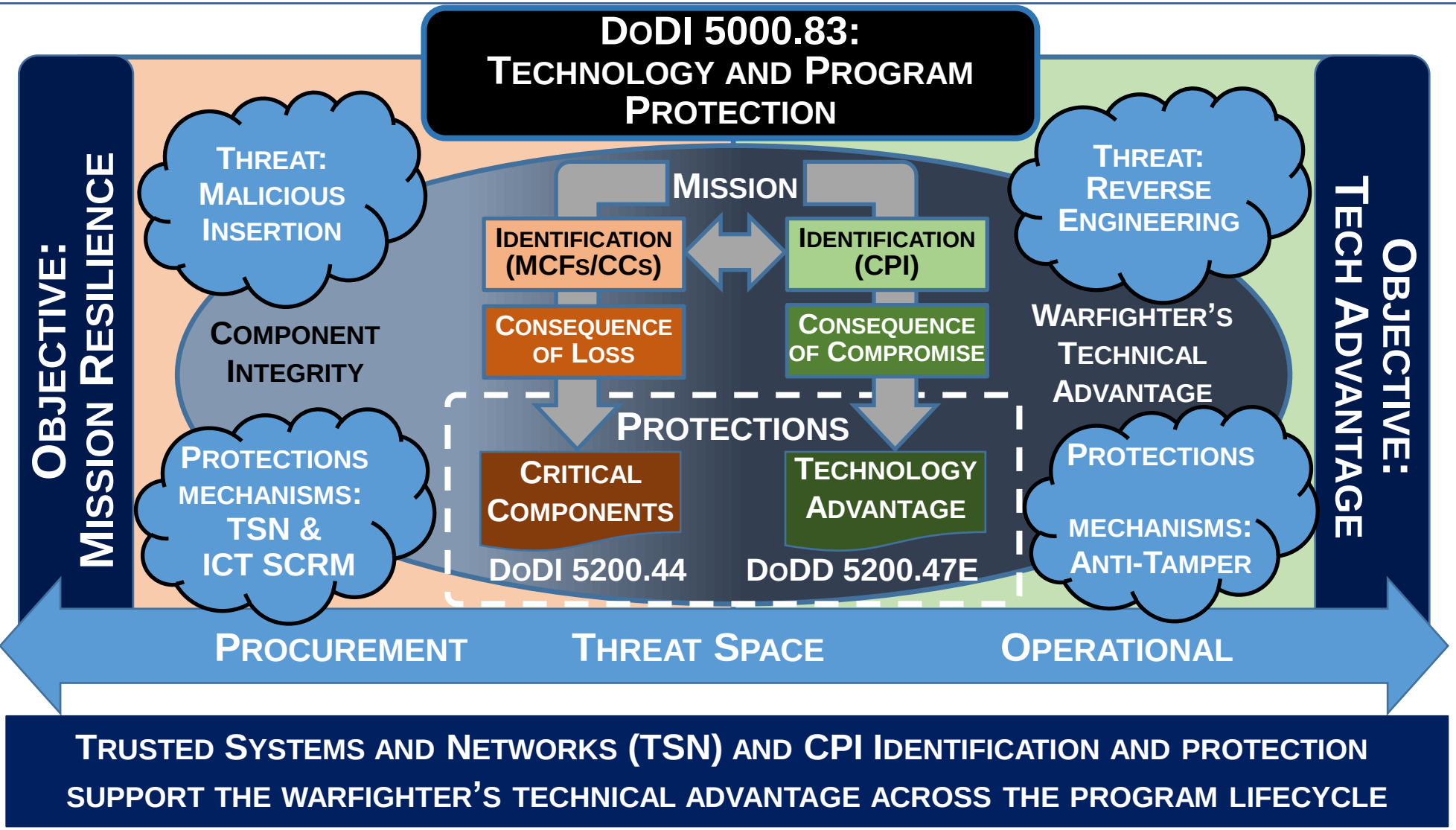
Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Criticality Analysis DoDI 5200.44 Definition and Methodology



An end-to-end **functional decomposition** performed by systems engineers to **identify mission critical functions (MCFs) and components**. Includes identification of system missions, decomposition into the functions to perform those missions, and **traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s).**

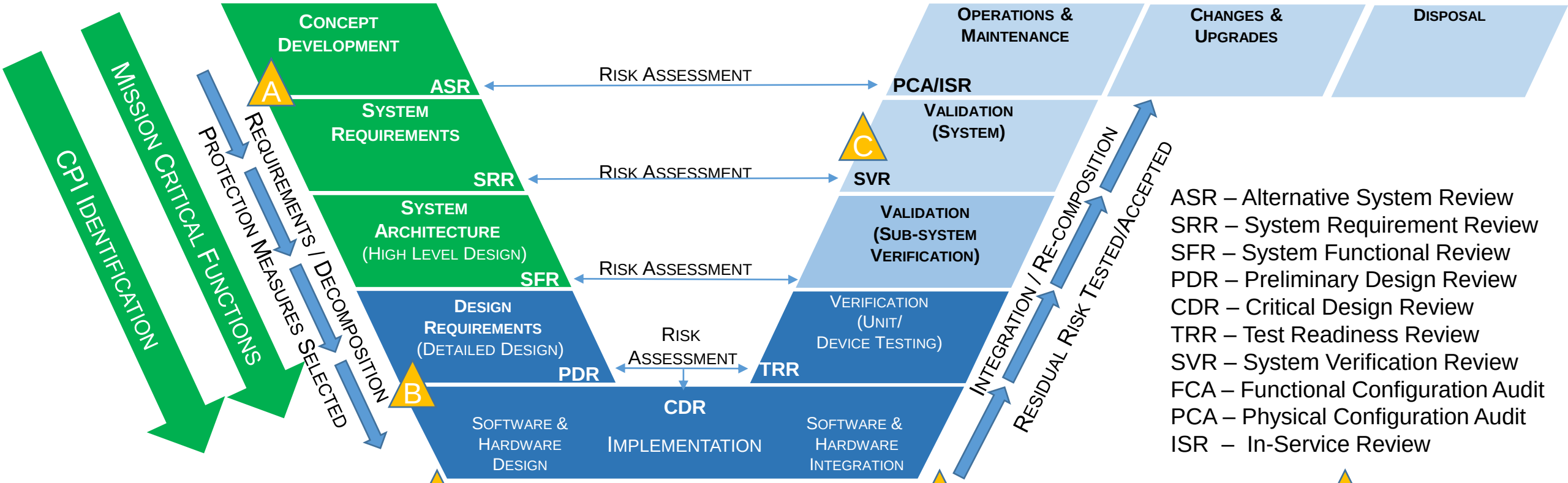
Technology and Program Protection in the Adaptive Acquisition Framework



- DoDI 5000.83 provides S&T managers and lead engineers responsibilities for all technology and program protection activities
- DoDI 5200.44 and DoDD 5200.47E provide additional responsibilities for protections from specific vulnerabilities prioritized based on operational mission
- Each Component implements the policies in the manner that works best for them

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Systems Engineering "V": CPI Identification and Trusted Systems and Networks Criticality Analysis



ASR – Alternative System Review
SRR – System Requirement Review
SFR – System Functional Review
PDR – Preliminary Design Review
CDR – Critical Design Review
TRR – Test Readiness Review
SVR – System Verification Review
FCA – Functional Configuration Audit
PCA – Physical Configuration Audit
ISR – In-Service Review

	ASR	A	SRR	SFR	PDR	B	CDR	SVR	C	PCA/ISR
Criticality Analysis (CA)	Mission-based functions		System requirements	Sub-system/ sub-function level	Assembly/ component		Component (updated)	Component (updated)		Component (updated)
CPI Identification and Protection	AT Plan (concept) (105 Days before MS A)			AT Plan (initial)	AT Plan (final) AT Eval Plan (draft)		AT Eval Plan (final) AT Eval Report	CPI Validated		CPI Validated

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

Next Steps

- **Next steps**
  - Conduct use-case analysis with:
    - Anti-Tamper Program Office (ATPO)
    - Special Access Program Central Office (SAPCO)
    - International cooperation
  - Identify efficiencies to be gained in the process
  - Work to develop a DoD tool for CPI identification
  - Out-brief Industry on output

Distribution Statement A: Approved for public release. DOPSR case #23-S-0021 applies. Distribution is unlimited.

USD(R&E)

Secure Cyber Resilient Engineering (SCRE) Practice

Standardizing the SCRE Practice

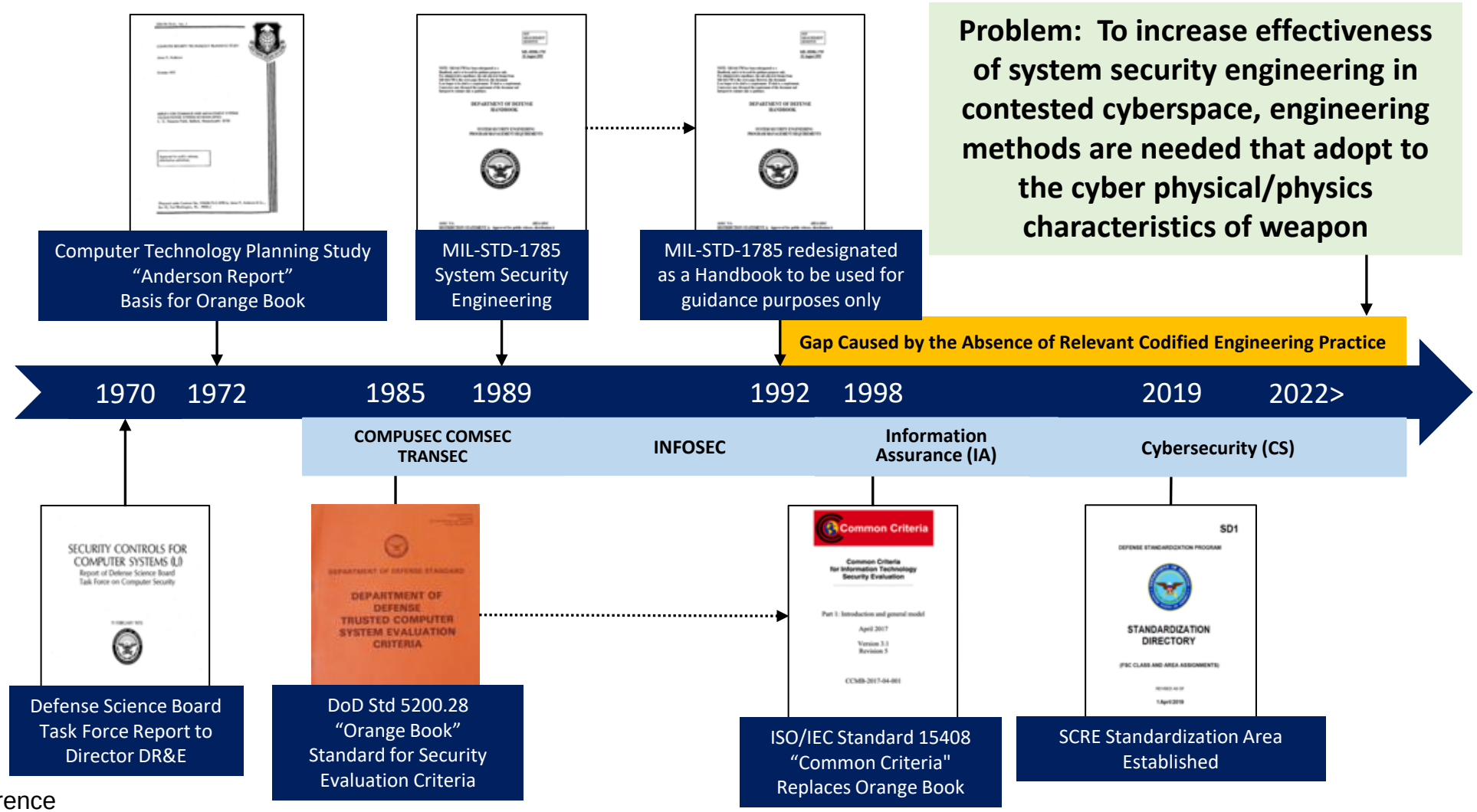
Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for Research and Engineering
Science and Technology Program Protection

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

DoD System Security Engineering Timeline



Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

While Times Have Changed…
The Fundamental Engineering Problem Remains…

How do we know our approach works?

Assessing Performance Across the System Life Cycle

1970's

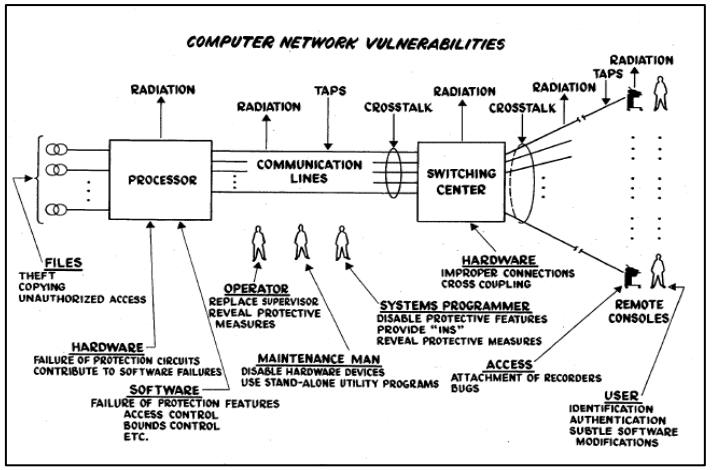


Figure 3 - "Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security", 1970

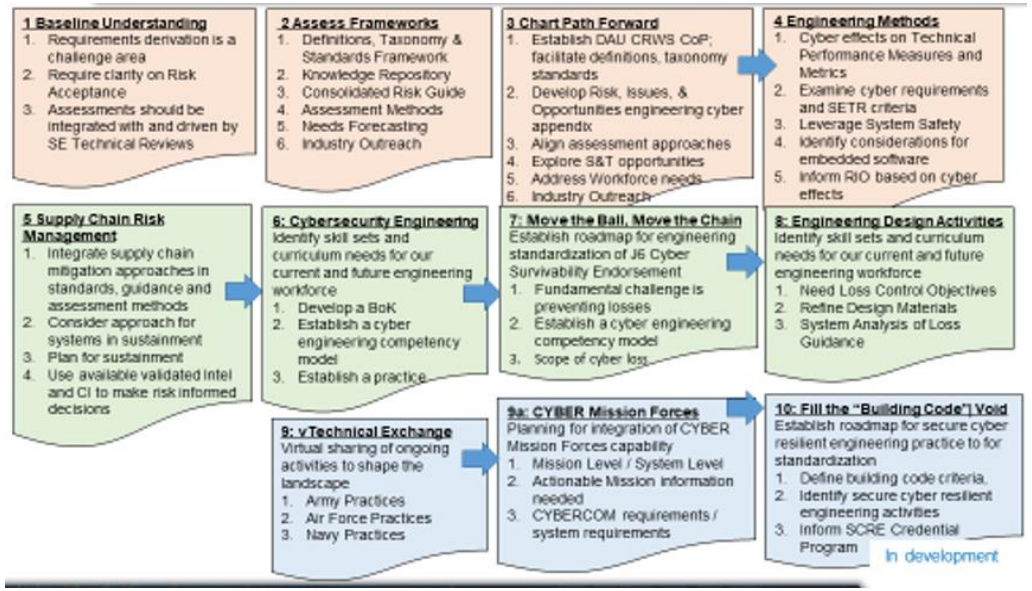
> 2030's

SCRE Goals

1. Structured standards and methods to evaluate requirements for testability, traceability, and de-confliction
2. Traceable evidence for appropriate decisions at every level of design
3. Cumulative evidence acquired through verification methods conducted by engineering and test organizations
4. Operational Behavior Prediction and Recovery: real time monitoring, just-in-time prediction, and mitigation of undesired decisions and behaviors
5. Reusable assurance arguments based on previous evidence "building blocks"

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Implementation: Engineering Cyber Resilient Weapon Systems Workshop



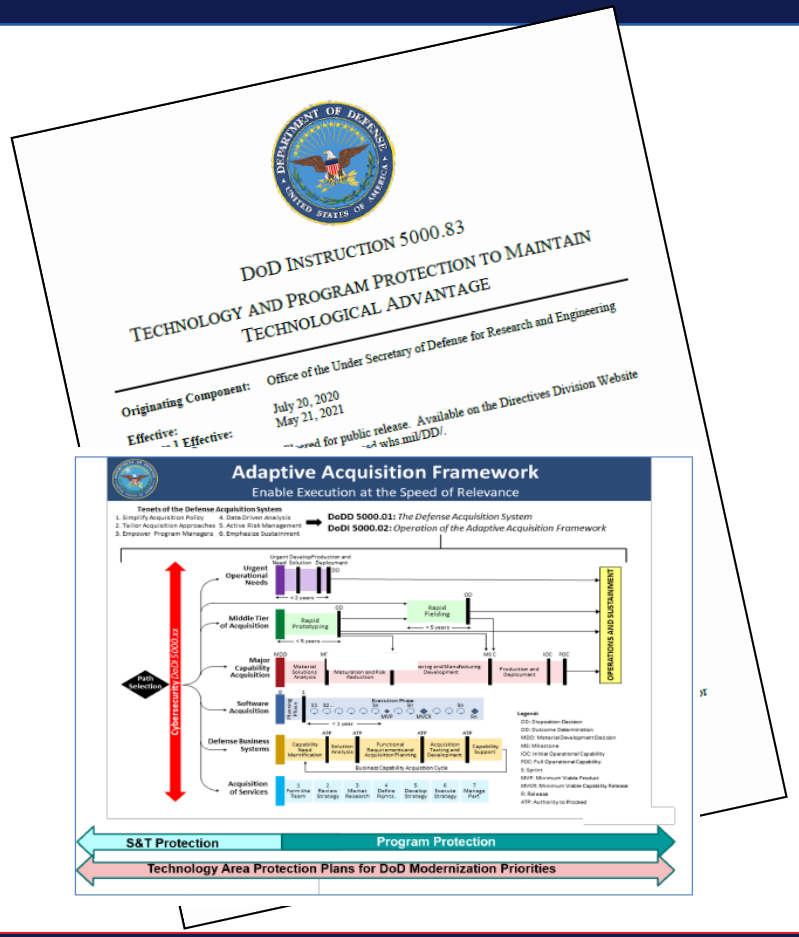
Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

March 2017: SCRE Standardization Area
– Defense Standardization Program

- **August 2018: Cyber Resilient Weapon System (CRWS) Workshop Report: Preparing the Engineering Workforce for Cybersecurity Challenges**
- **March 2019: Draft SCRE Competency Model**
- **November 2020: Defense Acquisition University Approved to Establish the SCRE Credential Program**
- **June 2021: CRWS Body of Knowledge Deployment**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

DoDI 5000.83: Technology and Program Protection to Maintain Technological Advantage

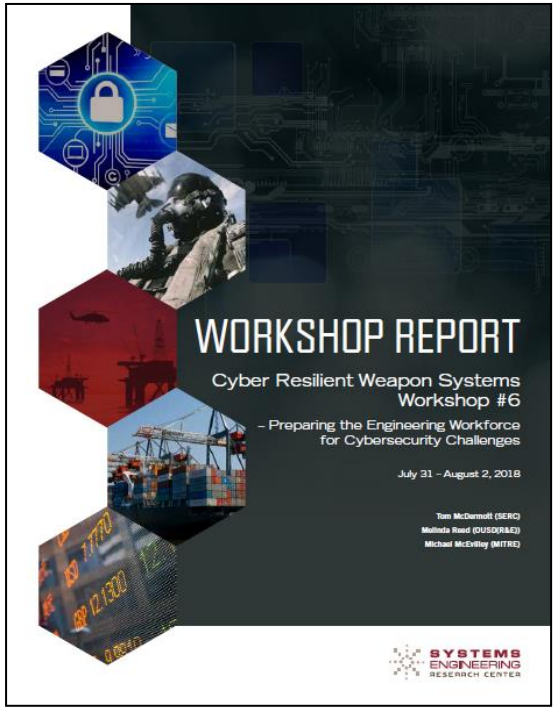


- **Establishes responsibilities and procedures for *S&T managers and engineers* to manage system security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **System security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration
- **Introduces S&T protection and Technology Area Protection Plans**
- **Points to engineering and test and evaluation issuance**
- **Aligns Program protection planning with acquisition pathways**

Design for security and cyber resiliency includes allocation of requirements to the system architecture and design and assess the design for vulnerabilities

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE: Design for Security and Cyber Resilience



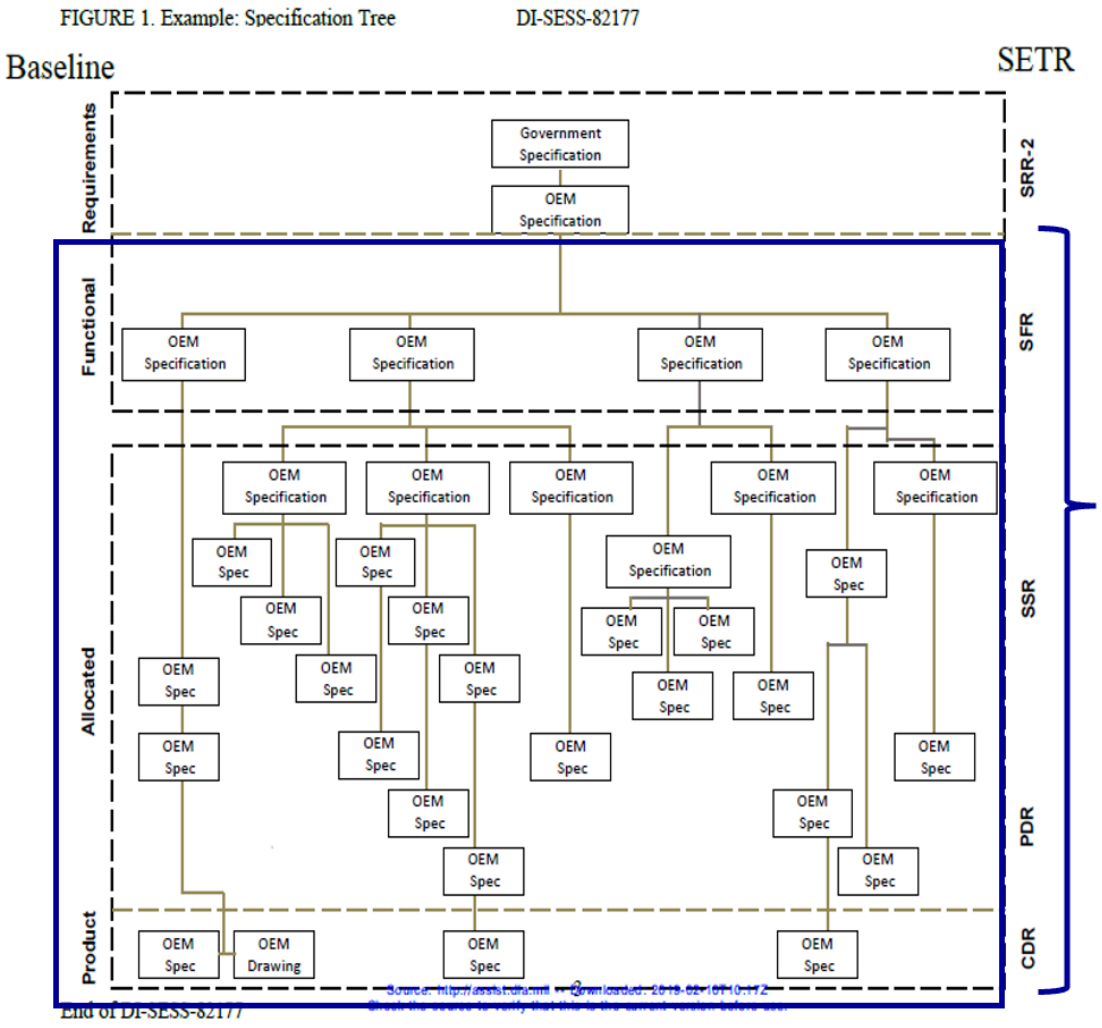
"Gap: Engineering domain knowledge, methods, and tools have not yet fully addressed the effect cyberspace has on for designing and evaluating safe and secure achievement of capability performance measures" – CRWS 6 Workshop Report

- **Develop application specific interpretation guides and use these to drive education and training outcomes**
- **Increase consistency and repeatability of engineering approaches, methods, tools, and outcomes; improve efficiency and effectiveness of safe and secure engineering practice**
- **Improve communication of requirements, methods, and tools, across government, industry, academia, and military operations and sustainment stakeholders**

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

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Approach to Codify the SCRE Practice

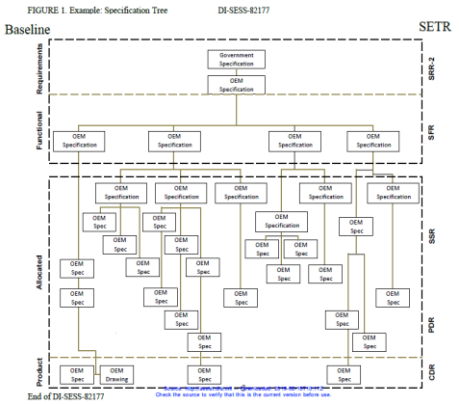


DoDI 5000.83 Expectations

- **Requirements**
  - Derive and include cybersecurity, security, and other system requirements into system performance specifications
  - Incorporate the derived requirements, design characteristics, and verification methods in the technical baseline and system requirements traceability verification matrix
  - Maintain bi-directional traceability among requirements throughout the system lifecycle
- **Design**
  - Allocate cybersecurity and related system security requirements to the system architecture and design
  - Manages access to, and use of, the system and system resources
  - Has a structure sufficient to protect and preserve system functions or resources
  - Maintains priority system functions under adverse conditions
  - Is configurable to minimize exposure of vulnerabilities that could adversely impact system function, intended operational use driven, and mission objectives.
  - Monitors, detects, and responds to security anomalies
  - Interfaces with supporting systems and external networks and external services
- **Analysis**
  - Assess the design for vulnerabilities

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE Activities: Engineering Method



Requirements Analysis
- Analyze capability and adversity driven by mission, operations, sustainment, and environments
- Identify functional requirements
- Define/refine performance and design constraint requirements

System Analysis
- Trade studies
- Effectiveness analysis
- Adversity-driven loss analysis
- Risk, issue, and opportunity analysis

Requirements Loop

Functional Analysis/Allocation
- Decompose to lower-level functions
- Allocate performance and other limiting requirements to all functional levels
- Define/refine functional interfaces
- Define/refine/integrate functional architecture

Design Loop

Verify

Synthesis
- Transform architecture (functional to physical)
- Define alternative system concepts, configuration items, and system elements
- Select preferred product and process solutions
- Define/refine physical interfaces

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE: Establishing Disciplines and Practices

- **Synergy with System Safety**
  - Adopt approaches and methods of system safety to establish secure cyber resilient engineering
- **System Resilience**
  - Characterize resilience as a graph of delivery of capability over time
  - Develop concept of resilience scenario and patterns expressing resilience in system requirements
- **System Security**
  - Characterize security as a control function to enforce authorized behaviors and outcomes and to protect against loss
  - Develop patterns expressing security in system requirements
- **Loss-Driven Protection Control**
  - Loss is the basis for security activities and judgments
  - Protection needs exercise control to prevent the occurrence of loss and to limit the extent of loss effects
- **Assured Trustworthy Secure Design**
  - Identify idealized design foundations and principles for security
  - Define multidisciplinary-influenced principles that underlie assured trustworthy secure system design
- **Assurance, Confidence, Risk**
  - Assurance: Justified confidence that a claim has been or will be achieved [IEEE 15026]
  - Insufficient confidence translates to risk
    - DoD MIL-STD 882E “Level of Rigor”
    - NASA System Safety “Assurance Deficit”
  - Differentiate
    - Known, insufficiently known, and unknown scenarios that contribute to risk
    - Risk and issue for security/cybersecurity
- **Software Contribution to Risk**
  - Uncertainty about composed software emergent behaviors and side-effects drives risk

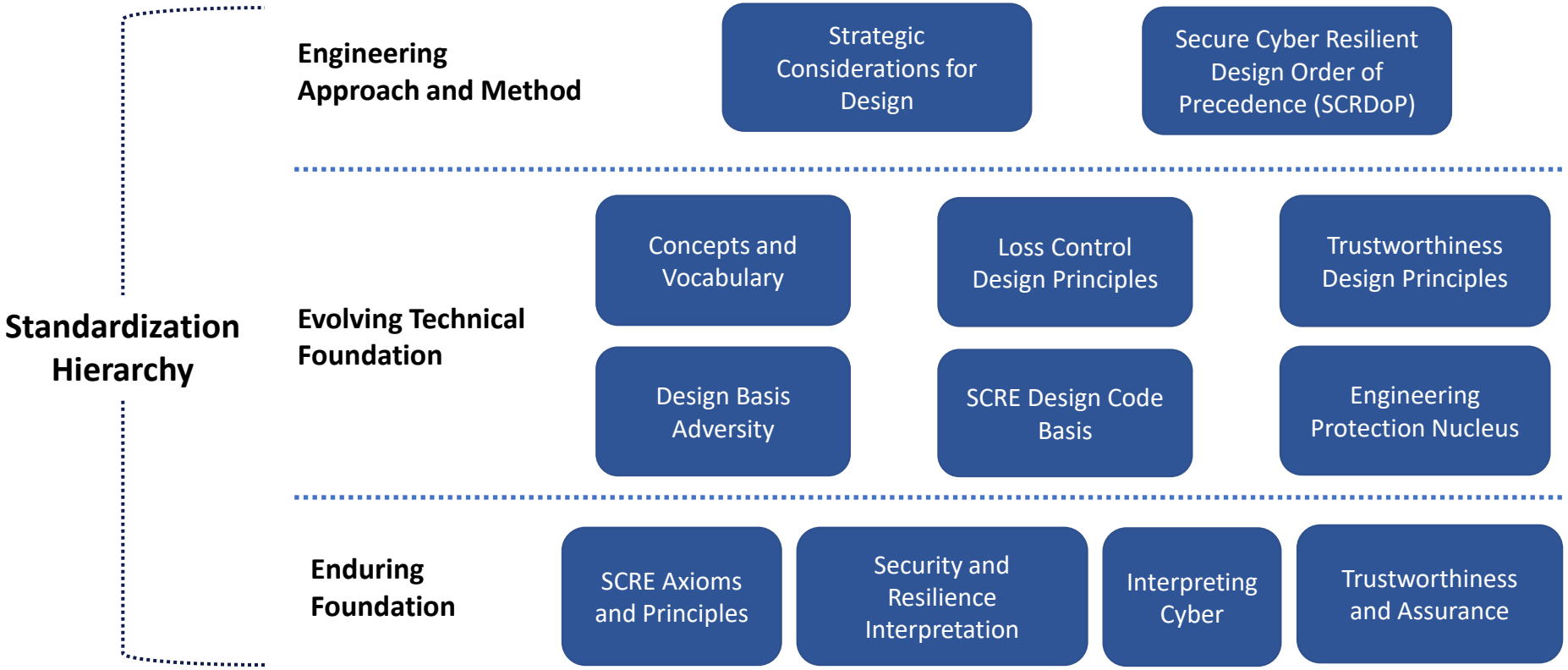
Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE: Standardization Approach

Engineering Approach and Method	Descriptive statement of engineering process, activities, and tasks
Evolving Technical Foundation	The basis of a standard and associated guidance: terms, principles, concepts, etc., that will evolve as appropriate as the practice evolves in response to advances in technology, capability, methods, tools, and the understanding of adversity and how to control adversity and its effects
Enduring Principled Foundation	Core ideas, concepts, philosophy, and interpretations that persist and are not likely to undergo significant change or evolution over time

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE: Technical Whitepapers



Provides basis for consensus building

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Peer Review Through Engineering CRWS Workshops

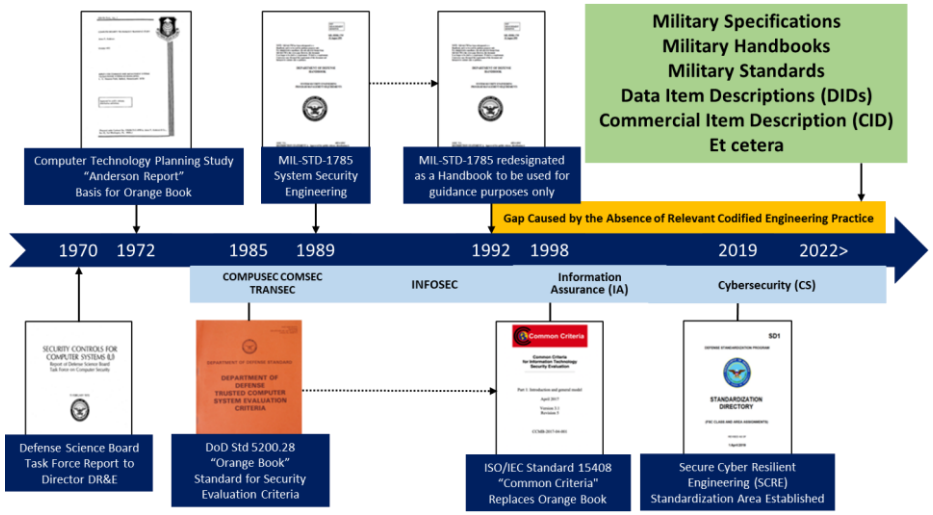
- **Design Code Criteria**
  - Assess, validate, alter the strawman criteria provided
- **Derivation and decomposition of protection requirements**
  - Identify the activities and tasks
- **Assured trustworthy design**
  - Identify the activities and tasks
- **SCRE Analyses**
  - Assess, validate, alter the strawman guidance provided

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Advancing the Practice

CRWS Workshops, NDIA Systems Security Engineering Working Group, and other community engagements

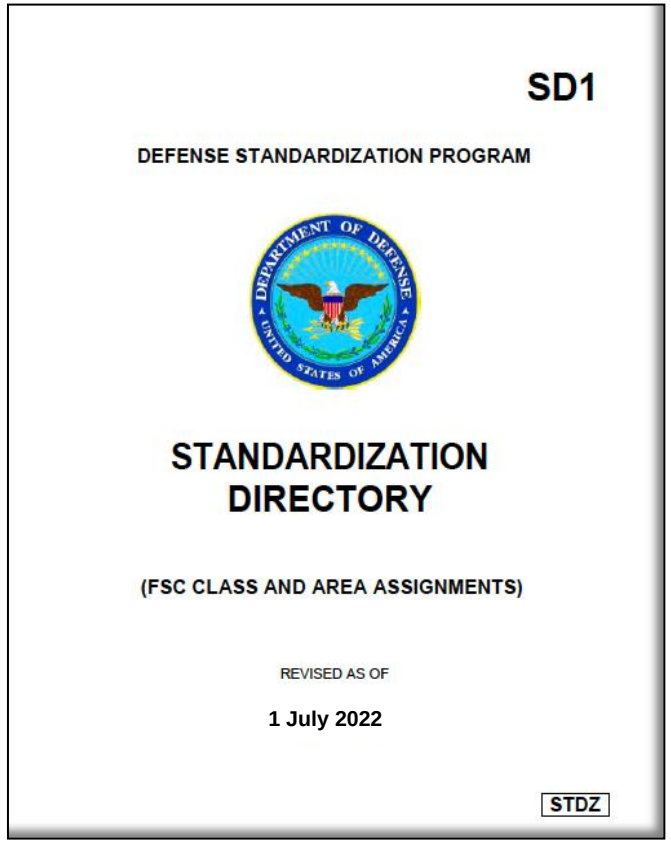
Whitepapers and (future) draft guides and other products



Guidebooks
Military Specifications
Military Handbooks
Military Standards
Data Item Descriptions (DIDs)
etc.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

SCRE Standardization Area


SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

REVISED AS OF

1 July 2022

STDZ

SCRE Area Category

- Covers the ***integration of life cycle security and protection considerations*** in the requirements, design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems that operate in physical and cyberspace operational domains

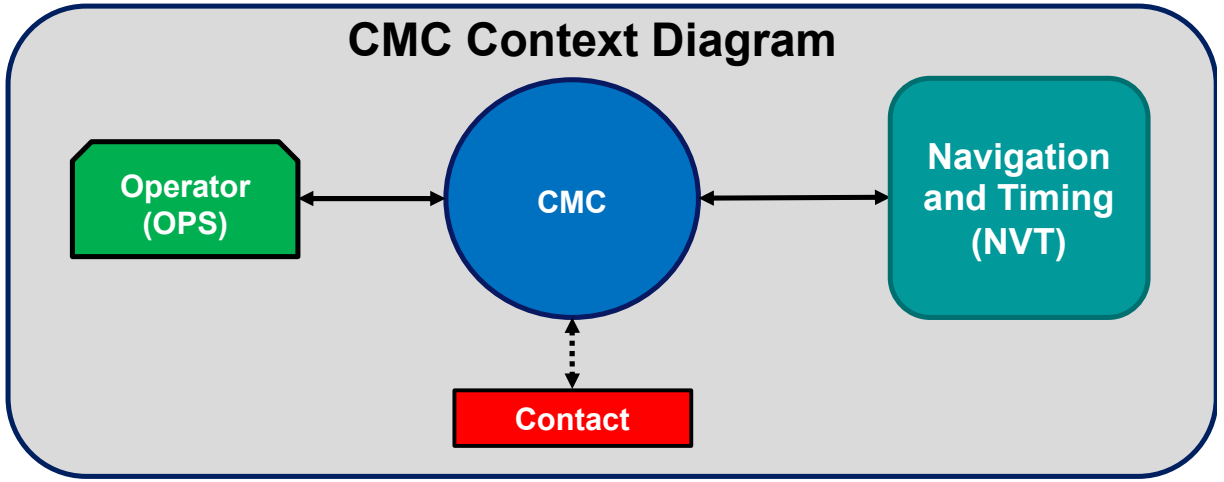
- Specifically encompasses the standards, specifications, methods, practices, techniques, and data requirements ***for the security aspects of systems engineering*** activities executed and artifacts produced, with explicit consideration of malicious and non-malicious adversity

Defense Standardization Program Standards Area for SCRE Engineering Technologies, Disciplines, and Practices

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Next Steps

- **Analysis of CRWS 10 outcomes**
- **Continued work with the Cybersecurity Industry Technical Advisory Group (CITAG)**
- **Additional CRWS Workshops**
- **Release of whitepapers for adoption to CRWS BoK**



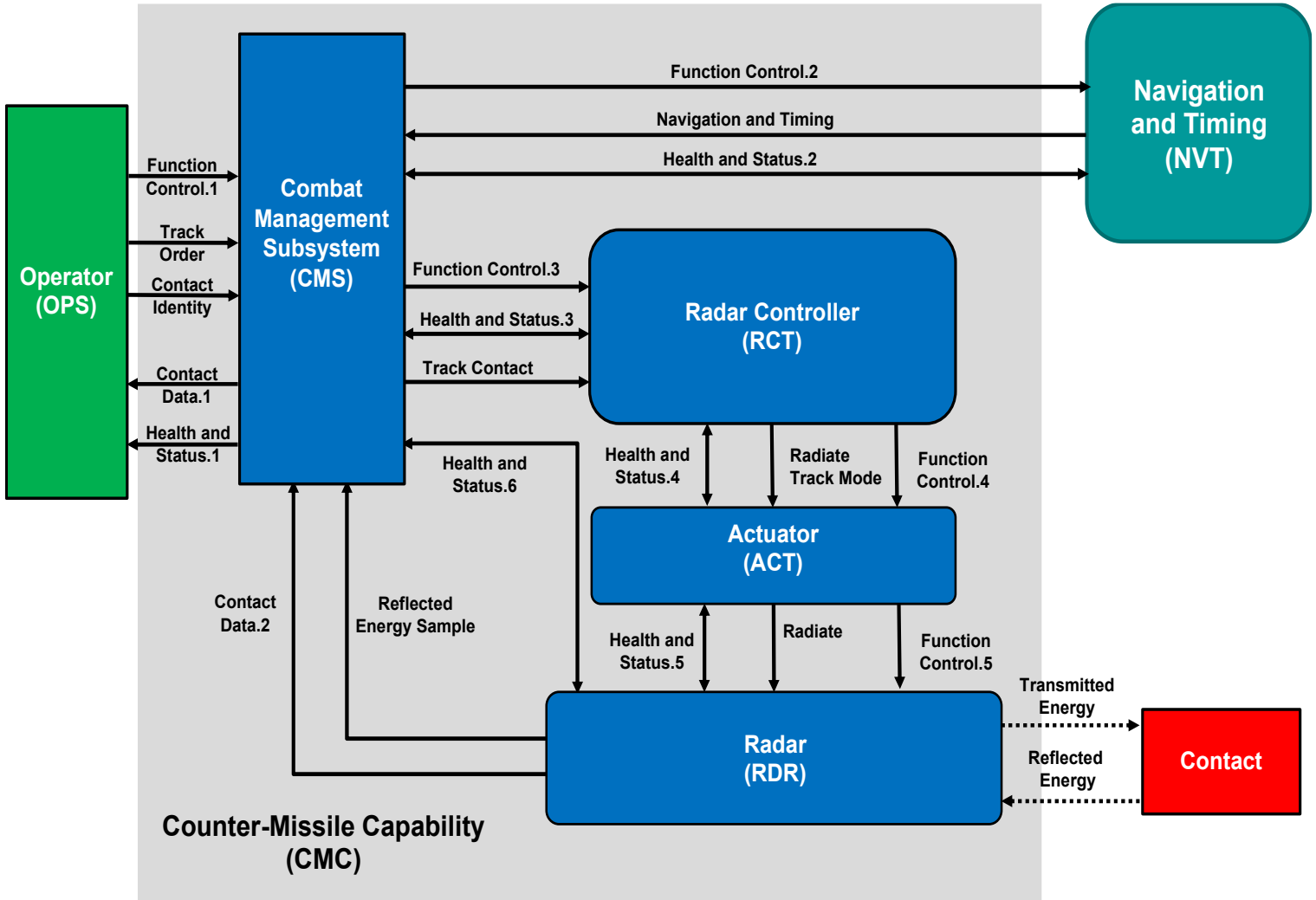
Engineering Cyber Resilient Weapon System Workshop Notional Use Case: Counter-Missile Capability

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Questions?

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

Notional Use Case



Engineering Cyber Resilient Weapon System (CRWS) Workshop Notional Use Case: Counter-Missile Capability

Distribution Statement A: Approved for public release. DOPSR case #23-S-0170 applies. Distribution is unlimited.

NDIA Systems & Mission Engineering Conference
November 1-3, 2022
Orlando, FL

Cyber Supply Chain Risk Management a System Security Role in the Future of Systems Engineering

Holly Dunlap
Hdunlap@MITRE.org
850-796-6510

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347
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 Cyber Supply Chain Risk Management SME

MITRE LABS
Cyber Solutions Innovation Center Division
Cyber SCRM, Principal System Security Engineer
Supply Chain Security System of Trust (SoT)

Raytheon Missiles & Defense (+15 years)

- NDIA System Engineering Division Elected Chair (+13 Committees, +500 members; government, industry, academia, FFRDC)
- NDIA System Security Engineering Committee Chair, +9 years
- Systems Engineering Council – Cyber Resiliency & System Security Project Lead
- Cyber Enterprise Campaign
- CODE Center
- PI Security & Trustworthy Foundations for Electronics Resurgence (STryFER) IDIQ CRAD Proposal
- Defense & Intelligence Programs

Ktech Later Acquired by RTN RMS

- USD(I) Contract Supply Chain & Logistics Layered Analysis; Data & Information Exploitation. 18 month effort.

OSD DDR&E Technical Intelligence, Pentagon +3 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.

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)
- Certified 6 Sigma Black Belt – Microelectronics

BS Electrical Engineering & MBA

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

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.

Introduction

- Microelectronics hardware, software, and firmware are the keys to technological superiority, but also house extensive opportunities for cyber attack.
- Lurking in the interconnected value-added global microelectronics supply chain networks are new challenges relating to the lack of control, transparency, visibility, integrity, availability, and confidentiality.
- As the logic bearing component supplier base increases, high assurance systems becomes more reliant on each contributing participant to ensure that these challenges are addressed.
- Managing the cyber risks to these new technology and capability supply chains' forms the basis and need for new academic disciplines and skillsets.
- The associated global supply chain security challenges and risks are not currently addressed and integrated holistically into System Security Engineering education, training, or roles and responsibilities.
- Therefore, this article proposes the development and formalization of Cyber Supply Chain Risk Management (C-SCRM) Engineering as new role and responsibility.

Cyber Supply Chain Risk Management Engineering in the Security Future of Systems Engineering

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Introduction

Microelectronics

- Logic-bearing components include Application Specific Integrated Circuits (ASICs), Field-programmable gate arrays (FPGAs), Single Board Computers (SBCs), Complex programmable logic devices (CPLDs), microcontrollers, and other programmable devices.
- According to GlobalFoundries, a specialized component in an Apple iPhone is made up of 8.5 billion transistors and each transistor 10,000 times smaller than a human hair. These transistors control the electrons through a circuit and provide today's computing power.
- ASICs provide the greatest opportunity for efficiency in size, weight, and power to achieve optimal performance.
- Field Programmable Gate Arrays (FPGAs), provide a compromise of both worlds COTS & Custom but does not achieve the premier performance of ASICs.
- Both ASICS and FPGA ICs often include billions of transistors.
- Producing a single microelectronics component may include 5 to 50 different suppliers with multiple entities contributing to each stage of design, manufacturing, test, and packaging. And every entity or suppler has risks for adversarial cyber attack.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

BACKGROUND

Traditional Supply Chain Risk Management vs Cyber Supply Chain Risk Management

TRADITIONAL SUPPLY CHAIN RISK MANAGEMENT

Supply chain risk management is traditionally focused on component quality, supplier stability, affordability, and the ability of these suppliers to reliably deliver components to meet just-in-time production schedules.

The ultimate risk in the traditional supply chain is that the systems integrator will not be able to procure and receive quality components needed to build a system.

CYBER SUPPLY CHAIN RISK MANAGEMENT

The cyber risk in the supply chain faces 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.*"

The ultimate cyber risk in the supply chain is not that a systems integrator will procure or receive a counterfeit or maliciously modified component; the risk is that such a component will go undetected and be integrated into a critical system that requires high assurance with national security implications.

DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Vision:

- C-SCRM Engineering as a role within System Security Engineering, with official recognition and ample resources, will provide a stable foundation for an integrated defense against cyber exploited weaknesses and vulnerabilities resident in the supply chain of logic bearing components.

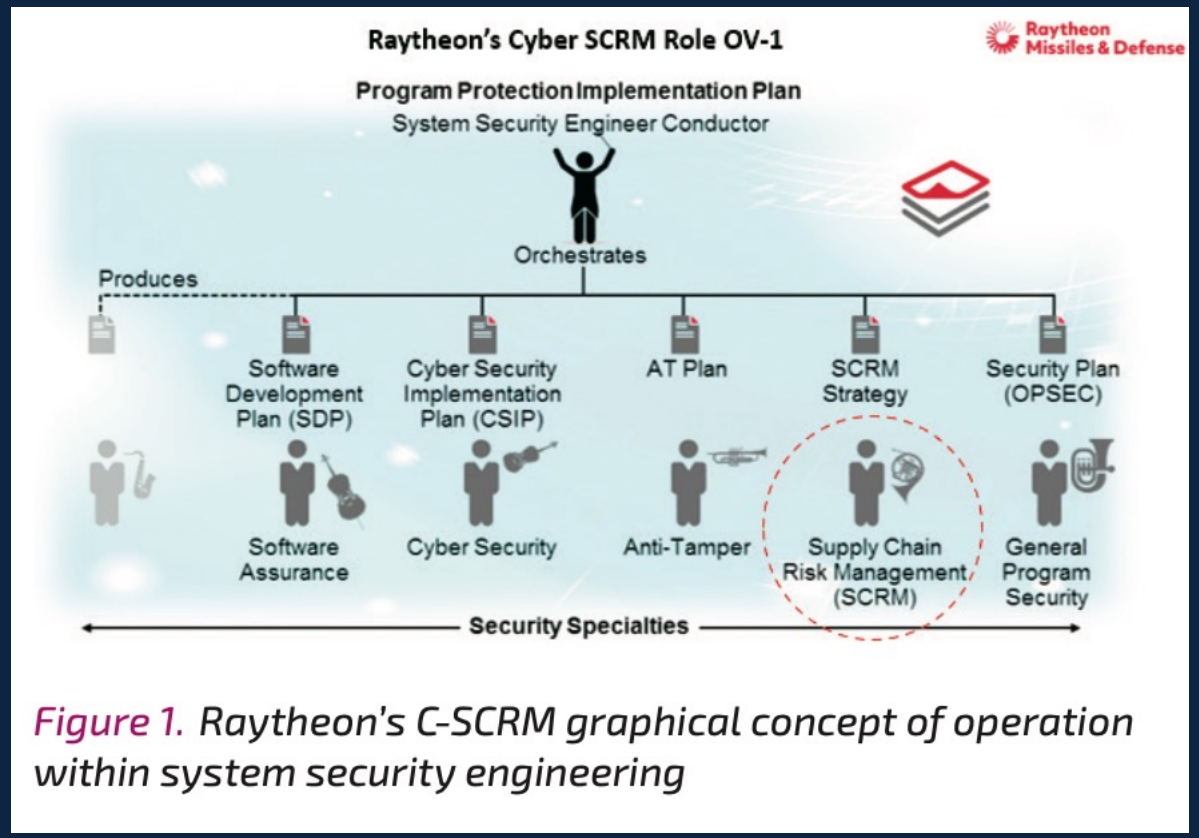


Figure 1. Raytheon's C-SCRM graphical concept of operation within system security engineering

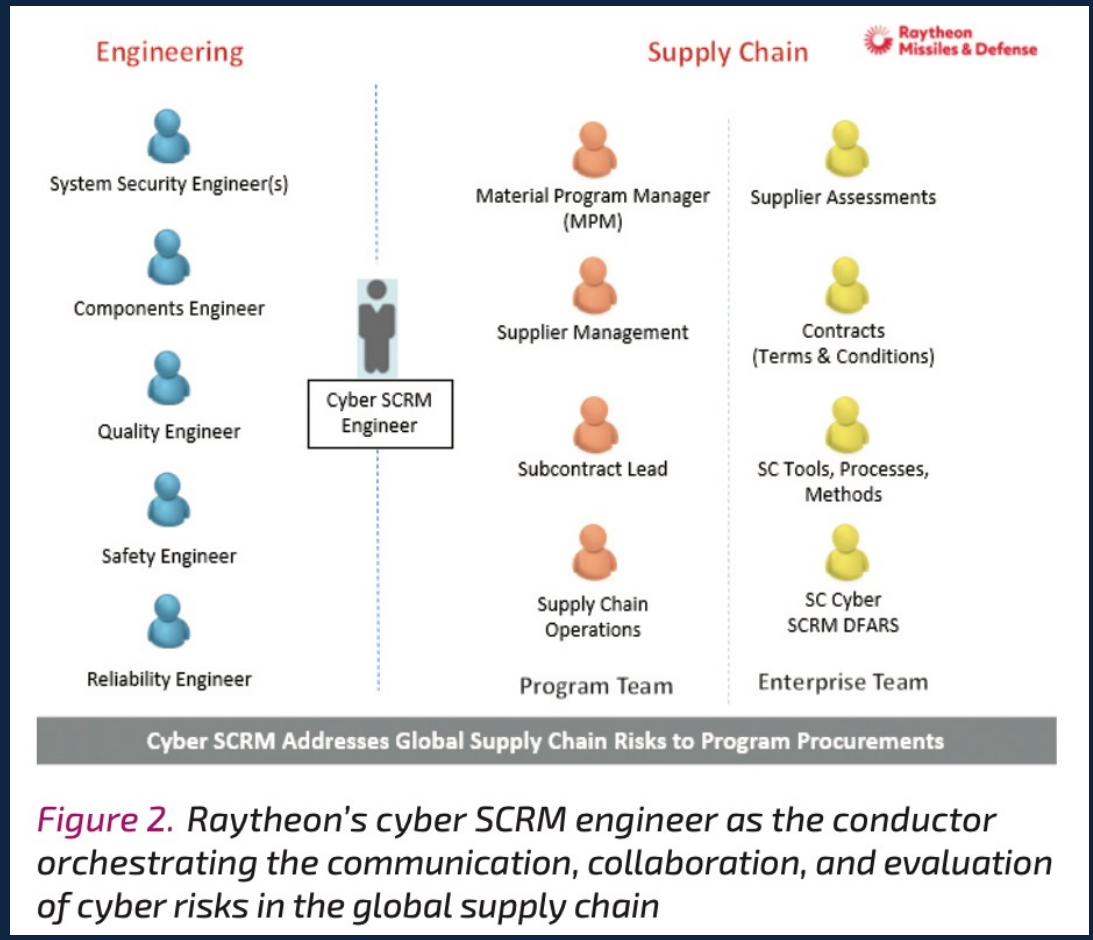


Figure 2. Raytheon's cyber SCRM engineer as the conductor orchestrating the communication, collaboration, and evaluation of cyber risks in the global supply chain

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Current State:

- C-SCRM for product security lacks dedicated and recognized leadership roles, a common security framework, and coordination of effective strategies. Without leadership, there is no empowered advocate to bring together the disparate and diverse community of stakeholders and range of countermeasures essential to effectively manage the cyber risks within the global supply chain.
- The creation of a C-SCRM role in engineering provides a stable locus for an integrated and coordinated response to cyber threats in the supply chain. With official recognition, this role can serve as the connective tissue for disparate efforts and unique needs of the diverse range of stakeholders who are essential to C-SCRM. If provided adequate resources, this role can provide guidance along with a common security framework for C-SCRM strategies that have been proven successful, as well as promising new countermeasures, which require expertise and holistic systems awareness to effectively implement.
- Without this role, C-SCRM efforts will remain dangerously isolated, lacking a unified threat matrix mapping to coordinated and characterized countermeasures. Each supplier will continue to represent a potential vector for malicious actors to launch deliberate and targeted attacks. The logic bearing component supply chain will continue to feature layered vulnerabilities, rather than layered security.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Cyber-SCRM Engineering Overlay

11 foundation concepts included in the Security FuSE Roadmap

Concept 1	C-SCRM Engineering Proficiency in the SSE Team
Concept 2	C-SCRM Education and Competency Development
Concept 3	C-SCRM Stakeholder Alignment
Concept 4	Extending Safety and Mission Assurance Failure Modes Effects and Criticality Analysis (FMECA) to derive C-SCRM requirements for procurements and subcontractor build to specifications
Concept 5	C-SCRM Architecture Framework to provide program layered defense solution diversity and agility
Concept 6	Operational Agility through C-SCRM Forensics
Concept 7	Capability-Based C-SCRM Engineering
Concept 8	Security as a functional requirement in the procurement of products, subcontracts, and services.
Concept 9	Assurance modeling for Cyber SCRM to increase confidence in component authenticity and integrity.
Concept 10	C-SCRM Orchestration
Concept 11	Concept 11: Techno-Social Contracts

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

11 foundation concepts included in the Security FuSE Roadmap

Concept 1: C-SCRM Engineering Proficiency in the SSE Team	
Problem to Address	Insufficient knowledge of holistic approaches to managing risks posed by the distributed global supply chain.
Need to Fill	A formally recognized new role for C-SCRM Engineering as a responsibility within System Security Engineering.
Barriers to Overcome	Formal recognition and ownership by Engineering. Partnership with Supply Chain, Quality, Mission Assurance, and Whole Life is essential but Engineering and specifically SSE must own to address the technical security requirements and manage the global supply chain cyber threats and vulnerabilities.
Concept 2: C-SCRM Education and Competency Development	
Problem to Address	Cyber-attack vectors in the microelectronics hardware, software, firmware, and their interconnected value-added global supply chain networks lack holistic integration into SSE education, creating a skills gap.
Need to fill	Education and proficiency development to manage distributed global supply chain risks that accompany procuring components and skills to create program material security strategy with subcontractors.
Barriers to Overcome	Perception that the existence of mitigations and countermeasures in the form of processes, technologies, tools, and testing are evaluated, selected, and integrated with intent during the procurement process. Just because mitigations exist, does not mean they are used in a layered defense approached today.
Concept 3: C-SCRM Stakeholder Alignment	
Problem to Address	No formally recognized holistic set of requirements or guidance to drive stakeholder needs to an integrated tailored set of system solutions that manage cyber risks in the supply chain.
Need to fill	C-SCRM trade space-based risk mitigations or countermeasures catalog. (For cost, risk, and performance.)
Barriers to Overcome	Common framework and set of metrics and measures for evaluating mitigation effectiveness in context of a system and its intended operational environment.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Foundation concepts 4-6 included in the Security FuSE Roadmap

Concept 4: Extending Safety and Mission Assurance Failure Modes Effects and Criticality Analysis (FMECA) to derive C-SCRM requirements for procurements and subcontractor build to specifications	
Problem to Address	Suppliers and subcontractors are often selected early in a program proposal or system development lifecycle before system security risks are considered.
Need to fill	Extending FMECA to a program's bill of materials analysis to influence supplier selection and procurement and subcontractor technical security requirements.
Barriers to Overcome	Tools to analyze and visualize system bill of materials (BOM), BOM decomposition, logic bearing component (hardware, software, and firmware) identification, and FMECA results. Ensure the term "Program Critical Suppliers" includes C-SCRM criteria. "Program Critical Suppliers" definition may currently include criteria beyond security considerations (cost, single source, financial stability, geographical relocation, etc.)
Concept 5: C-SCRM Architecture Framework to provide program layered defense solution diversity and agility	
Problem to Address	No composable OpenSystems architecture to design blocks with security attributes.
Need to fill	Hierarchical architectural contracts using modeling languages such as SysML, AADL, DSL, RUST connecting to design blocks with security profiles.
Barriers to Overcome	Interoperability of modeling languages. Development and adoption of domain security profiles.
Concept 6: Operational Agility through C-SCRM Forensics	
Problem to Address	No ability to characterize and determine intentional verses unintentional failures.
Need to fill	Analysis of failures to differentiate the root cause to include quality, counterfeit, and malicious modification. Ability to identify, analyze, isolate, and respond to component failures.
Barriers to Overcome	Access to component provenance and pedigree data to forensically analyze root cause of failures, develop trends, and indicators to predict failures from unintentional and intentional based effects.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Foundation concepts 7-9 included in the Security FuSE Roadmap

Concept 7: Capability-Based C-SCRM Engineering	
Problem to Address	Security strategies are based on known available (limited view) solutions or pre-determined (selected) supplier security offerings.
Need to fill	Establish C-SCRM risk-based framework with technical requirements to drive desired results.
Barriers to Overcome	The risks are not simply addressed by flowing down policy or federal acquisition requirements in contracts. Effective technical C-SCRM demands critical thinking to develop the tailored derived requirements and ensure those requirements are implemented and executed to deliver components that meet an acceptable program risk tolerance.
Concept 8: Security as a functional requirement in the procurement of products, subcontracts, and services.	
Problem to Address	As a non-functional requirement, system security does not get prime SE attention. Product security requirements are often absent in contracts for suppliers and subcontractors.
Need to fill	Establishment of a C-SCRM Engineering role responsible for the overall Supply Chain product security architecture to include procurements, subcontracts, and services.
Barriers to Overcome	The assumption that product technical security requirements and criteria are magically integrated into supplier selection, data and information management, transportation and logistics, and testing requirements. DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting contributes but does not directly address product security. DFARS 7012 addresses information protection related to products on business system IT networks.
Concept 9: Assurance modeling for Cyber SCRM to increase confidence in component authenticity and integrity.	
Problem to Address	NIST Risk Management Framework controls and checklist approaches for compliance without expertise and critical thinking are ill-equipped to increase customer confidence in the system's assurance level.
Need to fill	Reinvigorate formal methods of data driven evidence to support claims of assurance while embracing digital engineering analysis and automation tools.
Barriers to Overcome	Lack of skilled and experienced system security and C-SCRM engineers with elevated critical thinking and system domain experience.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Foundation concepts 10-11 included in the Security FuSE Roadmap

Concept 10: C-SCRM Orchestration	
Problem to Address	No identified role responsible for translating technical product security requirements to the supply chain and contracting community. The supply chain and contracts team are the mechanism in which technical requirements authored are communicated from the engineering teams to suppliers and subcontractors. Disparate cyber global supply chain risk mitigations range from emerging technology to proven solutions with little to no ability to latch them together for a holistic approach. No ability to easily compare mitigations to assess their effectiveness and value.
Need to fill	A formal C-SCRM role within SSE responsible for orchestrating collaboration and communication across the engineering community and translate technical product security requirements to supply chain suppliers and subcontracts statements of work requirements in contracts. A visible and accessible C-SCRM semantic ontology risk mitigation catalog for technical capability cyber supply chain risk mitigation selection and orchestration.
Barriers to Overcome	No obvious advocate, champion, or leader with influence and resources to bring the disparate and diverse community together.
Concept 11: Techno-Social Contracts	
Fulfilling the C-SCRM overlay of the FuSE foundational concepts 1-10 provides procured components and subsystems at an acceptable level of risk. Successful execution of C-SCRM enables agile, resilient, and secure system capability options composed of an integrated set of high assurance critical components to support the Techno-Social Contract concept in fielded operations.	

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Conclusion

The geographically distributed globally connected supply chain provides unprecedented access to legacy, state of play, and leading-edge advanced technology but with it comes layers of complex threats and vulnerabilities presenting potential cyber risks to the supply chain and therefore our products and services. The breadth and depth of the opportunities and rising challenges establishes the need to develop a new Cyber SCRM Engineering role as a System Security Specialty within Systems Engineering to focus investments, coordinate and collaborate with disparate communities, and develop repeatable and reliable methods for evaluating and reducing global supply chain risks.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Cited Works:

NIST. (2018). Risk Management Framework for Information Systems and Organizations.
NIST Special Publication 800-37, Revision 2. Gaithersburg, MD: National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations.
NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST Special Publication 800-160 Vol. 1, Gaithersburg, MD: National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

NIST. (2021). Cyber Supply Chain Risk Management Practices for Systems and Organizations
NIST Special Publication 800-161 Rev. 1 (Draft). Gaithersburg, MD: National Institute of Standards and Technology.
https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/archive/2021-04-29

Rick Dove, Tom McDermott, Delia Pembrey MacNamara, Keith Willett, Holly Dunlap, Cory Ocker
"Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts", 31st Annual INCOSE International Symposium, 2021
http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Joel Heebink, “Zero Trust for Hardware Supply Chains: Moving from Absolute Trust to a Quantifiable Assurance Model”, NDIA 2021 Virtual Systems and Mission Engineering Conference.
https://ndia-se21.visiond.com/en/NDIA-1596229109/SE21/tab-embed.php?eventTabID=1659094

References

Daniel DiMase, Zachary A. Collier, John Chandy, Brian S. Cohen, Gloria D'Anna, Holly Dunlap, John Hallman, Jay Mandelbaum, Judith Richie,
"A Holistic Approach to Cyber Physical Systems Security and Resilience," 2020 IEEE Systems Security Symposium (SSS), 2020, pp. 1-8, doi: 10.1109/SSS47320.2020.9197723.
https://ieeexplore.ieee.org/document/9197723/authors#authors

Rick Dove, Tom McDermott, Delia Pembrey MacNamara, Keith Willett, Holly Dunlap, Cory Ocker
"Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts", 31st Annual INCOSE International Symposium, 2021
http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Report of the Defense Critical Supply Chain Task Force, House Armed Services Committee, July 22, 2021
https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf

Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War
Author: Chris Nissen, John Gronager, Robert Metzger, Harvey Rishikof
https://www.mitre.org/sites/default/files/publications/pr18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf

Koon, J 2021, ' Complex Chips Make Security More Difficult', Semiconductor Engineering Deep, Insights for the Tech Industry
4 November, viewed 15 November 2021,
<https://semiengineering.com/complex-chips-make-security-more-difficult/>.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-3347

Building Hardware Assurance with Trusted Suppliers: Creating Multi-layered Security

Systems and Mission Engineering Conference 2022

November 2, 2022

Dave Chesebrough

Defined Business Solutions

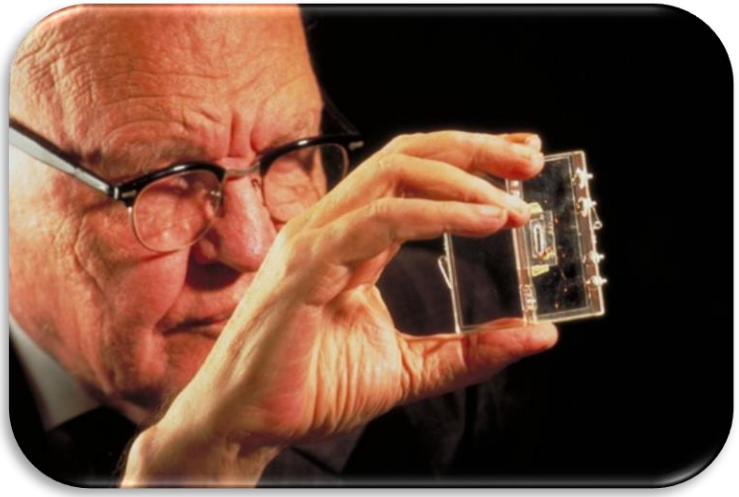
Approved for Public Release

Today's Talk

- Microelectronics Background and Threats
- Cyberspace Domain
- Hardware Assurance and Zero Trust
- Multi-layer Security
- Trusted Foundry and Trusted Suppliers
- Policy
- Systems Engineering Context
- Conclusion

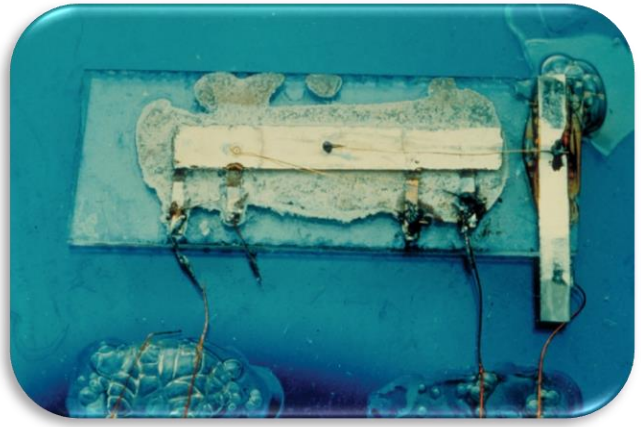
Approved for Public Release

Early Microelectronics



Nobel Laureate Jack Kilby at Texas Instruments

Kilby's original integrated circuit patented in 1959



Fairchild Semiconductor founders, 1960

Department of Defense and NASA were the primary research sponsors and key customers

Design and manufacturing by small, self-contained teams

Performance key focus, Security not a consideration

Why Worry?

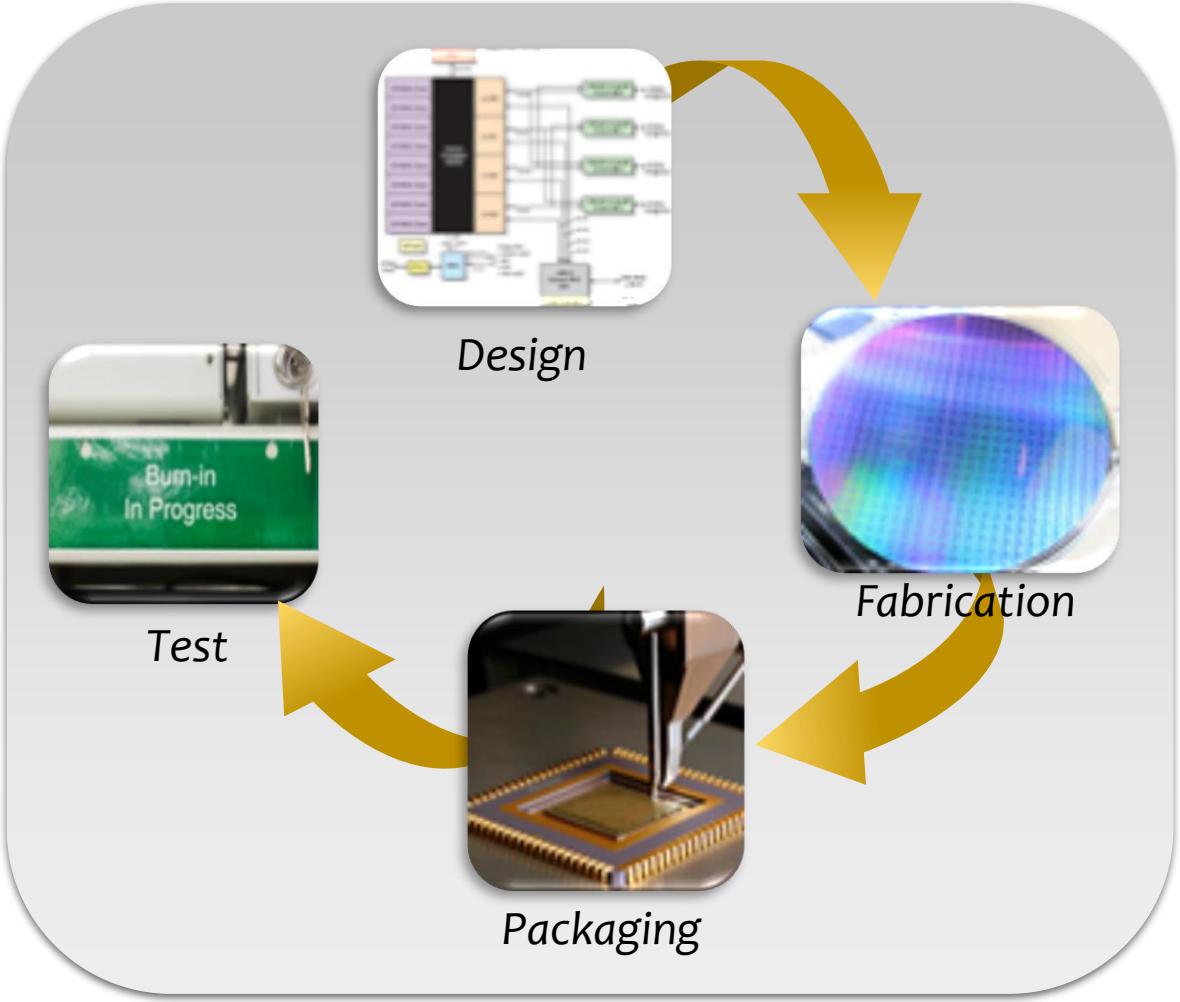
- *Over the past decades the United States has built an increasingly sophisticated suite of defense and intelligence capabilities . . .*

  The application of technology has yielded incredible improvements in system performance . . . but has simultaneously created a significant vulnerability by basing this performance on components that are susceptible to counterfeiting and tampering

- *Microelectronics purchasers encounter multiple supply chain threats. . .*

  The demand domain in which program managers are far-removed from the component purchasing decisions and . . . the supply domain in which the global semiconductor industrial capacity is increasingly found outside the U.S.

Multiple Threats in Semiconductor Production Cycle



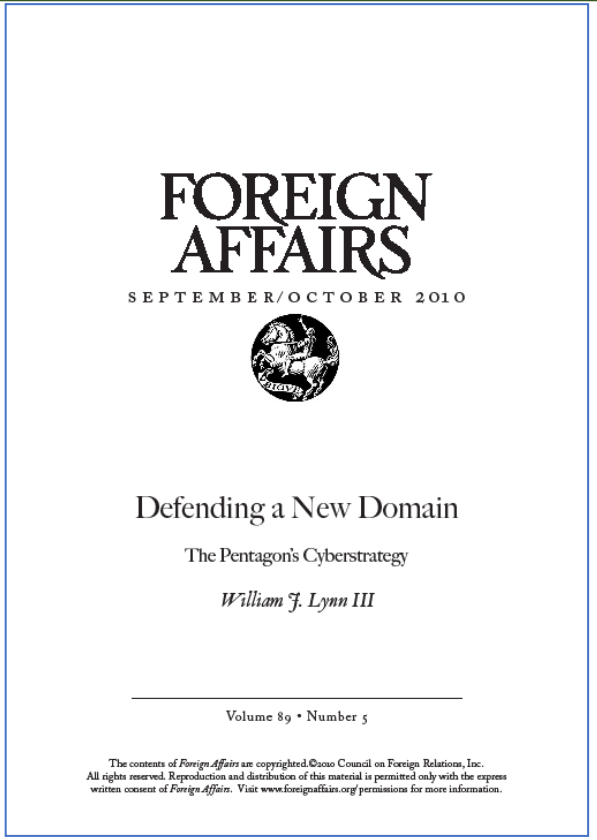
Risks:

- Lack of trustable designs
- Lack of supply chain security
- Tampering potential
- Reverse engineering and IP siphoning
- Lack of chain of custody
- Unauthorized copies
- Remarking and counterfeiting
- Scrap diversion

Cybersecurity Hardware Vulnerabilities

- "The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat . . .
- Tampering is almost impossible to detect and even harder to eradicate . . .
- Remotely operated 'kill switches' and hidden 'backdoors' can be written into the computer chips . . .
- allowing outside actors to manipulate the systems from afar."
  -- Deputy Secretary of Defense William Lynn III

Much of early cybersecurity discussion focused on threats from software and process vulnerabilities . . . the semiconductors may present even greater risks


FOREIGN AFFAIRS

SEPTEMBER/OCTOBER 2010

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

Volume 89 • Number 5

The contents of *Foreign Affairs* are copyrighted.©2010 Council on Foreign Relations, Inc. All rights reserved. Reproduction and distribution of this material is permitted only with the express written consent of *Foreign Affairs*. Visit www.foreignaffairs.org/permissions for more information.

http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Cyberspace Domain

Cyberspace is the digital infrastructure that enables our collective aspirations as a nation and includes people, technology (hardware and software), and doctrine

- Hon. Chris Inglis, National Cyber Director

- Microelectronics and software are the foundations of secure critical cyberspace infrastructure
  - All 16 critical national infrastructure sectors require hardware and software assurance for cyberspace resilience
  - When combined with physical security and proper authentication & authorization, using Trusted Suppliers enables multi-layered security

Approved for Public Release

Multi-layer Security – HwA + Cybersecurity

- 2008 Comprehensive National Cybersecurity Initiative (CNCI)
  - Initiative #11 - Develop a multi-pronged approach for global SCRM
  - Threat actor accesses system, alters its operation, and steals data
  - Exploits vulnerabilities remotely, inserted through supply chain
- In the last 20 years we have seen more -
  - Networked and software intensive systems, internet enabled-operational technology, IoT, off-shoring of chip production
- Cybersecurity includes protecting networks and data and physical systems (CISA ICT SCRM Task Force)
  - Cyber-physical systems blur the distinction and expand the attack surface
  - Zero Trust has become the catch phrase of today for ICT

Hardware assurance is more critical than ever, and more difficult

Zero Trust Principles - Always Verify

- Assume that threats (external and internal) are always present
- Explicitly and continuously verify every transaction
- Authentication and authorization across the enterprise
- ZTA principles for HwA can complement Trusted Supplier protections

Approved for Public Release

Multi-layer Security – HwA + Cybersecurity

- Zero Trust is necessary for IT infrastructure security (OSI Layer 7)
- Hardware supply chains are different (OSI Layer 1)
  - Design, manufacturing, packaging, test, procurement, distribution, integration, and sustainment (material sourcing to end use)
  - Complex, distributed, fragile and dynamic environment
- Assured hardware is critical the comprehensive system security required for mission success

Microelectronics from a Defense Microelectronics Activity (DMEA) accredited Trusted Supplier provide multi-layered security

Hardware Assurance (HwA)

- Confidence that microelectronics and embedded software function as intended and are free of vulnerabilities during the microelectronics life-cycle
- Program Protection Planning and Trusted and Secure Systems analysis
  - Requires early identification of Critical Program Information and components
  - Endorses Trusted Suppliers as viable mitigations
  - Leverages long-term C-I-A (confidentiality-integrity-availability) attributes of Trusted Suppliers

Multi-layer security combines trusted and assured hardware with cybersecurity measures

DMEA Trusted Foundry and Trusted Supplier Program

Trusted - Is the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components (i.e. microelectronics).

- DMEA Website /Trusted Program

- Within this context, "trusted sources" will:
  - Provide an assured "Chain of Custody" for both classified and unclassified ICs
  - Ensure that there will not be any reasonable threats related to disruption in supply
  - Prevent intentional or unintentional modification or tampering of the ICs
  - Protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities

Approved for Public Release

Trusted Foundry and Trusted Supplier Program

- Provides important benefits for mission assurance
  - Selecting components from Trusted Suppliers mitigates the risk of technology corruption, tampering, cyber-attacks, and counterfeiting
  - Using Trusted Suppliers improves parts management for legacy systems by assuring access to supply well past the normal commercial product sunsetting practices
- Trusted Supplier will be an established mitigation in the Microelectronics Assurance Framework
  - DMEA accreditation is being mapped to custom microelectronics threat space and existing guidance

When used in conjunction with ZTA principles, Trusted Microelectronics can provide comprehensive, multi-layer risk-based security

Defense Microelectronics Activity (DMEA)

- Program Manager for the DoD Trusted Foundry program
  - Provides a cost-effective means to assure the confidentiality, integrity and availability of integrated circuits during design and manufacturing
  - Provides US Government offices with access to leading edge, state-of-the-practice, and legacy microelectronics for national security applications
- DMEA has been designated as the DoD Center for Industrial Technical Excellence (CITE) for defense microelectronics
  - Allows greater utilization of DMEA resources
  - Leverages public-private cooperative arrangements
  - Enables partnering among depots/arsenals and private industry
  - Enhances DoD's ability to provide support to critical warfighting capabilities

Approved for Public Release

Defense Microelectronics Activity

Pillars of DMEA

Trusted Access Program Office (TAPO)	Ensure access to cutting-edge microelectronics and accredit Trusted Suppliers
Advanced Technical Support Program (ATSP)	Accelerate microelectronics acquisition and provide technical oversight
Organic Engineering	Provide flexible, full-spectrum microelectronics solutions
Radiation Testing	Deliver secure, cost-effective radiation qualification testing and research

Approved for Public Release

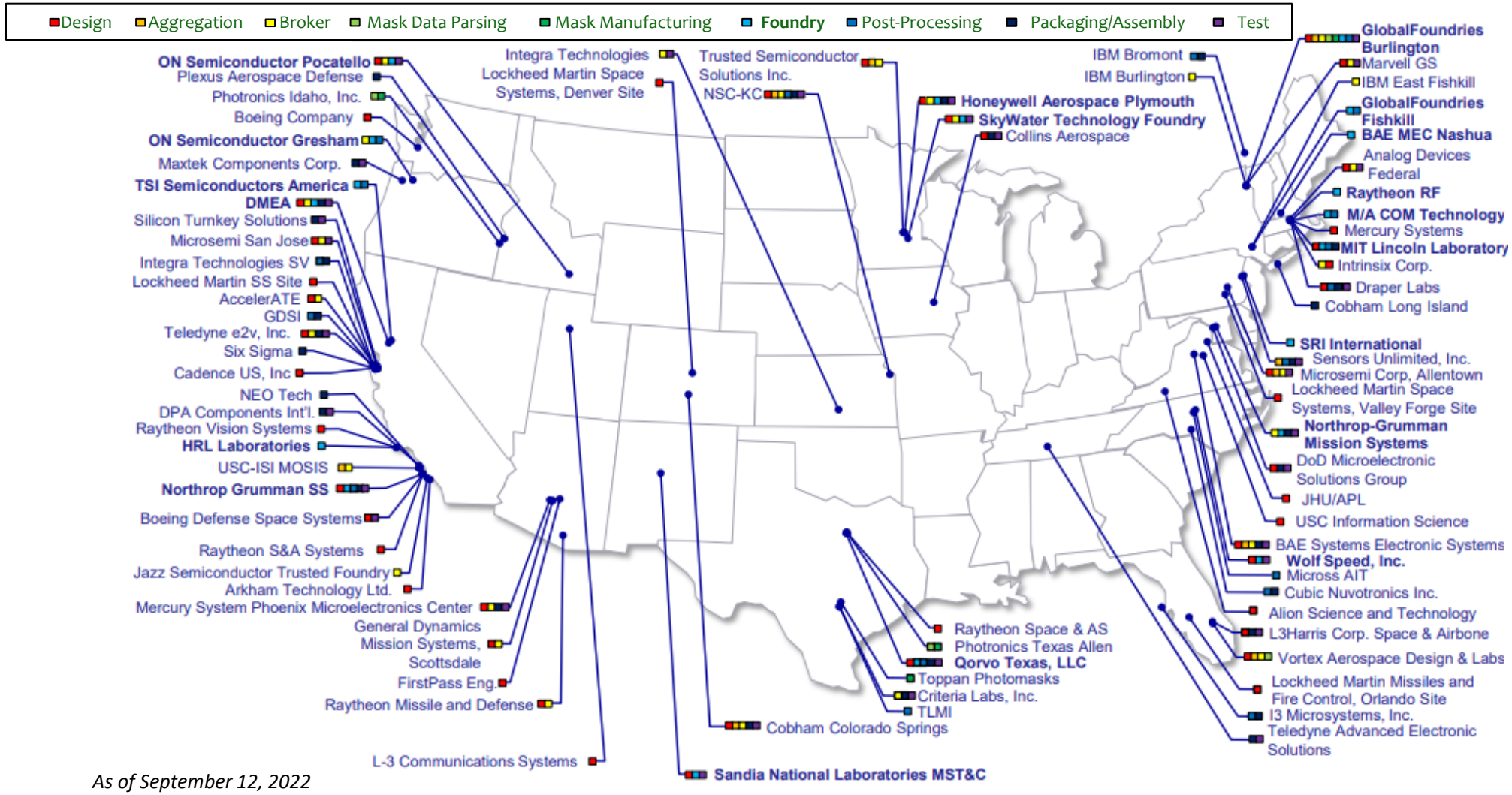
Trusted Access Program Office

- TAPO facilitates and administers the contracts and agreements with industry to provide US Government users with
  - Advanced foundry services including multi-project wafer (MPW) runs, dedicated prototypes, and production in both high- and low-volume models
  - A library of standard IP blocks (most margined down to the Mil-Std-Temp range)
  - Packaging and test services
  - Accredits suppliers per DoDI 5200.44

Trusted Foundry program provides the US Government with guaranteed access to advanced, state-of-the-practice, and legacy Trusted microelectronics for the typically low volume needs of government programs.

Approved for Public Release

80 Trusted Suppliers



As of September 12, 2022

Approved for Public Release

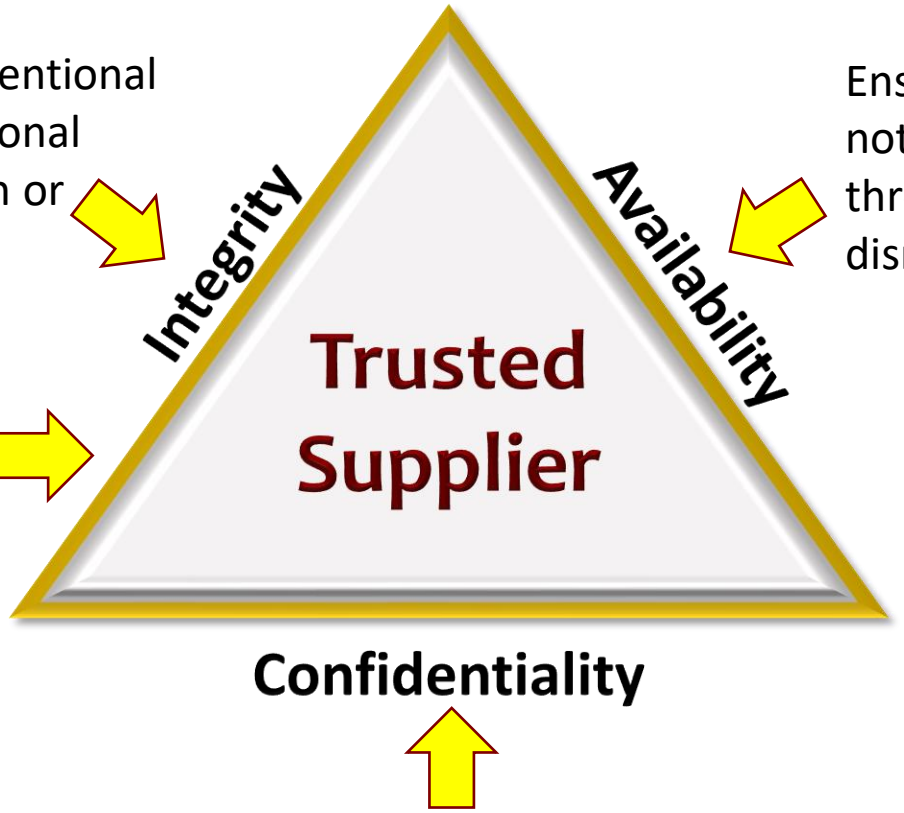
Trusted Suppliers Products and Services Offered

- Trusted packaging design, test and assembly
- MEMS
- Trusted product evaluations such as failure analysis, counterfeit design evaluation, environmental testing, trade studies, non-destructive testing . . .
- RAD HARD microcircuit design and fabrication
- Trusted microcircuit emulation
- Anti-cloning protection
- Trusted photomask development and parsing
- Trusted ASIC and FPGA design and broker services

Trusted sources are available for a full range of microelectronics design, production, and test for leading-edge, state-of-the-practice, & legacy microelectronics

Approved for Public Release

Benefits of Using Trusted Suppliers



Prevents intentional or unintentional modification or tampering

Ensures that there will not be any reasonable threats related to disruption of supply

Provides an assured "Chain of Custody" for both classified and unclassified components

Protects components from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities

Approved for Public Release

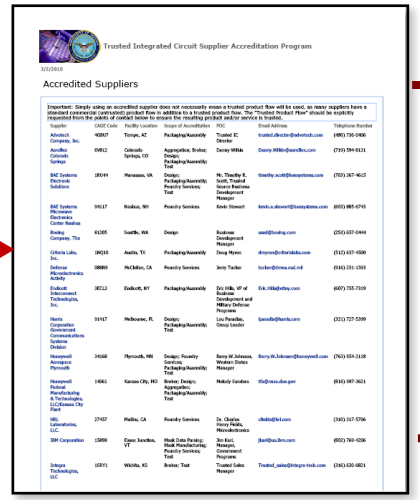
Trusted Microelectronics Options

Trusted IC Requirement

State-of-the-Practice or Legacy?

Determine Trusted products and services needed

Review Trusted Accredited Suppliers (TAS) capabilities


Trusted Integrated Circuit Supplier Accreditation Program

Accredited Suppliers

Supplier services and POCs listed on DMEA website

Initiate direct engagement with one or more TAS

- OR -

Initiate direct engagement with aggregator or broker

State-of-the-art Leading Edge?

TAPO
Trusted Access Program Office

Government Sponsor

Explicitly request Trusted Flow at each stage of engagement

Goal of Technology and Program Protection Policy

- Protect mission critical components (hardware, software, firmware)
  - Software assurance (SwA)
  - Hardware assurance (HwA)
    - Trusted/assured microelectronics
- Consideration of Trusted Suppliers begins early in development
  - Identify notional critical functions to implement with microelectronics
  - Trade studies should include C-I-A attributes of Trusted Suppliers
  - TSN analysis to identify ASICs and applicability of DODI 5000.44
- Program offices can incorporate requirement in RFPs and SOWs
  - Include the requirement for a Trusted Process Flow in the solicitation, directing the use of a DMEA-accredited Trusted Supplier

Approved for Public Release

Mission Critical Microelectronics Policy

- DoDI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

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

- Applicability
  - All mission critical functions and critical components within applicable systems identified through a criticality analysis, including spare or replacement parts

Approved for Public Release

Mission Critical Microelectronics Policy

- Other applicable instructions
  - DoDI 5000.83 - Technology And Program Protection To Maintain Technological Advantage
  - Technology and Program Protection (T&PP) Guidebook (July 2022) https://rt.cto.mil/wp-content/uploads/TPP_Guidebook_Jul2022_cleared.pdf
  - DoDI 5200.39 - Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
  - DoDI 5200.47 - Anti-Tamper (AT)
  - DoDI 4140.67 - DoD Counterfeit Prevention Policy
- Inclusion in contracts
  - For policy to have effect program offices should include applicable provisions in contractual documents and requirements

Approved for Public Release

Systems Engineering Decision Points

- Trade studies should include early assessment of use of Trusted Suppliers for microelectronics
  - When defining alternative system concepts or configuration items determine if microelectronics from a Trusted Supplier can be used to provide desired functionality
- Program Protection Plan identifies Critical Program Information
  - Trusted Suppliers' Trusted Flow is adequate to protect Critical Program Information as required by DODI 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense
  - An ASIC with a CPI designation should be sourced from a Trusted Supplier

Approved for Public Release

Conclusion

- Programs should understand when to select components from Trusted Suppliers during their system development
- Engineers should factor benefits into program protection systems security engineering planning and protocols
- Programs should engage with TAPO and Trusted Suppliers early to ensure products and services are accessed
- The Trusted Foundry and Trusted Supplier Programs are key resources for defense programs

Approved for Public Release

Contacts

DMEA – DOD Program Management & Accreditation

tapo@dmea.osd.mil

DBS – Outreach (contractor)

dchesebrough@definedbusiness.com

Approved for Public Release

2022 Systems & Mission Engineering Conference

Capability-Based Security Engineering for Strategy Formulation and Stakeholder Alignment

November 3, 2022

Presentation: Rick Dove

Collaborators: Rick Dove, Holly Dunlap, Matthew Hause, Aleksandra Scalco, Garry Stoneburner, Keith Willett, Adam Williams, Beth Wilson, Mark Winstead

Approved for Public Release

rick.dove@parshift.com, attributed copies permitted

Abstract

The Future of Systems Engineering (FuSE) is an INCOSE-led multiorganizational collaborative initiative pursuing INCOSE's *Vision 2035* across a number of topic areas. One of those topic areas is concerned with system security.

INCOSE's System Security Engineering working group, in collaboration with NDIA's System Security Engineering group, developed and then published in mid 2021 a near-term roadmap of eleven concepts and six objectives.

Subsequent work has been focused on advancing the understandings of those concepts sufficient to facilitate transition to operational practice.

Collaborative team work in early 2022 identified one of those eleven concepts, Capability-Based Security Engineering (CBSE), as having high value and strong synergy with virtually all of the other concepts. CBSE at core is about needs oriented requirements engineering – expressing requirements as strategic needs and desired outcome values rather than as tactical configuration and employment of readily available solutions and knowledge.

A project emerged to design a systems engineering process that channels thinking and communication of security needs as desired outcomes rather than as prescribed solutions. Expression and understanding of security requirements as needs and values offers a path for coherent stakeholder alignment, innovative solution development, and understandable strategy formulation.

This presentation will cover the considerations and status of process design, with an emphasis on means to gain traction.

rick.dove@parshift.com, attributed copies permitted

SYSTEMS ENGINEERING
VISION 2035
ENGINEERING SOLUTIONS FOR A BETTER WORLD
Cyber-security
will be as foundational a perspective
in systems design
as system performance and safety
are today (p.37)
INCOSE
Vision35

Security is a Mission – Not a System

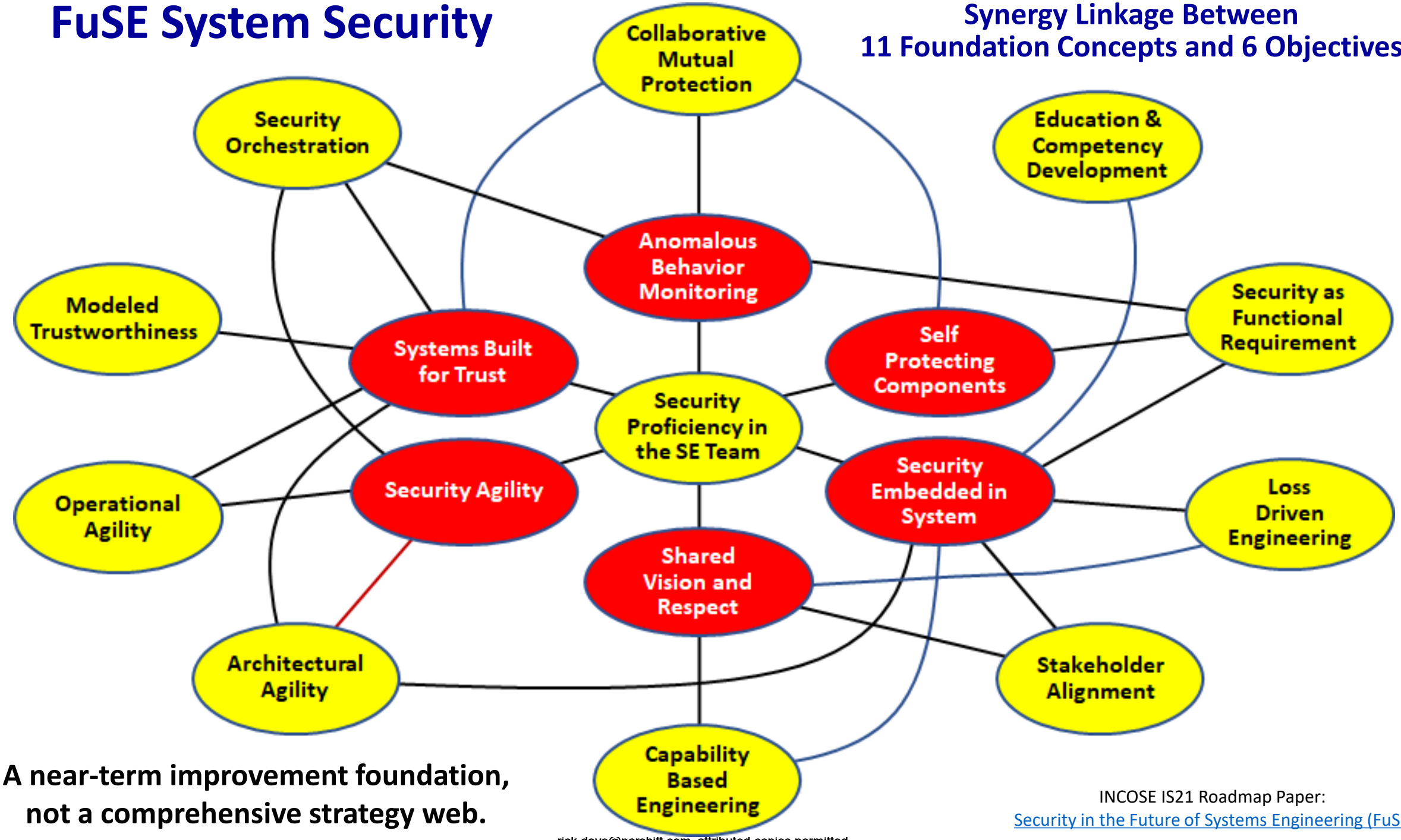
Stakeholders and technology are there to support the mission

24/7 always on:

- **situational awareness**
- **protection**
- **incident response**
- **recovery**
- **improvement**
- **evolution**

FuSE System Security

Synergy Linkage Between 11 Foundation Concepts and 6 Objectives



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

INCOSE IS21 Roadmap Paper:
Security in the Future of Systems Engineering (FuSE)

rick.dove@parshift.com, attributed copies permitted

Capability Based System Security Engineering

Problem	**Security often starts with available solutions rather than desired results.**
Need	**Top-down approach to security starting with desired results/value.**
Barriers	**Difference between capability and features; solution-dominant thinking; trust that the outcome will be satisfactory; "just tell me what to do."**

A capability is an expression of a desired result agnostic of a solution that produces that result. It permits and encourages innovation.

Capability Based Engineering variations:

- **Needs Oriented Requirements Engineering**
- **Goal Oriented Requirements Engineering (GORE)**
- **Security Quality Requirements Engineering (SQUARE)**

Capability needs emerge as centrally most important:

- **They identify the foundation of a security strategy fit for context.**
- **They are intelligible to all stakeholders, a platform for alignment.**

Stakeholder Alignment

Problem	**Misalignment of security vision among stakeholders.** **Inconsistent appreciation for security among stakeholders.**
Need	**Common security vision and knowledge among all stakeholders.**
Barrier	**Stakeholder willingness to engage in collaborative convergence.**

Stakeholders of interest are not "who should be listened to;"
rather "who can affect the outcome."

We want stakeholders to come along, not go along.

We want stakeholders to be engaged in the mission.

We want an aligned sense of need, awareness, importance, attention, respect.

Well-defined capability needs are a key output from this alignment.

Security Proficiency in the SE Team

Problem	**Insufficient knowledge of system security engineering at the systems engineering level; communication across knowledge and expertise boundaries.**
Need	**System security and its evolution effectively enabled by systems engineering activity.**
Barriers	**Disrespect between SE and Sec people; perception of security as non-functional requirement; finding high level security expertise.**

Proficiency exercises high-level competencies in system security thinking, architecture, strategy, and empathy.

Stakeholder alignment is the "minimum viable product" demonstrating security proficiency in the SE team.

Loss-Driven Engineering

Problem	**Traditional vulnerability assessments and risk/consequence models for security occur too late in the SE process.**
Need	**Standard metrics and abstractions relevant to all system lifecycle phases.**
Barrier	**Insufficient respect for potential leverage; solution- rather than problem-dominant security thinking.**

"There is a need to emphasize protection against the effects of loss … it is prudent to ensure that there is focus on the effect to be controlled rather than on the cause when protecting against loss." **(NIST SP 800-160 volume 1 revision 1)**

Protection from losses are understandable to a broad base of stakeholders as needs.

Modeling Trustworthiness

Problem	**Systems Security has moved away from its traditional focus on trust to a more singular focus on risk.**
Need	**Reinvigorate formal modeling of system trust as an evidentiary core aspect of system security engineering.**
Barrier	**Entrenched risk-based practices and education; simplicity of communicating and comparing risk metrics; perception of security as a non-functional requirement.**

Security functions and assurance processes became separated in the early 2000s.

Since then the concepts of risk and assurance have dominated the community.

The community needs a return to "Security as a functional requirement" supported by formal security models that support system engineering decisions and V&V activities.

Evidence meriting trustworthiness by stakeholders can be modeled to show functional capabilities linked to needs.

Security as a Functional Requirement

Problem As a non-functional requirement, systems security does not get prime system engineering attention.
Need Systems engineering responsibility for the security of systems.
Barrier Cultural inertia that prioritizes system purpose over system viability.

System security engineering is concerned with achieving capabilities that satisfy stakeholder-defined needs.

To ensure security is designed in, these capabilities must be specified as functional requirements.

A functional requirement is a qualitative description of an activity to perform or purpose to achieve *in fulfillment of a need*.

rick.dove@parshift.com, attributed copies permitted

Security Orchestration

Problem	**Disparate security solutions operate independently with little to no coordination.**
Need	**Tightly coupled coordinated system defense in cyber-relevant time.**
Barrier	**Independent stovepipe solution tools; multiple disparate stakeholders; hesitation to explore interdependencies**

Security Orchestration provides a foundation to explore and develop autonomous governance and adjudication logic for dynamic security decisions in operations, for fast, relevant, and adaptable system defense.

Orchestration invokes static solutions as standard sequences, and dynamic solutions as composition (from available assets) or dynamic development (real-time production).

A cultural twist that requires stakeholder alignment on the need for (some) autonomous mission management and alignment on the means for exploring functional and cultural compatibility.

rick.dove@parshift.com, attributed copies permitted

Collaborative Mutual Protection

Problem	**Insufficient detection and response capability for innovative attacks with infrastructure-based security mechanisms.**
Need	**Widely distributed detection & mitigation of known and unknown attacks.**
Barrier	**Trust in the security of the approach; trust in the emergent result.**

Mutual protection behavior among technical system components is both beneficial and possible.

Beneficial in that security collaboration, cooperation, and teaming among system elements during system operation offers novel strategy for quick detection and mitigation of innovative security threats.

Possible in that human and animal communities employ effectively demonstrated approaches, and non-organic socially cooperating system aggregations already exists in the fields of robotics, drone swarms, and Mobile Ad Hoc Networks (MANETs).

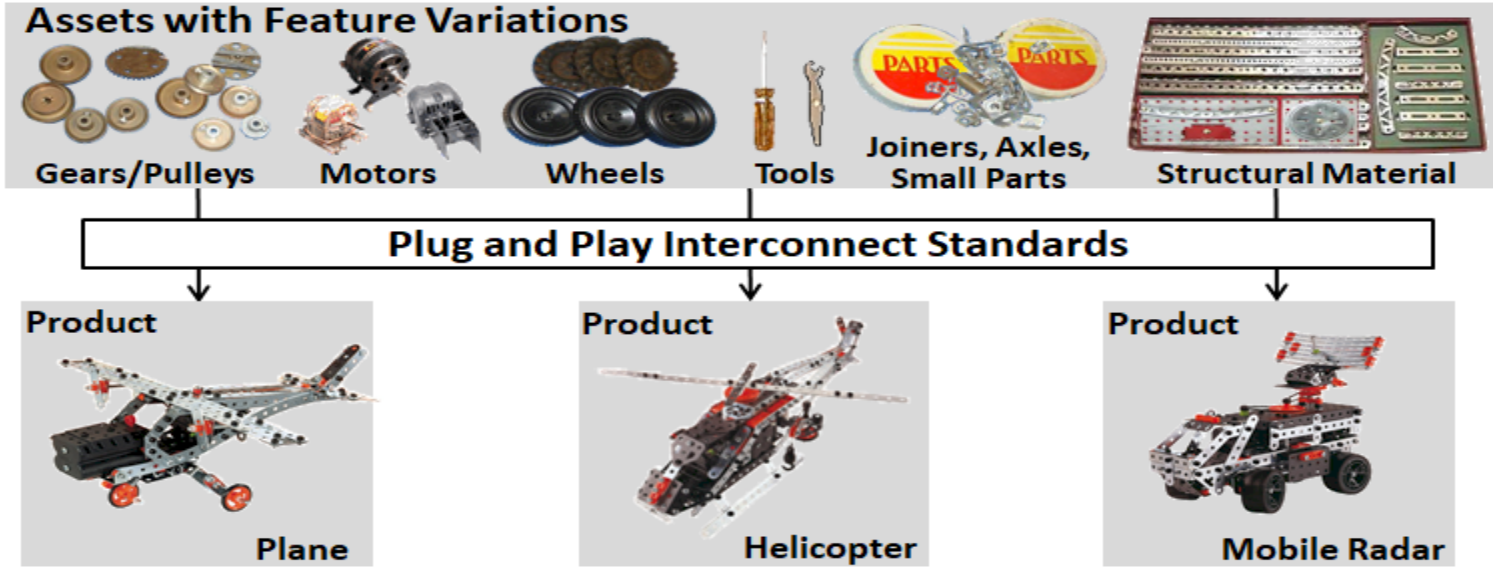
A human community concept understandable as a strategy and as a mission; but a twist on traditional security in need of stakeholder alignment for distributed interaction.

Architectural Agility

Problem Enabling effective response to Innovative threats and attacks.
Need Readily composable and re-composable security with feature variants.
Barrier Comfort with and acceptance of a dynamic security profile.

A product line security architecture with a product-family asset management strategy enables security resilience and composable innovation; and facilitates coherent security evolution.

A cultural twist that requires stakeholder alignment on the need for an agile capability and alignment on the means for exploring functional and cultural compatibility.



Operational Agility

Problem Timeliness of detection, response, and recovery.
Need Ability for cyber-relevant response to attack and potential threat; resilience in security system.
Barrier Comfort with and acceptance of a dynamic response and recovery capability.

Operational agility provide real-time composable response options in an operational environment that can present innovative threats continuously.

Architectural agility provides coherent response options for operational agility to select and execute as appropriate to the moment.

A cultural twist that requires stakeholder alignment on the need for agile operations and alignment on the means for exploring functional and cultural compatibility.

rick.dove@parshift.com, attributed copies permitted

Education and Competency Development

Problem	**Security education is not well integrated with engineering education, creating a skills gap.**
Need	**Education at all levels focused on security of cyber-physical systems (CPS).**
Barrier	**Perception of insufficient scientific/technical rigor for inclusion in engineering programs; engineering faculty security knowledge gap.**

Systems engineering is not addressing security well enough and is not addressing the specific concerns emerging in today's embedded systems and cyber physical systems.

Supply is created and sustained by demand. Educators and trainers on the supply side and acquirers and developers on the demand side can both contribute.

Security needs and strategy independent of implementation tactics can be taught and absorbed by a broad range of educators and engineers.

Holistic

more than the sum of the parts

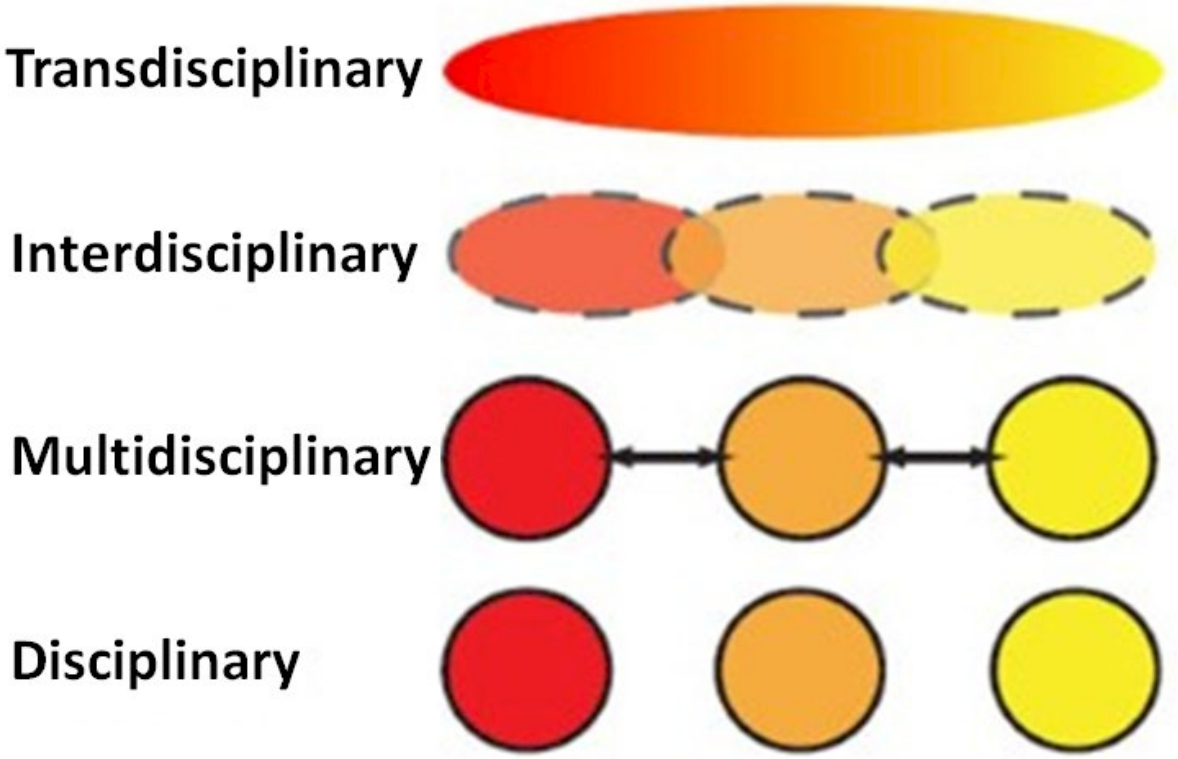
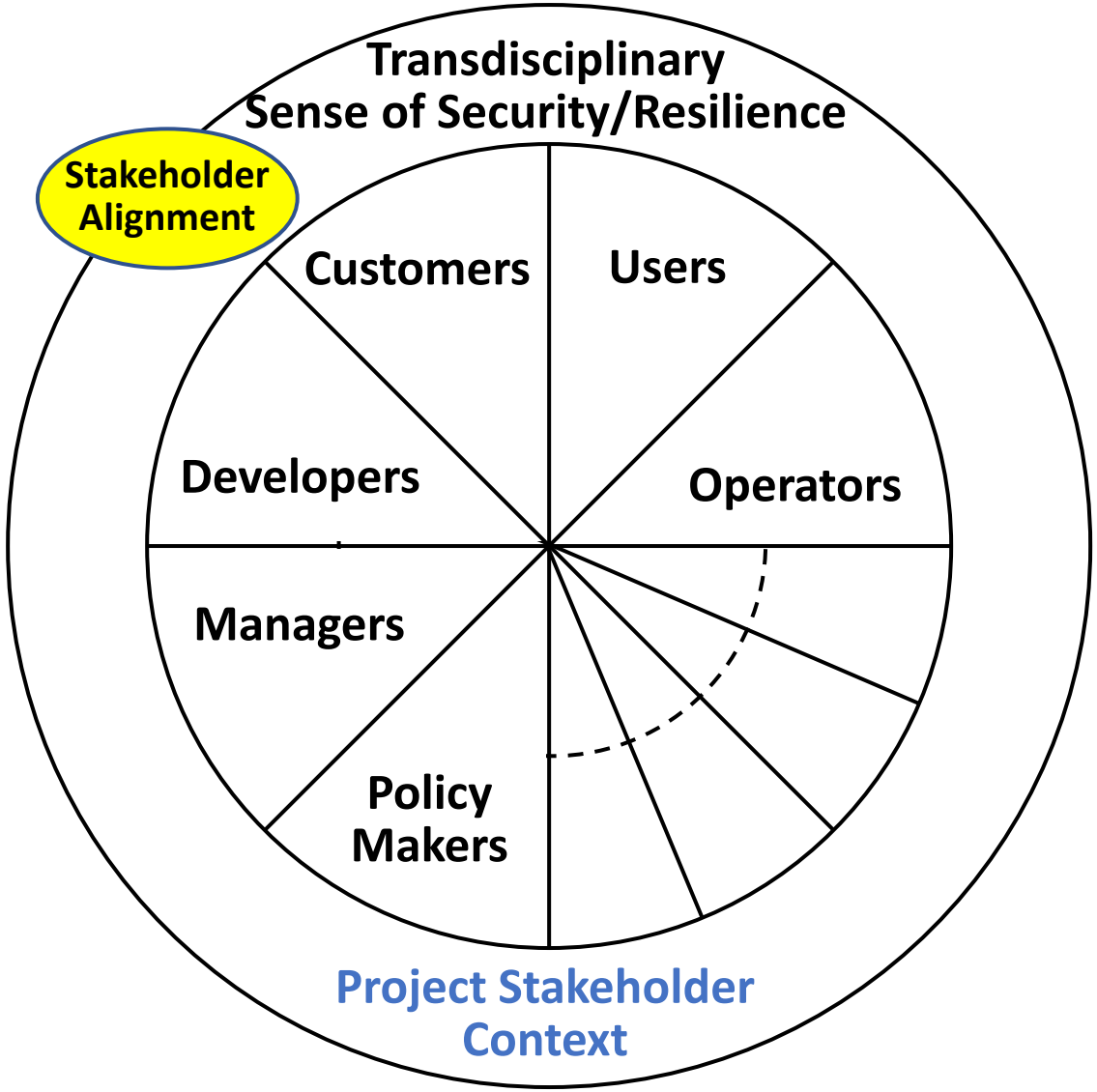


Figure Credit: https://doi.org/10.1038/nchembio0908-511
Colón, W., *et al.* Chemical biology at the US National Science Foundation.



A higher sense of common relevance.

An aligned sense of need, importance, awareness, attention, respect.

Security Quality Requirements Engineering (SQUARE)

Stakeholder alignment around goals to satisfying needs – proof of concept

Lessons Learned:

- **Every project is different, requiring tailored process flexibility.**
- **Facilitating reusable techniques, goals, and capabilities reduces cost and speeds results.**

Our interest is in the first 2 of 9 SQUARE Steps

Step 1: Agree on definitions (a technique for revealing stakeholder knowledge and misalignments)
Input – Candidate definitions from IEEE and other standards
Technique – Structured interviews, focus group
Participant –Stakeholders, requirements team
Output – Agreed-to definitions

Step 2: Identify security goals
Input – Definitions, candidate goals, business drivers, policies and procedures, examples
Technique – Facilitated work session, surveys, interviews
Participant – Stakeholders, requirements engineer
Output – Goals

SEI (N. R. Mead, E. D. Hough, T. R. Stehney II). 2005. Security Quality Requirements Engineering (SQUARE) Methodology.
SEI. 2008. SQUARE-Lite: Case Study on VADSoft Project
SEI. 2010. Security Requirements Reusability and the SQUARE Methodology

rick.dove@parshift.com, attributed copies permitted

We* want to ensure and hasten this Vision.

It is Cultural.
It is a mind set.

Cornerstones:
Stakeholder Alignment and Capability Based Security Engineering.

*INCOSE Systems Security Engineering working group. Chair: dove@parshift.com

Every project has different needs, different stakeholders.

The Vision will occur as grass roots initiatives.

Security is a community affair, not a proprietary competitive advantage.

We want case studies and lessons learned.

We will help develop these if you like.

- Setting Current Context for Security in the Future of Systems Engineering
- Measuring Stakeholder Alignment to Overcome Control System Cyber Vulnerability
- Functionally Interpreting Security
- Capability Engineering vs. "Problemeering" and "Solutioneering"
  - Prioritizing Stakeholder Needs over Requirements
- Very Small Entities (VSE): Outsourcing Risk to the Supply Chain Is Placing Systems Security Engineering on a Clay Foundation, but Playing Games May Help
- Framework for Operational Resilience in Engineering and System Test (FOREST)
  Part I: Methodology Part II: Case Study
- Modeling for Trustworthiness
- Multilayered Network Models for Security: Enhancing System Security Engineering with Orchestration
- Making the Puzzle Pieces Fit - Utilizing UAF to Model a Cybersecurity SoS
- Analyzing System Security Architecture in concept phase using UAF domains
- Cyber Supply Chain Risk Management (C-SCRM) a System Security Engineering Role in the Future of Systems Engineering

rick.dove@parshift.com, attributed copies permitted

References

Dove, R., K. D. Willett. 2020. Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering. INCOSE IS20. Virtual. www.parshift.com/s/200718IS20-FuSETechnoSocialContracts.pdf

Dove, R., Willet, K., McDermott, T., Dunlap, H., MacNamara, D.P., and Ocker, C., 2021. Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts. INCOSE International Symposium, Virtual: July 17-22. http://www.parshift.com/s/210717IS21-FuseSecurityRoadmap.pdf

Evans, J. July 29, 2014, What is Transdisciplinarity? Purdue Polytechnic Institute. https://polytechnic.purdue.edu/blog/what-transdisciplinarity

Maguire, L. 2020. How Many Is Too Much? Exploring Costs of Coordination During Outages. QCon London, May 11. Video and transcript at www.infoq.com/presentations/incident-command-system

Scalco, A. 2022. Measuring Stakeholder Alignment to Overcome Control System Cyber Vulnerability. INSIGHT, Vol. 25, No. 2. INCOSE. June.

SEI (N. R. Mead, E. D. Hough, T. R. Stehney II). 2005. Security Quality Requirements Engineering (SQUARE) Methodology. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf

SEI. 2008. SQUARE-Lite: Case Study on VADSoft Project. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8483

SEI. 2010. Security Requirements Reusability and the SQUARE Methodology. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15197.pdf

Tu, C.Z., Yuan, Y., Archer, N. and Connelly, C.E. 2018. "Strategic value alignment for information security management: a critical success factor analysis.“ Emerald Publishing Limited, Information and Computer Security, Vol. 26 No. 2, pp. 150-170. www.sci-hub.se/10.1108/ICS-06-2017-0042

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

USD(R&E)

Summary of Ongoing Cyber Analytic Landscape (CAL) Task

25th Annual Systems & Mission Engineering Conference

Sarah Standard
Cybersecurity/Interoperability Technical Director
OUSD R&E, ED,DTE&A
MC Suite 16F09-02

Washington, DC
2 November 2022

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Outline

- Introduction
- Background
- Approach and Data Collection
- Observations and Findings
- Synthesizing from the Observations and Findings
- Looking Ahead

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Introduction

- **DoD is more dependent on cyber-enabled systems than ever**
  - Stakes are very high
- **DTE&A Area of Emphasis: Shift cyber testing earlier in program development**
  - Integrated throughout acquisition life cycle
  - Cyber Analytic Tools - Increase applicability, efficiency, effectiveness, accuracy, objectivity, and repeatability across the T&E continuum
- **Cyber Analytic Landscape (CAL) Initiative – 2 year effort**
  - Characterize the state of the "cyber analytic landscape"
    - Identify test-relevant analytic questions and related analytics
    - Determine analytic utility to questions, validation status, data needs, integrability
    - Identify gaps (e.g., missing questions, analytics)
    - Hold workshops along way to work through key issues
    - Catalog analytic techniques
  - **Out-of-Scope**: exhaustive coverage of analytics

"Nearly every warfighting and business capability is now software-defined. Simply put, the system – plane, ship, vehicle, radio, operations center, missile, satellite, health records management – doesn't work if the software doesn't work."

DOT&E 2020 Annual Report

Advocate for validated, repeatable analytics that answer test-relevant questions

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Humans Involvement with Cyber Analysis and Test

- **Cyber analysis and test is a complex space**

- **Historically systems-level cyber analysis/test has been manually intensive**

Problem: Humans are slow, expensive, and inconsistent

The [cyber risk] results indicate that the consensus of the raters is too low for the assessment results to provide a sound basis for decisions.

Hallberg, et al., "The Significance of Information Security Risk Assessments," 2017

[We] noted a diversity of practice in the [red team] test discipline, reinforcing a need to further study the reproducibility of test results...

M. McNeil and T. Llansó, "An Analysis of Adversarial Cyber Testing Practice." 2020

Whenever you use humans as a part of your measurement procedure, you have to worry about whether the results … are reliable or consistent.

Trochim, "Research Method knowledge Base," 2006

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

What Do We Mean by “Analytic” ?

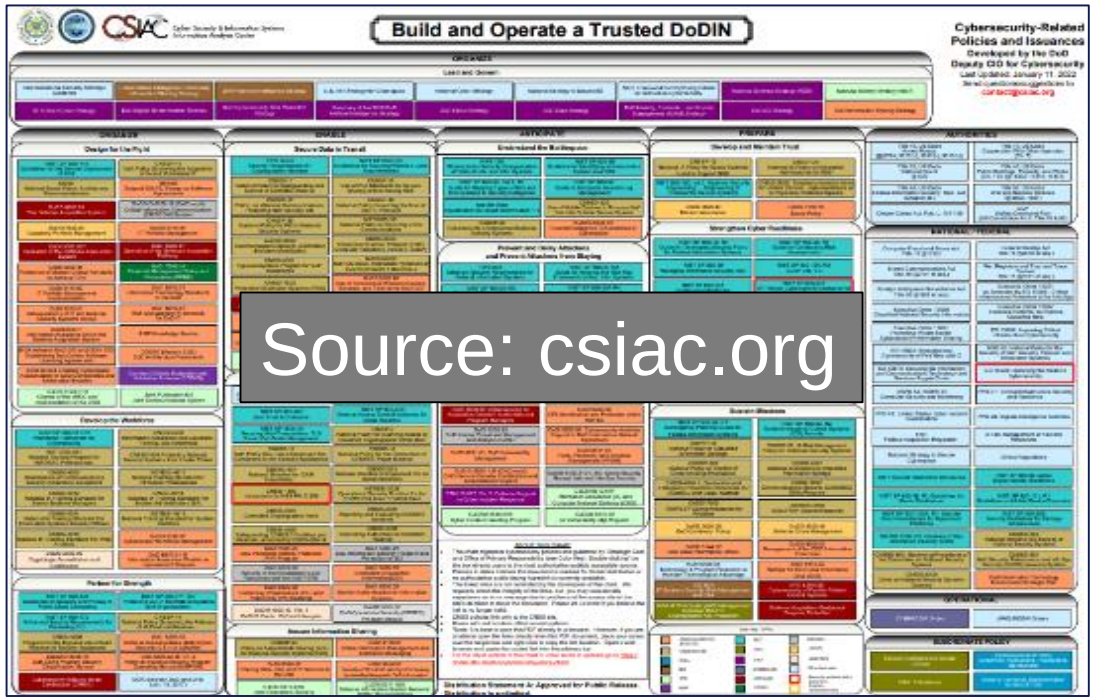
- **We mainly refer to executable analytics (but reusable data sets too)**
- **Computes some result (hopefully) of interest to security engineers and testers**
- **Examples – Compute / Identify**:
  - Cyber “Risk”
  - Cyber “Resilience” or “Survivability”
  - Attack paths
  - Vulnerabilities
  - Cyber component criticality
  - Mitigations

Ideally, Analytics Produce T&E Related ‘Objective Quality Evidence (OQE)’

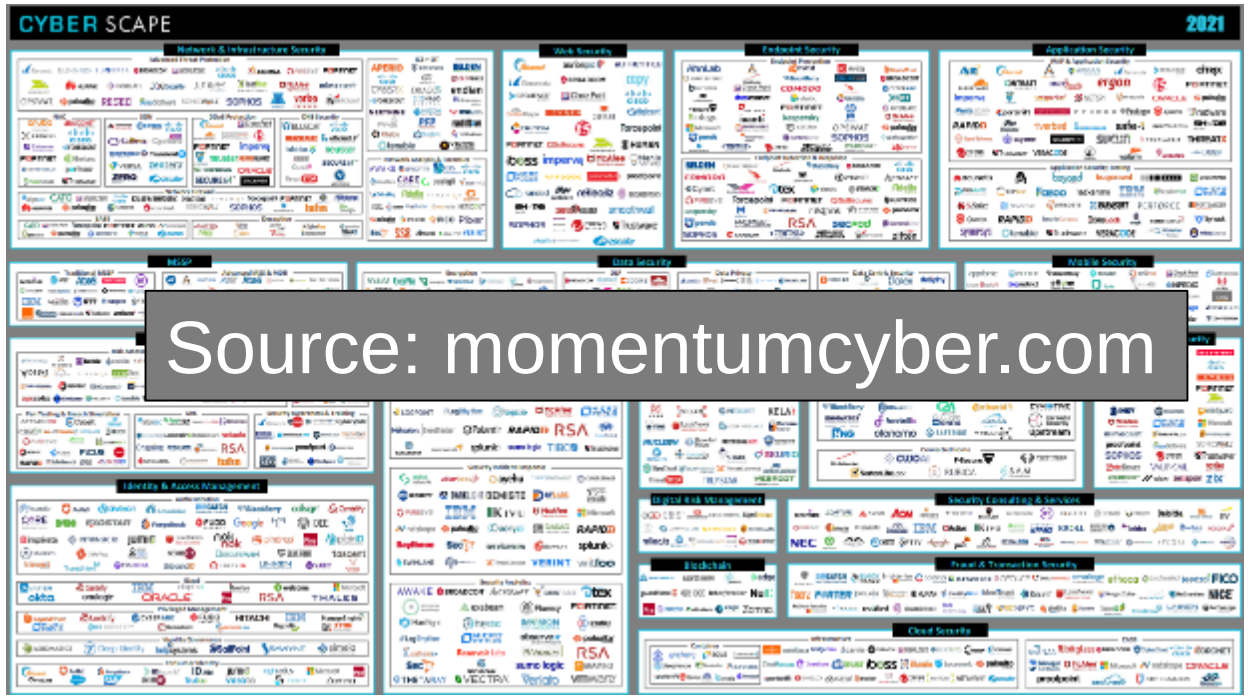
Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Community Response: Hundreds of Cyber Analytics

An increasingly crowded and chaotic space: How do we make sense of this landscape?



Source: csiac.org



Source: momentumcyber.com

Our focus is primarily on systems-level analytics and models with test relevance

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Approach and Data Collection

- **Methodology**
  - Convenience sampling approach:
- **Data Collection**
  - Identify decision-support questions
  - For the analytics:
    - Mapping to questions above
    - Input / output data
    - Maturity / support
    - Validation status
  - Across analytics
    - Integration possibilities?
  - Model-Based Systems Engineering (MBSE)
    - Analytic data standardization for SysML models, etc.

Top-down	Literature review – gov't, academic, commercial
Middle-out	Two CAL workshops
Bottoms-up	Our own knowledge, referrals

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Data Collection Stats as of September 2022

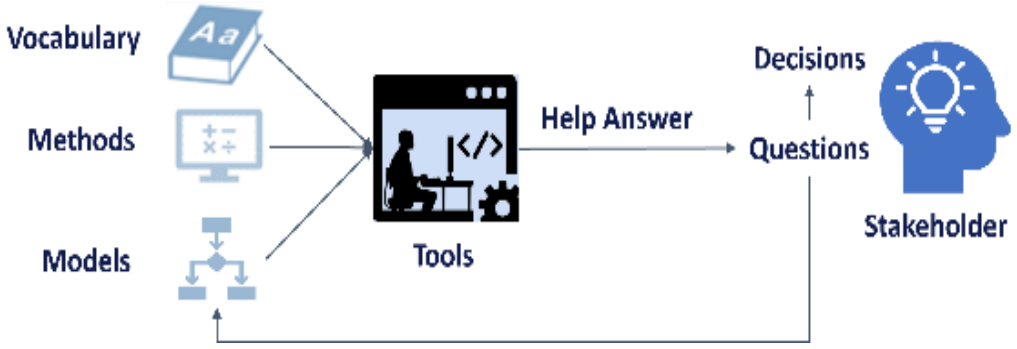
- **CAL team cataloged**:
  - 94 analytic questions in 13 categories
  - 72 representative analytics from 38 organizations
  - 119 mappings of analytics to questions
  - 59 data types tied to the analytics

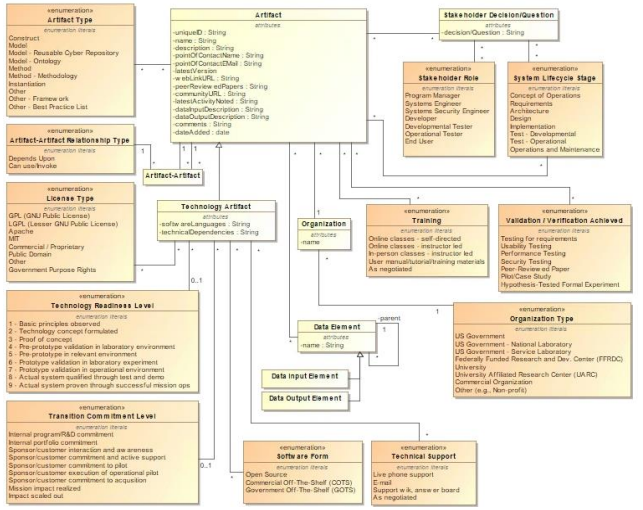
FY22 Performers

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

MITRE

Team developed an information capture model; data held in a relational database





Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Key Observations in FY22

- **Lexicon** – as a community, we struggle to agree on commonly-used terms
- **Large Number of Questions** – we're not always sure what to ask or how to use the answers
- **Large Number of Analytics** – low barrier to entry; everyone has their own approach
- **Hypotheses** – many competing hypotheses for how systems cyber analysis/test should work
- **Human Footprint** – remains large even with analytic use
- **Analytic Validation** – almost non-existent – used mostly "on faith"
- **Key Analytic Gap** – probability cyber-enabled system will perform as required despite cyber effects
- **Analytic Techniques** – analytic "black-boxes" – method and techniques often unknown

Proposed Key Areas of Focus for FY23

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Key Findings in FY22

- **Data** – obtaining detailed, accurate, repeatable data on target cyber systems for analysis is still too hard
- **Integration** – analytics tend to be stovepiped; difficult to integrate together (not designed to be integrated)
- **Human Dimension** – analytics tend to be technically focused; human side has less attention – is less mature
- **Resilience** – today's focus on resilience is almost always technical – also need mission-impact focus

Bottom Line:

Current state of system cyber analysis/test is a reflection of the immaturity of the field (engineering has outrun the underlying science)

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Synthesizing from the Observations and Findings

We should start here - It is all ultimately about the mission

Mission

What mission planners want to know:

(1) **Probability** I'll achieve my mission? (P_m)

(2) How to improve the **probability** above?

Supporting Cyber Systems

What cyber stakeholders want to know about each contributing cyber-enabled system:

(1) **Probability** system will perform adequately given cyber threat? (P_s)

(2) How to improve the **probability** above?

Today's Chasm

Even with (unvalidated) analytic artifacts, we still have a heavy reliance on subjective human judgment

- **Slow**
- **Expensive**
- **Not reproducible**

Cyber Artifacts Today

We analyze what we can, but don't validate the approaches

Threat actors?
Threat capabilities?
Risk?
Attack paths?
Criticality?
Dependency?
Vulnerabilities?
Resilience?
Mitigations?

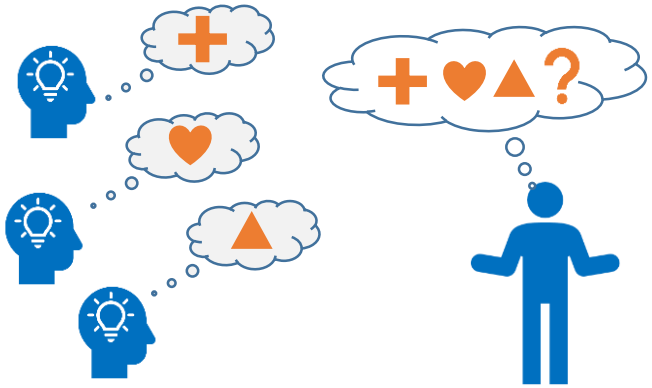
We want to be here

Today we are here

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

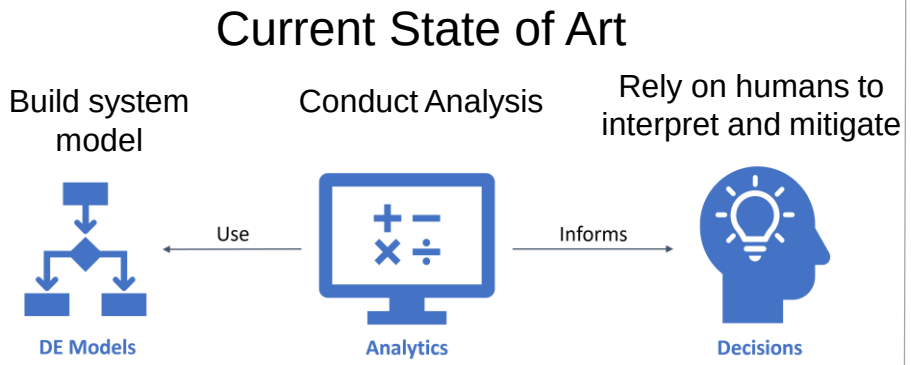
Summary of Current State of Systems Cyber Analysis and Related Challenges

Lack of an established foundation



- Varying Jargons
- Many Competing Hypotheses
- Incompatible Methods
- Unvalidated Data Sets
- Segregated Technologies

Immature cyberspace analytic processes



- Heavy Dependence on Human Input
- Nonrepeatable Processes
- Unknown Results Accuracy
- Slow Analysis

Creation of tools looking for problems

- Lack of Rigorous Validation
- Potential False Sense of Security
- Wasted Cost/Schedule/Resources
- Frustrated Stakeholders

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Long Term CAL Vision

Starting Place

- Varying Jargons
- Many Competing Hypotheses
- Incompatible Methods
- Unvalidated Data Sets
- Segregated Technologies

- Heavy Dependence on Human Input
- Nonrepeatable Processes
- Unknown Results Accuracy
- Slow Analysis

- Lack of Rigorous Validation
- Potential False Sense of Security
- Wasted Cost/Schedule/Resources
- Frustrated Stakeholders

Might be Good,
No Way to Know

Moving the landscape towards

Strategic Vision

- Consistent Vocabulary
- Well-supported Theories
- Compatible Methods
- Validated Data Sets
- Integrated Lifecycle Tools

- Reduced Human Dependence
- Repeatable Processes
- Validated Results
- Efficient Analysis

- Validated Analytics
- Increased Confidence in Security
- Reduced Cost/Schedule/Resources
- Satisfied Stakeholders

Label is Trustworthy

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-29

Looking Ahead – Year 2

- **Analytics Methods/Techniques**
  - Document analytic methods and techniques; capture in an “Analytic Characterization Framework” (ACF)
  - Create an ACF ontology and knowledge graph to enable consistent test and evaluation
- **Analytic Validation**
  - Develop validation approaches and describe the quality of evidence they produce
  - Look at validation piloting opportunities
  - Think through the longer term policy/resourcing implications
- **Analytic Gap for Key Questions**
  - Gap: What is the probability that a cyber-enabled system will perform as required despite cyber effects?
  - Gap: What are options for raising the probability above if deemed too low?
  - Develop an analytic approach to answer the questions above
  - Consider integration opportunities and validation

Workshops in Support of Above

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Questions

sarah.m.standard.civ@mail.mil

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Backup

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Examples of Analytic Questions

Mission	What systems support a given mission-essential task list (METL)?
	What systems are intended as backups to a given cyber-enabled system in case the cyber system fails or becomes distrusted?
Mission Probabilities	What is the probability, Pm, that my mission will succeed despite adverse cyber events in supporting cyber-enabled systems during the mission timeline?
	How do changes (e.g., systems used, dependencies) affect the probability, Pm? (see MP-1 for Pm definition)
Threat and Mitigation	What cyber threat capabilities by kill chain stage are possessed by a given type of adversary?
	Which mitigation capabilities can help defend against a given cyber threat capability?
	Which threat capabilities apply to a given cyber asset type?
System	What are the mission essential functions (MEFs) of the system under analysis?
	What are the performance metrics tied to a given MEF?
	What is the allowable range of values for each MEF performance metric?
	What are the cyber assets (components) in my system and what are their corresponding asset types?
	What cyber assets have network connectivity with other cyber assets?
	What is the impact on MEF performance of a cyber effect on a supporting cyber asset's data?
	What cyber mitigations are currently designed into the system?
	Which cyber assets benefit from which cyber mitigations?
	What is the rolled-up criticality of a cyber asset based on its support for supported MEFs?
	What is the worst-case adversary type expected for the system in a given mission context?
Adverse Cyber Events	What is the probability that a malicious attack involving a given cyber asset will occur at a given time during the mission timeline?
	What is the probability that a hardware cyber asset will physically fail at a given time during the mission timeline?
	What is the probability that an operator error will occur for a given cyber asset at a given time during the mission timeline?
	What is the probability that an undetected flaw/bug will manifest for a given cyber asset at a given time during the mission timeline?
	What is the probability that an act of God will occur for a given cyber asset at a given time during the mission timeline?
MEF Probability	What is the probability, Ps, that the performance of the mission-essential functions (MEFs) of a given cyber-enabled system will remain at or above their corresponding minimum threshold values despite adverse cyber events during a given mission timeline?
	How do changes (e.g., risk tolerance, mitigations, criticalities, budget) affect the probability, Ps? (see MEF-1 for Ps definition)
Risk and Mitigations	Which applicable adversary threat capabilities remain unmitigated for a cyber asset in my system?
	What is the risk to the system's MEFs from adverse cyber effects?
	What mitigations to cyber threat capabilities should I consider based on a set of tradespace constraints? (e.g., risk tolerance, budget)
	What is the priority of possible cyber mitigations based on a set of tradespace constraints?

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Examples of Analytics/Models Reviewed

ArcReACTOR	Dagger
Automated Vulnerability and Risk Assessment	HAMLET
BluGen	Integrated Resilience Analysis Tool
Common Attack Pattern Enumeration Classification	Mean Time to Failure/Compromise (MTTF & MTTC) Metric
Compromise Probability (stochastic model-based/attack graph-based/Bayesian attack graph-based)	Meta Attack Language
Critical Infrastructure Cyberspace Analysis Tool	Mission Focused Cyber Hardening: Mitigation Prioritization Framework
CSA Tool	Mission-Based Risk Assessment Process for Cyber
Cyber Assassin	NSA Technical Cyber Threat Framework
Cyber Operational Risk Tool	Ontology for Attacks in Cyber Risk Assessment
Cyber Operations Rapid Assessment	Path length (shortest path, mean path length, number of paths)
Cyber Security Game	PRUNE
Cyber Security Modeling Language	Resilience Index Simulator
Cyber Vulnerability Assessment Tool	Security, Agility, Resilience and Risk (SARR) Framework
CyberReason XDR	SOFIA, RMF/Cyber Automation
Cybersecurity Figure of Merit	Tabletop Mission Cyber Risk Assessment (TMCRA) Overview
CyberSpaceSuite	Unified Risk Assessment and Measurement System
D3FEND	

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Disclaimer:
This briefing, presentation, or document is for information only. No U.S. Government commitment to sell, loan, lease, co-develop or co-produce defense articles or provide defense services is implied or intended. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Air Force, Space Force, the Department of Defense, or the U.S. Government.

25th Annual Systems and Mission Engineering Conference
1-3 Nov 2022

A Rocket Scientist's Approach to Continuous Innovation and Improvement (CI2)

Continuous Innovation and Improvement
CI2
How We Launch Innovative Ideas

Mr. John Wong
Rocket Scientist and
Deputy Director of Engineering
Assured Access to Space
Space Systems Command
El Segundo, CA
john.wong.6@spaceforce.mil

Mr. Andy Inkeles
Rocket Scientist and
Risk and Innovation Management Lead
Assured Access to Space
Space Systems Command
El Segundo, CA
andy.inkeles@mantech.com

DISTRIBUTION STATEMENT A. This is approved for public release distribution is unlimited.

National Security Space Launch (NSSL)

NSSL, formerly Evolved Expendable Launch Vehicle (1994 to 2019), is a program of the USSF intended to assure access to space for the nation's most valuable DoD and other U.S. Government agencies' military satellites

Falcon 9	Atlas V	Vulcan	Falcon Heavy	Delta IV
SpaceX	**ULA**	**ULA**	**SpaceX**	**ULA**

NSSL

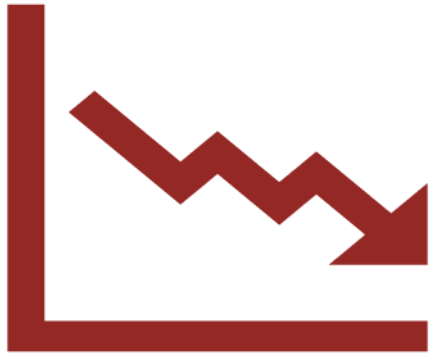
Highly reliable medium to heavy spacelift

Priorities

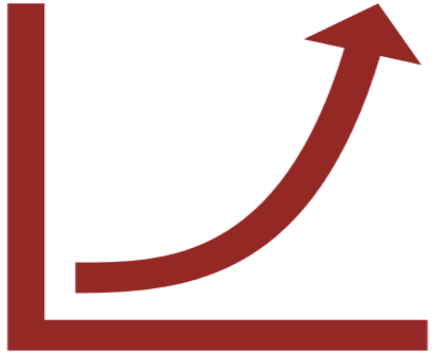
- 100% Mission success
- Assure access for current and future space architectures
- Transition National Security Space payloads to new launch vehicles
- Robust Domestic Industry
- Affordability
- Operational Flexibility

Define the Need for Change

Technical Staff Reduction



Increasing Launch Tempo



- We need to cultivate innovative mission assurance, and accelerate the rate and magnitude of change
- We need to drive culture change
- The USSF incentivized our SE&I contractor (ManTech) to develop and operationalize a structured framework for continual innovation and improvement (CI2)
- Year one CI2 Priorities
  - Designing and standing up a robust framework to identify and manage innovations and improvements
  - Capture of existing innovation and improvement activity
  - Identification and initiation of near-term and longer-term innovations and improvements

YEAR ONE — Innovative "Change Management 101"

Why?

Define the Need for Change

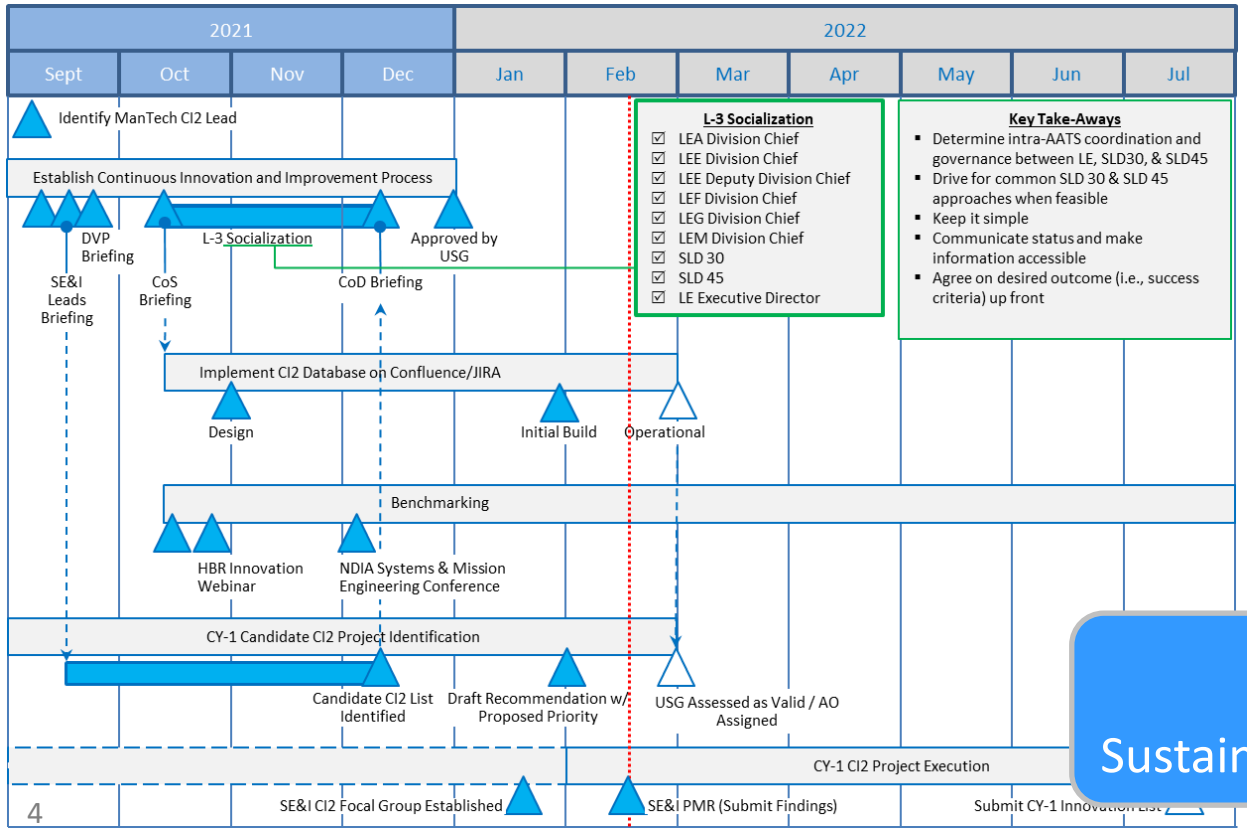
What?

Define the Change

Who?

Understand Stakeholders

When?



How?

Champion the Change

Socialize the Change

Facilitate & Automate the Change

Train About & Support the Change

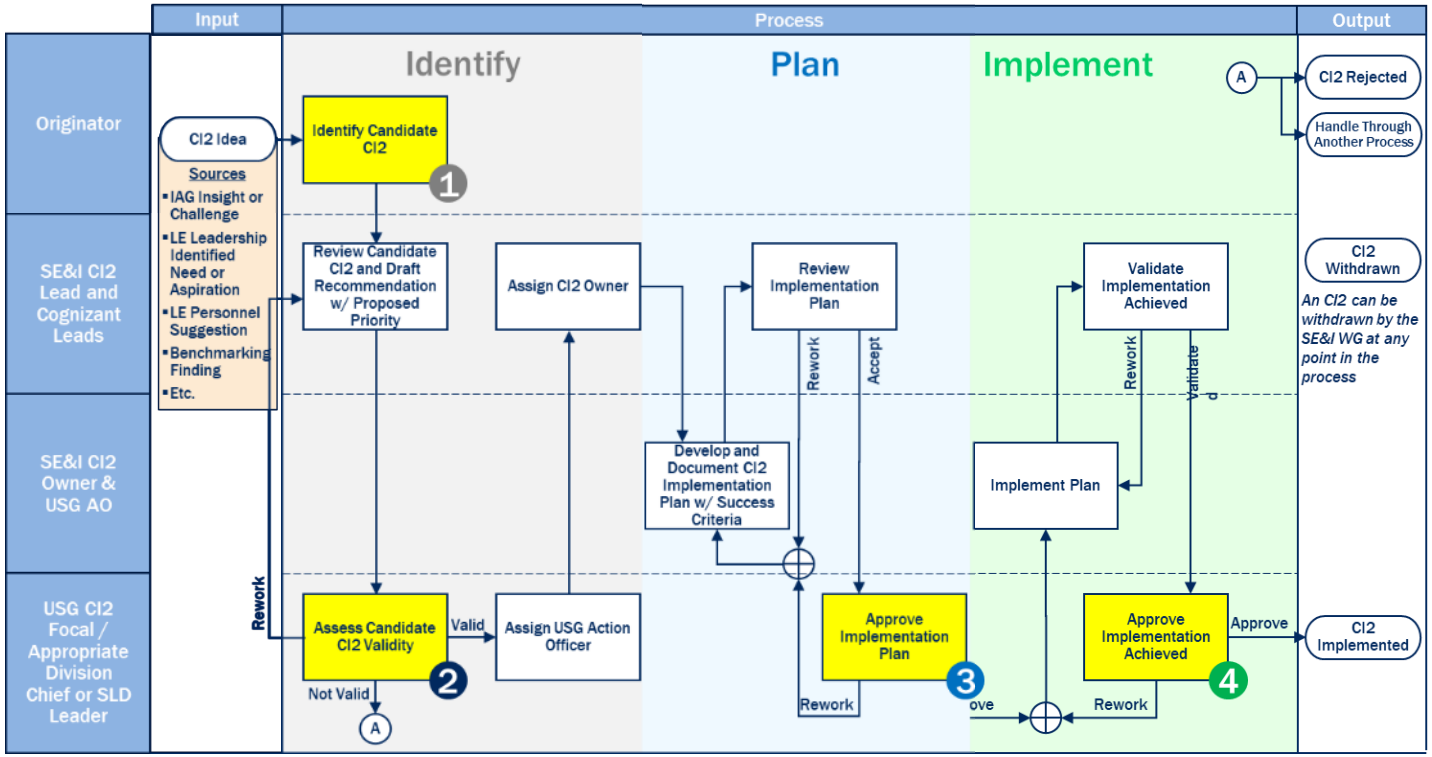
Sustain the Change

Define the Change

- ***Simple***
- ***Transparent***
- ***"Appropriate" formality***
- ***A robust foundation for transformative change***

APPROACH

1) Proactively Identify CI2 Ideas
2) Assess Candidate CI2 Validity
3) Approve CI2 Implementation Plans
4) Validate Implementation Achieved



INNOVATION "TARGETS"

- On-orbit assets meet 2026 warfighter needs
- Improved enterprise process methodology that supports effective utilization of resources
- Maintaining mission success and increasing launch tempo

Understand Stakeholders

Champions

Decision Makers

Influencers

Contributors

Competitors/Collaborators

NSSL Program
USSF, Aerospace, ManTech, etc.

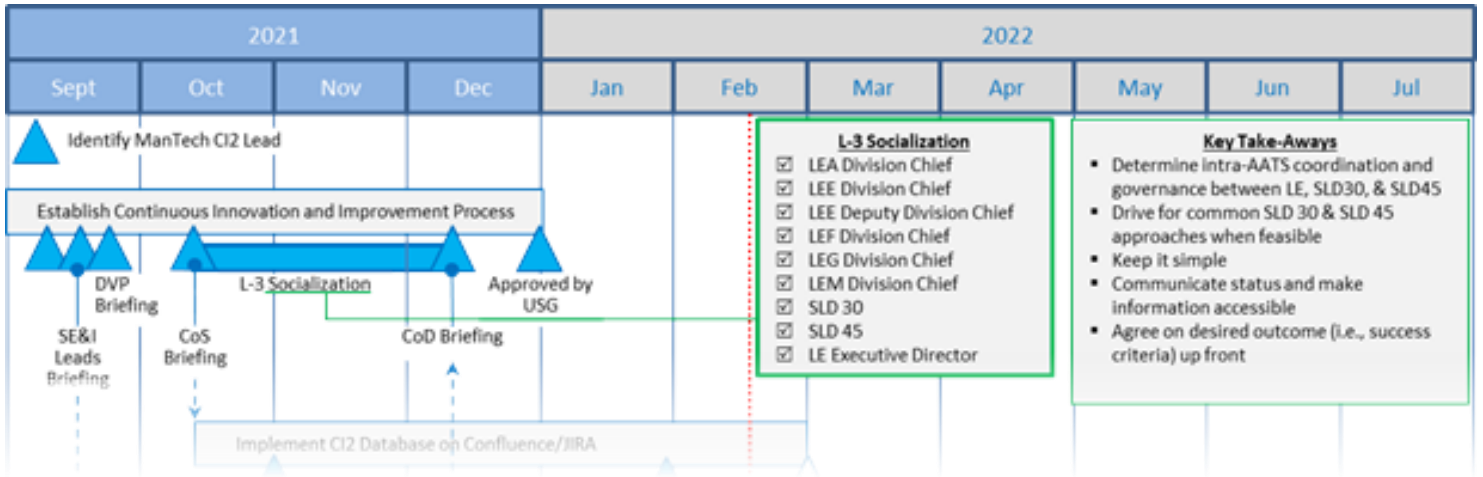
Other USG Entities
NRO, SSIO

Launch Sites
SLD 30 & SLD 45

Launch Service Providers

ManTech Leadership

- **Engage early and often**
- **Listen**
- **Incorporate Ideas**

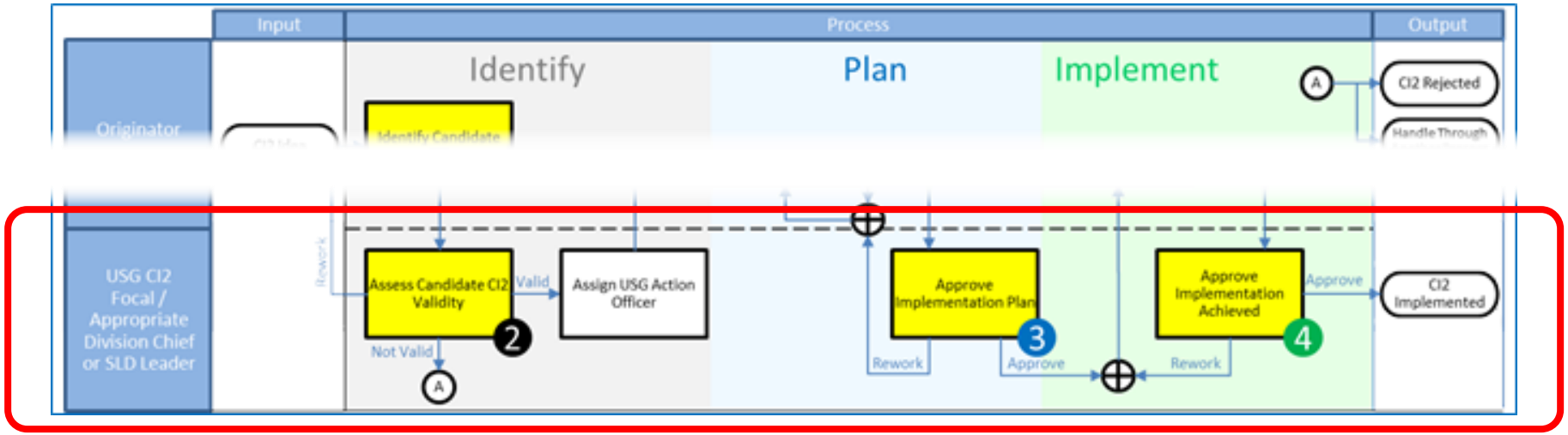


Champion The Change

Mr. John Steinmeyer
Executive Director
Assured Access to Space
United States Space Force

- Provide Government oversight and authority for action
- Drive transparency and collaboration
- Empower engagement at all levels of the organization
- Establish priorities
- Advocacy for resourcing
- Encourage risk taking and recognize effort

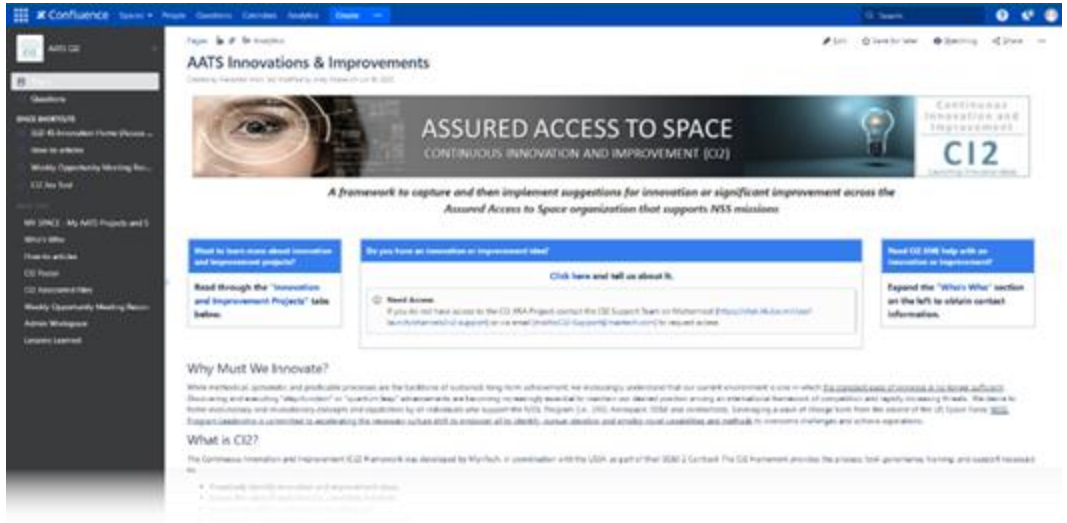
Mr. John Wong
Deputy Director of Engineering
Assured Access to Space
United States Space Force



Socialize the Change

One-on-one CI2 Introductory Meetings

Internal Organizational Marketing



CI2 Confluence Space

Continuous Innovation and Improvement

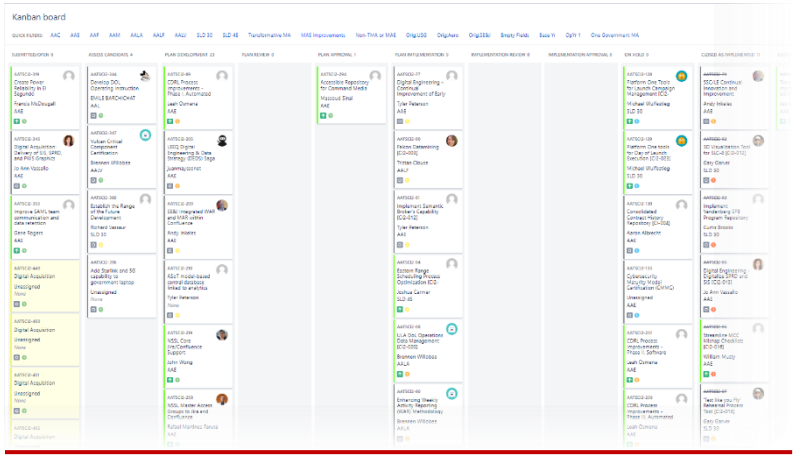
CI2

How We Launch Innovative Ideas

Launching Innovative Ideas

CI2 Icon & Catch Phrase

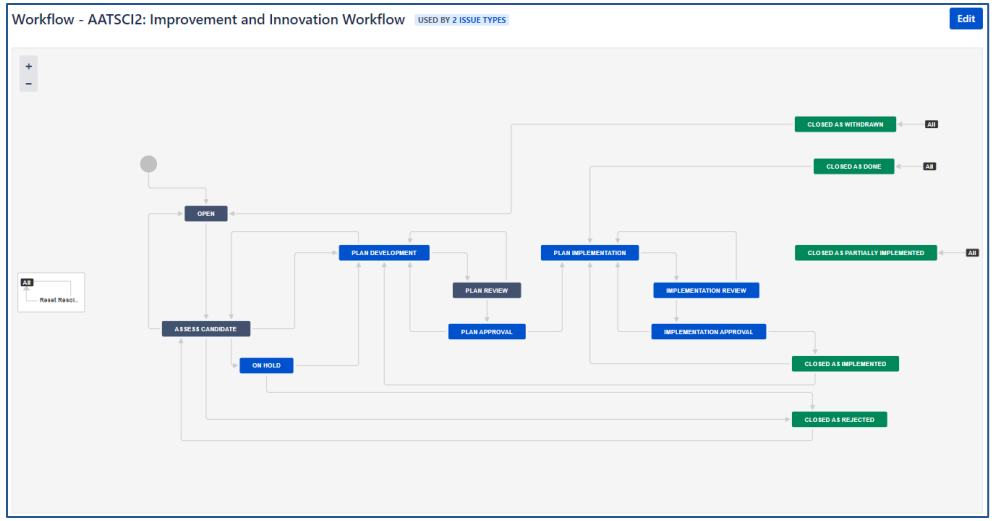
Champion CI2 Email Communications

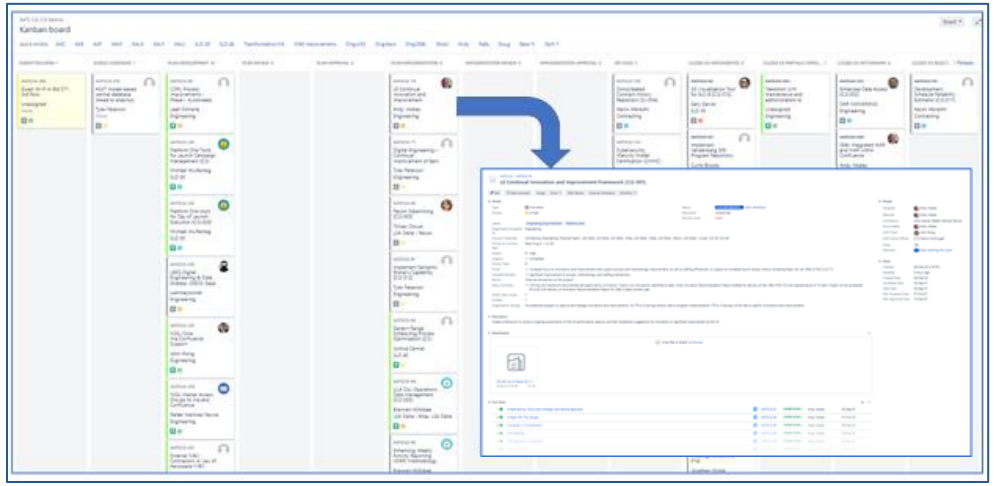


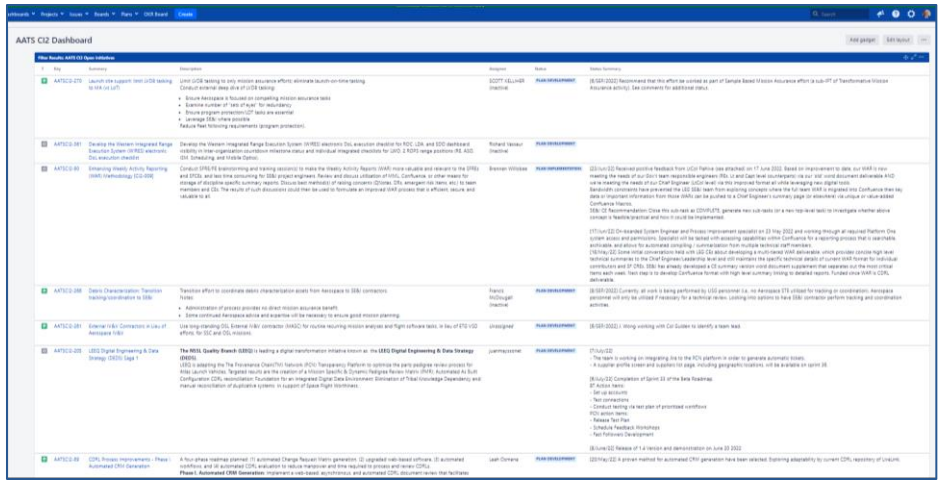
Up Front Spotlight at Weekly Program Management "Crosstalk" Review

Facilitate & Automate the Change

- Developed a tailored CI2 Jira Project and CI2 Confluence Space in the Program's Platform One Environment
  - Incorporates an automated workflow, which is aligned with the CI2 identify, assess, approve, and validate process
    - Supports simple initial idea capture with minimal data entry
      - Displays and reports tailored to an individual's CI2 role or area of focus (e.g., digital engineering)
        - Drives transparency of information, accountability, collaboration, and engagement







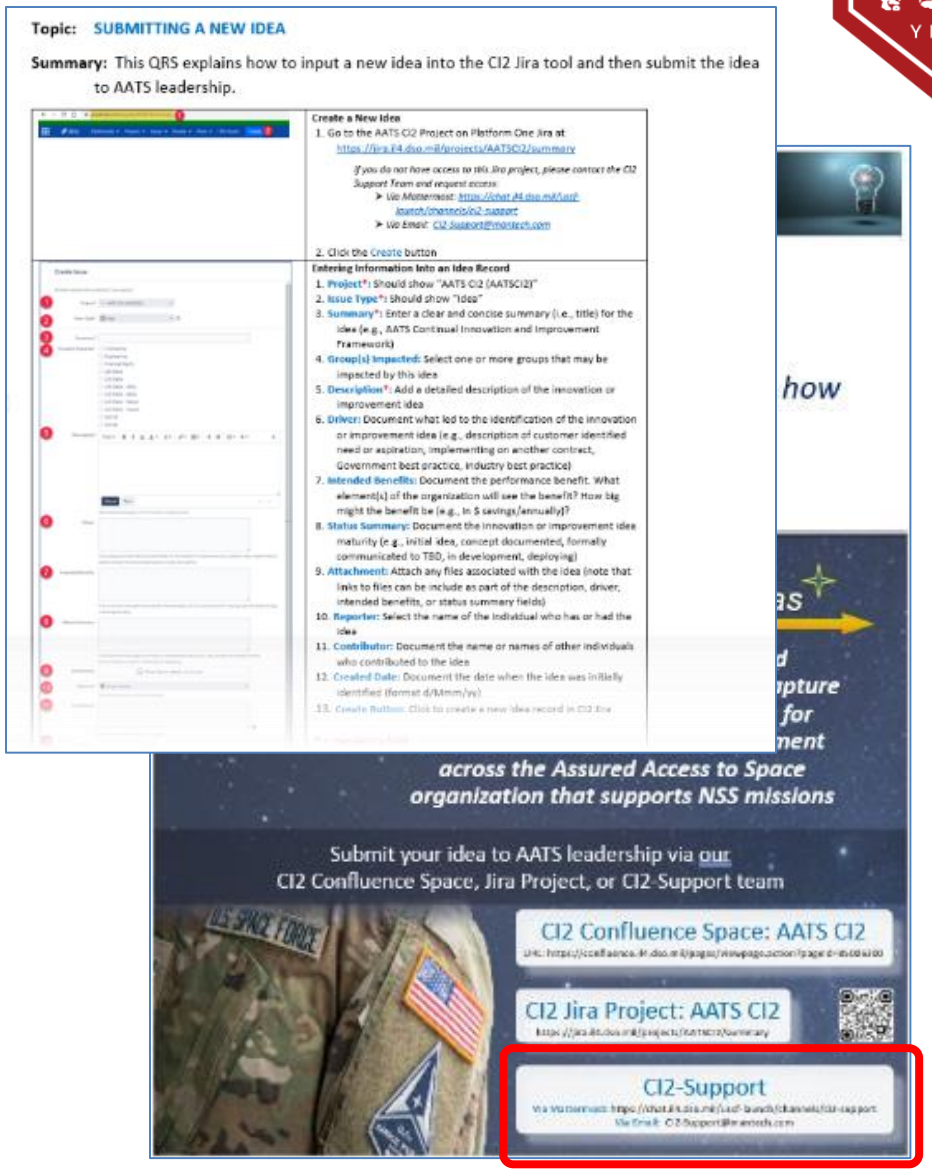
Train About & Support the Change

Training

- A simple and intuitive process, managed in an existing program IT platform (i.e., Platform One) resulted in minimal training or support during initial operationalization

  Exception: Establishing PlatformOne accounts

- Job Aids developed to assist new users with identification of a new idea within CI2 Jira



Support

- Two equivalent persons provide proactive support

- Support team also provides the CI2 Champions with CI2 Project Management support

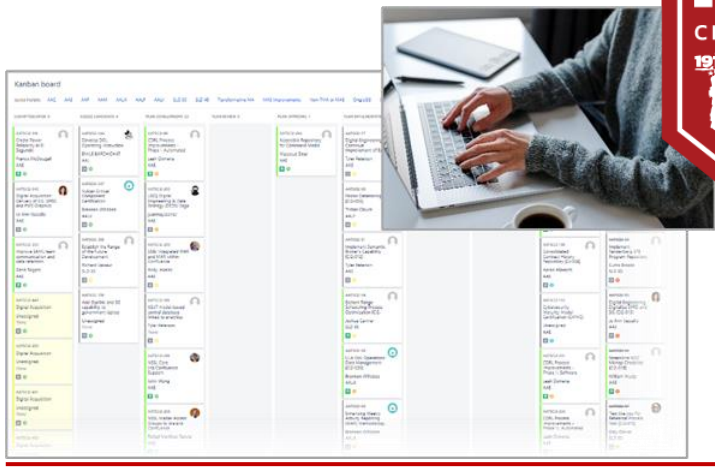
Sustain the Change

Mr. John Steinmeyer
Executive Director
Assured Access to Space
United States Space Force

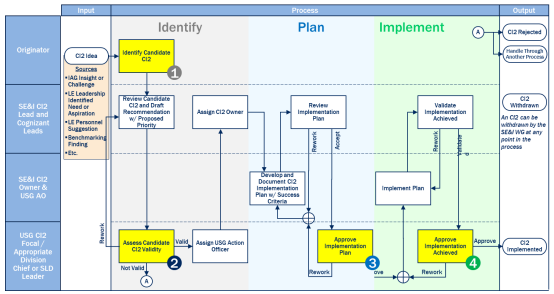
Mr. John Wong
Deputy Director of Engineering
Assured Access to Space
United States Space Force

Active Champion engagement for the long run

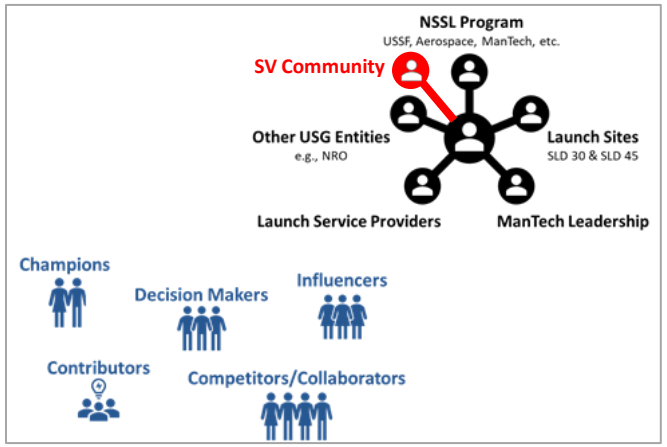
Continual threat awareness (i.e., the need for change sustainment)



Visibility at program reviews and within leadership communications

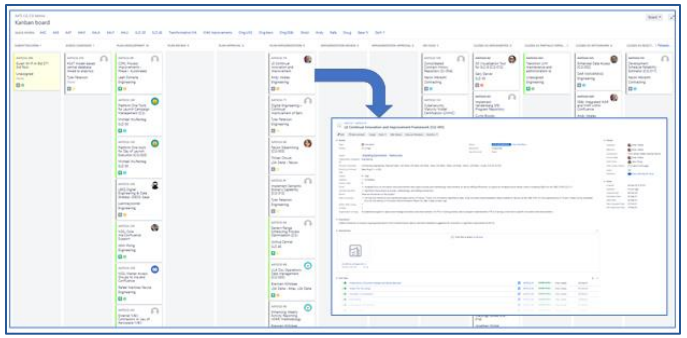


Maintain process discipline and support



Remain engaged with the stakeholders; adjust as needed

Challenge the paradigm, re-assess, & evolve



Evolve the tool

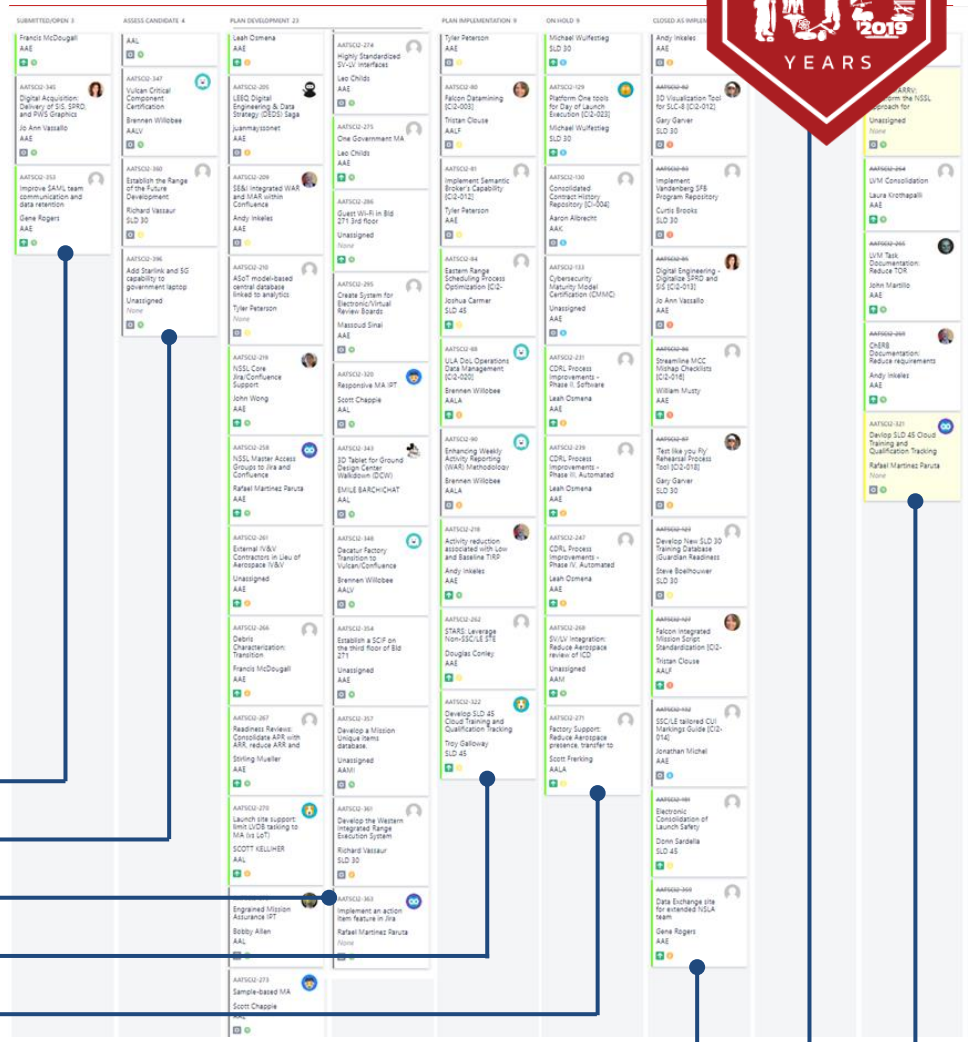
Results

- Ten initiatives successfully completed in the first year
  - AATSCI2-79 – SSC/LE Continual Innovation and Improvement Framework
  - AATSCI2-82 – 3D Visualization Tool for SLC-8
  - AATSCI2-83 – Implement Vandenberg SFB Program Repository (VXPR) on Platform One Jira / Confluence
  - AATSCI2-85 – Digital Engineering - Digitalize System Performance Requirements Document and Standard Interface Specification
  - AATSCI2-86 – Streamline Mission Control Center Mishap Checklists
  - AATSCI2-87 – 'Test like you Fly' Rehearsal Process Tool
  - AATSCI2-123 – Develop New SLD 30 Training Database (Guardian Readiness Education Management & Learning Network [GREMLN])
  - AATSCI2-127 – Falcon Integrated Mission Script Standardization
  - AATSCI2-132 – SSC/LE tailored CUI Markings Guide
  - AATSCI2-181 – Electronic Consolidation of Launch Safety Information
- Most initiatives required no additional funding
- CI2 Framework briefed to and actively supported by Major General (select) Steven Purdy, USSF Assured Access to Space Program Executive Officer

Current Status (as of 20 Sept.)

- Ideas being generated (3)
- Ideas being evaluated (4)
- In plan development (23)
- In plan implementation (9)
- On hold (9)
- Closed as implemented (11)
- Closed as partially implemented (1)
- Closed as withdrawn (6)

CI2 Confluence Space



In Summary

- ☑ Require Transparency
- ☑ Enable the Workforce
- ☑ Manage Change
- ☑ Champion the Change
- ☑ Continue to evolve

Questions?

Machine Learning Based Surrogate Modeling of Human Vehicular Vibration

25th Annual Systems and Mission Engineering Conference
November 1-3, Orlando, Florida

Will Kirkpatrick[1,2], Gehendra Sharma[1], Nayeon Lee[1], Michael A. Murphy[1], Raheleh Miralami[1], William G. Bond[3]

[1] Center for Advanced Vehicular Systems (CAVS), Mississippi State University, Mississippi State, MS, USA

[2] Department of Mechanical Engineering, Mississippi State University, Mississippi State, MS, USA

[3]The U.S. Army Engineer Research and Development Center (ERDC), Vicksburg, MS, USA

Outline

- Introduction
- Study Objectives and Approach
- Finite Element Simulation Models
- Finite Element Simulations
- Vibration Inputs
- Injury Criteria
- Surrogate Modelling
- Expected Outcomes and Conclusions

Introduction

- Vibration exposure is a known cause of several human medical issues, such as short-term and long-term pain and injury in the back and spine [1].
- This exposure can be found in several fields of work, including agriculture, transportation, forestry, and construction [2]. The military also has this issue, as military vehicles are often driven in terrains that expose the drivers to **whole-body vibration** (WBV) that affect the driver's comfort and health [3].
- It has been found that the resonance frequency of the human spine occurs at around 4.5-5 Hz [4], and many vehicles vibrate at a frequency close to the natural frequency of the human body [5].

Military Humvee

From https://en.wikipedia.org/wiki/Humvee, 9/30/22

[1] N. Arora, et al, *J. Electromyogr. Kinesiol*, 2013.
[2] M. Yung, et al, *PLoS ONE*, 2017.
[3] D. J. Park, et al, Int. *J. Ind. Ergon*., 2019.
[4] T. Hansson, et al, *Clin. Biomech*, 1991.
[5] M. H. Pope, et al, *J. Biomech*, 1987.

Study Objectives

- Investigate the effects of whole-body vibration (WBV) on injury to the spine
- **Establish a method to assess injury risk due to WBV.**

Approach

- Finite element (FE) method used for simulations
  - Human body models settled onto a care seat model
  - WBV vibration inputs will be used to obtain spine stresses and strains
  - Injury risk criteria calculated to determine injury risk level
- Machine learning-based surrogate models
  - Frequency and amplitude combinations used as WBV inputs
  - FE simulation and injury risk results used as to build model

FE Simulation Models

- LS-Dyna Finite Element Simulation software package
  - Human models placed into seat model using seat deformer tool within LS-PrePost
- Human Models (Elemance)
  - 50th percentile male human models
  - Simplified version (840,000 elements)
  - Detailed version (2,300,000 elements)
- Seat from 2021 Nissan Rogue

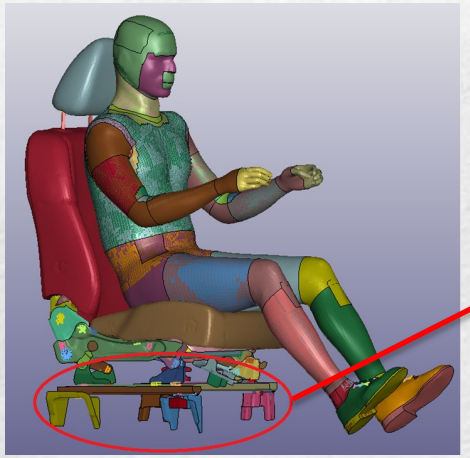
Nissan Rogue Seat Model

Human Detailed Model

From Elemance: "Virtual Human Models", https://www.elemance.com/models/

FE Simulations

- A settling period in the simulation is used to allow the human model to relax into the seat.
- Following this settling period, a **vibrational input is applied to the bottom components of the seat** to allow a realistic portrayal of the vibrations propagating through the seat.
- A seatbelt will be added onto upcoming simulations within this project to have a more accurate portrayal of the real-world case.

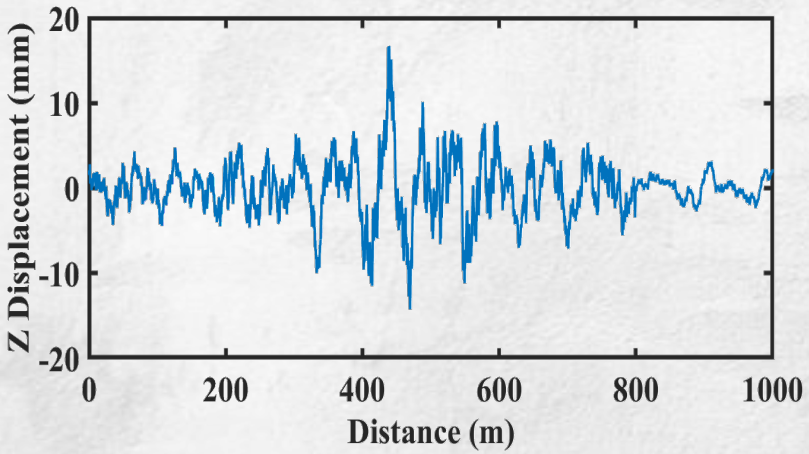


Seated Human Model (Detailed)

Parts with vibration input

Vibration Inputs

- The vibration inputs will be **time (ms) vs displacement (mm)** data generated using
  - CREATE-GV (military vehicles)
  - Non-stationary Laplace road terrain generator [1] paired with an 8 DOF car model [2] to create vibration profiles



Generated Road Profile

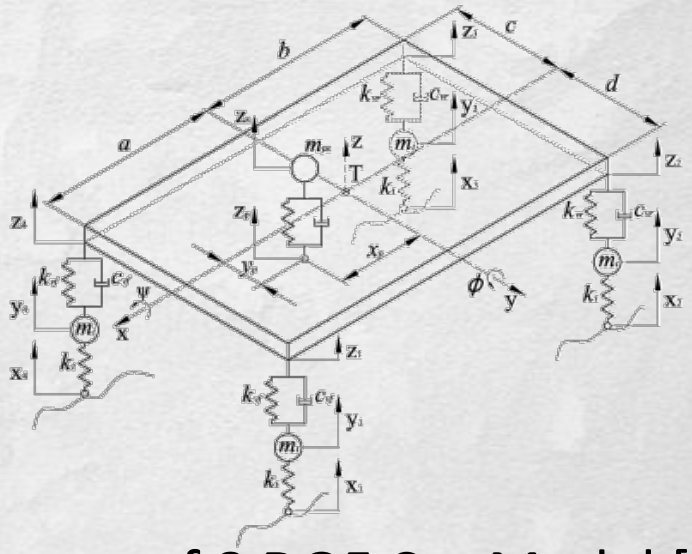


Diagram of 8 DOF Car Model [2]

[1] P. Johannesson and I. Rychlik, *Int. J. Veh. Des.*, 2014
[2] R. Žigulić et al, *Trans. FAMENA*, 2009.

Injury Criteria

- For the injury risk factor (IRF), three specific stresses on the lumbar spine will be needed
  - σ_{static} (compressive stress)
  - $\sigma_{dynamic}$ (dynamic stress)
  - $\sigma_{ultimate}$ (ultimate stress - 41.668 ρ $^{1.9}$ [2])

- The IRF has three tiers of injury risk
  - IRF < 30% is a low risk of injury
  - 30% < IRF < 50% is a moderate risk of injury
  - IRF > 50% is a high risk of injury

$$\sigma_{dynamic} = B\frac{\sqrt{1+(2*\xi)^2}}{2*\xi}\frac{A(f)*M}{s}*cos(\theta)$$

- The variables for the dynamic stress [1]
  - M = equivalent mass
  - A(f) = applied acceleration amplitude to the seat at the natural frequency (f)
  - S = cross-sectional area at the intervertebral disc
  - θ = posture angle
  - ξ = damping rate
  - B = statistical constant

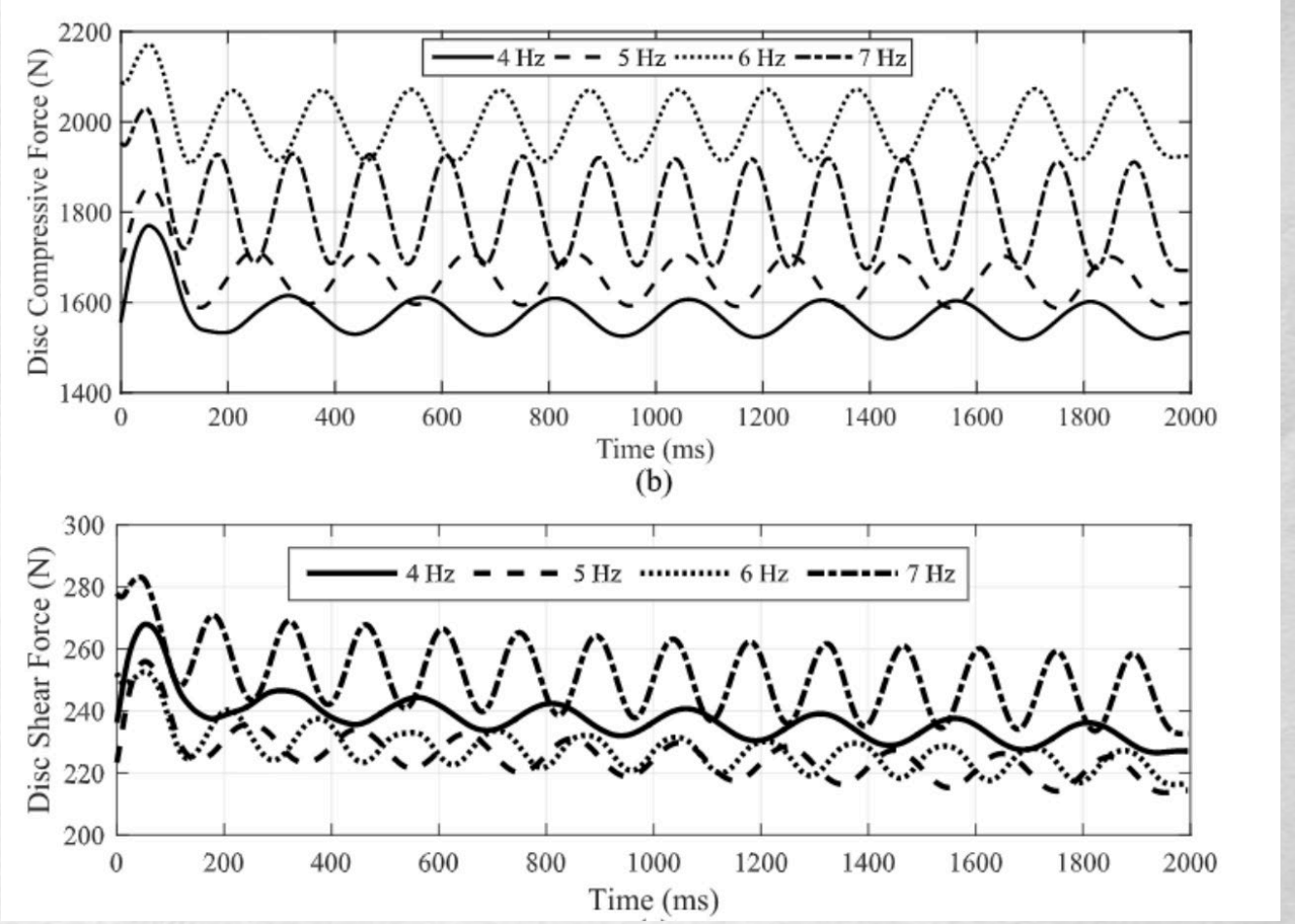
$$\text{IRF} = 100 * \frac{\sigma_{static}+\sigma_{dynamic}}{\sigma_{ultimate}}$$

[1] Ayari et. al, *Revue Internationale sur l'Ingénierie des Risques Industriel,* 2008.
[2] Ayari et al, *Journal of Sound and Vibration*, 2009.

Injury Criteria

- Further work will be done with the FE models to **identify the natural frequencies of the spine model**.

- These natural frequencies can be used to **avoid resonance** and see how resonance impacts the injury risk of the spine.

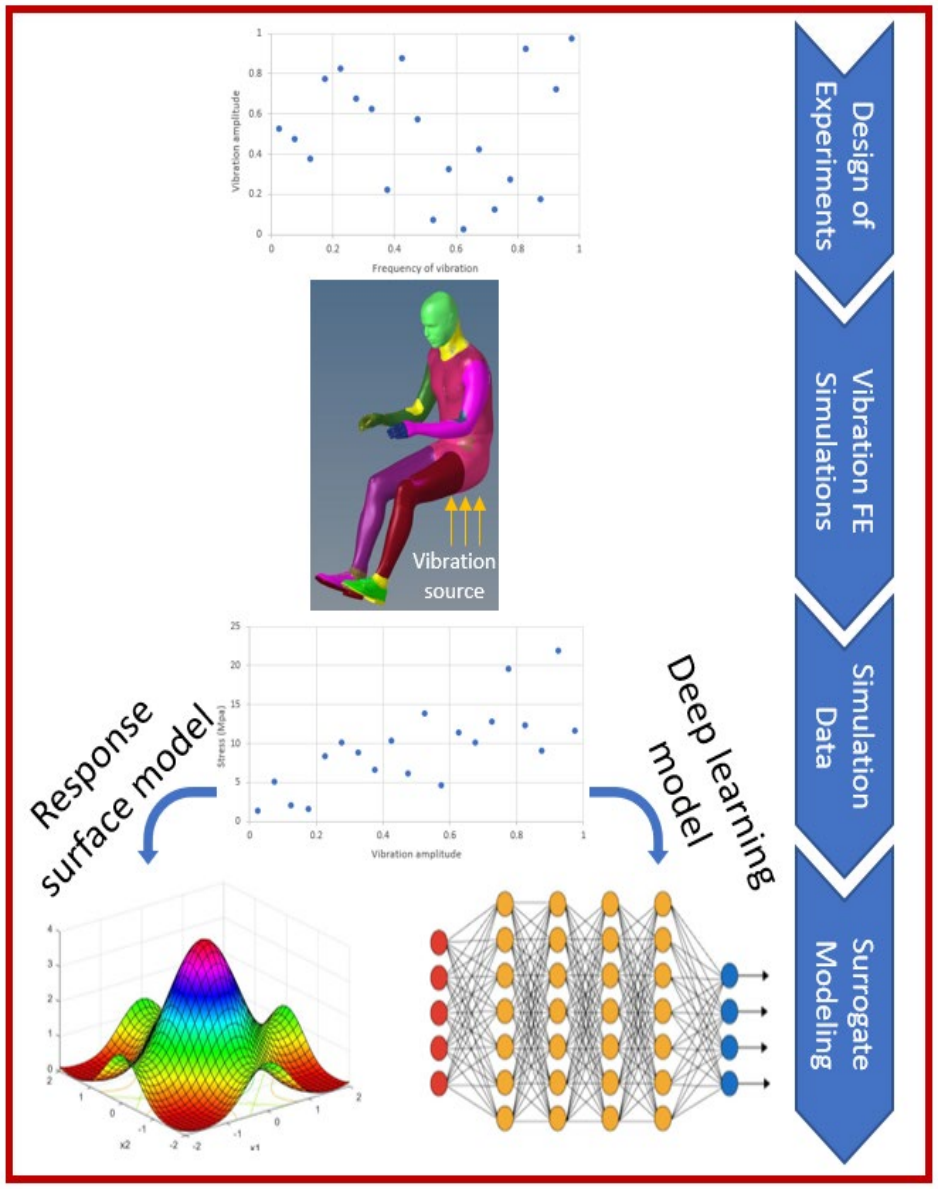


Compressive and Shear Forces in the Spine at Different Vibration Frequencies [1]

[1] S. Amiri, et al, *Comput. Biol. Med.*, 2019

Surrogate Modelling

- Finite element simulations coupled with surrogate modeling techniques
- Latin hypercube sampling used to design experiments for conducting the FE simulations
- Surrogate modeling employed to **establish a relationship between the finite element inputs (vibration variables) and outputs (injury risk metrics)**
- Outcome is an assessment method to predict risk of injury associated with vehicular vibration.



Overview of ML process

Expected Outcomes

- Certain combinations of amplitudes and frequencies of vibration will cause more of an injury risk than others.
- Finding the combinations with the least amount of injury risk can be used to see if vehicle's can be manufactured to have the passenger's vibration fit these combinations.
- **A method to assess risk of injury associated with vehicular vibration.**

Conclusions

- Investigating the effects of whole-body vibration on low-back pain can be important to reduce the pain in millions of people.
- Using FE simulations will give insight into whole-body vibration without having to risk injury to real subjects.

Acknowledgements

Mississippi State University

The U.S. Army Engineer Research and Development Center (ERDC)

The Center for Advanced Vehicular Systems (CAVS)

Thank you

References

- D. J. Park, M. G. Choi, J. T. Song, S. J. Ahn, and W. B. Jeong, “Attention decrease of drivers exposed to vibration from military vehicles when driving in terrain conditions,” *Int. J. Ind. Ergon.*, vol. 72, pp. 363–371, Jul. 2019, doi: 10.1016/j.ergon.2019.06.014.
- H. Ayari, M. Thomas, and S. Doré, “Development of an Injury Risk Factor for Drivers,” *Revue Internationale sur l’Ingénierie des Risques Industriels*, Vol. 1, No. 2, 2008.
- H. Ayari, M. Thomas, S. Doré, & O. Serrus, “Evaluation of lumbar vertebra injury risk to the seated human body when exposed to vertical vibration,” *Journal of Sound and Vibration*, vol. 321, no. 1, pp. 454–470, Mar. 2009, doi: 10.1016/j.jsv.2008.09.046.
- M. H. Pope, D. G. Wilder, L. Jorneus, H. Broman, M. Svensson, and G. Andersson, “The response of the seated human to sinusoidal vibration and impact,” *J. Biomech. Eng.*, vol. 109, no. 4, Art. no. 4, Nov. 1987, doi: 10.1115/1.3138681.
- M. Yung, A. E. Lang, J. Stobart, A. M. Kociolek, S. Milosavljevic, and C. Trask, “The combined fatigue effects of sequential exposure to seated whole body vibration and physical, mental, or concurrent work demands,” *PLoS ONE*, vol. 12, no. 12, Art. no. 12, 2017, doi: 10.1371/journal.pone.0188468.
- N. Arora and S. G. Grenier, “Acute effects of whole body vibration on directionality and reaction time latency of trunk muscles: The importance of rest and implications for spine stability,” *J. Electromyogr. Kinesiol.*, vol. 23, no. 2, Art. no. 2, Apr. 2013, doi: 10.1016/j.jelekin.2012.10.018.
- P. Johannesson and I. Rychlik, “Modelling of road profiles using roughness indicators,” *Int. J. Veh. Des*., vol. 66, no. 4, p. 317, 2014, doi: 10.1504/IJVD.2014.066068.
- R. Žigulić, S. Kršćanski, and S. Braut, “A numerical analysis of the behaviour of a vehicle model with driver’s seat at the road bump,” *Trans. FAMENA*, vol. 33, no. 4, pp. 19–30, Jan. 2009.
- S. Amiri, S. Naserkhaki, and M. Parnianpour, “Effect of whole-body vibration and sitting configurations on lumbar spinal loads of vehicle occupants,” *Comput. Biol. Med*., vol. 107, pp. 292–301, Apr. 2019, doi: 10.1016/j.compbiomed.2019.02.019.
- T. Hansson, M. Magnusson, and H. Broman, “Back muscle fatigue and seated whole body vibrations: an experimental study in man,” *Clin. Biomech.*, vol. 6, no. 3, Art. no. 3, Aug. 1991, doi: 10.1016/0268-0033(91)90030-T.