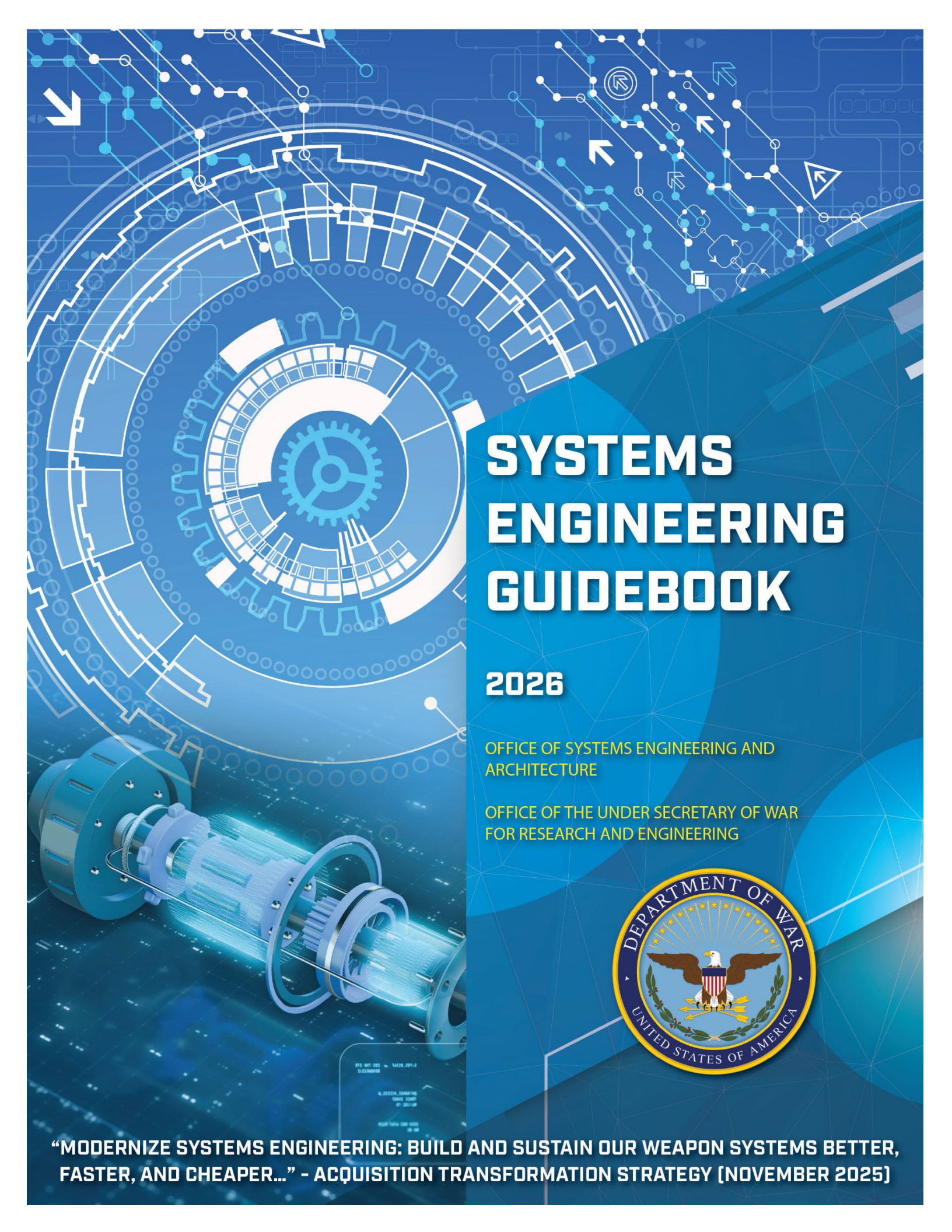




SYSTEMS ENGINEERING GUIDEBOOK

2026

OFFICE OF SYSTEMS ENGINEERING AND
ARCHITECTURE

OFFICE OF THE UNDER SECRETARY OF WAR
FOR RESEARCH AND ENGINEERING



**“MODERNIZE SYSTEMS ENGINEERING: BUILD AND SUSTAIN OUR WEAPON SYSTEMS BETTER,
FASTER, AND CHEAPER...” - ACQUISITION TRANSFORMATION STRATEGY (NOVEMBER 2025)**

Systems Engineering Guidebook

September 2026

Office of Systems Engineering and Architecture
Office of the Under Secretary of War for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd-sea@mail.mil
<https://www.cto.mil/sea/>

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 26-T-2032.

Approved by

Thomas W. Simms

Principal Deputy to the Deputy Assistant Secretary of War for Multi-Domain Joint Operations
Office of the Under Secretary of War for Research and Engineering

Systems Engineering Guidebook Change Record

Date	Change	Rationale
September 2026	Preface: new section 1 - Introduction: minor changes 2 - System-Level Considerations: Moved SoS content to updated SoS guide. 3 - SE Modernization – New section. 3.3 - Digital Engineering: moderate changes 3.4 - Model-Based Systems Engineering: new section 3.5 - Mission Engineering: moderate changes 3.6 - Software Engineering: minor changes 3.7 - Modular Open Systems Approach: moderate changes 3.8 - Systems Engineering in Agile: new section 4.2.1 - Qualifications - New section. 4.3 - Value Engineering: minor changes 4.6 - Systems Engineering Role in Contracting: moderate changes 5 -Technical Reviews and Audits: minor changes 6.1.3 - Technical Assessment Processes: minor changes 6.1.5 - Risk Management Process: new subsections 6.2.3 - Architecture Design Process: minor changes 7 - Design Considerations: minor to moderate changes	Fact-of-life revisions for currency. Alignment with acquisition transformation efforts.

CONTENTS

Preface	viii
1 Introduction.....	1
1.1 Purpose of Systems Engineering	1
1.2 Definition of Systems Engineering.....	3
1.3 Development Planning.....	4
1.4 Systems Engineering Processes	5
1.5 Systems Engineering Policy and Guidance	9
1.6 Systems Engineering Approach.....	11
2 System-Level Considerations	15
2.1 SoS as Enterprise Systems.....	15
2.2 Applying Systems Engineering in SoS	16
3 Systems Engineering Modernization	17
3.1 Systems Engineering Tools and Techniques Overview.....	17
3.2 Models and Simulations.....	20
3.3 Digital Engineering.....	22
3.4 Model-Based Systems Engineering	23
3.5 Mission Engineering.....	24
3.6 Software Engineering.....	25
3.7 Modular Open Systems Approach.....	29
3.8 Systems Engineering in Agile Development	30
3.8.1 Overview.....	30
3.8.2 Agile Development and Systems Engineering.....	30
3.8.3 Continuous Agile Review and Learning.....	33
4 Engineering Resources, Enablers, and Lessons Learned.....	38
4.1 Roles and Responsibilities	38
4.1.1 Stakeholders	41
4.1.2 Integrated Product Teams	42
4.2 Qualifications and Certifications	43
4.2.1 Qualifications.....	43
4.2.2 Certifications.....	44
4.3 Value Engineering	44
4.4 Sustainability Analysis.....	46
4.5 Lessons Learned, Best Practices, and Case Studies.....	47
4.6 Systems Engineering Role in Contracting	49
5 Technical Reviews and Audits	50
5.1 Roles and Responsibilities	54
5.2 Review Criteria	58

5.3	Alternative Systems Review	58
5.4	System Requirements Review	61
5.5	System Functional Review	65
5.6	Preliminary Design Review	67
5.7	Critical Design Review	75
5.8	System Verification Review/Functional Configuration Audit.....	81
5.9	Production Readiness Review.....	83
5.10	Physical Configuration Audit	86
6	Systems Engineering Processes.....	90
6.1	Technical Management Processes	94
6.1.1	Technical Planning Process	94
6.1.2	Decision Analysis Process	102
6.1.3	Technical Assessment Process.....	104
6.1.4	Requirements Management Process	112
6.1.5	Risk Management Process	114
6.1.6	Configuration Management Process	117
6.1.7	Technical Data Management Process	120
6.1.8	Interface Management Process	126
6.2	Technical Processes	128
6.2.1	Stakeholder Requirements Definition Process.....	128
6.2.2	Requirements Analysis Process	130
6.2.3	Architecture Design Process	132
6.2.4	Implementation Process	135
6.2.5	Integration Process.....	136
6.2.6	Verification Process	137
6.2.7	Validation Process	138
6.2.8	Transition Process.....	139
7	Design Considerations	140
7.1	Accessibility (Section 508 Compliance).....	156
7.2	Affordability – Systems Engineering Trade-Off Analyses.....	156
7.3	Anti-Counterfeiting.....	157
7.4	Commercial-Off-the-Shelf.....	159
7.5	Corrosion Prevention and Control	161
7.6	Critical Safety Item.....	163
7.7	Demilitarization and Disposal.....	165
7.8	Diminishing Manufacturing Sources and Material Shortages	166
7.9	Human Systems Integration.....	167
7.10	Insensitive Munitions.....	169
7.11	Intelligence (Life Cycle Mission Data Plan).....	170
7.12	Interoperability and Dependencies	172

7.13 Item Unique Identification.....	174
7.14 Manufacturing and Quality	175
7.15 Modular Design	177
7.16 Operational Energy	178
7.17 Packaging, Handling, Storage, and Transportation.....	181
7.18 Reliability and Maintainability Engineering.....	181
7.19 Spectrum Management	183
7.20 Standardization	185
7.21 Supportability.....	187
7.22 Survivability.....	189
7.23 System Safety	192
7.24 System Security Engineering.....	194
Acronyms.....	197
References.....	202

Figures

Figure 1-1. The System.....	4
Figure 1-2. SE Processes.....	6
Figure 1-3. SE Processes in the V Diagram.....	7
Figure 1-4. System Life Cycle Process	8
Figure 3-1. Digital Engineering throughout System Development	23
Figure 3-2. DoW DevSecOps Process for Continuous Integration/Continuous Delivery	26
Figure 3-3. Notional Multiple Agile Subsystem Iterations.....	32
Figure 3-4. Generic Agile Iteration.....	34
Figure 5-1. Generic Life Cycle Including Agile	51
Figure 5-2. Technical Reviews and Audits for the Major Capability Acquisition Life Cycle.....	52
Figure 5-3. Technical Review Process.....	57
Figure 6-1. Notional Emphasis of SE Processes during the Major Capability Acquisition Life Cycle.....	94
Figure 6-2. IMP/IMS Hierarchy and Content	100
Figure 6-3. Schedule Risk Assessment Histogram	102
Figure 6-4. Technical Performance Measure Hierarchy	110
Figure 6-5. Leading Indicators Influence Risk Mitigation Planning	111
Figure 6-6. TPM Contingency Definitions	112
Figure 6-7. Risk, Issues, and Opportunities	115
Figure 6-8. Data Management Activities	121
Figure 6-9. Data Taxonomy	124

Figure 7-1. Intelligence Mission Data Life Cycle Timeline (MCA Pathway).....	171
Figure 7-2. Spectrum-Related Activities by MCA Life Cycle Phase	185

Tables

Table 1-1. SE-Related Policy.....	9
Table 3-1. SE Process-Related Tools.....	18
Table 3-2. Agile Technical Reviews Description	35
Table 5-1. ASR Products and Criteria	60
Table 5-2. SRR Products and Criteria.....	63
Table 5-3. SFR Products and Criteria	67
Table 5-4. PDR Products and Criteria	71
Table 5-5. CDR Products and Criteria	78
Table 5-6. SVR/FCA Products and Criteria.....	83
Table 5-7. PRR Products and Criteria.....	85
Table 5-8. PCA Products and Criteria	89
Table 6-1. SE Processes	91
Table 6-2. SE Processes/Activities Mapped to ISO/IEC/IEEE 15288 SE Processes	92
Table 6-3. Core TPM Category Definitions.....	108
Table 7-1. Design Considerations.....	141
Table 7-2. Links to Section 508 Government Resources.....	156
Table 7-3. Anti-Counterfeit Design Considerations Relationships.....	158
Table 7-4. Product Support Considerations	188

PREFACE

The Department of War (DoW) operates in an increasingly complex and rapidly evolving technological landscape. To maintain its competitive edge, the DoW must deliver systems that are capable, affordable, and adaptable to meet mission-critical requirements. This updated Systems Engineering (SE) Guidebook aligns with the acquisition reform directed by Executive Order (EO) 14265, “Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base,” and fully supports the Secretary of War memorandum, “Transforming the Defense Acquisition System into the Warfighting Acquisition System to Accelerate Fielding of Urgently Needed Capabilities to Our Warriors,” November 7, 2025, and the accompanying Acquisition Transformation Strategy. This guidebook serves as a set of concepts, activities, and processes that make up the SE domain. It is designed to serve as a flexible reference guide, not as a mandatory checklist, empowering programs to tailor best practices to their unique needs while embracing innovative approaches.

“The WAS is dependent on many parts to deliver the world’s most sophisticated and capable weapon systems; *systems engineering* is one of its *most critical disciplines*.”

— 2025 Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom

As stated in the Acquisition Transformation Strategy, the Warfighting Acquisition System (WAS) is dependent on many parts to deliver the world’s most capable weapon systems, and SE is one of the most critical disciplines. The DoW must continually modernize SE processes and tools to provide the most modern capabilities, ensuring that the foundational SE processes remain sound while the associated practices evolve to fully leverage the shift from document-based communication to digital models and their underlying data. The Department is dedicated to continuously advancing its SE approach:

- Embracing modernization to support agile development
- Accelerating technology integration
- Informing calculated risk decisions

“As part of this comprehensive acquisition transformation, the Department will *modernize systems engineering across all acquisition pathways* to enable agile development, technology insertion, improved technology and manufacturing risk management, and reduced need for testing, rework, and re-testing to certify a system.”

— 2025 Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom

Modernizing SE necessitates seamless integration of iterative and incremental development practices across key activities—including digital engineering (DE), the modular open systems approach (MOSA), mission engineering (ME), software engineering (SWE), and developmental test and evaluation (DT&E). It also requires alignment across the diverse pathways of the Adaptive Acquisition Framework (AAF) to ensure cohesive, agile, and mission-focused capability development. Modern SE should support accelerated prototyping and delivery of new capabilities to our warfighters at speed.

“The Department must *continually modernize systems engineering processes and tools* to provide the most modern capabilities and guidance...”

— 2025 Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom

Risk management is central to transforming acquisition practices to enable the rapid delivery, sustainment, and evolution of systems at scale. Proactively identifying and managing risks is essential to aligning acquisition with urgency and velocity, while balancing speed with rigor in execution, as directed by the Acquisition Transformation Strategy. To effectively identify and manage technical risks in acquisitions, a complete and thorough knowledge of the SE domain is needed to analyze and take measured and calculated risks during acquisition.

The goal of SE modernization is to create a more agile, data-driven process that empowers decision makers with timely, actionable insights. By leveraging digital tools, fostering collaboration, and embracing innovation, the Department can accelerate the delivery of adaptable, mission-ready systems that meet the evolving needs of the warfighter.

The Acquisition Transformation Strategy states, “this [systems engineering] transformation is critical, given rapid modernization of technology and the increased use of software acquisition, advanced computing, artificial intelligence, and model-based acquisition.” When applied effectively, these tools can help reduce design defects and manage risks and issues early and throughout the program. This update to the SE Guidebook provides a flexible framework programs can use to deliver on these expectations.

This SE Guidebook is intended to serve as a living resource and will be reviewed on a regular basis (at least annually) to ensure accuracy and relevance. Updates will be issued as necessary to reflect new information, changes in policy, or evolving best practices. Systems engineers across the DoW are encouraged to submit recommendations for improvements and provide feedback to ensure the guidebook remains a valuable and effective tool.

The table below lists important topics identified in the Acquisition Transformation Strategy and the locations in the SE Guidebook where they are addressed. Additional detailed guidance for these topics is located on the Systems Engineering and Architecture (SE&A) website library page (<https://www.cto.mil/sea/pg>).

Acquisition Transformation Strategy Topics in SE Guidebook

Acquisition Transformation Strategy Topic	SE Guidebook Updated Section Location
Agile Development/Iterative Development	1.4 SE Processes, 1.6 Systems Engineering Approach, 3.6 Software Engineering, 3.6 Modular Open Systems Approach, 3.7 SE in Agile
Application Programming Interfaces	3.6 Software Engineering
Digital Engineering	3.2 Modeling and Simulation, 3.3 Digital Engineering, 4 Engineering Resources, 5 Technical Reviews, 6.1 Technical Planning Process, 6.17 Technical Data Management Process
Manufacturing & Manufacturing Risk Management	1.6 Systems Engineering Approach, 3.8 SE in Agile, 5.4 System Requirements Review, 5.6 Preliminary Design Review, 5.7 Critical Design Review, 5.9 Production Readiness Review, 5.10 Physical Configuration Audit, 6.1.5 Risk Management, 6.1.7 Technical Data Management, 7.14 Manufacturing and Quality
Manufacturing Readiness Assessments	5.9 Production Readiness Reviews, 7.14 Manufacturing and Quality
Mission Engineering	1.4 Systems Engineering Processes, 3.5 Mission Engineering, 3.8.2 Agile Development and SE
Model-Based Systems Engineering	1.3 Development Planning, 2 System-Level Considerations, 3.3 Digital Engineering, 3.4 Model-Based Systems Engineering, 4 Engineering Resources
Modeling and Simulation	3.2 Models and Simulations, 3.3 Digital Engineering
Modular Open Systems Approach	1.6 Systems Engineering Plan, 3.6 Software Engineering, 3.7 Modular Open Systems Approach, 3.7.2 Agile Development and SE, 5.6 Preliminary Design Review, 5.7 Critical Design Review, 6.1.7 Technical Data Management Process, 6.1.8 Interface Management Process, 6.2.3 Architecture Design Process, 6.2.4 Implementation Process, 7.15 Modular Design
Software Engineering	3.6 Software Engineering
Technology Insertion	1.6 Systems Engineering Plan, 3.8 SE in Agile Development, 6.1.1 Technical Planning Process, 6.1.8 Interface Management Process, 7.4 Commercial-Off-the-Shelf, 7.8 Diminishing Manufacturing Sources and Material Shortages, 7.11 Intelligence
Technology Readiness Assessments	6.1.3 Technical Assessment Process, Technology Readiness Assessments
Value Engineering	4.3 Value Engineering

1 INTRODUCTION

The SE Guidebook provides guidance and recommended best practices for DoW acquisition programs. The DoW Office of the Under Secretary of War (OUSW) for Research and Engineering (R&E), Office of SE&A, prepared this guidebook in cooperation with subject matter experts (SMEs) from the Military Services,¹ Defense Agencies, industry, and academia.

This guidebook is intended for DoW program managers (PMs), systems engineers, and all disciplines related to system development and may be tailored for programs in any of the DoW AAF pathways. DoD Instruction (DoDI) 5000.02 describes the six AAF pathways that serve as examples of defense program structures tailored to the type of product being acquired or to the need for accelerated acquisition. See the Engineering of Defense Systems Guidebook (2022) for more information on these pathways and the expected application for each pathway, highlighting the relevant SE and other engineering activities. Programs can use this guidebook, along with other acquisition business resources, to plan and execute program SE activities across the system life cycle.²

1.1 Purpose of Systems Engineering

SE establishes the technical framework for delivering materiel capabilities to the warfighter. Systems engineering uniquely connects program management and warfighters with specialty component teams during a system's development. It does this by allocating requirements, tasking, and testing to ensure the final components work together to achieve all program and mission goals. It provides the foundation upon which a program builds its detailed technical and management processes.

SE seeks to ensure the effective development and delivery of capability through a balanced approach to cost, schedule, and performance through risk management. Cost, schedule, and performance are the key program attributes tracked as part of program management and are captured in the Acquisition Program Baseline (APB). The APB, an agreement between the PM and Milestone Decision Authority (MDA)/Decision Authority (DA), serves as the basis for program reporting.

SE promotes using integrated, disciplined, and consistent activities and processes regardless of when a program enters the acquisition life cycle. SE enables the development of resilient systems that are trusted, assured, and easily modified. This is increasingly accomplished through integrated digital engineering approaches that use digital models and their underlying data as specified in DoDI 5000.97, "Digital Engineering." Government Accountability Office (GAO)

¹ In this document, the term "Service" implies "Military Service."

² "Systems engineering" has countless interpretations and definitions across Government, academia, and industry, but the information in this guide focuses on the DoW's application of systems engineering to acquisition.

report “Detailed Systems Engineering Prior to Product Development Positions Programs for Success” (GAO-17-77) emphasized the value, stating:

Systems engineering is the primary means for determining whether and how the challenge posed by a program’s requirements can be met with available resources. It is a disciplined learning process that translates capability requirements into specific design features and thus identifies key risks to be resolved. Our prior best practices work has indicated that if programs apply detailed SE before the start of product development, the program can resolve these risks through trade-offs and additional investments, ensuring that risks have been sufficiently retired or that they are clearly understood and adequately resourced if they are being carried forward.

SE planning, as described in a program’s SE approach, identifies the technical path for delivering a capability. SE event-driven technical reviews and audits assess program maturity and determine the status of the technical risks associated with cost, schedule, and performance goals. The SE approach and program planning should account for funding stability. Multi-year assured funding profiles and mission-area resource allocations are required to minimize annual re-baselining, reduce schedule delays, and ensure continuity of workforce and materiel procurement.

In addition, SE:

- Supports development of realistic and achievable program performance, schedule, and cost goals as documented in the program requirements documents, APB, and Acquisition Strategy (AS), or similar acquisition planning artifacts dependent on the acquisition pathway.
- Provides the end-to-end, integrated perspective of the technical activities and processes across the system life cycle, including how the system fits into a larger system-of-systems (SoS) construct.
- Emphasizes the use of integrated, consistent, and repeatable processes to reduce risk while maturing and managing the technical baseline³ (functional, allocated, and product—Sections 5.5, 5.6, and 5.7). The final product baseline (Section 5.10) forms the basis for production, sustainment, future changes, and upgrades.
- Provides insight into system life cycle resource requirements and impacts on human health and the environment.

³ Technical baselines include the *functional baseline*, *allocated baseline*, and *product baseline*. Each of the technical baselines is a reference from which to measure progress of the system development.

This guidebook uses the following terms:

- “Systems engineer” refers to the chief engineer, lead engineer, program lead systems engineer, or the engineering staff responsible for SE processes, including the planning, conduct, or management of SE activities and the incorporation of design considerations throughout the program life cycle.
- “Software engineer” refers to the lead software engineer who is responsible for overseeing SWE and development efforts, and the planning, management, and conduct of activities that require special software expertise. The software engineer works in conjunction with the PM and lead systems engineer to manage SWE and development activities throughout the program life cycle.
- “End user” includes the warfighter and other operational users, including support personnel, maintainers, and trainers who use or support the system.
- “Developer” refers to the system prime contractor and associated subcontractors or the agency, organization, or entity responsible for designing and building the system.
- “Design considerations” are concepts that should be accommodated or applied to each program or system throughout the SE life cycle and assessed when making trade-offs. Some design considerations include constraints, boundaries, or limitations, with values that can sometimes be tailored or negotiated within mission constraints.

1.2 Definition of Systems Engineering

SE is a methodical and disciplined approach for the specification, design, development, realization, technical management, operations, and retirement of a system (see Warfighting Acquisition University (WarU) Glossary (<https://waru.edu/glossary>) for this and additional definitions). This is increasingly achieved using digital models and authoritative data sources, enabling digital continuity across all life cycle phases. As illustrated in Figure 1-1, a system is an aggregation of system elements and enabling system elements to achieve a given purpose or provide a needed capability. The enabling system elements provide the means for delivering a capability into service, keeping it in service, or ending its service, and may include those processes or products necessary for developing, producing, testing, deploying, and sustaining the system.

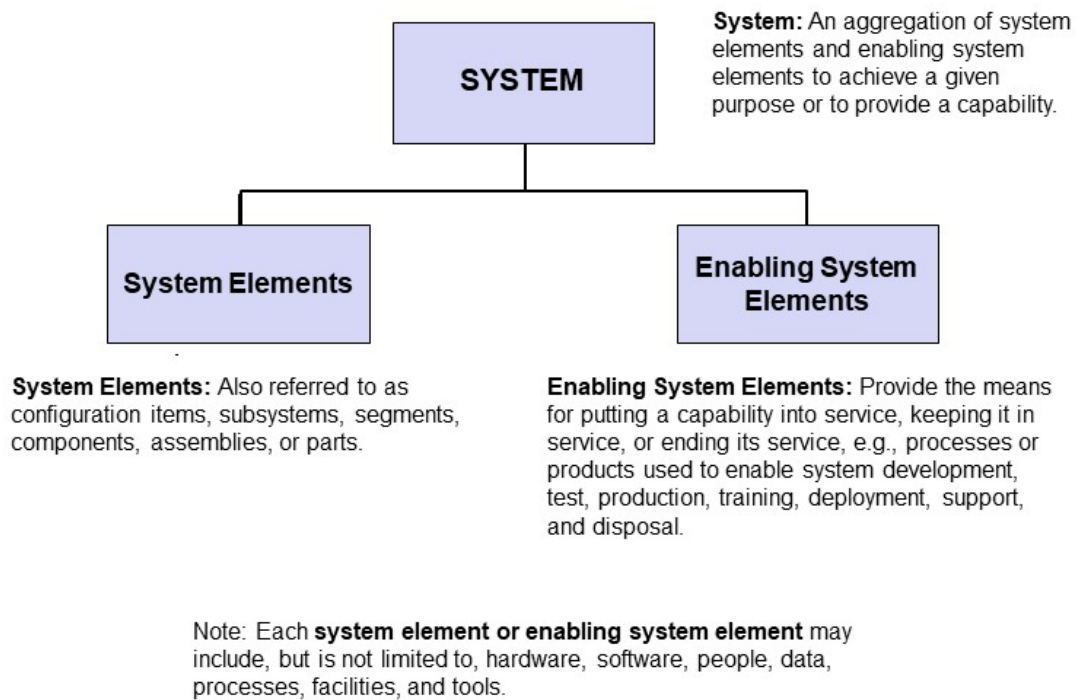


Figure 1-1. The System

SE applies critical thinking to the acquisition of a capability. It is a holistic, integrative discipline, whereby the contributions from other engineering disciplines (e.g., structural engineers, electrical engineers, mechanical designers, software engineers, safety engineers, human factors engineers, reliability engineers) and other fields associated with development, employment, and retirement of systems (e.g., logistics) are evaluated and balanced to produce a coherent capability – the system.

The systems engineer balances the conflicting design constraints of cost, schedule, and performance while maintaining an acceptable level of risk. SE solves systems acquisition problems using a multidisciplined approach. The systems engineer should possess the knowledge, skills, and critical thinking ability to identify and focus efforts on the activities needed to enhance the overall system effectiveness, suitability, survivability, and sustainability.

1.3 Development Planning

SE activities, including design considerations, begin before a program is officially established and are applied throughout the acquisition life cycle. Any effective SE approach should support and be integrated with sound program management. Before the program begins, the PM, or Service lead if no PM has been assigned, should perform development planning to lay the technical foundation for successful acquisition.

To build a robust, adaptable, and modern SE program, using DE methodologies, technologies, and practices is crucial throughout the life cycle of defense acquisition programs, system, and SoS. Successfully implementing DE requires upfront planning to identify and allocate the necessary financial and other resources for digital methods like model-based systems engineering (MBSE), computer-aided design, and digital twins.⁴ DE needs to be addressed in the initial AS, including how and when DE will be used in the system life cycle and expected benefits of its use.

Development planning encompasses the engineering analyses and technical planning activities that provide the foundation for informed investment decisions prior to initiating a formal acquisition program. Development planning addresses the current and evolving capability gap(s), desired operational attributes, and associated dependencies of the desired capability. In addition, development planning seeks to ensure a range of technically feasible solutions exist from across the entire solution space and that the program has considered near-term opportunities to provide a rapid interim response to the capability need.⁵ The PM initiates development planning in advance of a Materiel Development Decision (MDD) review and transfers the knowledge (documents, tools, and related data) to the designated program.

1.4 Systems Engineering Processes

DoW SE includes 16 processes: 8 Technical Processes and 8 Technical Management Processes, as illustrated in Figure 1-2 and described in Section 6. These 16 processes provide a structured approach to increasing the technical maturity of a system and increasing the likelihood that the capability will balance mission performance with cost, schedule, risk, and design constraints.

The eight Technical Processes include design and realization processes that the program employs to transform operational needs into operational capabilities. A program implements the eight Technical Management Processes across the acquisition life cycle to assist the PM, systems engineer, and software engineer to meet performance, schedule, and cost goals.

⁴ As defined in DoDI 5000.97, a digital twin is a computerized representation (integrated set of models) that serves as the real-time digital counterpart of a physical object or process.

⁵ Programs should evaluate Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) technologies to identify candidate solutions that address key technical risks or requirements gaps.

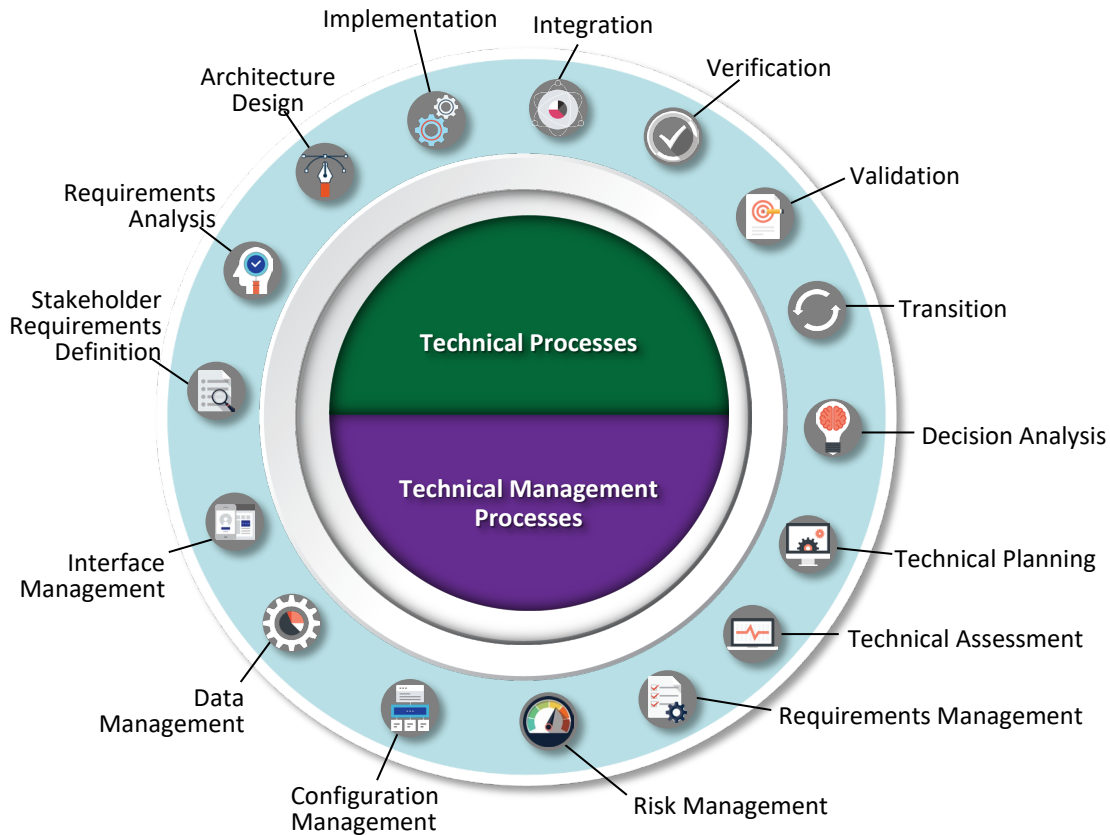


Figure 1-2. SE Processes

The SE processes provide a framework for the program to structure and conduct its technical efforts efficiently to deliver a capability that satisfies a validated operational need. A program implements the SE Technical Processes in an integrated and overlapping manner to support the iterative maturation of the system solution.

The program starts by identifying an operational need as shown in the top left corner of the V-Diagram (Figure 1-3). The SE team uses the Technical Processes to ensure the delivered capability accurately reflects the operational needs of the stakeholders. The Technical Processes include the following major activities:

- During the Stakeholder Requirements Definition process, the SE team translates operational requirements from relevant stakeholders into a set of top-level technical requirements. The SE team decomposes the requirements during the Requirements Analysis process to produce a complete set of system functional and performance requirements. These top-level requirements should leverage flexible solution attributes, where possible, to free up trade space for industry to propose innovative solutions.

- During the Architecture Design process, the SE team, often through system modeling, trade-offs, and decision analyses, captures the functional requirements and interdependencies in the system architecture. Trade-offs and analyses are also used to mature and realize the design of the system and system elements during the Implementation process, generating the product baseline.
- During the Integration process, the program assembles the system elements to provide the system for testing in the Verification process (developmental tests verifying the functional requirements) and Validation process (operational tests validating the system meets the operational need), resulting in a validated solution.
- During the Transition process, the program formally delivers the system capability to the end users, including all enabling system elements to support operational use and sustainment activities.

The Technical Management Processes, depicted in Figure 1-3, provide a consistent approach to managing the program's technical activities and controlling information and events that are critical to the success of the program.

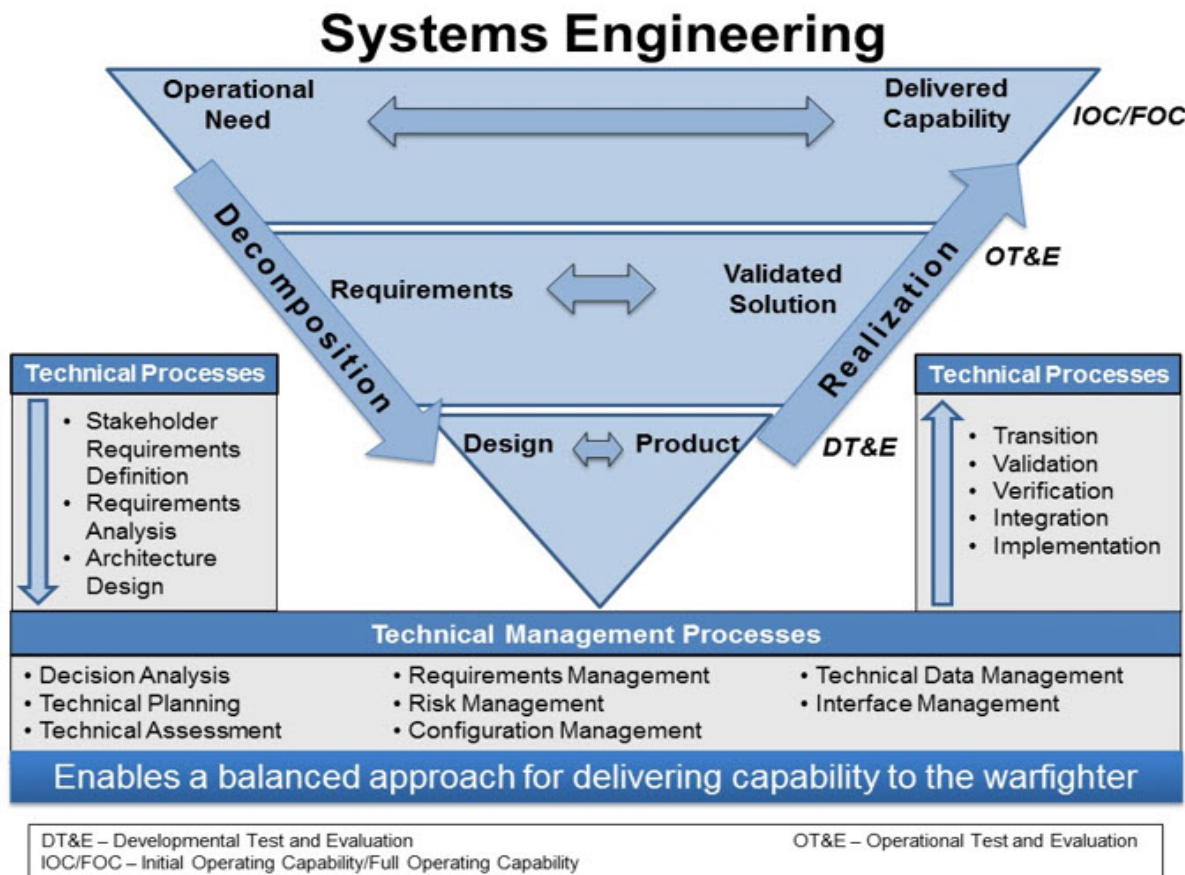


Figure 1-3. SE Processes in the V Diagram

It is essential to recognize that SE is an iterative process. As the program progresses through each stage, new information and insights are gained, and it is common for requirements to evolve, designs to be refined, and testing to reveal areas for improvement. To accommodate this iterative nature, the SE team should adopt an agile and incremental approach to development, allowing for continuous refinement and adaptation of the system design and requirements. This may involve revisiting earlier stages of the V-Diagram, such as revising requirements or re-evaluating design trade-offs, based on lessons learned during later stages, such as testing and validation. By embracing this iterative approach, the program can respond more rapidly to changing stakeholder needs, reduce technical risk, and deliver a system that meets the operational needs of the end users. The Technical Management Processes should be flexible and adaptable to support this iterative approach, enabling the SE team to make informed decisions and adjust the development trajectory as needed to ensure the delivery of an effective system.

ISO/IEC/IEEE 15288 (2023) identifies four process groups for the system life cycle, providing “a common process framework for describing the life cycle of engineered systems, adopting a System Engineering approach”: (1) Organizational Project-Enabling Process, (2) Technical Management Processes, (3) Technical Processes, and (4) Agreement Processes. In modern DoW SE, the system life cycle processes are intended to be applied concurrently, iteratively, and recursively throughout the stages of the life cycle. International Council on Systems Engineering (INCOSE) created a graphical overview of these processes. Figure 1-4 depicts the processes being applied in the more modern, iterative, and recursive manner.

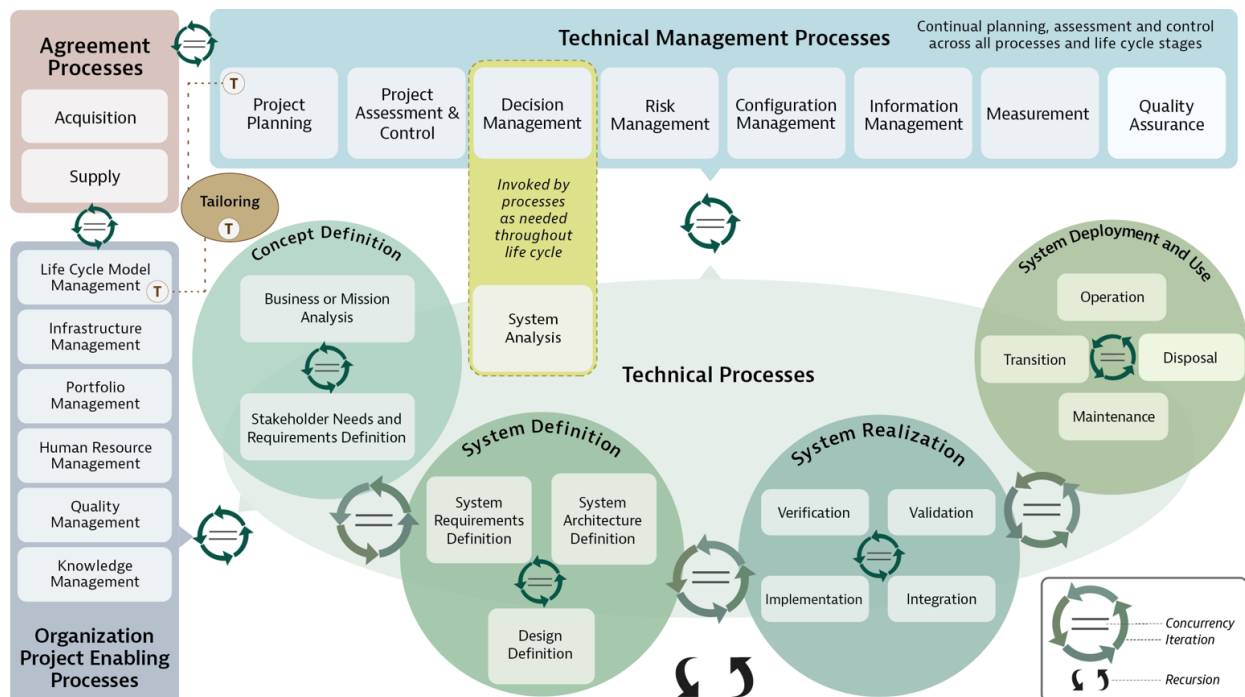


Figure created by Garry Roedler and Dave Walden for INCOSE. This figure appears in the SE Handbook, Fifth Edition, © 2023 Wiley and Sons, Publishers.

Figure 1-4. System Life Cycle Process

All organizations performing SE should scale their application of the processes, further described in Section 6, to reflect the unique needs of the program and the type of product or system being developed. This scaling should reflect the system’s maturity and complexity, size and scope, AAF pathway, life cycle phase, and other relevant considerations. For example, lower risk, less-complex programs may scale the processes to ensure SE activities are effective but not overly cumbersome (e.g., simpler and less-expensive tools, less-frequent reporting, and activities adjusted to fit smaller organizations with fewer personnel). Most successful programs spend about 15 percent of their approved budget on SE activities (Honour 2010; INCOSE SE Handbook 2023). In addition, to align with industry best practices, the SE activities should use modeling and simulation to the greatest extent that is cost-effective.

1.5 Systems Engineering Policy and Guidance

DoW SE policy and guidance are intended to reduce the burden and cost on programs while maintaining technical integrity through the planning and execution of SE activities across the acquisition life cycle. PMs, systems engineers, and software engineers should know and understand the statutory and regulatory SE mandates. Table 1-1 identifies top-level SE-related policy.

Table 1-1. SE-Related Policy

SE-Related Policy	Source
DoD Directive 5000.01, The Defense Acquisition System	Office of the Under Secretary of Defense (OUSD) for Acquisition and Sustainment (A&S), July 28, 2022
DoD Directive 5137.02, Under Secretary of Defense for Research and Engineering (USD(R&E))	Office of the Department of Defense (DoD) Chief Management Officer, July 15, 2020
DoW Instruction 5000.02, Operation of the Adaptive Acquisition Framework	OUSW(A&S), April 8, 2026
DoD Instruction 5000.88, Engineering of Defense Systems	OUSD(R&E), November 18, 2020
DoD Instruction 5000.97, Digital Engineering	OUSD(R&E), December 21, 2023

Additional SE-related policy and guidance are provided on the SE&A and AAF websites.

SE-related policy, guidance, specifications, and standards are intended to successfully guide the technical planning and execution of a program across the acquisition life cycle. Understanding the use and value of SE specifications and standards is fundamental to establishing, executing, and maintaining disciplined SE processes. The ASSIST tool (<https://assist.dla.mil>) serves as DoW’s official source for standardization documents it develops, maintains, and uses. With numerous specifications and standards related to SE, it is important for programs to spend adequate resources reviewing those that apply to their program.

DoW policy and guidance provide a framework for structuring the program and help define the areas available for tailoring to effectively and efficiently deliver capability to the warfighter. Programs tailor the acquisition effort to meet program cost, schedule, and performance goals in accordance with DoD Instruction 5000.88. Every program has its own optimal structure, and that structure is dependent on many variables that contribute to program success or failure. In accordance with applicable laws and regulations, programs should tailor their specific plans based on the product being acquired, the selected AAF pathway, complexity, acquisition category, risk factors, and required timelines to satisfy validated capability requirements. For example, programs should consider tailoring the following areas:

- Documentation of program information
- Acquisition Strategy
- Timing and scope of decision reviews
- Decision approval levels

The PM identifies the areas of policy to tailor and submits this plan to the MDA/DA for approval.

Program structuring should start with a deep understanding of the nature of the capability intended to be acquired and the effort needed to realize that capability. Programs must identify the internal and external stakeholders, system interdependencies, technological opportunities, contractual and budgetary constraints, and policy mandates. The optimal program structure includes the set of technical activities, events, and management mechanisms that best address the unique circumstances and risks of the program.

All program acquisition strategies and planning documents depend on SE activities to define and balance requirements against cost, schedule, and risks; identify potential solutions; assess the maturity and feasibility of available technologies; develop a realistic schedule; and allow for multiple other considerations affecting the final cost and delivery of capability to the warfighter. Therefore, the PM should build a program office structure that ensures the systems engineer is an integrated part of the program planning and execution activities.

The systems engineer leads in the planning and execution of the program's technical approach. To aid this planning, the systems engineer should proactively seek experience from similar past and current programs and map this learning as applicable into the SE planning of the program (see Section 4.5, Lessons Learned, Best Practices, Case Studies).

1.6 Systems Engineering Approach

Regardless of acquisition pathway, PMs should develop an SE approach for their programs. This approach should be captured within the program's digital ecosystem but may be contained in a traditional Systems Engineering Plan (SEP) document or a combination of both. The PM can tailor an SE approach to meet program-unique needs, allowing agile and innovative development of joint capability requirements to address the joint operational problems (see DoD SEP Outline 4.1, May 2023).

The purpose of the SE approach is to guide PMs in the development, communication, and management of the overall SE approach and technical activities of the program. The SE approach describes technical risks, performance evolution strategy (including use of MOSA to the maximum extent practicable), processes, resources, metrics, SE products, organizations, design considerations, DE activities, and completed and scheduled SE activities. The SE approach, captured in the digital ecosystem, should be updated as needed to reflect the program's evolving SE approach or plans and current status.

The SE approach should be tailored with approval by the approval authority. DoDI 5000.88 requires the lead systems engineer, under the direction of the PM, to prepare the SE approach to guide the SE activities on the program. PMs should use the SEP Outline to guide preparation of the SE approach. The SEP Outline identifies the recommended content to be addressed. The SE approach should be consistent with and complementary to the APB, AS, Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP), Life Cycle Sustainment Plan (LCSP), and other program plans as appropriate, or as required by the acquisition pathway. The SE approach or SEP should be written in plain language to clearly communicate plans for each phase of the acquisition pathway and life cycle and should be written to avoid redundancy and maintain consistency with other planning documents (see DoDI 5025.13, "DoD Plain Language Program," for additional information).

The PM should formally charter an SE Working-Level Integrated Product Team (WIPT), led by the systems engineer, to assist in developing and monitoring SE activities as described in the program SE approach. Approval of the SE approach will be in accordance with DoDI 5000.88. As a best practice, SE approach updates should be approved by the Portfolio Acquisition Executive (PAE) or direct reporting portfolio manager in advance of each technical review and when the program changes in a way that has an impact on the technical strategy. The PM may approve other periodic updates to the SE approach.

The SE approach describes the integration of SE activities with other program management and control efforts, including the Integrated Master Plan (IMP), Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), Risk Management Plan, Technical Performance Measures (TPMs), and other documentation fundamental to successful program execution. The SE approach also describes the program's technical requirements, engineering resources and

management, and technical activities and products as well as the planning, timing, conduct, and success criteria of event-driven SE technical reviews throughout the acquisition life cycle.

PMs should include the SE approach (either an approved or a draft) in the Request for Proposal (RFP) to the offerors as either guidance or as a compliance document depending on the maturity of the plan and the AS.

Before providing the SE approach or SEP to the offerors, the PM, systems engineer, and software engineer should determine whether the document contains sensitive information and, if so, remove this sensitive information from the SE approach before attaching it to the RFP. The developer's Systems Engineering Management Plan (SEMP), which is the contractor-developed plan for the conduct, management, and control of the integrated engineering effort, should be consistent with the Government SE approach to ensure that Government and contractor technical plans are aligned. The SEMP should define the contractor technical planning and how it is accomplished from the contractor perspective, and articulate details of their processes, tools, and organization.

As the program's blueprint for the conduct, management, and control of all technical activities, the SE approach captures decisions made during the technical planning process and communicates objectives and guidance to program personnel and other stakeholders. The SE approach should define the "who, what, when, why, and how." For example:

- The program organization with roles and responsibilities, authority, accountability, and staffing resources. This includes the coordination of the program's Integrated Product Teams (IPTs) and their products, resources, staffing, management metrics, and integration mechanisms.
- The activities, resources, tools, and events that support execution of the SE Technical Processes and Technical Management Processes (see Section 6, Systems Engineering Processes) to deliver a balanced solution to meet the warfighter's needs. It should identify unique processes, tools, or tailoring of specifications and standards, how these processes and tools are integrated, and how products are developed and managed. For instance, the SEP should document or summarize and reference the documents providing the description of the program's risk management approach and the status of top-level technical risk, issues, and opportunities (RIOs), including risk mitigation and handling activities. As a best practice, the RIOs should be collected monthly and reported to senior leadership stakeholders at least quarterly (see Section 6.1.5, Risk Management Process).
- The event-driven technical review approach based on successful completion of activities as opposed to calendar-based deadlines. The SE approach should document the plans for conducting each technical review with particular emphasis on the entry and exit criteria and details of the SE technical reviews planned in the program's next acquisition phase. The SE approach should identify the timing of SE events in relation to other program events and knowledge points, and it should describe how technical activities are

integrated in the program's overall plan and schedule. The SE approach should include the assumptions made in developing the schedule and the process for conducting schedule risk assessments (SRAs) and updates. SE approaches submitted to the approval authority should include a current schedule, with all appropriate technical reviews, no more than 3 months old.

- The plan and description of how the system employs a modular design to enable benefits, such as technology insertion and refresh (see Section 7.15, Modular Design).
- The plan and description of how manufacturing planning and quality planning will be incorporated into the SE Plan and SE processes.
- The prototyping strategy, as defined in the AS or SE approach, that ensures the system requirements (including Key System Attributes (KSAs)) are achievable within cost and schedule constraints.
- The description of the architecture products that will be developed as part of the organization's Enterprise Architecture (EA) to better describe and understand the system, including internal and external interfaces. As a best practice, to ensure architectures are properly formulated, the SE approach should include a description of mission thread⁶ analysis completed to support materiel development and the mapping between interoperability and interface specifications.
- The approach for how requirements and technical performance trade-offs are balanced within the larger program scope to deliver operationally effective, suitable, survivable, and affordable systems. Design considerations and criteria (see Section 7) should be listed in the mandatory tables, with all the associated documentation provided with each SE approach submission.
- The program's strategy for identifying, prioritizing, and selecting the set of TPMs and metrics (TPMMs), as documented in the SE approach, should provide sufficient insight into the technical progress and program risks, and each measure or metric should have threshold, margin, and contingency values.
 - The values should measure achievement over time and should be reported at every major program event.
 - The measures and metrics should be specific, measurable, achievable, relevant, and time bound.
 - As a best practice, the measures and metrics should be collected monthly and reported to senior leadership stakeholders at least quarterly. If the program is developed within a DE ecosystem, stakeholders can access program data and review metrics at will throughout the program's life cycle.

⁶ As defined in the Mission Engineering Guide (2023), a mission thread is a sequence of end-to-end mission tasks, activities, and events presented as a series of steps to achieve a mission.

- The following TPMMs should be considered for inclusion:
 - Risk Management
 - Schedule Risk
 - Operational Resilience
 - Cyber Survivability
 - Number of Class 1 Engineering Change Proposals (ECPs)
 - Number of Class 2 ECPs.
- The program should ensure that each Critical Technical Parameter (CTP) has a corresponding TPM (see also Section 6.1.3, Technical Assessment Process; DoD SEP Outline Version 4.1).

2 SYSTEM-LEVEL CONSIDERATIONS

A system should not be acquired in isolation from other systems with which it associates in the operational environment. The PM, systems engineer, and software engineer should understand (1) how the system fills the needs for which it was designed, (2) the design considerations (Section 7) needed to deliver the capability, and (3) the enterprise context within which it operates. Whether the system functions as a stand-alone system or as part of a Family of Systems (FoS)/SoS, systems engineers should examine the Concept of Operations (CONOPS)/Operational Mode Summary/Mission Profile (OMS/MP), and applicable requirements document(s) for dependencies and interfaces. These documents should adequately describe the interactions between the proposed system and the associated FoS/SoS dependencies/interfaces. This includes understanding the diverse or dissimilar mix of other systems (hardware, software, and human) with which the system needs to exchange information.

To that end, the PM, systems engineer, and software engineer should define intersystem interfaces using Interface Control Documents⁷ or MBSE equivalents. In addition, they should pursue a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with companion programs regarding interfaces, data exchanges, and advance notice of change interdependencies and schedule (timing) that may affect either program. These agreements are a means of mitigating the inherent risk in planning to deliver a capability to an anticipated future technical baseline when there is uncertainty that the other programs will be able to maintain schedule and have adequate resources to deploy the capabilities as planned. The agreements should indicate responsible organizations for all interactions requiring cost allocation (e.g., training, facilities, and staffing).

2.1 SoS as Enterprise Systems

SE is recognized as key to addressing the evolution of complex SoS. SE principles and tools are used to apply systems thinking and engineering to the enterprise levels. An enterprise in this usage is understood to be the organization or cross-organizational entity supporting a defined business scope and mission, and includes the interdependent resources (people, organizations, and technology) to coordinate functions and share information in support of a common mission or set of related missions (see System of Systems Engineering Guidebook 2026).

DoW Services and Agencies, and the Department itself, are examples of enterprises as systems. Such organizations have the challenge of integrating and developing multiple portfolios of systems, often with conflicting sets of objectives, constraints, stakeholders, and demands for resources.

⁷ The Interface Control Document provides a record of all interface information generated for the project. It is essential for managing both internal and external interfaces and ensuring compliance with the configuration management process.

The systems engineer should be cognizant of the enterprise context and constraints for the system in development and should factor these enterprise considerations into acquisition technical decisions from the outset. For all systems, the systems engineer should assess the interdependence and integration of all design considerations and should ensure that all design considerations are addressed at the enterprise level. Mission areas, for example, can be viewed as cross-organizational enterprise systems in the SoS architecture system design.

In some cases, enterprise considerations have been articulated as standards, reference architectures, and certification requirements. In other cases, to ensure that delivered capability is reliable, maintainable, and supportable, system decisions need to be made in the context of the larger enterprise portfolio of systems and mission area needs as defined in the organization-wide enterprise architecture. In accordance with the Secretary of War (SecWar) memorandum “Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities” (November 2025), mission areas should be managed with oversight from the Mission Engineering and Integration Activity (MEIA), which integrates mission analyses, experimentation campaigns, and industry engagement. National teams of contractors, with rotating leadership, serve as the technical integration body for mission capabilities, reducing stovepipes and ensuring rapid subcontracting. Government oversight should focus on mission outcomes rather than subsystem micromanagement.

2.2 Applying Systems Engineering in SoS

An SoS is a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers its own unique set of capabilities that none of the constituent systems can deliver on its own. The collection of systems combines resources and capabilities to create a new, more complex system that offers more functionality and performance than simply the sum of the constituent systems.

For complex SoS, the interdependencies that exist or are developed between or among the individual systems being integrated need to be tracked. Each SoS may consist of varying technologies that matured decades apart and were designed for different purposes but are now used to meet new objectives that may not have been defined at the time the systems were deployed.

The SE community is paying increased attention to issues of SoS, complex systems, and enterprise systems. Perspectives vary on the nature of these types of systems and their implications for SE, and research in this area is ongoing. For additional information on SoS, see the DoD System of Systems Engineering Guidebook (2026).

3 SYSTEMS ENGINEERING MODERNIZATION

SE modernization shifts traditional, document-heavy engineering to a digital, agile, and model-based approach. DoW initiated SE modernization to implement the digital transformation in systems engineering technical reviews and process flows that support the acquisition decision process. The goal of SE modernization is to leverage authoritative data sources across the life cycle to increase speed, reduce costs, and improve adaptability to new threats using tools, techniques, and approaches described in the following subsections.

3.1 Systems Engineering Tools and Techniques Overview

SE data, tools, and techniques, including modeling and simulation, support the performance of activities, the development of products, and the completion of specific tasks. SE tools and techniques support the PM, systems engineer, software engineer, and technical management team in performing and managing the SE activities and processes to improve productivity and system cost, schedule, capabilities, and adaptability. The PM, systems engineer, and software engineer should begin applying SE tools and techniques during the early stages of program definition to improve efficiency and traceability and to provide a technical framework for managing the system development. Identifying and resolving risks early in development is much less costly than resolving issues later in the life cycle.

Collaboration and analytical tools should be integrated directly into the digital engineering ecosystem. Rather than simply exchanging static data files or documents, these tools should connect to the descriptive system model via a digital thread. This ensures that analyses (e.g., performance, reliability, cost) are always performed on the current design baseline and that all stakeholders are collaborating on a single, shared source of truth. It is critical that the systems engineer understand the constraints and limitations of any particular analysis tool or technique and apply this understanding when making assessments or recommendations based on its output.

Before selecting and implementing an SE tool or technique, the systems engineer should consider:

- Needs and constraints of the program (e.g., complexity, size, and funding)
- Applicability to required tasks and desired products
- Computer system requirements, including peripheral equipment
- Licensing and maintenance costs
- Technical data management (see Section 6.1.7)
- Integration with the digital ecosystem and other SE tools in use within the program, by the developer, and by externally interfacing programs
- Cost to train the user to apply the tool or technique

- Number and level of expertise of Government and contractor staff (both users of the tool and users of the tool outputs)
- Feasibility of implementing the tool or technique throughout the acquisition life cycle

All programs, regardless of AAF pathway, should clearly (1) identify tools in use (documented in the SE approach), (2) define tool interfaces when the Government and developer select different tools to use for the same purpose, and (3) describe how the tools support the program's SE approach.

Table 3-1 lists general features of the SE processes. When implementing a digital engineering approach, programs should seek to acquire an integrated suite of tools that are interoperable and centered on the descriptive system model, rather than procuring a separate, disconnected point solution for each process area.

Table 3-1. SE Process-Related Tools

Systems Engineering Process	Tool Capabilities/Features
Technical Planning	• Assists in planning and scheduling activities • Assists in resource planning, tracking, and allocation • Facilitates cost estimation
Decision Analysis	• Assists in trade-off analysis • Provides optimization and sensitivity analysis capability • Assists in recording, tracking, evaluating, and reporting decision outcomes
Technical Assessment	• Assists in tracking, measuring, and assessing metrics • Assists in metric collection
Requirements Management	• Provides requirements bi-directional traceability capability • Provides requirements flow-down capability • Tracks requirements changes
Risk Management	• Assists in risk, issue, and opportunity planning, identification, analysis, mitigation/management, and monitoring
Configuration Management	• Assists in the identification of configuration items • Assists in baseline/version control of all configuration items • Assists in ensuring configuration baselines and changes are identified, recorded, evaluated, approved, incorporated, and verified
Technical Data Management	• Assists in identification of data requirements • Assists in recording and managing data rights • Assists in storage, maintenance, control, use and exchange of data including digital artifacts • Assists in document preparation, update, and analysis

Systems Engineering Process	Tool Capabilities/Features
Interface Management	- Assists in capturing system internal and external interfaces and their requirement specifications - Assists in assessing compliance of interfaces among system elements of the system or SoS - Produces a view of interface connectivity
Stakeholder Requirements Definition	- Assists in capturing and identifying stakeholder requirements - Assists in analyzing and maintaining stakeholder requirements
Requirements Analysis	- Assists in requirements definition and decomposition - Interfaces with architecting tools - Supports requirements validation
Architecture Design	- Assists in development of functional and physical architectures - Provides traceability among system elements - Supports multiple views
Implementation	- Assists in development of the system design, prototypes and alternate solutions - Assists in realization of the system, system elements and enabling system elements
Integration	- Assists in integration-planning activities - Assists in assembling lower-level system elements into successively higher-level system elements - Provides analysis and simulation capability
Verification	Assists in determining the performance of the system and system elements, as designed, through demonstration, examination, analysis, and test
Validation	Assists in determining the effectiveness, suitability, and survivability of the system in meeting end-user needs
Transition	Assists in planning and executing delivery and deploying of the system to the end user for use in the operational environment

Automated Tools

A DE ecosystem (e.g., Golden Forge, Platform One) includes the infrastructure and architecture necessary to support automated approaches for system development, design, testing, evaluation, production, operation, training, and sustainment throughout the defense acquisition process. Automated tools, such as those for requirements management, risk management, schedule management, and architecture development, within the DE ecosystem, should be used by the PM, systems engineer, and software engineer to accelerate engineering activities and reduce the time to develop and field systems. Planning to use these tools should include identifying specialized skills to develop the products, and training in how to access and use the information or digital artifacts within the tools and the DE ecosystem. Additional information on planning

for, selection and interoperability of, and training on the use of automated tools within a DE ecosystem, can be found in MIL-HDBK 539, Digital Engineering and Modeling Practices.

3.2 Models and Simulations

Models and simulations are the cornerstone of modern SE. Models, simulations, data, and other artifacts should be developed and used in a well-defined and controlled engineering ecosystem to support an effort's reuse of the information across the life cycle of activities. Models, simulations, data, and artifacts should be integrated, managed, and controlled so the products remain consistent with the system and external dependencies. They should provide a comprehensive view of the effort and increase efficiency and confidence throughout the project's life span.

Models, simulations, distributed simulations, and associated data used to support DoW processes, products, and decisions should undergo verification and validation (V&V) throughout their life cycles and should be accredited for their specific intended use. The fidelity of the verification, validation, and accreditation (VV&A) (see DoDI 5000.61, "DoD Modeling and Simulation Verification, Validation, and Accreditation") should be balanced with the importance, risk, and impacts of using model or simulation results to inform DoW and DoW Component processes, products, procedures, or decision making. VV&A of models should be flexible, tailorable, and adaptable to meet requirements, objectives, and the specific intended use.

The WarU Glossary defines a model as a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. Within an MBSE approach, this is formalized as an integrated descriptive system model. This model serves as the Authoritative Source of Truth (ASoT), providing a robust machine-readable database of the system's requirements, structure, behavior, and parametric relationships, from which various views, analyses, and documents are generated.

A simulation is defined as a method for executing a model over time. To ensure precision and interoperability, models should be created using standard, non-proprietary languages, such as Systems Modeling Language (SysML™). For architectural views, the Department of Defense Architecture Framework (DoDAF) and Unified Architecture Framework (UAF®) provide a standardized way to represent complex architectures and mission threads, ensuring alignment across system-of-systems. Simulation has the following benefits:

- Provides results that can predict the behavior of modeled entities under specific conditions.
- Affords a means to explore concepts and system characteristics.
- Opens up the trade space.
- Facilitates informed decision-making.

- Supports training.
- Enables study of the stochastic interactions among different entities (systems, individuals, and the environment) in the battlespace whereas static models do not.

Models and simulations are key digital tools used to make informed, data-driven decisions throughout all DoW activities. The results of models and simulations form a digital record of the effort's activities, phases, and baseline information in decision making.

Roles, Responsibilities, and Activities

The model and simulation support to any effort should be planned and should be:

- Scoped to the purpose and objective of the effort based on user expectations and stated outcomes.
- Appropriate to the context (e.g., application domain, life cycle phase).
- Complete, comprehensive, and trusted, by including all efforts anticipated throughout the life cycle, including planning, development, and acceptance as well as verification, validation, and accreditation (see DoDI 5000.61, "DoD Modeling and Simulation Verification, Validation, and Accreditation").
- Designed to drive technical planning, with the system model being used to inform the WBS, IMS, and risk management activities.
- Appropriately resourced, including a properly skilled workforce.
- Within agreement or contractual requirements.
- Established and managed under configuration control as the ASoT for the evolving technical baseline.
- Supported by regular reviews and management of artifacts and stakeholders' changing needs.
- Based on appropriate digital artifacts that are consistent, interoperable, accessible, uncorrupted, and properly and securely stored.

The systems engineer should ensure that the effort's modeling and simulation activities are coordinated, managed, and controlled such that products are consistent with the architecture and design at all levels.

Models and simulations should be:

- Developed and matured through the life of the effort.
- Documented, including metadata, widely supported and consensus-based standards (if available and suitable) and model assumptions to maximize opportunity for reuse and repurposing.
- Properly managed and controlled as part of the ASoT.
- Included as part of the technical data package (TDP) to be transitioned into the next phase of the life cycle or into other efforts.

Models, data, and artifacts should be evident in the contents of any technical reviews and in the baselined technical data needed to support other decisions.

3.3 Digital Engineering

DE, as codified in DoDI 5000.97 and guided by MIL-HDBK-539 and the Digital Engineering Body of Knowledge (de-bok.org), is the DoW's initiative to transform the way it conceives, designs, develops, delivers, operates, and sustains complex systems in a formidable and changing threat environment. The DoD Digital Engineering Strategy (2018) defines DE as "integrated digital approach using authoritative sources of system data and models as a continuum across disciplines to support life cycle activities from concept through disposal." DE implementation depends on common digital standards that establish semantic meaning across tools and data. Controlled vocabularies, ontologies, and machine-interpretable models provide the foundation for interoperability, enabling automated validation, trusted digital threads, and consistent reasoning across the life cycle, in alignment with DoDI 5000.97.

This approach creates a trusted digital thread by establishing explicit, machine-readable relationships across the entire system model. For example, using a standard language like SysML, an operational requirement can be formally traced to system functions, which are in turn allocated to physical components whose behaviors and interfaces are also defined in the model. Frameworks like the UAF extend this capability by providing a common ontology to link capability and operational views with system and service views, providing end-to-end traceability from mission objectives down to implementation details. This ensures that the "semantic meaning" is not only established but actively maintained and verifiable throughout the life cycle.

Across the full life cycle of both emerging and legacy systems, DE tools and techniques afford improved ways of developing, acquiring, and sustaining capabilities across a program's full life cycle (Figure 3-1). The overall goal is to harness the power of digital computing to move DoW programs away from traditional, monolithic, paper-driven processes to use more virtual artifacts, greater automation of processes, and fewer manual transactions. The primary means of achieving this transformation from paper-driven processes to integrated digital artifacts is through the practice of MBSE, which is further detailed in Section 3.4. The DoW embraces digital engineering across the project life cycle to bring improved capabilities to the warfighter in a timelier and more iterative manner. For additional information, see the SE&A DEM&S website.

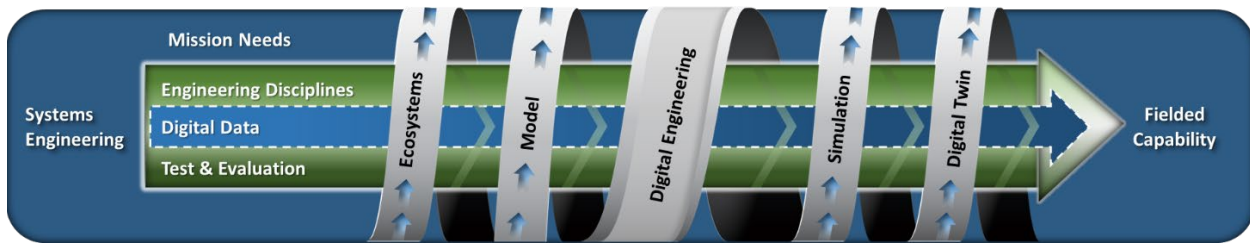


Figure 3-1. Digital Engineering throughout System Development

3.4 Model-Based Systems Engineering

As one of the enabling components of DE, MBSE is the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities associated with the development of complex systems. It begins with the concept stage and continues throughout development and later life cycle stages. The practice of modern SE is enabled by an integrated digital ecosystem. At the core of this ecosystem is a data-centric, descriptive system model that serves as the ASoT for the program. This model, often developed using standard languages like SysML and UAF, is the primary enabler from which activities like requirements analysis, design, simulation, and verification are performed and their results are managed.

MBSE is a multifaceted endeavor and enhances the ability to capture, analyze, share and manage product information. A robust MBSE approach delivers significant, measurable benefits to a program, including:

- **Improved Communication:** Provides unambiguous, precise views of the system tailored to different stakeholders (e.g., warfighters, testers, leadership), reducing misunderstandings.
- **Enhanced Product Quality:** Enables early and continuous verification and validation by integrating requirements with the design and analysis, identifying defects when they are cheapest to fix.
- **Reduced Cycle Time:** Aids in the generation of documentation and reports for technical reviews, dramatically reducing manual effort.

- **Improved Risk Management:** Provides a holistic view of the system, making it easier to assess the system-level impact of proposed changes and identify integration risks.
- **Enhanced Knowledge Capture:** Creates a persistent, integrated asset that captures design decisions and rationale, which is invaluable for managing the system through its entire life cycle, including sustainment and technology refresh.

For more information, see MIL-HDBK-539.

3.5 Mission Engineering

Section 855 of the FY 2017 National Defense Authorization Act (NDAA) directed the Secretary of Defense to develop “mission integration management” to use mission-based information to inform concept, technology, requirements, and systems development. Acting on this direction, the OUSW(R&E) established an ME directorate to develop the Department’s infrastructure, procedures, and guidance on how to conduct analyses to generate and integrate mission information for use during investment decisions.

ME is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects. Through ME, DoW practitioners use mission-based, threat-informed results to better inform the decisions and “roadmaps” of Joint Warfighting Concept development, technology, prototyping, requirements setting, acquisition portfolios, and the budgeting process. ME is most effectively executed using an MBSE approach that is aligned with the DoDAF or UAF. These architectures allow practitioners to model operational activities, mission threads, capability gaps, and the systems that support them in an integrated fashion, directly aligning with the goals of ME.

ME studies and analyses provide a quantifiable basis to inform technical and budgetary decisions on potential solutions to fulfill mission capability gaps. The solutions address Joint Forces Requirements Council (JFRC)-identified Key Operational Problems (KOPs), resourced by the Requirements and Resourcing Alignment Board (RRAB) and validated through MEIA experimentation campaigns to align mission concepts, system requirements, technologies, and budgets. ME studies and analyses evaluate capability solutions, enhanced capabilities, technologies, system interdependencies, and architectures. They also inform the acquisition and operational communities with reference architectures to guide technology development, prototypes, experiments, and SoS portfolio management to achieve reference missions and meet warfighter needs.

ME outputs should include validated ME threads, reference architectures, and experiment-based risk assessments that are incorporated into the SE approach and acquisition strategies. ME provides a framework for conducting systems and SoS engineering in an operational mission context to inform stakeholders on “building the right things, not just building things right.” The outputs of ME analyses include data on mission measures of effectiveness and performance,

examples of successful mission threads and architectures, and potential trades that can be made in an SoS context to achieve mission success.

These processes conform to the SecWar memorandum “Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities” (November 2025) for acquisition reform. The DoD Mission Engineering Guide (2023) establishes best practices for conducting mission-focused, threat-informed analyses. These practices enable DoW practitioners to prioritize and pursue materiel and non-materiel solutions to critical warfighting challenges.

3.6 Software Engineering

Software is critical to national security, an integral part of every DoW weapon system, and vital to future battlefield dominance. Software has become ubiquitous and increasingly significant to every warfighting system. Software is a key element in all advanced warfighting cyber physical weapon systems and a driver of system performance, capability, security, functionality, complexity, and risk.

The purpose of SWE is to influence the processes for software and system architecture, design, and development and to increase the rate of newly fielded mission capabilities to the warfighter. Properly planned SWE processes can mitigate cost and schedule risks by allowing DoW programs to identify and remove software-related technical debt early in development. This early action can increase acquisition efficiency and lead to higher success rates during operational testing and during operations and sustainment.

Software development never ends. The Department has embraced this phrase and recognizes that SWE processes that mimic hardware development/waterfall acquisition processes take too long to mature, accumulate technical debt and risk, and do not apply to software. DevSecOps is an organizational SWE culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops).

By adopting commercial best practices, such as Agile/DevSecOps software development, with modern tool stacks and skilled personnel, the Department can work to begin delivering new software capabilities to the warfighter rapidly and incrementally, rather than monolithically only after months or years of development. Such findings have resulted in valuable changes in public law, acquisition policy, and workforce development. The most significant acquisition policy change in the DoW was the establishment of the AAF and DoDI 5000.87, “Operation of the Software Acquisition Pathway.” The DoW established the AAF and policy in accordance with the requirements of Section 800 of Public Law 116-92 (NDAA for FY 2020) requiring the timely delivery of secure software. The policy advocates the use of streamlined processes, elimination of low- to no-value regulatory documentation, and establishment of a DevSecOps software factory with continuous integration and continuous delivery (CI/CD) pipelines as the preferred approach in the DoW for software development and sustainment.

Recent rapid advances in commercial sector SWE skills and technology, and modern software development practices including the Agile/DevSecOps for automation, pipelines, tools, metrics, and CI/CD have proven successful in a competitive industrial marketplace and should be adopted in the DoW. To adopt commercial best practices and advances, Program Management Offices (PMOs) should use the DoDI 5000.87 for software acquisition, establish enterprise-wide cloud native solutions and tool sets with their PAE and Service leads whenever practicable, modernize workforce competencies, and establish a culture that unifies previous “siloed” activities such as development, safety, security, test, and sustainment into a CI/CD process.

DevSecOps is the Department’s preferred approach for software development, and adopting DevSecOps is the primary focus area for delivering secure resilient code. Figure 3-2 shows the DevSecOps continuous software development process with security embedded (not bolted on) throughout the process. Advancing cyber survivability in DoW DevSecOps pipelines should be part of all DoW SWE team processes, which will also enable the ability to execute a continuous Authority to Operate process. Refer to the DoD Enterprise DevSecOps Fundamentals guidebook (2024) for more information.

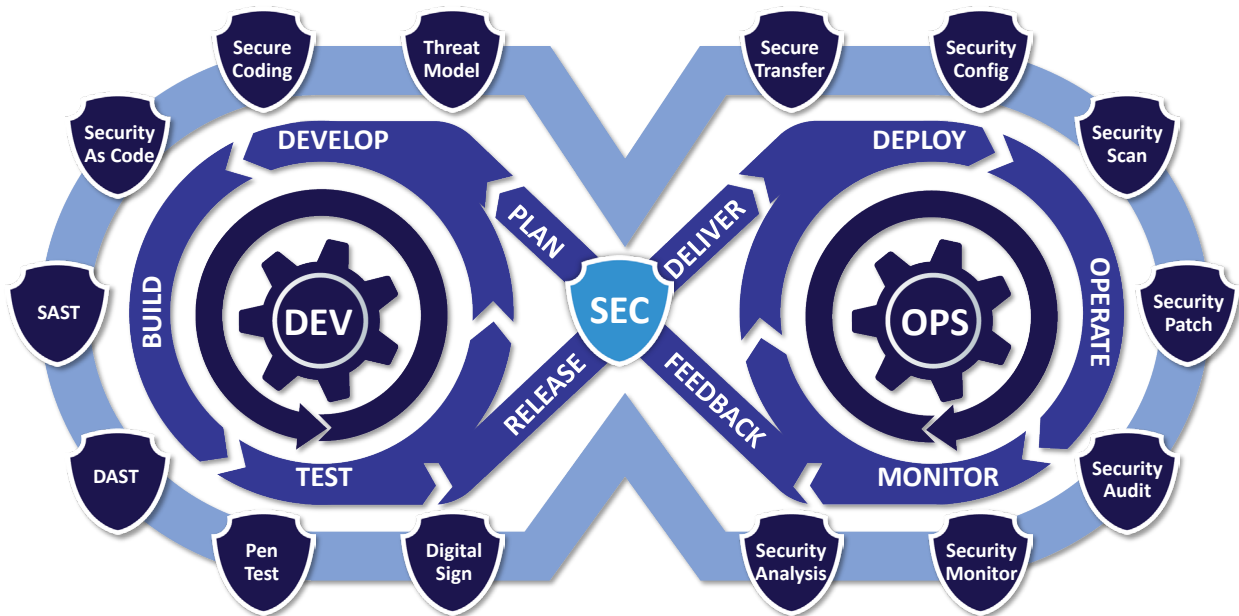


Figure 3-2. DoW DevSecOps Process for Continuous Integration/Continuous Delivery

Specific Software Engineering Program Recommendations

The PM should understand and emphasize the following:

- Maintain consistent awareness of software’s contribution to the overall program and system risks and manage those aspects of the program. More information on software considerations in RIO management are in the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (2023).

- Use early prototyping in software and exploration of alternative implementations for solution viability and overall risk reduction.
- Set aside 5 to 20 percent of software developer capacity per sprint for technical debt reduction and unplanned work. Programs should organize sprints around the delivery of configurable items or capability increments that can be independently integrated, tested, and verified, enabling early validation of end-to-end performance.
- Integrate SWE into the SE processes:
 - Plan for and integrate SWE activities within SE processes and acquisition documents, particularly for system-level technical reviews and technical baselines.
 - Integrate SWE design analysis, test, and demonstrations within SE processes.
- Commit to measurement: use predictive software metrics and quantitative analysis techniques to support data-driven decisions at every level.
- Continuously evaluate and update software schedule estimates:
 - Substantiate software schedule realism with a rigorous basis of estimate.
 - Continuously evaluate the viability and degree of optimism in software schedules and how they relate to sprint in an agile velocity.
- Measure and document software maturity and readiness for test and evaluation (T&E) and users (e.g., defects, stability).
- Rigorously manage software requirements:
 - Integrate software considerations into system requirements and design.
 - Ensure software requirements are captured in user stories, traceable, allocated to iterations, and assessed for dependencies to meet iteration goals for capability and test.
 - Manage cascading/deferred requirements and mitigate development concurrency.
 - Ensure there is a complete “definition of done” and acceptance criteria for each user story in a sprint before beginning work.
- Adopt CI/CD and automated testing:
 - Measure and incrementally deliver end-to-end performance and capabilities.
 - Verify and validate capabilities, including prototypes, through early, incremental user demonstrations and tests in high-fidelity environments.
 - Use software development environments that enable continuous builds and automated test.
- Continuously assess sufficiency of software staffing quantity/experience within the PMO/Contractor Program Office.

- Continuously assess agile maturity of the software team and ensure the roles of the team are well defined.
- Ensure user involvement in software development through user agreements.
- Ensure adequate planning and resources for modern tools, infrastructure, software testing, and quality assurance.
- Understand how agile teams operate and interact accordingly.
- Provide the future team with access to software tools, the software factory, and software environment as the program transitions from one contract to another.

The systems engineer, in coordination with the software engineer, should ensure that the technical planning and the SE approach address:

- Software-unique risks, issues, and opportunities.
- Software architecture integration with the system architecture.
- Inclusion of software in technical reviews.
- Software technical performance, process, progress, and quality metrics, especially those associated with end-to-end performance and capability delivery.
- Software safety, security, and protection, including associated software processes, architecture, and interfacing systems.
- Management of technical debt, specifically the problem/change reporting process, process for maintaining the system backlog, and role of the Government in the Problem Reporting and Deficiency Reporting processes.
- Management of software obsolescence.
- Configuration management (CM) for software integration facilities and laboratories; V&V and development tools.
- Software technology and infrastructure such as cloud, common operating environments (COEs), and MOSA; associated data rights; and sustainment considerations.
- Independent verification and validation (IV&V) if practical, especially for contractor-proprietary software.
- Verification of documentation, CM, test relevancy, and other considerations for reuse of legacy software as well as new software.
- How SE requirements and system design flow down into SWE and how SWE feedback informs system requirements and design.
- Any intellectual property concerns with the software acquisition.

- Future team access to software tools and environment as the program transitions from one contract to another or from one acquisition phase to another.

Additional information, including DoW guidance for SWE and application programming interface (API), can be found in the Application Programming Interface Technical Guidance and on the SWE portion of the SE&A website (<https://www.cto.mil/sea>). Additional SWE guidance for each of the acquisition pathways can be found in the Engineering of Defense Systems Guidebook (2022).

3.7 Modular Open Systems Approach

MOSA is an integrated business and technical strategy to help reduce development time, cost, and variation. MOSA promotes using common, reusable hardware and software components that can be adapted and refreshed more readily than traditional components. MOSA is required for all defense acquisition pursuant to 10 USC 4401, 4402, and 4403 and in accordance with USW(A&S) policy memorandum “Establishment of Department-Wide MOSA Policy and Minimum Expectations” (MOSA memorandum).

The DoW uses MOSA as an acquisition and design strategy, consisting of technical architectures, that uses open standards where suitable, or efficient translators, adapters, mappings, and other objective integration approaches when interfaces differ. This supports a modular, loosely coupled, and highly cohesive system structure. MOSA allows the Department to deploy and support the latest technologies and to affordably and competitively acquire and sustain systems across the defense acquisition life cycle. MOSA supports acquisition and sustainment of new or legacy systems, or components within systems, over the entire system engineering life cycle. It includes contracting mechanisms, legal considerations, and prioritizing data rights and intellectual property. This enables a more rapid evolution of capabilities and technologies. MOSA is intended to minimize the impact of unique interface designs, improve interoperability, maximize the use of commercial components, and improve the capacity for future technical upgrades.

In accordance with the MOSA memorandum, programs use MOSA to create practical options to add, replace, reuse, and/or compete modules by exposing selected interfaces with the documentation, data rights, repository access, and objective verification an authorized third-party needs to integrate without prime-contractor coordination. PMs, subject to portfolio PAEs direction, characterize the desired modularity of their programs. A government reference architecture, standard, or profile may be used to implement MOSA. In all cases, MOSA is accomplished at selected boundaries by delivering the as-implemented interface package, securing interface rights, and proving independent integration. For additional MOSA information, see the OUSW(R&E) SE&A website (<https://www.cto.mil/sea>).

3.8 Systems Engineering in Agile Development

3.8.1 Overview

The Department is embracing an agile development approach for acquisition of defense systems to enable shorter development cycles, faster and more frequent technology insertion, and better technology and manufacturing risk management. This shift to agile approaches will reduce the traditional, often rigid, approaches and introduce a more flexible iterative approach. The Department seeks to evolve beyond compliance-driven processes toward commercial-grade agility similar to industry's "test, fly, fail, fix" approach, empowering companies to iterate rapidly while the Government monitors outcomes through digital evidence and realized results, and planning is adjusted based on learning throughout iterations.

Implementing agile system development and modified SE, particularly for major weapon system development, requires a skilled workforce to execute a higher risk and faster paced approach. Agile system development should emphasize frequent collaboration among stakeholders, including the program manager, systems engineers, developer, and the warfighter (end user). Ideally, most stakeholders will be involved in program activities on a day-to-day basis to improve communication and reduce misunderstandings. Stakeholders should be involved in iterative technical reviews to ensure alignment on requirements and priorities. Recommended phases and technical reviews are discussed below.

3.8.2 Agile Development and Systems Engineering

In agile system development, requirements do not need to be finalized before prototyping begins. An initial set of capability-based requirements is satisfactory for SE teams to begin prototyping and testing to discover the limits on capabilities and where challenges exist. Agile implementation accepts evolving requirements as a strength, not a weakness. Early prototyping begins with capability-based needs and evolves as data emerges from tests and operational feedback. This approach values development within a rapid campaign of learning rather than a checklist-focused path toward milestones.

To achieve design, development, integration, and test in an iterative manner, the program should maximize use of tools and techniques such as modeling and simulation, hardware in the loop, and system integration lab environments early in the process. Establishing a digital ecosystem, implementing a MOSA, and relying heavily on MBSE are vital for effective and efficient implementation of agile system development. Programs should also use modeling languages such as SysML and align to the DoDAF or UAF.

One approach to agile SE is to implement a planning phase and an execution phase. The planning phase is used to set general expectations for iterative development. The execution phase is where the repetitive increments are executed to develop the evolving capability.

Programs should use a planning phase to understand the warfighter’s mission needs and should develop a plan to deliver the capabilities into the operational environment in a rapid and iterative fashion. Every acquisition is different, so programs must carefully tailor their iterative approach to account for the complex variables that affect program development. To reduce the chance of iteration failures or extensive delays, engineers should balance the technical aggressiveness planned for each iteration with acceptable risk. This includes carefully examining not only Technology Readiness Levels (TRLs) (see TRA Guidebook 2025) of individual components but also the potential for substantial integration challenges. Programs may choose to break development into smaller, manageable increments (less technical aggressiveness per increment) that can deliver minimum viable products or prototypes that demonstrate key capabilities (those that impact operational effectiveness and mission success). The authoritative digital system model should be the primary source for defining and managing the program increments.

The purpose of an execution phase is to leverage the understanding of the warfighters’ mission needs and mature the strategies, roadmap, and other artifacts developed during the planning phase to rapidly and iteratively “test, fly, fail, fix” capabilities that meet the warfighter priorities and mission needs. Five artifacts, or tailored equivalents, should be considered to transition to the execution phase: a Capability Need Statement, an AS, an SE approach, or equivalent, a test strategy (e.g., TEMP), and a cost estimate. For an iterative approach to be effective, these artifacts must be thoroughly integrated and consistent.

As illustrated in Figure 3-3, execution can occur with potentially simultaneous ongoing prototyping activities providing opportunities for SE teams to explore multiple avenues for technology development. Sharing results between development teams taking different approaches or assessing different technologies and methodologies can provide a more robust and rapid development process.

In iterative development, engineering teams could start with incremental prototyping in which components and subsystems can be matured with iterative repeatable development and testing while gauging progress against a current set of requirements. With discovery of capabilities in this manner, programs can adjust and refine requirements, if appropriate, as the capability matures. Engineers performing early rapid prototyping may identify technical challenges that will be extremely difficult to overcome and may require additional resources and time. This allows the engineers to determine early in development where the risks and challenges are in achieving required capabilities and to provide off-ramps in the event the capability is not achievable at this point in time.

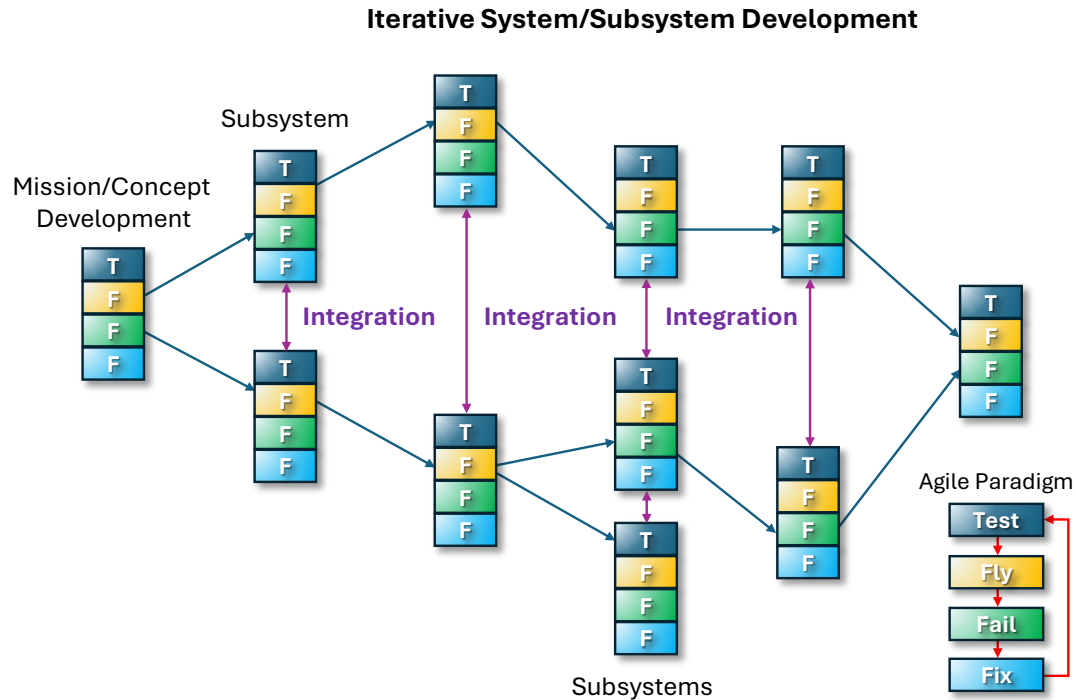


Figure 3-3. Notional Multiple Agile Subsystem Iterations

Continuous integration across subsystems enables simultaneous discovery and risk reduction. Each subsystem may be matured at its own pace, guided by integrated digital dashboards. Programs should track iteration metrics—risk burn-down, throughput, and learning velocity—to monitor effectiveness rather than milestone completion.

Given the nature of the iterative process, programs can insert modernized technology throughout. Requirements and design can be adjusted with technology insertion, and another iteration can proceed. Each subsystem potentially could have its own iterative development cycles, ultimately progressing to integration activities. With these subsystems at various stages of maturity, systems engineers need to carefully manage these staggered development and test cycles.

Through fast-paced agile development, the program will likely accumulate technical debt, and the program must treat and manage this debt closely as a risk to the program. Programs should address challenging capabilities early in the process to minimize technical risk and identify feasibility issues.

Principles to Facilitate Agile SE

The following list summarizes principles that programs should implement when developing defense systems in an agile environment:

- **Rapid iteration:** Build prototypes quickly, test them in real-world conditions, and embrace early, significant failures as learning opportunities.

- **Data-driven improvements:** Analyze test information quickly. Each test, whether a success or failure, generates critical data. Faster analysis and action of data allows engineers to implement improvements and insert technology more rapidly than traditional methods.
- **Sprint cycles:** Apply software development principles, such as frequent sprint cycles, to hardware projects. This ensures consistent development rhythm, creates fast feedback loops, and increases accountability.
- **Cross-functional teams:** Organize teams around products, not specialized functions, breaking down traditional departmental silos. This enables direct, immediate collaboration among diverse experts, including electrical, mechanical, materials, and manufacturing engineers, for example.
- **Daily stand-up meetings:** Conduct short, focused meetings to keep team members aligned, address obstacles quickly, and promote better coordination across complex systems.

Mission Engineering and Agile SE

ME results, preferably captured as digital artifacts, feed this agile process, allowing for a more dynamic adjustment of requirements and design based on input of existing military capabilities and evolving adversary capabilities. This coordination between mission engineers and systems engineers ensures that SE activities remain aligned with operational needs. For KOPs, as set out in the SecWar memorandum “Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities” (November 2025), the MEIA should provide inputs to capability planning through the RRAB. MEIA engages with industry and Services to identify potential solutions.

3.8.3 Continuous Agile Review and Learning

Modifying the traditional technical review and audit process to fit agile iterative development is essential to modernizing SE for weapon system acquisition programs. Agile reviews should be continuous, data-driven assessments integrated with each sprint cycle rather than milestone-based gates. They should inform learning, not just approval, and should provide ongoing visibility to both developers and Government monitors.

Technical reviews should fit the agile workflows for the specific acquisition. Each traditional SE review has a distinct purpose. By carefully planning the conduct of technical reviews, program offices can still meet the intent of each SE technical review, while customizing those reviews to fit the flexibility and adaptability of agile methodologies. Programs should streamline reviews to be much less formal than traditional technical reviews, and should cover topics pertinent to the specific iteration activities (Figure 3-4). These reviews assess progress and validate requirements, designs, and tests iteratively.

3. Systems Engineering Modernization

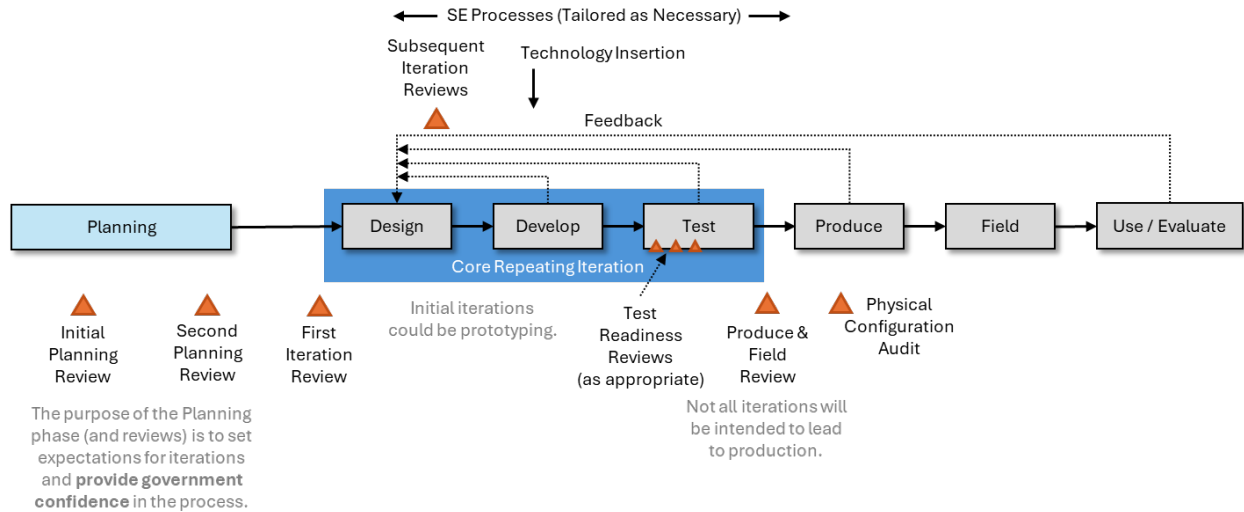


Figure 3-4. Generic Agile Iteration

Agile development requires continuous V&V throughout the life cycle, and therefore programs should conduct these V&V activities in each sprint or iteration. Programs should use automated testing tools and frameworks to continuously verify system functionality and performance. This automation allows for continuous review, feedback, and validation throughout the development life cycle and reduces the risk of late-stage issues by addressing development incrementally.

Where possible, programs should implement digital engineering tools and automated reporting to support agile technical reviews (including the potential to support real or near real-time reporting). Digital engineering tools, MBSE models, and digital twins form the authoritative evidence base (source of truth) for reviews. Automated dashboards, reports, and simulations replace static, extensive documentation, allowing near-real-time assessment of maturity and readiness.

Failure serves as feedback. Agile reviews capture learning from test failures. Programs should treat early failure data as critical feedback loops that reduce long-term risk. Programs must measure learning velocity—the time between test discovery and design adjustment—and use it as a performance indicator.

Agile development typically includes five types of review: planning review, sprint/iteration review, quarterly integration review, vertical integration review, and production review (Table 3-2).

Table 3-2. Agile Technical Reviews Description

Review Type	Purpose	Cadence	Key Evidence
Planning Review	Set Government and contractor expectations for iterative development	Before beginning iterations	High-level requirements, Acquisition Strategy, SE approach
Sprint/Iteration Review	Validate iteration objectives, assess learning outcomes	Every 2–4 weeks	MBSE deltas, test data, user feedback
Quarterly Integration Review	Evaluate subsystem maturity and integration risk	Quarterly	Simulation dashboards, digital twin data
Vertical Integration Review	Evaluate coordination of phases of development	6 Months	Learning Velocity Index (LVI), risk burn-down, iteration throughput, Failure Utilization Ratio (FUR), Mean Time from Test to Decision (MTTD)
Production Review	Confirm manufacturability and sustainment readiness	As triggered	Digital twin validation, supplier data

Planning Review

In the initial planning phase, planning reviews should align with the AS and provide a roadmap for capability development. This alignment allows the Government and developer to set overall technical strategy expectations (e.g., how iterations will progress, development environment and methods, review and reporting requirements). The planning phase must provide the Government with trust in the iteration process that will follow. These should be substantial reviews and can contain elements of the traditional Alternative Systems Review (ASR), System Requirements Review (SRR), System Functional Review (SFR), and Preliminary Design Review (PDR).

Sprint/Iteration Review

During Sprint or Iteration Reviews, programs identify and review requirements, design, and functions to be delivered in the specific iteration. This will include exit criteria and whether there are plans to produce and deliver a capability after the iteration. These reviews should also describe specific developmental and operational testing (verification and validation) requirements, including plans for user engagement and feedback. Iteration reviews will provide specific details on the general plans covered in the planning reviews.

Quarterly Integration Review

This review focuses on the integration of all subsystems both in terms of their technical and temporal compatibility. First and foremost, is to review the day-to-day products from iterative reviews for models that reflect the behavior of the system as verified from actual testing. Here the focus is on the interfaces between subsystems to find potential risks. This is not an extensive dive into interfaces but a review of existing indicators by more objective members of the team (leadership) across the system.

Evidence that would be assessed includes simulations and digital twin data:

- Simulations – These reflect the behavior of the system and subsystems and are a part of continuous evaluation from the sprints or iterations. Results are reviewed by more senior members of the team to identify potential risks for both technical integration and timing of subsystem development.
- Digital twin data – Mimics the actual behavior of the system or subsystem as verified by test data. This data is much more detailed than the simulation and breaks down the behavior of each subsystem in a more granular form. Senior team members review this data looking for detailed interface issues like the incompatible use of the same standards.

Vertical Integration Review

Agile hardware programs should periodically assess the proximity among design, manufacturing, and testing. By ensuring these functions work closely together, teams can identify and solve problems early, enabling faster iteration and higher product quality. Engineering and production teams should collaborate directly or via digital surrogates to shorten problem-resolution cycles.

Agile reviews should rely on quantitative, automated metrics that measure iteration performance. Key metrics include:

- *Learning Velocity Index (LVI)* – time from test completion to design improvement
- *Risk Burn-Down Rate* – risk reduction per iteration
- *Iteration Throughput* – validated features per sprint
- *Velocity* – amount of work done per iteration
- *Burndown* – visualization of the amount of work remaining in an iteration, PI, or release
- *Cycle Time* – total elapsed time for a work item to move from “in progress” to “done”
- *Failure Utilization Ratio (FUR)* – percent of failures leading to design change
- *Mean Time from Test to Decision (MTTD)* – lag between data availability and decision

Digital dashboards should display these metrics live to both Government and industry stakeholders.

Each subsequent iteration review will consider results from the previous iteration (e.g., previous iteration plans deferred to later iterations), feedback from production activities, and evaluations from users.

Production Review

If the iteration calls for production to commence, the production review will determine if the results of the iteration confirm production can begin. In iterative development, the evidence up to this point should provide developers and users with capability value information and whether there is value in moving forward with production and fielding. It may also point to a decision to

end the effort when capability is not maturing adequately (learn quickly and fail fast if necessary). Production teams should be working throughout the iteration to identify potential production issues that may be separate from the demonstrated functional capability (i.e., it works, but we may not be able to produce it). Production reviews can contain traditional System Verification Review (SVR), Functional Configuration Audit (FCA), and Production Readiness Review (PRR) elements.

Before large-scale production and fielding, this review should contain a Physical Configuration Audit that ensures the as-built system matches the design documentation and meets all configuration requirements. A failed configuration audit can stop fielding. Programs should examine production samples early and regularly to prevent fielding issues.

Agile SE reviews become continuous learning checkpoints rather than bureaucratic gates. Using model-based artifacts, data-driven evidence, and a monitoring posture, the Department can achieve commercial-grade agility with retained engineering discipline. By embracing an industry-like culture of iterative testing, data-driven improvement, and vertical integration, agile development redefines how defense hardware can evolve at commercial speed. The Government remains the steward of risk and alignment—but the engine of innovation lies within empowered, learning-driven industry teams.

4 ENGINEERING RESOURCES, ENABLERS, AND LESSONS LEARNED

Organizing and staffing the SE organization and providing supporting resources and tools are critical tasks that merit attention from the PM, systems engineer, and software engineer because these tasks influence the effective implementation and control of the SE approach. The PM is responsible for developing a tailored strategy that enables a cost-effective program to deliver a required capability within the needed delivery time.

Program tailoring should include SE assessments of maturity and risk in order to determine the appropriate entry point into the acquisition life cycle and to identify opportunities to streamline the acquisition strategy. Therefore, the PM should create a program office structure ensuring the systems engineer and software engineer are an integrated part of the program planning and execution activities. This planning includes ensuring that program offices for Major Defense Acquisition Programs (MDAPs) will have a qualified chief engineer/lead systems engineer with key leadership position criteria defined in DoDI 5000.66, “Defense Acquisition Workforce Education, Training, Experience, and Career Development Program.”

Building an integrated SE team with the expertise and knowledge to implement and execute an effective program is a key to success. Providing the SE team with the necessary SE tools and techniques to perform and manage SE activities and processes will increase productivity of the organization, reduce system cost and schedule, and improve capabilities and adaptability. The structure and size of the SE organization should reflect both the risk and complexity of the system under development and its life cycle phase. The SE approach should describe the SE organizations of both the Government program office and, when available, the developer organization.

4.1 Roles and Responsibilities

To provide the required capabilities in the most efficient and effective manner, the PM should ensure completion of the following activities that affect the technical approach:

- Establishing program office organization (roles, responsibilities, authorities, accountabilities) and staffing the program office and Government technical team with qualified (trained and experienced) systems engineers and other relevant technical professionals.
- Ensuring coordinated development, update, and execution of AS documents, program plans (e.g., SEP, PPP (including the Cybersecurity Strategy (CSS)), TEMP, LCSP), and cost and budget documents.
- Interfacing with the end users and developers to determine changes in operational requirements or CONOPS that may affect the development of the desired capability.
- Integrating all aspects of the program office, including business processes relating to program management, SE, test, and program control, to include a program IMS.

- Ensuring all necessary MOA/MOUs with external organizations/program offices (e.g., for SoS) are in place and sufficiently detailed.
- Resourcing the managers of all functional areas, such as administration, engineering, logistics, test, etc.
- Managing program risks and opportunities by developing, resourcing, and implementing realistic mitigation and management strategies.
- Approving the CM plan and ensuring adequate resources are allocated for implementing CM throughout the life cycle.
- Reviewing/approving ECP requests in coordination with the SE team, and determining the path forward required by any baseline changes.
- Ensuring contracting activities are coordinated with the program SE team.
- In coordination with the SE team, approving the contractor SEMP; ensuring consistency between the program SEP, or equivalent, and SEMP.

The systems engineer is responsible for planning and overseeing all technical activity within the program office and for managing effective SE processes. The systems engineer should ensure the PM has sufficient and clear information for scheduling and resource-allocation decisions. In addition, the systems engineer implements and controls the technical effort by:

- Implementing and maintaining disciplined SE processes.
- Understanding the nature of the system under development, the needs of the end user, and the operating environment as described in the CONOPS.
- Implementing a DE and MBSE approach as early as concept development, carried through design, development, production, fielding, and sustainment, including digital artifacts, digital twins, models and simulations, etc., to support life cycle activities, as appropriate.
- Conducting activities in support of contract award and execution.
- Ensuring that no unauthorized changes or commitments are made with the contractor or developer.
- Understanding how the system fits into a larger SoS context, and coordinating so the requisite mission analysis efforts are undertaken.
- Providing recommendations on the contract strategy.⁸

⁸ Using SBIR/STTR programs to accelerate the discovery, maturation, and transition of emerging technologies, for example.

- Assisting in generating affordability goals and caps and should-cost goals by analyzing and verifying technical assumptions used in the cost analyses and related cost and budget documents.
- Assessing process improvement activities in support of should-cost goals.
- Developing and maintaining the SE approach in coordination with key stakeholders and other functional experts who participate in the program development activities.
- Tracking and managing the execution of the contract's SE-related tasks and activities in each development phase.
- Working closely with developer's SE teams to ensure integrated and effective processes are executed and documented in the SEMP.
- Planning and executing the formal technical reviews and audits.
- Tracking and reporting baseline changes and recommending a path forward, as a part of CM.
- Supporting the PM in CM activities.
- Identifying and mitigating the program's technical risks throughout the life cycle, in accordance with the DoD Technical Risk Assessment Methodology (DTRAM) version 6.4.
- Measuring and tracking program maturity using TPMs, requirements stability, and integrated schedules.
- Updating the PPP across the life cycle and working closely with developer's SE teams to ensure integrated and effective processes are executed and documented in the Program Protection Implementation Plan (PPIP).
- Staffing the engineering team with qualified engineers.
- Supporting updates to the TEMP and LCSP when appropriate.
- Developing models and simulations to support design analysis, V&V activities, ME analysis, etc.
- Supporting T&E activities as documented in the TEMP.
- Reviewing requirements traceability matrix and cross-reference matrix (verification).
- Managing root cause and corrective action efforts along with supporting the risk and opportunity boards.
- Supporting the selection of qualified, trusted vendors for parts, materiel, and processes (for hardware and software).
- Reviewing deliverables on the contract to ensure compliance and utility, and to ensure appropriate format and content.

One of the responsibilities of the systems engineer is to provide the PM with insight and oversight of the technical activities of the capability acquisition. To ensure the success of integrated processes, the systems engineer should maintain continuous engagement with the developer responsible to build, test, deploy, and sustain the system or capability being acquired. This continuous engagement is necessary to ensure a common understanding of program goals, objectives, and activities. The program office and developer SE team should further maintain frequent, effective communication, in accordance with the contract, as they manage and execute program activities and trade-off decisions.

The PM, systems engineer, and software engineer collaborate to translate stakeholder needs and performance requirements into a viable system design. As the design solution evolves through the application of the eight Technical Processes, the verification component or test organization provides confidence that the design solution that evolved from the requirements analysis, functional allocation, and design synthesis properly addresses the desired capabilities. The chief developmental tester, working in tandem with the systems engineer, accomplishes the verification loop of the SE process.

For all DoW acquisition programs, systems engineers will be included on the T&E WIPT as required by DoDI 5000.89. In addition, a Cyber Working Group should be established under the T&E WIPT to leverage system security engineering expertise and enhance cyber T&E activities. Together the systems engineer and chief developmental tester generate and analyze data from the integrated tests. The developer uses the test results to improve system performance, the SE team uses the test results for risk assessments, and the acquisition community and operational evaluators use the test results for operational assessments of the evolving system. This strategy for T&E should be consistent with and complementary to the SE approach. The PM and the systems engineer work closely with the chief developmental tester to facilitate coordinated V&V activities.

4.1.1 Stakeholders

The PM and LSE develops an SE approach (See Section 1.6 and the SEP Outline) that includes all stakeholders. The systems engineer coordinates with all participants to translate the operational needs and capabilities into technically feasible, affordable, testable, measurable, sustainable, achievable (within scheduled need dates), and operationally effective and suitable system requirements. Requirements translation should use digital standards enabling machine-readable and machine-interpretable formats that support automated stakeholder access, validation, and digital thread maintenance across the engineering ecosystem as stakeholders transition to digital processes.

The systems engineer is responsible for planning and overseeing all technical activity within the program office and for managing stakeholder expectations. Early and frequent involvement with stakeholders by both the PM and the systems engineer facilitates the successful execution of SE activities throughout the acquisition life cycle.

Most program personnel are involved in one or more of the 16 SE processes. Personnel from non-SE organizations or from outside the program office (e.g., end users, requirements sponsors, maintainers, testers, planners) should be integrated within the program's technical management activities so they can participate throughout the life cycle in support of SE-related activities.

Following is a partial list of the stakeholders who contribute to and benefit from SE activities and processes:

- Warfighters and other end users
- Engineers for the design considerations
- MDA
- Resource sponsors
- Budget authority
- Developers
- Enabled or enabling systems in the SoS
- Information systems security manager and system security engineer
- Chief developmental tester
- Operational test organization
- Assessment and authorization and/or certification and accreditation authorities
- Maintainers and logisticians (materiel readiness and sustainment)
- Intelligence Community
- Trainers
- Budget and cost analysts
- Contracting officers and associated staff
- ESOH staff
- Contractors who manufacture, test, deploy, or support the capability under development
- Companion programs

4.1.2 Integrated Product Teams

An IPT is a multidisciplinary group of representatives who are collectively responsible for delivering a defined product or process. The purpose of an IPT is to conduct activities as an integrated, collaborative effort with a focus on delivering the required capability to the end user.

An effective SE organization is typically structured as one or more IPTs. In developing the program office and SE organizational structure, the PM, systems engineer, and software engineer should know and understand both the design and functions of the developer's technical organization along with the developer's business model (in-house versus outsourced). This understanding is critical to ensuring effective coordination and oversight of developer activities and can affect how meetings are set up and conducted, how CM is executed, etc. In some cases, the PM, systems engineer, and software engineer may organize multiple IPTs to align with the major products in the program's WBS (see Section 6.1.1, Technical Planning Process). In smaller programs, the SE organization may be organized as a single IPT.

IPTs provide both the Government and developer stakeholders with the opportunity to maintain continuous engagement. This engagement is necessary to ensure a common understanding of program goals, objectives, and activities. These Government and developer IPTs should further maintain effective communication as they manage and execute activities and trade-off decisions. The program's SE processes should include all stakeholders in order to ensure the success of program efforts throughout the acquisition life cycle.

Specifically, for MDAPs, the PM should ensure that the program office interfaces with the SE WIPT (a multidisciplinary team responsible for the planning and execution of SE) to address DoW leadership concerns and interests. The SE WIPT is chartered by the PM and is usually chaired by the systems engineer. The SE WIPT should include representation from OUSW(R&E) and the Component Acquisition Executive's (CAE) organization, both Government and developer IPT leads from the program, the PAE systems engineer, and the developer systems engineer. Additional information about IPTs can be found in the DoD SEP Outline version 4.1 (2023).

4.2 Qualifications and Certifications

In modern DoW acquisition, qualification and certification should be tailored, risk-based processes to ensure a supplier's manufacturing capability and verify that systems are safe and effective for use in the intended operational environment. To support the Acquisition Transformation Strategy objective of "aligning with urgency and velocity, balancing speed with rigor in execution," the Department is looking to rapidly qualify and certify additional supply sources for industrial capabilities while maintaining product quality, reliability, and safety standards. It is therefore essential for PMs, systems engineers, and SMEs to identify program qualification and certification requirements early and execute the activities necessary to reduce qualification and certification timelines.

4.2.1 Qualifications

Qualification involves a systematic assessment of a potential supplier to ensure it is capable of meeting the acquirer's contractual and technical requirements. It is the formal process of

verifying that a supplier has the technical capability, quality standards, and organizational stability required to reliably deliver mission-critical goods or services.

4.2.2 Certifications

Certifications provide a formal acknowledgment by an approval authority that a system or program meets specific requirements, and they play a critical role in managing program risk. While certifications are often based on statute or regulations, programs should leverage the flexibilities inherent in the acquisition system to appropriately tailor their approach to certifications, ensuring that program risk is balanced with innovation, agility, and timely delivery of capability. Used throughout the acquisition life cycle, certifications reduce program risk and increase understanding of the system. Certain specific certifications are required before additional design, integration, network access, or testing can take place. For example, airworthiness certifications need to be in place before an aircraft or aerial system can begin flight testing and before safety confirmations and safety certifications need to be provided for materiel releases. Often programs insufficiently plan for the number of required certifications, which can have a negative impact on program costs and schedule.

Obtaining the various certifications has typically been a lengthy process, but proactive planning and early engagement with certification authorities can help mitigate delays. The PM should ensure that the time necessary to obtain any required certification is factored into technical planning and that the program takes advantage of opportunities for executing parallel and iterative efforts wherever possible. By embracing a flexible and adaptive approach to certification planning, the PM, systems engineer, and software engineer can facilitate the development of innovative solutions while ensuring that all necessary certifications are obtained. Early planning allows the systems engineer and technical team to begin interacting with certification authorities, establishing a collaborative relationship that can help identify and address potential certification challenges.

The SEP Outline requires programs to provide a certification matrix that identifies applicable technical certifications and when they are required during the acquisition life cycle. Programs should include certification activities and events in the IMS and the IMP and should use these tools to identify potential opportunities for streamlining the certification process.

4.3 Value Engineering

Value engineering (VE) is a systematic approach that analyzes the functions of systems, equipment, facilities, services, and supplies to ensure they achieve their essential functions at the lowest life cycle cost consistent with required schedule, performance, reliability, quality, and safety. At its core, value is defined as the ratio of function to cost ($\text{Value} = \text{Function} / \text{Cost}$). By increasing function or reducing cost—without sacrificing one for the other—VE aims to enhance overall value. DoW Components implement VE when it is advantageous to improve military worth or reduce acquisition and life cycle costs. The U.S. military developed VE initially during

World War II to enhance military-industrial production. VE's proven contributions to the war effort and subsequent enhancements to the methodology have led a range of Government and private sector organizations to adopt the practice. It is intended to lower cost, increase the speed of delivery, or both, without sacrificing performance or reliability.

The DoW provides VE policy through DoDI 4245.14, "Value Engineering (VE) Program," which implements 41 USC 1711 and Office of Management and Budget (OMB) Circular No. A-131 (Revised), "Value Engineering." VE has two parts: Value Engineering Proposals (VEPs) and Value Engineering Change Proposals (VECPs). VEPs are developed in-house by Government personnel or contractors specifically hired to provide VE services. VECPs use contractor-initiated change proposals to implement Government-approved changes.

SD-24, "Value Engineering: A Guidebook of Best Practices and Tools" provides details on VE activities, VEPs, and VECPs. SD-24 provides extensive information on applying VE to promote innovation, improve value, and reduce costs over the acquisition and operation life cycle.

Federal Acquisition Regulation (FAR) Subpart 48.102 ("Policies"), para (a) requires contracting activities to include VE provisions in appropriate supply, service, architect-engineer, and construction contracts for the DoW to provide contractors with a fair share of the savings on accepted VECPs.

The PM's VE activities include the following:

- Scope the issue, improvement targets, risk mitigation, and evaluation factors.
- Identify specific areas or functions for evaluation.
- Collect and analyze data.
- Explore alternative approaches.
- Develop and present specific recommendations.
- Implement directed changes.

PMs, systems engineers, and software engineers should encourage the development and submittal of VEPs and VECPs along with applying VE principles in the development, procurement, production, and life cycle support of services, materiel, and facilities for:

- Hardware, software, and/or human components.
- Development, production, test, or manufacturing.
- Specifications and standards.
- Facilities design and construction.
- Contract requirements.

- Program documentation.
- Operation, maintenance, and disposal.

VE is the application of the Value Methodology to ensure that every dollar spent delivers optimal value. When integrated at the right time and managed effectively, VE can enhance performance, reduce costs, and improve sustainability across all phases of a project or product life cycle.

4.4 Sustainability Analysis

Large military systems and platforms can have a life cycle of 30 years or more. To meet evolving mission needs far into the future, the system design should incorporate long-term sustainability considerations in order to reduce life cycle costs. Without a full understanding of life cycle impacts, significant costs may be inserted unintentionally during development or procurement and later exposed by the logistics and operational communities.

The sustainability analysis, using a Life Cycle Assessment (LCA) method, is a tool to assist the systems engineer in designing more sustainable systems – those that use fewer resources over the life cycle, and thus have a lower total ownership cost (TOC). The PM should make sustainability considerations an integral part of both a robust trade space analysis and a comprehensive supportability analysis. These sustainability analyses can help reduce system TOC by uncovering previously hidden or ignored life cycle costs, leading to more informed decisions earlier in the acquisition life cycle. They can also help improve the accuracy of life cycle cost estimates.

A sustainability analysis compares alternative designs or sustainment activities regarding their use of energy, water, chemicals, and land. Outputs include impacts on resource availability, human health and the environment and the TOC of the alternatives that meet the minimum performance requirements. The life cycle costs can include both internal (to DoW) and external (to society) by monetizing the impacts.

A sustainability analysis can support numerous acquisition activities, including:

- Trade-space analysis to compare how sustainability attributes (e.g., chemical or material choices, water or solid waste) affect life cycle cost, TOC, performance, human health, and the environment.
- Business Case Analysis using the LCA method, including sustainability as one of the elements in the analysis.
- Preliminary design to select the most sustainable system that meets performance requirements and end-user needs.
- Supportability analysis to help ensure the use of resources throughout the life cycle is considered.
- Detailed design to select the most sustainable components.

The streamlined LCA process for sustainability in DoW acquisitions (Sustainability Analysis Guidance, OASD Sustainment 2020) combines LCA with multi-attribute analysis; it integrates a number of trade-space and design considerations and provides a procedure to compare conceptual or detailed design alternatives. It is intended to ensure consideration of important downstream impacts and costs in trade-off and design decisions. The method is consistent, without duplication, with other design considerations, such as operational energy, supportability, and ESOH (Section 7.23 System Safety).

4.5 Lessons Learned, Best Practices, and Case Studies

Most programs represent a new combination of existing capabilities or the insertion of incremental advances in technology. By reviewing the successes, failures, problems, and solutions of similar programs, PMs, systems engineers, and software engineers can gain insights into risks, uncertainties, and opportunities their programs may encounter.

Lessons learned and case studies generally describe areas of risk, pitfalls encountered in programs, and strategies employed to mitigate or fix problems when they arise. Best practices are proven techniques and strategies that can prevent common problems and improve quality, cost, or both.

Best practices and lessons learned are applicable to all aspects of a program – technical, managerial, and programmatic – and at any point in the acquisition life cycle. However, they are not universal or “one-size-fits-all” solutions. The greatest benefits occur when PMs, systems engineers, and software engineers judiciously select and tailor successful practices or strategies from analogous programs/systems and tailor them to meet current program needs.

Programs should create structured opportunities for smaller or non-traditional entities to compete for mission-specific work, modeled on the National Aeronautics and Space Administration’s (NASA) directorate competition approach. SBIR/STTR is a key tool for accessing the small business innovation base and rapidly maturing technologies to meet warfighting needs. PMs and system engineers should leverage SBIR/STTR pilot initiatives, partnerships, and acceleration mechanisms to inform iterative experimentation, prototyping, and technical risk reductions that support improved acquisition outcomes. This disrupts entrenched stovepipes and drives innovation across the industrial base.

Standards, such as those for design, build, test, and certification, are a compilation of lessons learned over time from across management, engineering, manufacturing, or sustainment. PMs, systems engineers, and software engineers should be aware that standards are not ad hoc requirements developed by a single engineer or program office.

The ASSIST tool is the official source for standardization information and documents, such as defense specifications and standards and adoptions of Non-Government Standards (NGS). In many cases, the DoW uses NGS, as required in 15 USC 272 Notes “Utilization of Consensus Technical Standards by Federal Agencies” and implemented in OMB Circular A-119, DoDI

4120.24 (3.b. – Page 1), and FAR (Subpart 11.101, para (b)) in preference to developing and maintaining Government specifications and standards, unless it is inconsistent with applicable law or otherwise impractical. PMs should consider the following sources when considering which specifications and standards to apply: the DoD Information Technology Standards Registry (DISR), the Standardization Directory (SD) 21 (Listing of Specifications and Standards Mandated for use by the DoD by Public Laws or Government Regulations), and U.S.-ratified materiel international standardization agreements.

Various organizations in the DoW, industry, and academia produce and maintain online repositories of standards, lessons learned, best practices, and case studies. These resources can serve as a starting point for PMs, systems engineers, and software engineers to search for and find relevant data that can be applied to their current program. Knowledge-sharing resources include, but are not limited to:

- Service lessons learned repositories (including Service safety centers).
- GAO reports.
- Defense Standardization Program Office (DSPO).
- Other departments and agencies such as NASA, Department of Energy, or National Institute of Standards and Technology (NIST).
- Professional organizations such as the INCOSE or the Institute of Electrical and Electronics Engineers.
- Industry organizations such as National Defense Industrial Association (NDIA) or Aerospace Industries Association (AIA).
- NGS development organizations such as Society of Automotive Engineers (SAE) International and International Organization for Standards (ISO).

PMs, systems engineers, and software engineers are encouraged to research current analogous programs, not just past programs that may be experiencing similar challenges and have not yet formally documented what they have learned. In order to aid both internal program activities and external collaborative information sharing, the PM, systems engineer, and software engineer should ensure the program establishes and uses a robust process to identify and document best practices and lessons learned. This process should focus on ensuring accurate and timely documentation of all relevant information, and the systems engineer should monitor its use and products throughout the life cycle.

Each best practice or lesson learned developed throughout the program execution should include enough contextual information about the program and surrounding circumstances so future practitioners can discern the relevancy and usefulness of the best practice. PMs, systems engineers, and software engineers should consider using this data as a form of process improvement feedback, or as evidence for proposing policy and guidance changes.

4.6 Systems Engineering Role in Contracting

The systems engineer should participate in developing program contract tasks to ensure that the appropriate technical activities are contained, properly scoped, and resourced in the contract. Effective scoping of the technical tasks in the SOW, Statement of Objectives, or Performance Work Statement is necessary to ensure that the final system meets the end user's needs. By actively participating in the development of contract tasks, the systems engineer can help ensure that the contract includes the necessary technical activities, milestones, and deliverables to support successful system development, integration, and testing.

Often contracting activities may appear to be primarily programmatic in nature (e.g., acquisition strategy development, writing RFPs, performing market research, developing the CDRL), but, in fact, they reflect technical planning and should be influenced by the necessary technical content. For example, technical understanding of data rights can be a key element in planning for modularity and open systems design, or the decision to choose an incremental acquisition strategy depends on generic functionality groupings that may not be appropriate for every system.

The systems engineer and technical management team should contribute to the development of contract incentives or incentive approaches that promote an understanding of the technical risks and opportunities inherent in the selected development approach. Incentive fees and penalties such as award fees may be tied to program performance that may be evaluated during technical reviews, or more frequently the incentive or penalty is tied to the completion of a technical review. If that is the case, however, the developer may have a strong incentive to call the review complete as soon as possible. The systems engineer and PM should exercise best judgment in an objective and informed manner to ensure the reviews are not prematurely completed in order for the developer to qualify for the contract incentive.

Although there are many opportunities for contract-related interactions between the Government and potential offerors before contract award, the RFP remains the primary tool for shaping the contract, the program, and ultimately the system.

Acquisition strategies should enable delegated subcontracting authority for primes to reduce contracting cycles from years to months. Government oversight should focus on interoperability standards, mission outcomes, and architecture control, while allowing industry teams greater flexibility in subcontracting.

5 TECHNICAL REVIEWS AND AUDITS

For DoW systems development, a properly tailored series of technical reviews and audits provide key points throughout the system development to evaluate significant achievements and assess technical maturity and risk. Pursuant to DoDI 5000.02, the Adaptive Acquisition Framework Document Identification (AAFDID) Tool identifies the statutory and regulatory requirements for acquisition programs. Regardless of acquisition pathway, the PM, systems engineer, and software engineer should work to properly align the applicable technical reviews to support knowledge-based acquisition decisions that streamline the acquisition life cycle and save taxpayer dollars. Technical reviews and audits allow the PM, systems engineer, and software engineer to jointly define and control the program's technical effort by establishing the success criteria for each review and audit. A well-defined program facilitates effective monitoring and control through increasingly mature points.

The Engineering of Defense Systems Guidebook (2022) provides guidance on selecting and tailoring technical reviews and audits for each of the AAF pathways. Underpinning most if not all of these technical reviews and audits is the need to conduct a wide range of program-related analyses. Regardless of acquisition pathway, the ability to conduct such analyses can be profoundly affected by the extent to which the program adopts a DE approach (as described more fully in Section 3.3, Digital Engineering). As mentioned there, the DoW's approach to implementing DE is to "securely and safely connect people, processes, data, and capabilities across an end-to-end digital enterprise. This will enable the use of models throughout the life cycle to digitally represent the system of interest (i.e., SoS, processes, equipment, products, parts) in the virtual world."

The extent to which a program adopts a DE approach will not affect "what" technical reviews and audits need to be conducted, but it can have a profound and revolutionary impact upon "how" they are conducted. A well-defined digital ecosystem instantiated or leveraged with the associated authoritative sources of truth and static and dynamic models of systems and the battlespace will enable timely and iterative analyses. In addition, by leveraging constructive, virtual, and live simulation tools, the ecosystem can open up the trade space to enable exploration of options not easily analyzed otherwise.

Technical reviews of program progress should be event-driven and conducted when the system under development meets the review entrance criteria documented in the SE approach. As noted in Section 1.6 of this guidebook, all programs should have an SE approach in the form of a SEP, as part of the digital ecosystem, or a combination of both, regardless of AAF pathway. As part of this process, technical risks associated with achieving entrance criteria should be identified and managed in accordance with the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. The SE approach or SEP should clarify the timing of events in relation to other SE and program events. While the initial SEP and IMS provide a baseline for the expected SE activities, the plan should be updated to reflect changes to the actual timing of SE activities, ensuring it remains aligned with program progress.

Figure 5-1 illustrates a generic end-to-end acquisition life cycle depiction including the integration of traditional SE technical reviews and audits across the life cycle in addition to agile development embedded within the overall life cycle. The figure contains the activities and reviews that should be considered for programs developing hardware-centric systems as well as hardware-reliant software-centric systems, regardless of acquisition pathway. MDAPs and major systems may use agile methodologies to mature components and subsystems before integration into the full system development. Smaller, less complex programs may choose to implement a strictly agile approach. Regardless, PMs should tailor according to the specific program requirements.

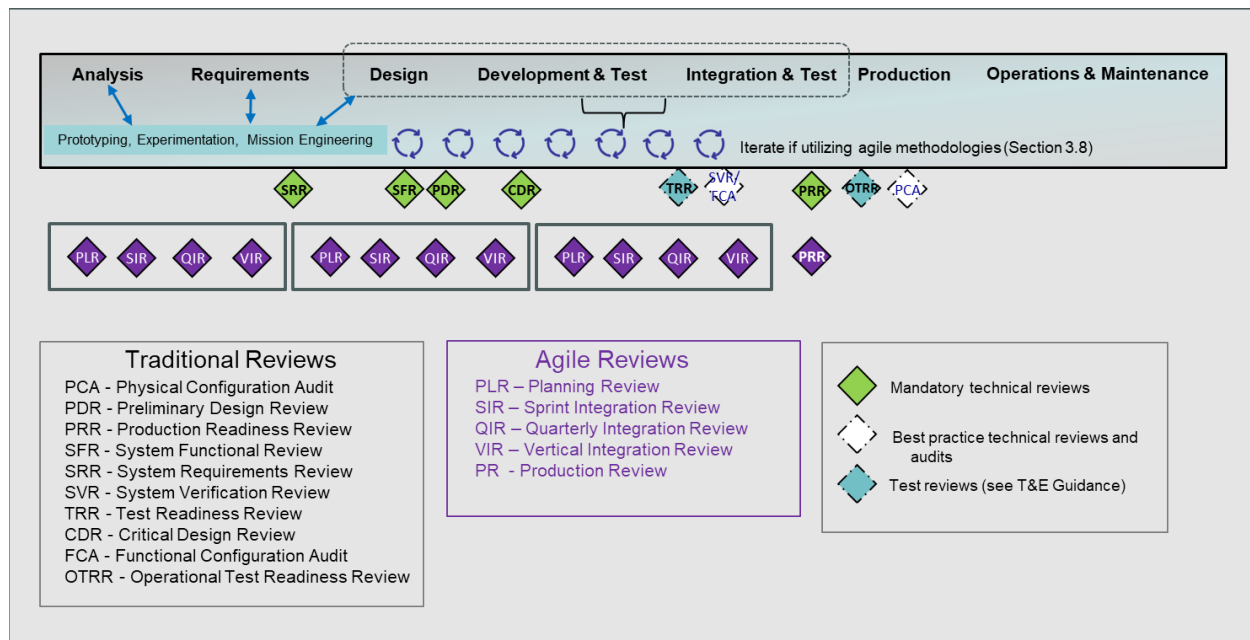
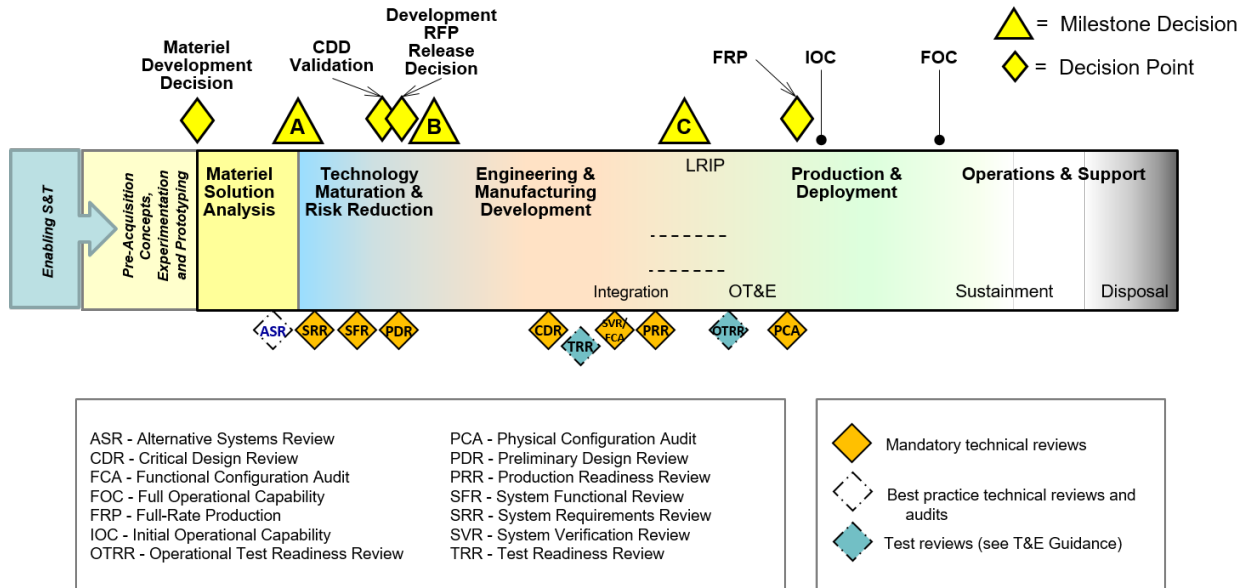


Figure 5-1. Generic Life Cycle Including Agile

Figure 5-2 provides the end-to-end perspective and the integration of SE technical reviews and audits across the system life cycle, as represented by the Major Capability Acquisition (MCA) pathway. Although this guide employs terminology mainly applicable to the MCA pathway, the principles and practices should be applied, as appropriate and tailored, to all DoW system development. Although an MDAP or major system using the MCA pathway typically will employ the majority of technical reviews described in this section, it is prudent for the PM and systems engineer to consider all of these technical reviews for their respective program regardless of AAF pathway.



Notes:

- Derived from DoDI 5000.85, Major Capability Acquisition Model

Figure 5-2. Technical Reviews and Audits for the Major Capability Acquisition Life Cycle

Properly structured, technical reviews and audits support the Defense Acquisition System by:

- Providing a disciplined sequence of activities to define, assess, and control the maturity of the system's design and technical baseline, reducing risk over time.
- Facilitating an accurate technical assessment of the system's ability to meet Key Performance Parameters (KPPs) and associated thresholds.
- Facilitating an accurate technical assessment of the system's ability to satisfy operational requirements established in capability requirements documents.
- Providing a framework for interaction with the requirements and funding (e.g., Planning, Programming, and Budgeting Execution (PPBE)) processes.
- Providing a technical assessment and assurance that the end product fulfills the design and process requirements.

Successful development of a complex system requires a knowledge-based approach. Increasing levels of knowledge are a natural consequence of design maturation; however, successful programs establish a deliberate acquisition approach whereby major investment decision points are supported by requisite levels of knowledge. The GAO report "Assessments of Selected Weapon Programs" (GAO-12-400SP) provides quantitative evidence to affirm this best practice.

Technical reviews should occur when the requisite knowledge is expected and required. This section provides guidance on entrance and exit criteria for the level of maturity expected at each technical review and audit. OSD established the expected reviews and audits for each phase of systems development in the outline for the SE approach or SEP. These policy and guidance documents provide a starting point for the PM, systems engineer, and software engineer to develop the program's unique set of technical reviews and audits. Tailoring is expected to best suit the program objectives. The SE approach or SEP captures the output of this tailoring and is reviewed and approved to solidify the program plan.

Programs that tailor the timing and scope of these technical reviews and audits to satisfy program objectives increase the probability of successfully delivering required capability to the warfighter. Technical reviews provide the forum to frame issues and assumptions. They define options necessary to balance risk in support of continued development.

The technical baselines established at the conclusion of certain technical reviews inform all other program activity. Accurate baselines and disciplined reviews serve to integrate and synchronize the system as it matures, which facilitates more effective milestone decisions and ultimately provides better warfighting capability for less money. The technical baseline provides an accurate and controlled basis for:

- Managing change
- Cost estimates, which inform the PPBE process and the APB (or equivalent)
- Program technical plans and schedules, which also inform the APB (or equivalent)
- Contracting activity
- Specialty Engineering (e.g., Human Systems Integration (HSI), Reliability and Maintainability (R&M), Manufacturing and Quality (M&Q), System Security, Cyber, System Safety (SS), and VE) efforts
- T&E efforts
- Risk analysis and risk balancing
- Reports to acquisition executives and Congress

The PM and the systems engineer need to keep in mind that technical reviews and audits provide visibility into the quality and completeness of the developer's work products. These requirements should be captured in the contract specifications or SOW. The program office should consider providing the SEP (or equivalent) with the RFP and requiring the contractor deliver a SEMP that is consistent with the SEP. As a best practice, the SEMP should include entrance criteria and associated design data requirements for each technical review and audit. The configuration and technical data management plans should clearly define the audit requirements.

For complex systems, reviews and audits may be conducted for one or more system elements, depending on the interdependencies involved. These incremental system element-level reviews lead to an overall system-level review or audit. After all incremental reviews are complete, an overall summary review is conducted to provide an integrated system analysis and capability assessment that could not be conducted by a single incremental review. Each incremental review should complete a functional or physical area of design. This completed area of design may need to be reopened if other system elements drive additional changes in this area. If the schedule is being preserved through parallel design and build decisions, any system deficiency that leads to reopening design may result in rework and possible material scrap.

To design for system security, the program protection planning and execution activities should be integrated into the SE technical reviews and audits. See Technology and Program Protection (T&PP) Guidebook (2022) for system security engineering criteria for each technical review and audit.

5.1 Roles and Responsibilities

For each technical review, the Service designates a technical review chair, who could be the PM, systems engineer, or other SME according to the Service's guidance. The chair is responsible for evaluating products and determining the criteria are met and action items are closed. The Service guidance also may identify other roles and responsibilities associated with technical reviews and audits and may specify the types of design artifacts required for various technical reviews. In the absence of additional guidance, each program should develop and document its tailored design review plan as part of the SE approach.

The following are typical duties and responsibilities associated with the PM, systems engineer, and software engineer.

The PM is typically responsible for:

- Co-developing with the systems engineer the technical objectives of the program that guide the technical reviews and audits.
- Co-developing with the systems engineer the earned value credit derived from the review.
- Approving, funding, and staffing the planned technical reviews and audits; documenting this plan in the SE approach and applicable contract documents.
- Ensuring the plan for each review includes participants with sufficient objectivity with respect to satisfying the pre-established review criteria.
- Ensuring the plan addresses the need for timely and sufficient data to satisfy the statutory and regulatory requirements of DoDI 5000.02.

- Controlling the configuration of each baseline and convening capability trade councils when user requirement changes are warranted. This can lead to a need to revisit the requirements review and approval process with the requirements owner/stakeholder.

The systems engineer is typically responsible for:

- Enabling efficient program execution, informed decision-making, and accelerated delivery of defense systems by strategically managing technical risk (i.e., accepting calculated risks while proactively mitigating critical risks that could jeopardize program success) and providing expert SE guidance to the PM.
- Co-developing with the PM the technical objectives of the program that guide the technical reviews and audits.
- Developing and documenting the technical review and audit plan in the SE approach, carefully tailoring each event to satisfy program objectives and SEP outline guidance associated with the tailored set of technical reviews and audits.
- Defining clear entrance and exit criteria for each review, based on program knowledge point objectives and acquisition pathway, to ensure objective assessment of progress.
- Identifying the resources required to support the plan; ensuring the activities leading up to the official review and audit are integrated.
- Ensuring technical reviews and audits are incorporated into the IMP and IMS (or equivalent).
- Coordinating with the chief development tester to provide the following at each technical review: DT&E activities to-date, results, assessments to-date, planned activities, and updates to risks.
- Ensuring a status of applicable design considerations are provided at each technical review.
- Establishing technical reviews and audits and their review criteria in the applicable contract documents (e.g., SOW, IMP).
- Monitoring and controlling execution of the established plans.
- Partnering with the technical review chairperson to ensure efficient and effective execution of technical reviews.
- Driving timely closure of review action items and advising the chairperson and PM on review completion (Figure 5-2).
- Providing expert technical analysis and guidance to program decision makers, enabling informed decisions based on a realistic assessment of technical maturity, progress, and risk, enabling programs to proceed at the optimal pace and maximizing efficiency while mitigating the risk of catastrophic failure.

The software engineer is typically responsible for:

- **Software Architecture Integration.** Ensure that software architecture alignment with the system architecture is assessed, documented, and presented at each technical review. In agile programs, this includes demonstrating how sprint-delivered increments contribute to the evolving system architecture and support end-to-end capability delivery.
- **Software Maturity and Readiness Metrics.** Provide quantitative software maturity and readiness metrics as entrance and exit criteria for each review. Relevant metrics include defect density, code coverage, velocity, technical debt levels, and — in agile programs — iteration throughput, risk burn-down rate, and LVI. These metrics should be automated where possible and presented via digital dashboards consistent with the program's DevSecOps ecosystem.
- **Software-Unique Risk Assessment.** Assess and present software-unique risks, issues, and opportunities at each review, with associated mitigation plans and risk burn-down trends. The software engineer should coordinate with the systems engineer to ensure that software risks are integrated into the program-level risk register and reflected in end-to-end performance assessments.
- **Requirements Traceability.** Verify that software requirements are traceable to system requirements, user stories, and capability increments. In agile programs, traceability should be maintained dynamically across sprints and validated at each iterative review gate to ensure delivered increments satisfy system-level performance and capability objectives.
- **DevSecOps and CI/CD Pipeline Health.** Confirm the health and compliance status of the CI/CD pipeline and DevSecOps practices at each review. Security should be embedded — not bolted on — throughout the software development process. Ensure that automated testing, continuous builds, and incremental delivery practices are in place and that pipeline health is a standing agenda item at all technical reviews.
- **Software Integration and Test Readiness.** Evaluate and present software readiness for integration and test at each review gate. This includes confirming that software components are independently integrable and testable, that technical debt is being actively managed as a program risk, and that the program's Problem Reporting and Deficiency Reporting processes are current and complete.
- **Inclusion of Software.** Ensure inclusion of software as documented in the SE approach. This includes working with the systems engineer and program manager during SE approach development to define the scope of software content, entrance and exit criteria, and artifacts the software engineer is responsible for delivering at each review.
- **Coordination with Systems Engineer.** Continuously coordinate with the systems engineer to ensure that software technical performance, process health, progress, and quality metrics are reported at all technical reviews — with particular emphasis on metrics associated with end-to-end system performance and capability delivery.

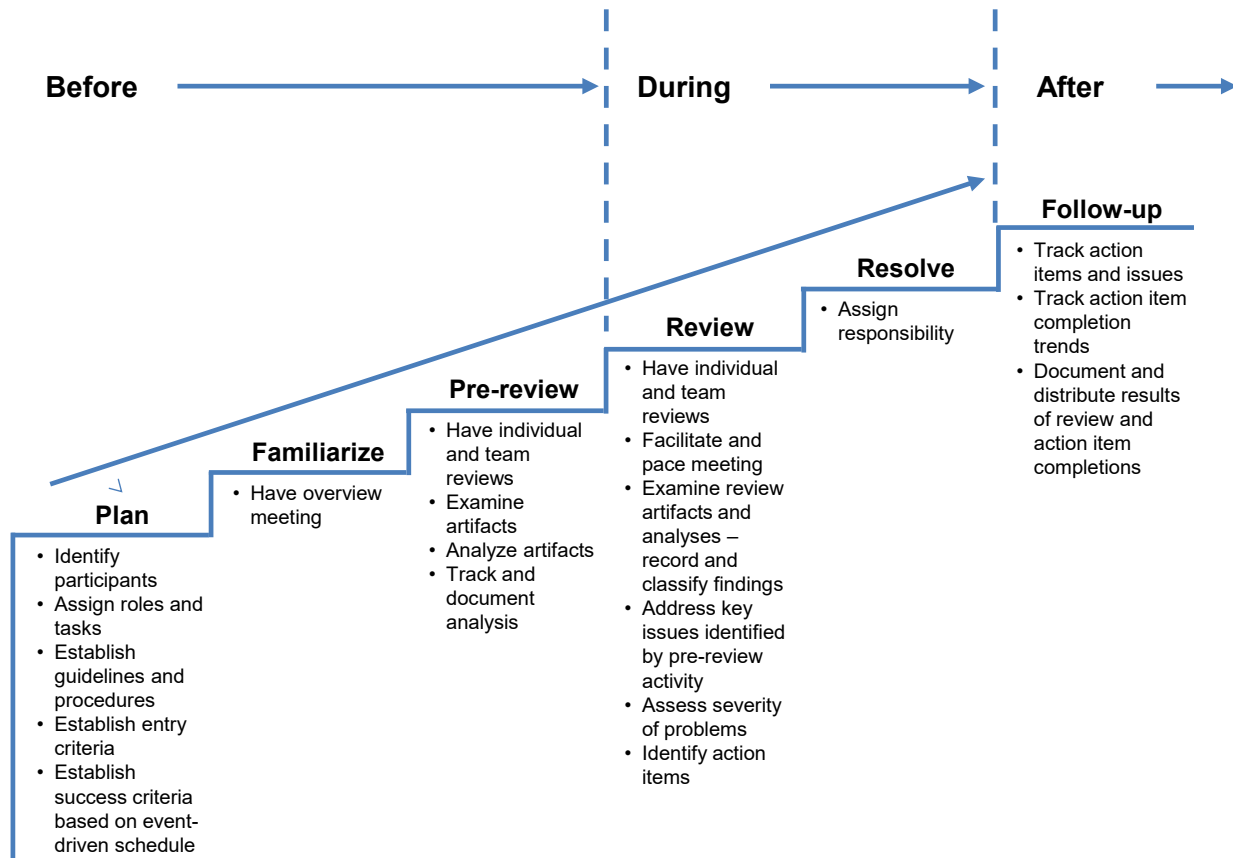


Figure 5-3. Technical Review Process

The PM, systems engineer, and software engineer should identify key stakeholders who have an interest or role in the review, which may include:

- Technical review chairperson
- PAE
- Direct Reporting Portfolio Manager
- Contracting officer
- Defense Contract Management Agency (DCMA) and Defense Contract Audit Agency
- Product support manager (PSM)
- Product improvement manager/requirements officer
- End-user community
- Chief developmental tester
- Interdependent acquisition programs
- Business financial manager

- OSD oversight organizations as required Service technical leadership such as chief engineers
- SMEs

5.2 Review Criteria

Specific review criteria are provided in each technical review and audit section below. These criteria should be achieved and all action items closed before a technical review is considered complete. The systems engineer may refer to ISO/IEC/IEEE 24748-8, Systems and Software Engineering–Life Cycle Management, Part 8: Technical Reviews and Audits on Defense Programs, as a resource. If a PMO chooses to use ISO/IEC/IEEE 24748-8, additional guidance for implementing the DoW-adopted SE standard on acquisition program contracts can be found in the guidance document “Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288 Series) on Contracts for Department of Defense Acquisition Programs” (2017). When comparing this section on technical reviews and audits with ISO/IEC/IEEE 24748-8, keep in mind:

- The ASR focuses on achieving a government-to-government understanding of the user’s needs and the preferred materiel solution. It occurs in the Materiel Solution Analysis phase before a development contract is awarded.
- The Test Readiness Review (TRR) is addressed in the T&E Enterprise Guidebook (2022).
- With the exception of TRR, this section addresses all technical reviews and audits in ISO/IEC/IEEE 24748-8. The standard has annexes that address software-specific and other reviews that may be useful, depending on program needs.

Contract incentives are frequently tied to completion of technical reviews. Some stakeholders may have a strong incentive to call the review complete as soon as possible. The review chairperson and systems engineer should exercise best judgment in an objective, informed manner to ensure the reviews are not prematurely declared complete.

5.3 Alternative Systems Review

The ASR supports communication between the end user and acquisition community and leads to a performance specification for the preferred materiel solution. The ASR typically occurs early in the requirements analysis phase and focuses the technical efforts on requirements analysis.

The ASR should evaluate whether there is sufficient understanding of the technical maturity, feasibility, and risk of the preferred materiel solution, in terms of addressing the operational capability needs in the applicable requirements document and meeting affordability, technology, and operational effectiveness and suitability goals.

The ASR helps the PM, systems engineer, and software engineer ensure that further engineering and technical analysis needed to draft the system performance specification is consistent with customer needs.

Roles and Responsibilities

The unique PM responsibilities associated with an ASR include:

- Approving, funding, and staffing the ASR.

The unique systems engineer responsibilities associated with an ASR include:

- Ensuring adequate plans are in place to complete the necessary technical activities for the ASR.
- Ensuring results of all technical trade studies are captured in documents that are carried through to the next phase.
- Ensuring technical risk items are identified and analyzed, and appropriate mitigation plans are in place. This activity should include, for example, the identification of critical technologies and identification of key interfaces with supporting or enabling systems.

Inputs and Review Criteria

The ASR typically occurs after a preferred materiel solution is selected by the lead Service or Component but before the requirements oversight review. This timing allows the focus of the ASR to be on the preferred materiel solution and allows for some technical analysis to be completed and inform the requirements oversight deliberations (if applicable).

- ME, experimentation, and prototyping results are an input to the ASR. These activities should have evaluated a number of candidate materiel solutions and identified those alternatives that can meet the user requirements within the remaining trade space (including cost and affordability constraints).
- After initial ME, experimentation, and prototyping results are completed, the operational requirements community and the acquisition community collaboratively identify one or more preferred materiel solution(s) with the potential to be affordable, operationally effective and suitable, sustainable, and technically and technologically achievable (i.e., able to provide a timely solution to the stated operational capability need at an acceptable level of risk). This preferred materiel solution is also an input to the ASR.
- The draft CONOPS/OMS/MP (or equivalent) should be available as an input to the ASR. It can then be used to support development of missions and operational scenarios to evaluate the preferred materiel solution.

Table 5-1 identifies the products and associated review criteria normally seen as part of the ASR. The chief engineer should review this table and tailor the criteria for the program. The ASR should not begin until the criteria are met. A resource for ASR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-1. ASR Products and Criteria

Product	ASR Criteria
Refined Joint Requirements	- Joint context and initial CONOPS/OMS/MP updated to reflect current user position about current and evolving capability gap(s), supported missions, mission analysis, Target Audience Description (TAD), interfacing/enabling systems in the operational architecture; overall SoS context - Required related solutions and supporting references (e.g., Initial Capabilities Document (ICD) and Capability Development Document (CDD) or equivalents) identified - Joint refined thresholds and objectives initially stated as broad measures of effectiveness, performance, and suitability (e.g., KPPs, KSAs, need date)
Initial Architecture for the Preferred Materiel Solution(s)	- High-level description of the preferred materiel solution(s) is available and sufficiently detailed and understood to enable further technical analysis - SoS interfaces and external dependencies are adequately defined - Task analyses, function allocation, human viewpoints
System Performance Specification	- Clear understanding of the system requirements consistent with the applicable requirements document - System requirements are sufficiently understood to enable functional definition - Draft system performance specification has sufficiently conservative requirements to allow for design trade space - Relationship between draft system performance specification and risk reduction prototyping and competitive prototyping objectives is established
Preferred Materiel Solution(s) Documentation	- Comprehensive rationale is available for the preferred materiel solution(s), based on the ME, experimentation, and prototyping results - Key assumptions and constraints associated with preferred materiel solution(s) are identified and support the conclusion that this solution can reasonably be expected to satisfy the applicable requirements document in terms of technical, operational, risk and schedule/cost (affordability) criteria - Results of trade studies/technical demonstrations/evaluation of innovative technologies (such as SBIR/STTR) for concept risk reduction, if available - Initial producibility assessments of solution concepts
Risk Assessment	- Technical risks are identified, and mitigation plans are in development - Initial hazard analysis/SS analysis for preferred solution(s) complete - HSI risk identification and mitigation plans

Outputs and Products

The technical review chair determines when the review is complete. ASR technical outputs should include, but not be limited to, the following products, including supporting rationale and trade-off analysis results:

- Refined description of the preferred materiel solution to support further development.

5.4 System Requirements Review

The SRR is a multidisciplined technical review to ensure that the developer understands the system requirements and is ready to proceed with the initial system design. This review assesses whether the system requirements as captured in the system performance specification (sometimes referred to as the System Requirements Document (SRD)):

- Are consistent with the preferred materiel solution (including its support concept)
- Are consistent with technology maturation plans
- Adequately consider the maturity of interdependent systems
- Are clearly stated and are measurable and testable

All system requirements and performance requirements derived from the applicable requirements document should be defined and consistent with cost, schedule, risk, and other system constraints and with end-user expectations. Also important to this review is a mutual understanding (between the program office and the developer) of the technical risk inherent in the system performance specification.

The program office should perform an SRR to assess readiness and risks of the technical content of the draft RFP(s) before RFP release and to ensure performance requirements are traceable to user or operational requirements. This review should occur after the selection of the preferred solution and after sufficient analysis has occurred to develop a draft performance specification.

If the program's AS (or equivalent) includes competing contractual efforts during the Technology Maturation and Risk Reduction (TMRR) phase, an SRR should be held with each participating developer to ensure the requirements are thoroughly and properly understood and they are ready to proceed into initial system design with acceptable risk. This review is designed to ensure that SoS requirements, in the form of logical and physical interfaces and desired performance outcomes, have been levied on the system to be procured and are consistent with the applicable requirements document. These requirements are documented in the system performance specification and managed through external communication and technical interfaces in accordance with the SE approach.

Roles and Responsibilities

The unique PM responsibilities associated with an SRR include:

- Approving, funding, and staffing the SRR as planned in the SE approach developed by the Systems Engineer.
- Managing and approving changes to the system performance specification.
- Establishing the plan to SFR in applicable contract documents, including the SEP, IMS, and IMP (or equivalents).
- Ensuring the plan includes SMEs to participate in each review.

The unique systems engineer responsibilities associated with an SRR include:

- Ensuring all performance requirements, both explicit and derived, are defined and traceable (both directions) between requirements (including KPPs, KSAs, other system attributes and the system performance specification).
- Ensuring verification methods are identified for all system requirements.
- Ensuring risk items associated with system requirements are identified and analyzed, and mitigation plans are in place.
- Ensuring adequate plans are in place to complete the technical activities to proceed from SRR to the SFR (if applicable).
- Ensuring plans to proceed to SFR allow for contingencies.
- Ensuring all interfaces are documented for the SoS and included in the performance specification.

Inputs and Review Criteria

Table 5-2 identifies the products and associated review criteria normally seen as part of the SRR. The chief engineer should review this table and tailor the criteria for the program. The system-level SRR review should not begin until the criteria, identified by the chief engineer and documented in the SEP, are met and any prior technical reviews are complete and action items closed.

This is also an opportunity to assess whether technical requirements from all acquisition documentation (e.g., PPP; Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report) flow to specifications. If the program's AS includes competing contractual efforts, an SRR should be held with each developer. A resource for SRR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-2. SRR Products and Criteria

Product	SRR Criteria
Cost Estimate	• Preliminary Cost Analysis Requirements Description (CARD), or equivalent, is consistent with the approved system performance specification • Preliminary software development estimates established with effort, schedule, and cost analysis • Updated cost estimate fits within the existing budget
Risk Assessment	• Technical risks are identified, and mitigation plans are in place • Initial Mission-Based Cyber Risk Assessment (MBCRA) is completed
System Performance Specification	• Contractor clearly demonstrates an understanding of the system requirements consistent with the requirements documents (e.g., ICD and draft CDD (or equivalents)) • System requirements, including those generated by the design considerations, are sufficiently detailed and understood to enable functional definition and functional decomposition • System requirements are assessed to be verifiable (see Chief Developmental Tester in Test and Evaluation (T&E) Enterprise Guidebook (2022)) • Requirements can be met given the plans for technology maturation • External interfaces to the system have been documented in Interface Control Documents • SoS technical interfaces are adequately defined, including interdependences associated with schedule, test, and configuration changes • Preliminary identification of all software components (tactical, support, deliverable, non-deliverable, etc.) are completed • Requirements generated by the design considerations (e.g., R&M requirements) have been reviewed and included in the overall system design (see Section 7) • Sustainment requirements have been reviewed and included in the overall system design (per the program's Product Support Strategy (PSS) and LCSP or equivalent documentation) • Reliability and maintainability quantitative requirements have been assessed to be valid and feasible (See RAM-C Rationale Report Outline Guidance) • Contractor has adequately expanded the system performance specification to reflect tailored, derived and correlated design requirements • Bidirectional requirements traceability between the draft CDD (or equivalent), the SOW, and the system performance specification has been documented • System performance specification is approved, including stakeholder concurrence, with sufficiently conservative requirements to allow for design trade space
Technical Plans	• Contractor SEMP (or equivalent) is complete and adequate • Cost and critical path drivers have been identified • The program schedule is executable with an acceptable level of technical and cost risk

Product	SRR Criteria
	• Adequate processes and metrics are in place for the program to succeed • SE is properly staffed • Program is executable within the existing budget • Software functionality in the system performance specification is consistent with the software-sizing estimates and the resource-loaded schedule • Programming languages and architectures, security requirements and operational and support concepts have been identified • SS, occupational, and, health hazards, and force protection and survivability (FP&S) domain (i.e., HSI/FP&S) considerations have been reviewed and mitigating measures have been allocated within the overall system design • Hazards have been reviewed as part of the MBCRA with cyberspace threat emulation representatives • Key technology elements have been identified, readiness assessed and maturation plans developed • Software development strategy is complete and adequate • Program technical risks are adequately identified and documented such that there is a clear understanding regarding the contractor's ability to meet the specification requirements • Draft verification methodologies have been adequately defined for each specification requirement • Certifying agencies have been identified and certification requirements are understood • Draft test plans have been developed in support of the TMRR phase (If applicable; See Chief Developmental Tester in T&E Enterprise Guidebook (2022)) • Initial Cyber DT&E Strategy and plan for MBCRA • Government and contractor CM strategies are complete and adequate • The contractor's R&M plans specified in the SOW have been delivered and approved • R&M engineering plans and activities have been integrated into program plans • Planning for creation and/or use of models and simulations has begun and is captured in appropriate program plans. • Planning for the creation of a DE ecosystem has begun and is captured in the SEP and in other appropriate program plans. • The manufacturing and production strategy is complete and adequate • IMS adequately identifies the critical path and is resourced at reasonable levels, based on realistic performance/efficiency expectations • Unique work requirements for risk reduction prototyping and competitive prototyping have been identified • Product support plan and sustainment concepts have been defined with the corresponding metrics • HSI Plan (or equivalent) is complete and adequate, and updated, as appropriate

Outputs and Products

The technical review chair determines when the review is complete. Once the products have been reviewed and approved in SRR, they provide a sound technical basis for proceeding with the system's functional definition and preliminary design.

5.5 System Functional Review

The SFR is held to evaluate whether the functional baseline satisfies the end-user requirements and capability needs and whether functional requirements and verification methods support achievement of performance requirements. At completion of the SFR, the functional baseline is normally taken under configuration control.

The functional baseline describes the system's performance (functional, interoperability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics. The functional baseline is directly traceable to the operational requirements contained in the applicable requirements documents. The PM establishes Government control of the functional baseline at the SFR and verifies it through FCAs leading up to the system-level FCA or the SVR. For additional information, see Section 6.1.6, Configuration Management Process.

A successful SFR reduces the risk of continuing the technical effort toward the PDR. The SFR is used to:

- Assess whether a balanced definition of the system's major elements has been developed, including their functionality and performance requirements with human capabilities and limitations.
- Assess whether the functional baseline is technically achievable with regard to cost, schedule, and performance.
- Confirm that the system performance specification (typically put on contract) is realistic and provides a sound technical foundation for preliminary design.
- Establish functional baseline and verification criteria to be used during FCA.

Roles and Responsibilities

The unique PM responsibilities associated with an SFR include:

- Approving, funding, and staffing the SFR as planned in the SE approach developed by the systems engineer.
- Managing and approving changes to the system performance specification.
- Establishing the plan to PDR in applicable contract documents, including the SEMP, IMS, and IMP (or equivalents).

- Ensuring the plan includes SMEs to participate in each review.
- Controlling the configuration of the Government-controlled subset of the functional baseline.
- Chairing the configuration control board (CCB) for the system performance specification and other documentation used to control the functional baseline.

The unique systems engineer responsibilities associated with an SFR include:

- Ensuring adequate plans are in place to complete the necessary technical activities to proceed from SFR to PDR.
- Ensuring plans to proceed to PDR allow for contingencies.
- Ensuring all performance requirements, both explicit and derived, are defined and bi-directionally traceable between requirements in the draft CDD (or equivalent) and the system performance specification. This would include requirements such as KPPs, KSAs, and other system attributes.
- Ensuring verification methods are identified for all requirements.
- Ensuring risk items associated with functional requirements are identified and analyzed, and mitigation plans are in place.

Inputs and Review Criteria

The SFR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP, or equivalent.

Table 5-3 identifies the products and associated review criteria normally seen as part of the SFR. The chief engineer should review this table and tailor the criteria for the program. The system-level SFR review should not begin until the criteria, identified by the chief engineer and documented in the SEP, are met and any prior technical reviews are complete and their action items closed. If the program's AS includes competing contractual efforts, an SFR should be held with each participating developer. A resource for SFR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-3. SFR Products and Criteria

Product	SFR Criteria
Functional Baseline Documentation/Digital Artifacts	• Understood and assessed to be achievable within cost and schedule constraints • Established functional baseline by mapping system requirements in the system performance specification to lower-level elements and their segment and major subsystem performance specifications • Incorporate task analyses and functional allocations into the functional baseline • Documented performance requirements traced to draft CDD (or equivalent) requirements and reflecting clear linkage to the SoS context(s) (including use in multiple operational environments) • Documented performance requirements reflect design considerations • Documented performance requirements reflect designing for operation in contested cyberspace considerations where appropriate • Documented verification requirements, including testing, for SVR/FCA
Major System Element Definition	• Documented allocated requirements optimized through analyses (including functional analysis and sensitivity analysis), trade studies and risk assessments
Risk Assessment	• Identified and documented risks, including HSI and ESOH mitigation measure requirements • Updated MBCRA
Technical Plans	• Established detailed plan and schedule, sufficiently resourced to continue design and development • Updated design consideration plans and activities have been integrated into the program plan, as appropriate • The contractor R&M plans specified in the SOW have been delivered and approved • Updated R&M engineering plans and activities have been integrated into program plan

Outputs and Products

The technical review chair determines when the review is complete. Once the products have been reviewed and approved in SFR, they provide a sound technical basis for proceeding into preliminary design.

5.6 Preliminary Design Review

The PDR should provide sufficient confidence to proceed with detailed design. The PDR determines whether the preliminary design and basic system architecture are complete, that there is technical confidence the capability need can be satisfied within cost and schedule goals, and

that risks have been identified and mitigation plans established. It also provides the acquisition community, end user, and other stakeholders with an opportunity to understand the trade studies conducted during the preliminary design and thus confirm that design decisions are consistent with the user's performance, schedule needs, and applicable requirements documents. The PDR also establishes the allocated baseline.

The allocated baseline describes the functional and interface requirements to a level in the system architecture sufficient to define hardware configuration item requirements distinct from software configuration item requirements, together with the verification required to demonstrate achievement of those requirements. The allocated baseline for each lower-level system element (hardware and software) is usually established and put under configuration control at the system element PDR. This process is repeated for each system element and culminates in the PM establishing the complete allocated baseline at the system-level PDR. The PM then verifies the allocated baseline at the FCA and/or SVR (see Section 6.1.6, Configuration Management Process).

The timing of the review should consider the following:

- For all AAF pathway programs that are classified as MDAPs, the MDA grants the program Milestone B approval in accordance with 10 USC 4252, "Major Defense Acquisition Programs: Factors to be Considered before Milestone B Approval." This approval requires the conduct and assessment of a PDR, unless waived for national security reasons.
- The timing of the PDR relative to the Development RFP Release Decision Point is at the discretion of the DoW Component and should balance the need for more mature design information with the costs of extending the activities of multiple sources or having a gap in development.

Any tailoring with respect to establishing an allocated baseline at PDR should be consistent with the approved AS and documented in the SEP. In a competitive environment, each developer should establish an allocated baseline to meet the definition prescribed in the RFP and associated system performance specification, consistent with their individual design approach. Since the functional and allocated baselines are critical to providing the system development bidders with a complete technical package, best practices dictate that the PDR be completed before the Development RFP Release Decision Point. The tailoring strategy may also include conduct of a delta-PDR after contract award if the allocated baseline has changed significantly.

A successful PDR confirms that the system's preliminary design:

- Satisfies the operational and suitability requirements of the validated CDD or equivalent, as documented in the system performance specification.
- Is affordable, testable, producible, sustainable, and carries an acceptable level of risk.

- Is composed of technologies demonstrated in a relevant environment that can be integrated into a system with acceptable levels of risk.
- Is complete and ready for detailed design.
- Provides the technical basis for investment decisions and establishing the APB, or equivalent.
- Is fully captured and properly allocated in the specifications for each system element and all interface documentation (including SoS interdependencies).

The PDR establishes the allocated baseline, which is placed under formal configuration control at this point. The allocated baseline is complete when:

- System-level functional and interface requirements have been decomposed and allocated to the lowest level of the specification tree for all system elements (i.e., configuration item level). External interfaces to the system, as addressed at the SRR, have been documented in Interface Control Documents.
- Internal interfaces of the system (system element to system element) have been appropriately documented in accordance with the program's MOSA strategy. Verification requirements to demonstrate achievement of all specified allocated performance characteristics have been documented.
- Design and safety constraints have been captured and incorporated into the requirements and design.

Some of the benefits realized from a PDR with the attributes identified above would be to:

- Establish the technical basis for the CARD or equivalent, documenting all assumptions and rationale needed to support an accurate cost estimate for the APB or equivalent; technically informed cost estimates enable better should-cost/will-cost management.
- Establish the technical requirements for the detailed design, contract specifications and SOW.
- Establish an accurate basis to quantify risk and identify opportunities.
- Provide the technical foundation for Milestone B approval for all MDAPs.

Some design decisions leading up to PDR may precipitate discussions with the operational requirements community because they could have an impact on the CDD (or equivalent), contributing to trade-off analyses. Depending upon the nature or urgency of the capability required and the current state of the technology, incremental development might be required. In this case, the sponsor should document these increments in the CDD (or equivalent), and the PM, systems engineer, and software engineer should update relevant program plans.

Roles and Responsibilities

The PM, systems engineer, and software engineer may hold incremental PDRs for lower-level system elements, culminating with a system-level PDR. The system PDR assesses the preliminary design as captured in system performance specifications for the lower-level system elements; it further ensures that documentation for the preliminary design correctly and completely captures each such specification. The PM, systems engineer, and software engineer evaluate the designs and associated logistics elements to determine whether they correctly and completely implemented all allocated system requirements, and whether they have maintained traceability to the CDD (or equivalent requirements documentation). Although many Service systems commands or PAEs define the roles and responsibilities of the PM, systems engineer, and software engineer, the following notional duties and responsibilities should be considered.

The PM's responsibilities include the following:

- Approving, funding, and staffing the system PDR as planned in the SEP developed by the systems engineer.
- Establishing the plan to Critical Design Review (CDR) in applicable contract documents including the SEMP, IMS, and IMP (or equivalent documentation).
- Ensuring the SEP includes SMEs to participate in each review.
- Reviewing and approving trade-off analyses with SMEs to address design decisions.
- Controlling the configuration of the Government-controlled subset of the functional and allocated baselines; convene Configuration Steering Boards when changes are warranted.

The systems engineer's responsibilities include the following:

- Developing and executing the system PDR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives.
- Ensuring the pre-established PDR criteria have been met.
- Providing industry with an opportunity to participate in this PDR planning (pre-contract award is a best practice, where applicable).
- Ensuring analyses, assessments, and risks associated with all design constraints and considerations are conducted, documented, and provided.
- Updating RIO plans. Identifying, analyzing, mitigating, and monitoring risks and issues; and identifying, analyzing, managing and monitoring opportunities (see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs).
- Monitoring and controlling the execution of the PDR closure plans.
- Documenting the plan to CDR in the SEP and elsewhere as appropriate.

Inputs and Review Criteria

The PDR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP. Table 5-4 identifies the products and associated review criteria normally seen as part of the PDR. The chief engineer should review this table and tailor the criteria for the program. The system-level PDR review should not begin until the criteria, identified by the chief engineer and documented in the SEP, are met and any prior technical reviews are complete and their action items closed. A resource for PDR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-4. PDR Products and Criteria

Product	PDR Criteria
Cost Estimate	- System cost model has been updated, allocated to lower system element levels and tracked against targets; production cost model constructed - Updated CARD, or equivalent, is consistent with the proposed allocated baseline
Risk Assessment	- All risk assessments and risk mitigation plans have been updated, documented, formally addressed and implemented - Approach/Strategy for test and evaluation (T&E) defined in the TEMP, or equivalent, accounts for risks (e.g., SS) risks assessments) with a mitigation plan; necessary integration and test resources are documented within the TEMP and current availability align with the program IMS (SE coordinates with the chief developmental tester in this area; see T&E Enterprise Guidebook (2022)) - HSI and ESOH risks are known and being mitigated - MOSA risks, issues, and opportunities are adequately analyzed, tracked, and mitigated. - Risks are at an acceptable level to continue with detailed design - Unique software risks identified/assessed, and mitigation plans developed and implemented - Updated MBCRA (including results from initial MBCRA), and cybersecurity risks are documented - Diminishing manufacturing sources and material shortages (DMSMS) risks are being evaluated through health assessments and significant risks are being mitigated - Risks associated with intelligence mission data (IMD) dependencies have been identified and addressed; see Section 7.11, Intelligence (Life Cycle Mission Data Plan)
Technical Baseline Documentation/Digital Artifacts (Allocated)	- CDD, or equivalent, is validated by applicable requirements oversight - Analysis of system performance is complete and assessed to meet requirements - Preliminary design satisfies design considerations (see Section 6.2.2, Requirements Analysis Process) - Producibility assessments of key technologies are complete - Preliminary system-level design is producible and assessed to be within the production budget

Product	PDR Criteria
	• Assessment of the technical effort and design indicates potential for operational test and evaluation (OT&E) success (operationally effective and operationally suitable) • SS Engineering Program has been developed. • Hazard Analyses of the Hardware and Software (e.g., System Requirements Hazard Analysis, Preliminary Hazard Analysis, Functional Hazard Analysis, Systems-of-Systems Hazard Analysis) including analysis of technological advances such as autonomy and artificial intelligence are conducted. • Safety risk management and risk assessments are conducted. • Document hazards in the Hazard Tracking System (HTS) • All Critical Safety Items (CSIs) and Critical Application Items (CAIs) are identified • Functional failure mode, effects, and criticality analysis (FMECA) and human reliability analyses are complete • Estimate of system reliability and maintainability updated, based on engineering analyses, initial test results, or other sources of demonstrated reliability and maintainability • Computer system and software architecture designs have been established; all Computer Software Configuration Items (CSCIs), Computer Software Components (CSCs), and Computer Software Units (CSUs) have been defined • Software Requirements Specifications and Interface Requirements Specifications, including verification plans, are complete and baselined for all CSCs and satisfy the functional requirements • Interface Control Documents trace all software interface requirements to the CSCIs, and Computer Software Unit's preliminary software design has been defined and captured • All required software-related documents are baselined and delivered • Allocated baseline documentation is sufficiently complete and correct to enable detailed design to proceed with proper CM • Preliminary design (hardware and software), including interface descriptions (e.g., human-machine interface (HMI)), is complete and satisfies all requirements in the functional baseline • Requirements trace between functional and allocated baselines is complete and consistent • Parts lists have been evaluated for compliance with the Parts Management plan
Technical Plans	• All entrance criteria stated in the contract (e.g., SOW, SEP, approved SEMP, and system performance specification) have been satisfied • Technical plans documented in the SEP, or equivalent, and any additional plans for appropriate design considerations (e.g., R&M, cyber survivability, ESOH, manufacturing, HSI) • DMSMS Management Plan in place and being applied to mitigate DMSMS risk in preliminary designs • Integrating activities of any lower-level PDRs have occurred; identified issues are documented in action plans • Plan to CDR is accurately documented in the SEP as well as the IMP and IMS, or equivalents.

Product	PDR Criteria
	• Program is properly staffed • Technical strategy, tech reviews, and tech baseline identify plans to meet MOSA objectives, which include modularity, open architecture approaches, technology obsolescence/refresh, and the identification of modular system interfaces (MSIs) and open standards to support the incremental addition, modification, or replacement of modular system components. • Stakeholders are able to access needed data within the DE ecosystem to make informed decisions • Adequate processes and metrics are in place for the program to succeed. • MOSA metrics identify how progress will be measured for achieving MOSA objectives (i.e., percentage of components/subsystems modularized, progress toward achieving modular and open architecture-enabled mission-capabilities/objectives, and percentage of mission components successfully integrated to support MOSA implementation). • Program schedule, as depicted in the updated IMS (see Section 6.1.1) is executable within acceptable technical and cost risks • Program is executable with the existing budget and the approved product baseline • Trade studies and system producibility assessments are under way • Majority of manufacturing processes have been defined, characterized, and documented • Logistics (sustainment) and training systems planning and documentation are sufficiently complete to support the review • LCSP, or equivalent, is approved, including updates on program sustainment development efforts and schedules based on current budgets and firm supportability design features • Information Support Plan (ISP) is drafted and scheduled for formal review • LCSP includes software support requirements • Long-lead and key supply chain elements are identified • Computer system and software design/development approach have been confirmed through analyses, demonstrations, and prototyping in a relevant environment • Software increments have been defined and capabilities allocated to specific increments • Software trade studies addressing commercial off-the-shelf (COTS), reuse, and other software-related issues are completed • Software development process is defined in a baselined Software Development Plan (SDP) and reflected in the IMP and IMS, or equivalents. • Software development schedules reflect contractor software processes and IMP/IMS software events for current and future development phases • Software development environment and test/integration labs have been established with sufficient fidelity and capacity • Software metrics have been defined and a reporting process has been implemented; metrics are being tracked and assessed, and stakeholders can access the metrics within the digital ecosystem • The TEMP is drafted, documenting the overall structure and objectives of the T&E program and articulates the necessary resources to accomplish each phase of test. It provides a framework within which to generate detailed T&E

Product	PDR Criteria
	plans (hardware and software) and documents schedule and resource implications associated with the T&E program • Update the Cyber DT&E Strategy (including results from contractor cyber DT&E) • Update the PPP, or equivalent, when preliminary design activities result in new program scope, design, threats, vulnerabilities or protection needs • Software development estimates (i.e., size, effort (cost), and schedule) are updated • SS Program Plan should include the pre-defined Software System Safety (SSS) Level of Rigor task

Outputs and Products

The technical review chair determines when the review is complete. Completion of the PDR establishes that:

- The allocated baseline has been established and placed under configuration control.
- Technical data for the preliminary design are complete, satisfy the system performance specification and provide a sufficient foundation for detailed design to proceed.
- Architectures (functional, logical, and physical) maximize the use of open and consensus-based standards for modular system interfaces supporting mission requirements (including but not limited to mechanical, electrical, thermal, data, control, procedural, and other interactions).
- Descriptions of both software-defined and hardware-defined modular system interfaces are included in interface documentation (e.g., Interface Control Documents, Interface Requirements Specifications, Interface Design Description, APIs, and other relevant interface specifications) with functional descriptions of software-defined interfaces conveying syntax properties and semantic meaning of interface elements in machine-readable definition to support delivered interface and existing common standards or interface repositories) in accordance with 10 USC 4401.
- Risks have been assessed and are acceptable, with any risk mitigation plans approved and documented in the IMS.
- Feasibility, cost, and schedule are determined to be within acceptable risk margins.
- IMS or equivalent is updated (including systems and software critical path drivers) and includes all activities required to complete CDR (assuming same developer responsible for PDR and CDR).
- Corrective action plans for issues identified in the PDR have been completed.

- The Independent Cost Estimate (ICE) (includes CARD or equivalent) is updated and reflects the design in the allocated baseline.
- The LCSP, or program equivalent, is updated to reflect development efforts and schedules.

PDR Assessment

A system-level post-PDR assessment is required for MDAPs per 10 USC 4252. This assessment informs the MDA of the technical risks and the program's readiness to proceed into detailed design, supporting the Milestone B decision point and certification. MDAP PMs should invite the USW(R&E) and DoW Component representatives to their PDRs and make the PDR artifacts available.

The USW(R&E) or DoW Component reviews the conduct of the program's PDR, including system element-level reviews as appropriate, and should provide the MDA with an assessment of the following:

- The conduct and adequacy of the PDR including the participation of stakeholders, technical authorities and SMEs; status of the PDR entrance and exit criteria; open Requests for Action/Information; and closure of the system element and system-level reviews.
- The program technical schedule and SRAs.
- The program's risks, issues and opportunities.
- The establishment and configuration control of the allocated baseline as demonstrated by the completion of the development specifications for each configuration item (CI); internal and external Interface Control Documents; design constraints incorporated into the requirements and design; and system, system elements and CI verification plans.
- The conduct and results of any prototyping and trade studies conducted to reduce technical risk, validate design and assess integration.
- The preliminary design's ability to meet requirement thresholds (e.g., KPPs, KSAs, TPMs) and proposed corrective actions to address any performance gaps, as appropriate.
- Key SE design considerations.

5.7 Critical Design Review

The Critical Design Review (CDR) confirms the system design is stable and is expected to meet system performance requirements, confirms the system is on track to achieve affordability and should-cost goals as evidenced by the detailed design documentation, and establishes the initial product baseline.

The CDR provides stakeholders with evidence that the system, down to the lowest system element level, has a reasonable expectation of satisfying the requirements of the system performance specification as derived from the CDD (or equivalent) within current cost and schedule constraints. At this point in the program, system performance expectations are based on analysis and any prototype testing/demonstration efforts conducted at the system element and/or system level. Demonstration of a complete system is not expected to be accomplished by this point.

The CDR establishes the initial product baseline for the system and its constituent system elements. It also establishes requirements and system interfaces for enabling system elements such as support equipment, training system, maintenance, and data systems. The CDR should establish an accurate basis to assess remaining risk and identify new opportunities. At this point the system design has reached the necessary level of maturity to develop production software, and to start fabricating, integrating, and testing pre-production components and articles with acceptable risk.

The product baseline describes the detailed design for production, fielding/deployment, and operations and support (O&S). The product baseline prescribes all necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. It is traceable to the system performance requirements contained in the CDD, or equivalent. The initial system element product baseline is established and placed under configuration control at the system element CDR and verified later at the Physical Configuration Audit (PCA).

The PM assumes control of the initial product baseline Class I configuration changes from the contractor at the completion of the system-level CDR, as defined in accordance with the program's CM plan. This does not necessarily mean that the PM takes delivery and acceptance of the TDP (for more information, see Section 6.1.6, Configuration Management Process).

Roles and Responsibilities

The systems engineer documents the approach for the CDR in the SEP or equivalent. This includes identification of criteria and artifacts defining the product baseline. The PM reviews and approves the approach, ensures the required resources are available, and recommends review participants.

The PM, systems engineer, and software engineer may hold incremental CDRs for lower-level system elements, culminating with a system-level CDR. The system CDR assesses the final design as captured in system performance specifications for the lower-level system elements. The CDR further ensures that documentation for the detailed design correctly and completely captures each such specification. The PM, systems engineer, and software engineer evaluate the detailed designs and associated logistics elements to determine whether they correctly and completely implement all allocated system requirements, and whether they have maintained traceability to the CDD or equivalent.

The PM's responsibilities include:

- Approving, funding, and staffing the system CDR as planned in the SEP developed by the Systems Engineer.
- Establishing the plan to the SVR in applicable contract documents including the SEMP, IMS, and IMP (or equivalents).
- Ensuring the plan includes SMEs to participate in each review.
- Controlling the configuration of the Government-controlled subset of the functional, allocated and product baselines if applicable; convening Configuration Steering Boards (CSBs) when changes are warranted.

The systems engineer's responsibilities include:

- Developing and executing the system CDR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives.
- Ensuring the pre-established review criteria have been met to ensure the design has been captured in the allocated baseline and initial product baseline.
- Ensuring assessments and risks associated with all design constraints and considerations are conducted, documented and provided.
- Updating RIO plans. Identifying, analyzing, mitigating, and monitoring risks and issues; and identifying, analyzing, managing and monitoring opportunities (see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs). Monitoring and controlling the execution of the CDR closure plans.
- Documenting the plan to SVR in the SEP and elsewhere as appropriate.

Inputs and Review Criteria

The GAO report “Assessments of Selected Weapon Programs” (GAO-12-400SP) suggests a best practice is to achieve design stability at the system-level CDR. A general rule is that 75 to 90 percent of product drawings, software design specification(s) and associated instructions (100 percent for all CSIs and CAIs) should be complete in order to provide tangible evidence of a stable product design. When the design is based on a commercial system or a modification of a current system, drawing metrics should be based on new and revised drawings to minimize risk. The program should assess the incomplete drawings regarding complexity, criticality to system performance, time to complete, and risk to the program. A prototype demonstration shows that the design is capable of meeting performance requirements.

The CDR criteria are developed to best support the program's technical scope and risk and are documented in the program's SE approach or SEP. Table 5-5 identifies the products and associated review criteria normally seen as part of the CDR. In many cases documents and

digital artifacts have been updated from detailed analysis after PDR. The chief engineer should review this table and tailor the criteria for the program. The system-level CDR should not begin until the criteria, identified by the chief engineer and documented in the SEP, are met, any prior technical reviews are complete, and their action items closed. A resource for CDR preparation is ISO/IEC/IEEE 24748-8.

Table 5-5. CDR Products and Criteria

Product	CDR Criteria
Cost Estimate	• Updated ICE and CARD, or equivalents, are consistent with the approved initial product baseline • System production cost model has been updated, allocated to system-element level, and tracked against targets
Technical Baseline Documentation/ Digital Artifacts (Initial Product)	• Detailed design (hardware and software), including interface descriptions (e.g., human-machine interface (HMI)), are complete and satisfy all requirements in the allocated baseline • Requirements trace among functional, allocated, and initial product baselines, if applicable, is complete and consistent • Key product characteristics having the most impact on total system performance, assembly, cost, reliability and sustainment, or ESOH have been identified to support production decisions • Initial product baseline documentation or digital artifacts are sufficiently complete and correct to enable hardware fabrication and production software coding to proceed with proper CM • Assessment of the technical effort and design indicates potential for OT&E success (operationally effective, suitable, survivable) (see T&E Enterprise Guidebook (2022).) • 100% of CSIs and CAIs have completed drawings, specifications and instructions • FMECA and human reliability analyses are complete • Cybersecurity Security Technical Implementation Guides (STIGs) for implementation of controls are identified and referenced. • Estimate of system reliability and maintainability are based on engineering analyses, initial test results, or other sources of demonstrated reliability and maintainability • Detailed design satisfies product support/logistics sustainment and HSI requirements (see HSI Guidebook (2022)) • Software functionality in the approved initial product baseline is consistent with the updated software metrics and resource-loaded schedule • Software and interface documents and digital descriptions are sufficiently complete to support the review • Detailed design is producible and assessed to be within the production budget • Process control plans have been developed for critical manufacturing processes • Critical manufacturing processes that affect the product characteristics have been identified, and the capability to meet design tolerances has been determined • Mechanisms are established through exit criteria for testing, verifying, and validating that system components and selected commercial products conform to specified modular and open standards or interface specifications and demonstrate compliance with MOSA statute (Title 10 Sec. §4401, §4402, and §4403).

Product	CDR Criteria
	• Evaluated DT data, as well as other verification methodologies indicate, with sufficient confidence, that the product baseline configuration attains threshold performance for all KPPs with any shortcomings of KSA attainment identified.
Risk Assessment	• All risk assessments and risk mitigation plans have been updated, documented, formally addressed and implemented • Approach and strategy for T&E defined in the TEMP, or equivalent, accounts for risks with a mitigation plan; necessary integration and test resources for both hardware and software are documented in the TEMP and current availabilities align with the program's IMS (systems engineer coordinates with chief developmental tester in this area; see T&E Enterprise Guidebook (2022)) • Comprehensive Cyber DT&E plan for the Engineering and Manufacturing Development (EMD) phase, including results from all cyber DT&E events to date • Design consideration risks are known and being mitigated • DMSMS risks are being evaluated through health assessments, and significant risks are being mitigated • Risks associated with IMD dependencies have been identified and addressed; see Section 7.11, Intelligence (Life Cycle Mission Data Plan) • An updated MBCRA is completed and identified unacceptable risks mitigated
Technical Plans	• PDR is successfully completed; all PDR actions are closed • Integrating activities of any lower-level CDRs have occurred; identified issues are documented in action plans • All entrance criteria stated in the contract (e.g., SOW), SEP, approved SEMP, and system performance specification), or equivalents, have been satisfied • R&M technical plans have been updated (individual and as part of the Government's SEP and the contractor's SEMP) • Adequate processes and metrics are in place for the program to succeed • Program schedule as depicted in the updated IMS (see Section 6.1.1), or equivalent, is executable (within acceptable technical/cost risks) • Program is properly staffed • Program is executable with the existing budget and the approved initial product baseline • Detailed trade studies and system producibility assessments are under way • Issues cited in the ISP are being satisfactorily addressed • Materials and tooling are available to meet the pilot line schedule • Logistics (sustainment) and training systems planning, documentation, and digital artifacts are sufficiently complete to support the review • LCSP, or equivalent, including updates on program sustainment development efforts and schedules based on current budgets, T&E results and firm supportability design features, is approved • PPP, or equivalent, is updated when critical design activities result in new program scope, design, threats, vulnerabilities, or protection needs • CSS and Security Assessment Plan, or equivalents, are updated, as required • DMSMS Management Plan is in place and being applied to mitigate DMSMS risk in critical designs • Long-lead procurement plans are in place; supply chain assessments are complete

Outputs and Products

The technical review chair determines when the review is complete. Completion of the CDR should provide the following:

- An established initial product baseline.
- Acceptable risks with mitigation plans approved and documented in the IMS, or equivalent.
- Updated CARD (or program equivalent) based on the initial product baseline.
- Updated program development schedule including fabrication, T&E, software coding and critical path drivers.
- Corrective action plans for issues identified in the CDR.
- Updated LCSP, or equivalent, including program sustainment development efforts and schedules based on current budgets, test evaluation results, and firm supportability design features.

Note that baselines for some supporting items might not be detailed and may lag the system-level CDR. Enabling systems may be on different life cycle timelines. The CDR agenda should include a review of all this information, but any statement that all of the detailed design activity on these systems is complete may lead to misunderstandings. As an example, development of simulators and other training systems tends to lag behind system development.

CDR Assessment

This assessment informs the MDA of the technical risks and the program's readiness to proceed. MDAP PMs should invite USW(R&E) and DoW Component representatives to their CDRs and make the CDR artifacts available.

The USW(R&E) or DoW Component reviews the conduct of the program's CDR, including system-element level reviews as appropriate, and provides the MDA with an assessment of the following:

- The conduct and adequacy of the CDR, including the participation of stakeholders, technical authorities, and SMEs; status of the CDR entry and exit criteria; open Requests for Action/Information; and closure of the system elements and system-level reviews.
- The program technical schedule and SRAs.
- The program's risks, issues, and opportunities.

- The establishment and configuration control of the initial product baseline as demonstrated by the completion of build-to documentation for hardware and software configuration items, including production models, drawings, software design specifications, system security controls, materials lists, manufacturing processes, and qualification plans/procedures.
- The design's ability to meet requirement thresholds (such as KPPs, KSAs, and TPMs) and the proposed corrective actions to address any performance gaps, as appropriate.
- Key SE design considerations.

5.8 System Verification Review/Functional Configuration Audit

The SVR is the technical assessment point at which the actual system performance is verified to meet the requirements in the system performance specification and is documented in the functional baseline. The FCA is the technical audit during which the actual performance of a system element is verified and documented to meet the requirements in the system element performance specification in the allocated baseline. Further information on FCA can be found in MIL-HDBK-61B (Configuration Management Guidance). SVR and FCA are sometimes used synonymously when the FCA is at the system level.

When a full system prototype is not part of the program's acquisition strategy, the FCA is used to validate system element functionality. Other system-level analysis is then used to ascertain whether the program risk warrants proceeding to system initial production for OT&E. Verification of system performance is later accomplished on a production system.

A successful SVR/FCA reduces the risk when proceeding into initial production for the system to be used in OT&E. The SVR/FCA is used to:

- Assess whether system development is satisfactorily completed.
- Review the completed documentation or digital artifacts of the verification process for completeness and adequacy.
- Assess the results of developmental test to provide evidence of verification and readiness to proceed to the next phase and OT&E with acceptable risk (see T&E Enterprise Guidebook (2022)).
- Confirm that the product baseline meets the requirements of the functional baseline and therefore has a high likelihood of meeting the warfighter requirements documented in the CDD or equivalent requirements documentation.

Roles and Responsibilities

The unique PM responsibilities associated with an SVR/FCA include:

- Approving, funding, and staffing the SVR/FCA as planned in the SEP developed by the systems engineer.
- Establishing the plan to the PRR in applicable contract documents, including the SEMP, IMS, and IMP.
- Ensuring the SEP includes SMEs to participate in each technical review/audit.
- Continuing to control appropriate changes to the product baseline (see Section 6.1.6, Configuration Management Process).

The unique systems engineer responsibilities associated with an SVR/FCA include:

- Developing and executing the SVR/FCA plans with established quantifiable review criteria, carefully tailored to satisfy program objectives.
- Ensuring the pre-established technical review/audit criteria have been met.
- Ensuring all requirements in the system performance specification have been verified through the appropriate verification method and have been appropriately documented.
- Verifying that CIs and software CIs have achieved the requirements in their specifications.
- Verifying that cybersecurity controls have been implemented as defined in the STIGs.
- Ensuring technical risk items associated with the verified product baseline are identified and analyzed, and mitigation plans are in place.
- Monitoring and controlling the execution of the SVR/FCA closure plans.
- Ensuring adequate plans and resources are in place to accomplish the necessary technical activities between SVR, PRR, and PCA; these plans should allow for contingencies.

Inputs and Review Criteria

The SVR/FCA criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP. Table 5-6 identifies the products and associated review criteria normally seen as part of the SVR/FCA. The systems engineer should review this table and tailor the criteria for the program. The system-level SVR/FCA review should not begin until the criteria, identified by the systems engineer and documented in the SEP, are met and any prior technical reviews are complete and their action items closed. A resource for SVR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-6. SVR/FCA Products and Criteria

Product	SVR/FCA Criteria
Technical Baseline Documentation/Digital Artifacts (Functional and/or Allocated) Verification	• Documented achievement of functional and/or allocated baseline requirements through the appropriate documented verification method (analysis, demonstration, examination, testing or any combination thereof) are reviewed and verified (Note: verification testing may include developmental, operational (e.g., early operational assessments, operational assessments, and/or live-fire testing) • Assessment that the documented product baseline for the initial production system has an acceptable risk of operational test failure during OT&E • R&M performance meets the contractual specification requirements • CDD (or equivalent) R&M requirements are likely to be met
Risk Assessment	• Identified and documented risks (including HSI, cybersecurity, and ESOH) have been accepted at the appropriate management level before initial production for the system to be used in OT&E
Technical Plans	• Detailed plan and schedule have been established and sufficiently resourced to continue development

Outputs and Products

The technical review chair determines when the review is complete. Once the products have been reviewed and approved in SVR/FCA, they provide a sound technical basis for proceeding into initial production for the system to be used in OT&E.

5.9 Production Readiness Review

The PRR determines whether the system design is ready for production, and whether the developer has accomplished adequate production planning for entering Low-Rate Initial Production (LRIP) and Full-Rate Production (FRP). Production readiness increases over time with incremental assessments at various points in the program life cycle.

In the early stages, production readiness assessments should focus on high-level manufacturing concerns such as the need to identify high-risk and low-yield manufacturing processes or materials, or the requirement for manufacturing development efforts to satisfy design requirements. As the system design matures, the assessments should focus on adequate production planning, facilities allocation, producibility changes, identification and fabrication of tools and test equipment, and long-lead items. The system PRR should provide evidence that the system can be produced with acceptable risk and no breaches in cost, schedule, or performance thresholds. The PRR should also consider what production systems should be retained after system deployment to sustain and maintain the system through its life cycle.

For complex systems, a PRR may be conducted for one or more system elements. In addition, periodic production readiness assessments should be conducted during the development phase to

identify and mitigate risks as the design progresses. The incremental reviews lead to an overall system PRR.

Roles and Responsibilities

The unique PM responsibilities associated with a system PRR include:

- Approving, funding, and staffing the PRR as planned in the SEP developed by the systems engineer.
- Establishing the plan to PCA in applicable contract documents, including the SEMP, IMS, and IMP (or equivalents).
- Ensuring the plan includes SMEs to participate in each review.
- Determining if the readiness of manufacturing processes, quality management system (QMS), and production planning (facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.) provide low-risk assurances for supporting LRIP and FRP.
- Continuing to control appropriate changes to the product baseline (see Section 6.1.6, Configuration Management Process).

The unique systems engineer responsibilities associated with a system PRR include:

- Developing and executing the PRR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives.
- Ensuring the pre-established review criteria have been determined so the production capability forms a satisfactory, affordable, and sustainable basis for proceeding into LRIP and FRP.
- Advising the PM on whether production capability forms a satisfactory, affordable, and sustainable basis for proceeding into LRIP and FRP.
- Ensuring adequate plans and resources are in place to proceed from PRR to PCA and FRP Decision Review (DR).
- Ensuring plans to proceed to PCA and FRP DR allow for contingencies.
- Ensuring production implementation supports overall performance and maintainability requirements.
- Monitoring and controlling the execution of the PRR closure plans.

Inputs and Review Criteria

The PRR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP. Table 5-7 identifies the products and associated review

criteria normally seen as part of the PRR. The systems engineer should review this table and tailor the criteria for the program. The system-level PRR review should not begin until the criteria, identified by the systems engineer and documented in the SEP, are met, any prior technical reviews are complete, and their action items closed. A resource for PRR preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-7. PRR Products and Criteria

Product	PRR Criteria
Cost Estimate	• System, as designed, is producible within the production budget • Production cost model is based on the stable detailed design and supply chain, and has been validated
Risk Assessment	• Reliability and maintainability risks are known, and a mitigation plan exists to mitigate those risks. • Producibility trade studies and risk assessments are completed • Manufacturing, production, and quality risks are identified, and a mitigation plan exists to mitigate those risk(s) including the DMSMS risks • HSI and ESOH risks are known and mitigated • Cybersecurity vulnerabilities, threats, and risks have been assessed, prioritized, and mitigated to an acceptable level based on mission-critical requirements and risk tolerance. Processes are in place to continuously monitor, address, and adapt to emerging threats and vulnerabilities.
Technical Baseline Documentation/Digital Artifacts (Product)	• Product baseline is stable and under proper configuration control to enable hardware fabrication in low-rate production • Technologies are mature and proven in the final form, in operational environments • Design is ready for production • Manufacturing processes are stable and have been demonstrated in a pilot line environment • Adequate production line processes and metrics are in place for the delivery of on-time, quality products
Technical Plans	• Prior readiness reviews are completed, and action items closed • Supply chain is stable and adequate to support planned LRIP and FRP • Program is properly staffed with qualified production, quality (engineering and assurance) and manufacturing personnel • Product acceptance system, including acceptance test procedures and associated equipment, has been validated and put under configuration control • LRIP and FRP planning is complete and addresses R&M and quality • Failure Reporting Analysis and Corrective Action System (FRACAS) is in place to track defects and failures (and their resolutions) during and post production • Production facilities are ready and required personnel are trained • Delivery schedule is executable (technical/cost risks, long lead items) • DMSMS management plan is in place and mitigates the risk of obsolescence during LRIP and FRP

A follow-on PRR may be appropriate for Production and Deployment (P&D) for the prime contractor and major subcontractors if:

- Changes in the system design materials and/or manufacturing processes are required.
- Production start-up or re-start occurs after a significant shutdown period.
- Production start-up is with a new contractor.
- The manufacturing site is relocated.

The PRR is designed as a system-level preparation tool and should be used for assessing risk as the system transitions from development to FRP. For more information, see the approaches described in Section 7.14, Manufacturing and Quality.

Outputs and Products

The technical review chair determines when the review is complete. Results of the PRR and associated Manufacturing Readiness Assessments are typically documented in a written report or outbrief. The results should be reported, based on the criteria documented in the SEP, using the PRR checklist. Another source of information is the Manufacturing Readiness Level Deskbook to be used as appropriate.

5.10 Physical Configuration Audit

The PCA is a formal examination of the “as-built” configuration of the system or a configuration item against its technical documentation to establish or verify its product baseline. The objective of the PCA is to resolve any discrepancies between the production-representative item that has successfully passed OT&E and the associated documentation currently under configuration control. A successful PCA provides the MDA with evidence that the product design is stable, the capability meets end-user needs, and production risks are acceptably low. At the conclusion of the PCA, the final product baseline is established, and all subsequent changes are processed by formal engineering change action. Further information can be found in MIL-HDBK-61B (Configuration Management Guidance).

The PCA is an event-driven technical assessment that typically occurs during the P&D phase, after successful system validation but before the FRP DR. A PCA conducted during FRP may miss the opportunity to avoid costly defects built into production. While the system-level PCA typically occurs before the FRP DR, other system element PCAs may be conducted at various points in advance of the system-level PCA.

A properly conducted and documented PCA provides a major knowledge point in preparation for investment decisions at FRP DR. The PCA confirms:

- Any performance deficiencies have been resolved and appropriate changes implemented; changes to the product baseline have been incorporated into current design documentation.
- All production-related activities (tooling, acceptance/inspection equipment, instructions, molds, jigs and make-buy decisions) are focused on a validated and accurate design.
- Any system elements that were affected/redesigned after the completion of the FCA also meet contract requirements.
- All hardware CIs and software CIs are accurately represented by their product baseline information.
- The manufacturing processes, quality control system, measurement and test equipment and training are adequately planned, tracked, and controlled.

Roles and Responsibilities

The unique PM responsibilities associated with a system PCA include:

- Determining the scope of the PCA, including which specific system elements will be audited and to what depth and any associated risk.
- Approving, funding, and staffing the PCA as planned in the SEP developed by the systems engineer.
- Establishing the plan to FRP DR in applicable contract documents, including the SEMP, IMS, and IMP.
- Ensuring the plan includes SMEs to participate in each review.
- Determining if the readiness of manufacturing processes, QMS and production planning (facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.) provide low-risk assurances for supporting FRP.
- Continuing to control appropriate changes to the product baseline (see Section 6.1.6, Configuration Management Process).

The unique systems engineer responsibilities associated with a system PCA include:

- Developing and executing the PCA plans with established quantifiable review criteria, carefully tailored to satisfy program objectives.
- Coordinating with configuration management and manufacturing SMEs and the production contractor/production facility to develop an efficient approach to the PCA.

- Identifying method(s) of examining the production-representative item (e.g., disassembly, inspection and reassembly) and verifying the item against related design documentation or digital artifacts.
- Ensuring the pre-established review criteria have been met so the production capability forms a satisfactory, affordable and sustainable basis for proceeding with FRP.
- Ensuring that for software CIs a detailed audit of design documentation, listings, and O&S documents or digital artifacts are completed.
- Advising the PM on whether production capability forms a satisfactory, affordable, and sustainable basis for proceeding into FRP.
- Ensuring adequate plans and resources are in place to get from PCA to full operational capability.
- Ensuring plans to get to full operational capability allow for contingencies.
- Ensuring production implementation supports overall performance and maintainability requirements.
- Ensuring TDPs have been transferred to the Government in accordance with the contract.
- Monitoring and controlling the execution of the PCA closure plans.
- Identifying risks associated with meeting program objectives, given the proposed PCA plans.

When the program does not plan to control the detailed design or purchase the item's technical data, the developer should conduct an internal PCA to define the starting point for controlling the detailed design of the item and establishing a product baseline.

Inputs and Audit Criteria

The PCA criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP (no later than Milestone C for programs in the MCA pathway). The PCA is conducted when these criteria are considered to be met.

Table 5-8 identifies the products and associated review criteria normally seen as part of the PCA. The systems engineer should review this table and tailor the criteria for the program. The system-level PCA review should not begin until the criteria, identified by the systems engineer and documented in the SEP, are met and any prior technical reviews are complete and their action items closed. A resource for PCA preparation is ISO/IEC/IEEE 24748-8. This is a best practice review.

Table 5-8. PCA Products and Criteria

Product	PCA Criteria
Product Baseline Documentation/ Digital Artifacts	Assessment that the product baseline is complete and accurately reflects the configuration of the representative production item that was inspected and validated through OT&E
Risk Assessment	Risks are identified and documented at levels low enough to continue with FRP and deployment
Technical Plans	- A detailed plan and schedule are established and sufficiently resourced to proceed with FRP and deployment - Achieved design levels of R&M are sufficient to be retained through production, deployment, and operations, and essential activities will be used to identify, analyze, and correct deficiencies during FRP

Outputs and Products

The technical review chair determines when the review is complete. The primary output of the PCA is a verified product baseline that accurately reflects the validated system and supports a favorable FRP DR.

6 SYSTEMS ENGINEERING PROCESSES

The SE processes are used by contractor and Government organizations to provide a framework and methodology to plan, manage and implement technical activities throughout the acquisition life cycle. SE planning and execution should focus on applying the processes and tools in a rigorous, integrated, and disciplined manner to achieve a system solution that balances performance, cost, schedule, and risk.

While rigorous application of SE processes remains essential for ensuring technical integrity, balancing this rigor with the imperative for rapid deployment of needed military capabilities is paramount. Programs should strive to optimize the application of SE processes, focusing on value-added activities and leveraging modern tools and techniques to accelerate development and delivery without compromising essential quality and safety standards. This requires a flexible and adaptive approach, tailoring the depth and breadth of SE activities to the specific program context and risk profile, with a constant awareness of the need to deliver capability to the warfighter in a timely manner.

The eight Technical Management Processes, applicable to all acquisition pathways, provide a consistent framework for managing technical activities and identifying the technical information and events critical to the success of the program. Technical information includes controlled unclassified information (CUI) as well as classified and unclassified critical technical information about DoW-sponsored research, technology, programs, and systems being acquired. The eight Technical Processes ensure the system design and the delivered capability reflect the requirements that the stakeholders have expressed. The 16 SE processes are applicable to all the AAF pathways to some degree. The PM and SE will determine which processes to implement and manage for their program.

As mentioned in Section 5, Technical Reviews and Audits, regardless of acquisition pathway, the ability to conduct needed supporting analyses can be influenced by the extent to which the program adopts a DE approach (as described more fully in Section 3.3, Digital Engineering). DE will not affect “what” SE processes need to be followed, but, as with technical reviews and audits, it can have an important impact on “how” the processes are conducted. A well-defined and instantiated digital ecosystem typically will have wide applicability in support of the eight Technical Processes.

As a whole, the SE processes provide a systematic approach focused on providing needed capability to the operational end user. Successful implementation of the SE processes results in an integrated capability solution that is:

- Responsive to the needs of the end user.
- Balanced among multiple requirements, design considerations, and program costs and schedules.
- Able to operate in complex SoS environments as required.

All organizations performing SE should scale their application, based on selected acquisition pathway and use of these processes, to the type of product or system being developed. This scaling should reflect the system's maturity and complexity, size and scope, life cycle phase, and other relevant considerations. Disciplined application of the SE processes provides a technical framework that enables sound decision making, increases product knowledge, and helps reduce risk. This ultimately leads to the rapid delivery of effective defense systems to the warfighter, ensuring continued technological advantage over potential adversaries. Table 6-1 lists the processes, discussed in detail in the sections indicated.

Table 6-1. SE Processes

Technical Management Processes	Technical Processes
Technical Planning (Section 6.1.1)	Stakeholder Requirements Definition (Section 6.2.1.)
Decision Analysis (Section 6.1.2)	Requirements Analysis (Section 6.2.2)
Technical Assessment (Section 6.1.3)	Architecture Design (Section 6.2.3)
Requirements Management (Section 6.1.4)	Implementation (Section 6.2.4)
Risk Management (Section 6.1.5)	Integration (Section 6.2.5)
Configuration Management (Section 6.1.6)	Verification (Section 6.2.6)
Technical Data Management (Section 6.1.7)	Validation (Section 6.2.7)
Interface Management (Section 6.1.8.)	Transition (Section 6.2.8)

Industry SE standards that describe best practices in accomplishing SE include, but are not limited to, the following:

- ISO/IEC/IEEE 15288, Systems and Software Engineering–System Life Cycle Processes
- ISO/IEC/IEEE 24748-7, Systems and Software Engineering–Life Cycle Management, Part 7: Application of Systems Engineering on Defense Programs

ISO/IEC/IEEE 15288 is an NGS, developed jointly by SE stakeholders in industry, Government, and academia, that establishes a common process framework for describing the life cycle of man-made systems. The standard defines a set of SE processes and associated terminology for the full-system life cycle, including conception, development, production, use, support, and retirement. In addition, the Government-initiated NGS, ISO/IEC/IEEE 24748-7, expands on the SE life cycle processes of ISO/IEC/IEEE 15288 with additional detail specific to DoW acquisition projects. ISO/IEC/IEEE 24748-7 also adds requirements for SE outputs and the attributes (criteria) for each process.

The DoW has adopted both ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 24748-7. Adoption expresses formal acceptance of an NGS for use in direct procurement, as a reference in another document or as guidance in the design, manufacturing, testing, or support of materiel. An adopted NGS is not a mandatory document; it is deemed appropriate for use by DoW organizations. Therefore, it is up to each PMO to determine if and how these standards should be used to support a particular project. If a PMO chooses to use ISO/IEC/IEEE 15288 and 24748-7,

additional guidance for implementing the DoW-adopted SE standards on acquisition program contracts can be found in the guidance document, “Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288 Series) on Contracts for Department of Defense Acquisition Programs” (2017).

Although there is no one-to-one mapping between the SE processes in the ISO/IEC/IEEE 15288 and the SE Guidebook, the documents convey similar SE information. Table 6-2 shows how the SE Guidebook SE processes or activities map to the ISO/IEC/IEEE 15288 processes. The table does not cover the ISO/IEC/IEEE 15288 Agreement and Organizational project-enabling processes because, while important, these processes were developed by ISO/IEC/IEEE and are outside the scope of the SE processes covered in this guide. The PM and systems engineer are encouraged to examine and adopt these processes for use in their program, as appropriate.

Table 6-2. SE Processes/Activities Mapped to ISO/IEC/IEEE 15288 SE Processes

	DoW SE Processes (SE Guidebook Section)	ISO/IEC/IEEE 15288 Processes (Clause)
TECHNICAL MGMT PROCESSES	Technical Planning (6.1.1)	Project Planning (6.3.1)
	Decision Analysis (6.1.2)	Decision Management (6.3.3)
	Technical Assessment (6.1.3)	Project Assessment and Control (6.3.2)
		Measurement (6.3.7)
	Requirements Management (6.1.4)*	System Requirements Definition (6.4.3)
	Risk Management (6.1.5)	Risk Management (6.3.4)
	Configuration Management (6.1.6)	Configuration Management (6.3.5)
	Technical Data Management (6.1.7)	Information Management (6.3.6)
	Interface Management (6.1.8)	System Architecture Definition (6.4.4)
	<i>Covered by Section 7.14.4, Manufacturing and Quality; and DoD Producibility and Manufacturability Engineering Guide (2024)</i>	Quality Assurance (6.3.8)
TECHNICAL PROCESSES	<i>Covered by Sections 2, System-Level Considerations, and 3.4, Mission Engineering</i>	Business or Mission Analysis (6.4.1)
	Stakeholder Requirements Definition (6.2.1)	Stakeholder Needs and Requirements Definition (6.4.2)
	Requirements Analysis (6.2.2)*	System Requirements Definition (6.4.3)
	Architecture Design (6.2.3)	System Architecture Definition (6.4.4)
	Implementation (6.2.4)	Design Definition (6.4.5)
		Implementation (6.4.7)
	<i>Covered throughout Sections 5, Technical Reviews and Audits, and 7, Design Considerations</i>	System Analysis (6.4.6)

	DoW SE Processes (SE Guidebook Section)	ISO/IEC/IEEE 15288 Processes (Clause)
	Integration (6.2.5)	Integration (6.4.8)
	Verification (6.2.6)	Verification (6.4.9)
	Validation (6.2.7)	Validation (6.4.11)
	Transition (6.2.8)	Transition (6.4.10)
	<i>Covered by the Product Support Management Guidebook and Life Cycle Sustainment Plan Outline</i>	Operation (6.4.12)
	<i>Covered by the Product Support Management Guidebook and Life Cycle Sustainment Plan Outline</i>	Maintenance (6.4.13)
	<i>Covered by Section 7.7, Demilitarization and Disposal, and Life Cycle Sustainment Guidebook</i>	Disposal (6.4.14)
*Requirements Management and Requirements Analysis processes are covered by ISO/IEC/IEEE 15288–System Requirements Definition		

Roles, Responsibilities, and Activities

The PM, systems engineer, and software engineer use, depending on the chosen acquisition pathway, the Technical Management Processes as insight and control functions for the overall technical development of the system throughout the acquisition life cycle. They use the Technical Processes to design, create, and analyze the system, system elements, and enabling system elements required for production, integration, test, deployment, support, operation, and disposal.

The SE processes, and their constituent activities and tasks, are not meant to be performed in a particular time-dependent or serial sequence. The PM, systems engineer, and software engineer apply the processes iteratively, recursively, and in parallel (as applicable) throughout the life cycle to translate identified capability needs into balanced and integrated system solutions. The systems engineer is responsible for developing the plan and applying the SE processes across the program, monitoring execution throughout the life cycle, and taking necessary steps to improve process efficiency and effectiveness.

Figure 6-1 is a representation of how much effort programs typically focus on each of the SE processes throughout the MCA life cycle. The PM, systems engineer, and software engineer should apply appropriate resources with the requisite skill sets to ensure successful execution of each process.

Legend							
● = Major Use ◉ = Moderate Use ○ = Minor Use		Pre-MDD	MSA	TMRR	EMD	P&D	O&S
TECHNICAL MANAGEMENT PROCESSES	Decision Analysis	●	●	●	●	●	●
	Technical Planning	●	●	●	●	●	●
	Technical Assessment	◉	●	●	●	●	●
	Requirements Management	◉	●	●	●	●	●
	Risk & Opportunity Management	◉	●	●	●	●	●
	Configuration Management	○	◉	●	●	●	●
	Technical Data Management	○	●	●	●	●	●
	Interface Management	◉	●	●	●	●	●
TECHNICAL PROCESSES	Stakeholder Requirements Definition	◉	●	●	◉	○	○
	Requirements Analysis	◉	●	●	●	○	○
	Architecture Design	◉	●	●	●	○	○
	Implementation	○	◉	◉	●	◉	○
	Integration	○	◉	◉	●	●	○
	Verification	○	◉	◉	●	●	◉
	Validation	○	◉	◉	●	●	●
	Transition	○	○	◉	●	●	●

Figure 6-1. Notional Emphasis of SE Processes during the Major Capability Acquisition Life Cycle

6.1 Technical Management Processes

DoW SE consists of eight Technical Management Processes. These foundational, enabling processes are used consistently throughout the system life cycle to help manage the system development. Sections 6.1.1 through 6.1.8 describe the Technical Management Processes.

6.1.1 Technical Planning Process

The Technical Planning process provides a framework to define the scope of the technical effort required to develop, deploy, and sustain the system and provides critical quantitative input to program planning and life cycle cost estimates. Technical planning provides the PM, systems engineer, and software engineer with a framework to accomplish the technical activities that collectively increase product maturity and knowledge and reduce technical risks. Technical planning should anticipate the evolution of capabilities to meet changing threats, human performance requirements, technology insertion, and interoperability. Defining the scope of the technical effort provides:

- An accurate basis for program cost and schedule estimates, documented in the ICE, CARD, and APB, or equivalent documentation.
- A foundation for risk identification and management (see Section 6.1.5, Risk Management Process).
- Quantitative measures supporting the Technical Assessment process (see Section 6.1.3).
- An accurately constructed and resourced IMS supporting the assignment of earned value.

The resulting program cost estimates and risk assessments are essential to support program milestones or decisions. They allow the program to establish the plan to accomplish work against which contract performance is measured.

Technical planning includes the program's plan for technical reviews and audits (see Section 5). It should also account for resources (skilled workforce, support equipment/tools, facilities, etc.) necessary to develop, test, produce, deploy, and sustain the system.

Technical planning should be performed in conjunction with, and address, elements and products governing other SE processes to ensure the program's technical plan is comprehensive and coherent. For example, it should be used with the Technical Assessment process to evaluate the progress and achievements against requirements, plans, and overall program objectives. If significant variances are detected, this process includes appropriate replanning.

The PM, systems engineer, and software engineer should ensure technical planning remains current throughout the acquisition life cycle. They should initiate technical planning activities early in the life cycle before the MDD. Technical planning leverages the CONOPS/OMS/MP and mission analysis, or equivalent. The CONOPS/OMS/MP is a document consistent with the validated or approved capability requirements document, including operational tasks, events, durations, frequency, operating conditions, and environments under which the recommended materiel solution is to perform each mission and each phase of a mission. Mission analysis includes affected operational missions and phases (including degraded modes of operation), where system missions are analyzed and human/machine factors necessary to achieve performance requirements are assessed, and any lessons learned from legacy systems and mission-essential task lists are reviewed.

As the system matures and issues arise throughout the life cycle, the PM, systems engineer, and software engineer should consistently look for root cause(s) and implement corrective actions to enable programmatic and technical success. They may need to modify the SE processes and the SEP (or equivalent) to address the root causes.

Activities and Products

The PM is ultimately responsible for the development, management, and execution of all program plans. The systems engineer is responsible for:

- Developing, maintaining, and executing the program's SEP.
- Tracking alignment of the contractor's SEMP.
- Providing technical input and ensuring the SEP aligns with other program plans (e.g., AS, TEMP, LCSP, DoW Security Requirements Guides (SRGs) and DoW STIGs, and Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE), or equivalent documentation.

Technical planning should reflect the context of the organization and should comply with all applicable policies. The PM, systems engineer, and software engineer should consider all relevant constraints when identifying technical tasks, sequencing these tasks, and estimating resources and budgets. Inputs to the technical planning process vary over time as the program evolves and the system matures. Technical planning includes the following activities:

- Define the scope and objectives of the technical effort, including the performance evolution of system capabilities.
- Identify constraints and risks.
- Establish roles and responsibilities.
- Divide the program scope and objective into discrete elements.
- Identify technical reviews and audits as well as their timing.
- Establish schedules and costs.
- Prepare or update planning documentation.
- Scale SE processes based on the scope and complexity of the program or system.
- Identify areas for potential tailoring (including rationale) for MDA/DA, or equivalent, approval.

Key factors that the systems engineer should consider when accomplishing technical planning include the following:

- Capability needs (requirements, gaps, threats, operational context, CONOPS/OMS/MP, TAD).
- The system concept or materiel solution.
- Key interfaces and interdependencies that exist or need to be developed.
- The acquisition approach and strategy, from both a business and a contract perspective.
- The chosen SE approach, including design considerations, and development strategy, including modularity and standard interfaces in product designs where feasible and cost-effective.

- The strategy and approach for T&E, for both developmental and operational testing (see T&E Enterprise Guidebook (2022) for additional information regarding interactions with the chief developmental tester).
- Manufacturing and quality planning.
- Program management approach, including organization, processes and products.
- External dependencies and agreements with other systems or organizations that may be in place.
- Need date.
- Availability of resources, including funds, personnel, facilities, etc.
- Program risks.
- Risk management strategies.

In addition to the SEP, the technical planning effort supports the development of the following documents or digital artifacts, or their equivalents:

- WBS – a framework for specifying program objectives.
- IMP – an event-based plan consisting of a hierarchy of program events that need to be accomplished.
- IMS – an integrated, networked schedule that contains all lower-level tasks required to support program events.

Other useful resources available to assist the PM, systems engineer, and software engineer in the Technical Planning process can be found at the OUSW(R&E) SE&A website (<https://www.cto.mil/sea>).

Work Breakdown Structure

The Work Breakdown Structure (WBS) represents the decomposition of the scope of work and defines the hierarchically-related, product-oriented elements necessary to accomplish program objectives and develop required deliverables or populate the digital ecosystem. It provides a product-oriented division of tasks by breaking down work scope for authorizing, tracking, and reporting purposes. The WBS is defined, developed, and maintained throughout the acquisition life cycle based on a disciplined application of the SE process. The goal is to develop a structure that defines the logical relationship among all program elements to a specified level of indenture. Requirements for developing a WBS can be found in MIL-STD-881 (Work Breakdown Structures for Defense Materiel Items).

The WBS integrates technical, cost, and schedule parameters, giving the PM a tool to:

- Ensure the traceability of all program activities.

- Identify significant risk drivers.
- Forecast cost and schedule performance.
- Develop corrective action plans as needed.

An effective WBS takes into consideration several things. It should encompass the work defined by the project scope, and capture Government and contractor deliverables to provide adequate insight for effective program management. Keeping in mind that the definition of scope between elements should not overlap, a WBS dictionary should be created to clarify distinctions among all elements. These elements also should be defined in terms of outcomes, not actions, as decomposing planned outcomes to the desired end of the program provides a more accurate measure of cost, schedule, and technical progress.

There are two types of WBS: (1) the Program WBS; and (2) the Contract WBS (including flow-down reporting requirements). The Program WBS provides a framework for specifying program objectives. Each WBS element provides logical summary levels for assessing technical accomplishments, supporting the required event-based technical reviews, and measuring cost and schedule performance. It represents the entire program from the Government PM's responsibility, including elements such as program office operations, manpower, Government-furnished equipment (GFE), and Government testing. A program WBS is typically defined to level 3 or level 4 of indenture to provide a summary level, or starting point, for the Contract WBS that does not constrain the contractor in developing the program; however, the Program WBS may be defined to a lower level of indenture if the Government considers certain elements as high-cost, high-risk, or high-interest. If the program is implementing a DE approach, the program should consider the level of data access needed and may need to create a lower level of indenture to support technical reviews, sustainment planning, and support, etc.

The Contract WBS, of which there may be several for a single program, governs the elements of a specific contract. It is the Government-approved WBS for program reporting purposes that represents an agreement between the Government and contractor addressing the expected hierarchy of outcomes at a level that can be analyzed and assessed, and incorporates all program elements, such as hardware, software, services, data, and facilities, which are the contractor's responsibility. This includes the contractor's discretionary extension to lower levels, in accordance with Government direction and the contract SOW. The Contract WBS usually requires a contract modification before approved changes can be incorporated. If the WBS is revised, the contractor should maintain traceability to the previous version.

The WBS displays and defines the program and product, or products, to be developed or produced and provides a common thread for the Earned Value Management System (EVMS), the IMP, and the IMS to better communicate program cost and schedule performance. The PM, in conjunction with the systems engineer, should develop a comprehensive WBS early in the program to support planning, cost, and schedule estimation and risk management activities.

Additional information about EVMS can be found in the DoD Earned Value Management System Interpretation Guide (2019).

A WBS serves as the basis for mapping development of the technical baseline and aids the PM in estimating and scheduling resource requirements (people, facilities, and equipment). By breaking the system into successively smaller pieces, the PM ensures system elements and enabling system elements are identified in terms of cost, schedule, and performance goals, thereby reducing overall program risk in the process.

Integrated Master Plan

The IMP is a high-level, event-driven, schedule and planning document that outlines the events, significant accomplishments, and accomplishment criteria needed for successful program completion. The IMP should document the tasks required to define, develop, and deliver a system and to facilitate operation and support of that system throughout its life cycle. As a top-level document, the IMP should encompass all IPT and WBS elements. It should also depict the hierarchy of program activities and relate each major program event to supporting events.

In an environment of competitive contracts, the successful offeror's IMP should be included in the resulting contract for use in execution of the program. As a result, the IMP becomes a contractual document and forms the basis for schedule execution.

Integrated Master Schedule

The IMS is a low-level, event-driven, calendar-based schedule and planning document that describes the entire scope of work, including all Government, contractor, and subcontractor activities necessary for successful program execution, from start to finish. It is a logical extension of the IMP, depicting the scope of work as an integrated hierarchy of milestones, tasks, subtasks, activities, and deliverables. It should also describe the work required to complete the effort in sufficient detail, including start date, event duration, and finish date for all activities, to organize the overall hierarchical flow of work. This assists the PM in comprehending the links and relationships among various activities, including the resources supporting them.

Together, the PM, systems engineer, and software engineer should monitor development of the IMS to ensure that activity durations and resources are reasonable. This oversight aids analysis of program risks and development of mitigation plans in the event that any of those activities become delayed or over budget. As such, the IMS serves as a tool for time-phasing work, assessing technical performance, and once baselined, forms the framework for EVMS. IMS activities should be directly traceable to the IMP and the WBS, and together allow integrated assessments of cost, schedule, and technical performance, along with associated risks.

For effective program insight, management, and control, an IMS should:

- Establish a schedule with baseline start and finish dates.

- Identify critical path, milestones, and activities.
- Indicate significant constraints and relationships.
- Provide status and forecast completion dates of scheduled work to enable comparison of planned and actual program accomplishments.
- Provide horizontal traceability of interrelationships among activities.
- Provide interdependent sequencing of all work authorized on the contract in a manner compatible with the SOW, WBS, IMP events, and acquisition milestones.

Figure 6-2 depicts a hierarchical approach to developing and populating the IMS. The PM should review the IMS for completeness, consistency, and compatibility on a routine basis. During these reviews, the PM should evaluate logic relationships and event durations to ensure they align with program goals, identify and account for risk, and plan for desired mitigation. The PM, systems engineer, and software engineer should ensure that the SEP and other technical planning documents capture technical review criteria, event-driven outcomes, and mechanisms for assessing technical maturity and risk in a manner consistent with the tasks and schedules delineated in the IMS.

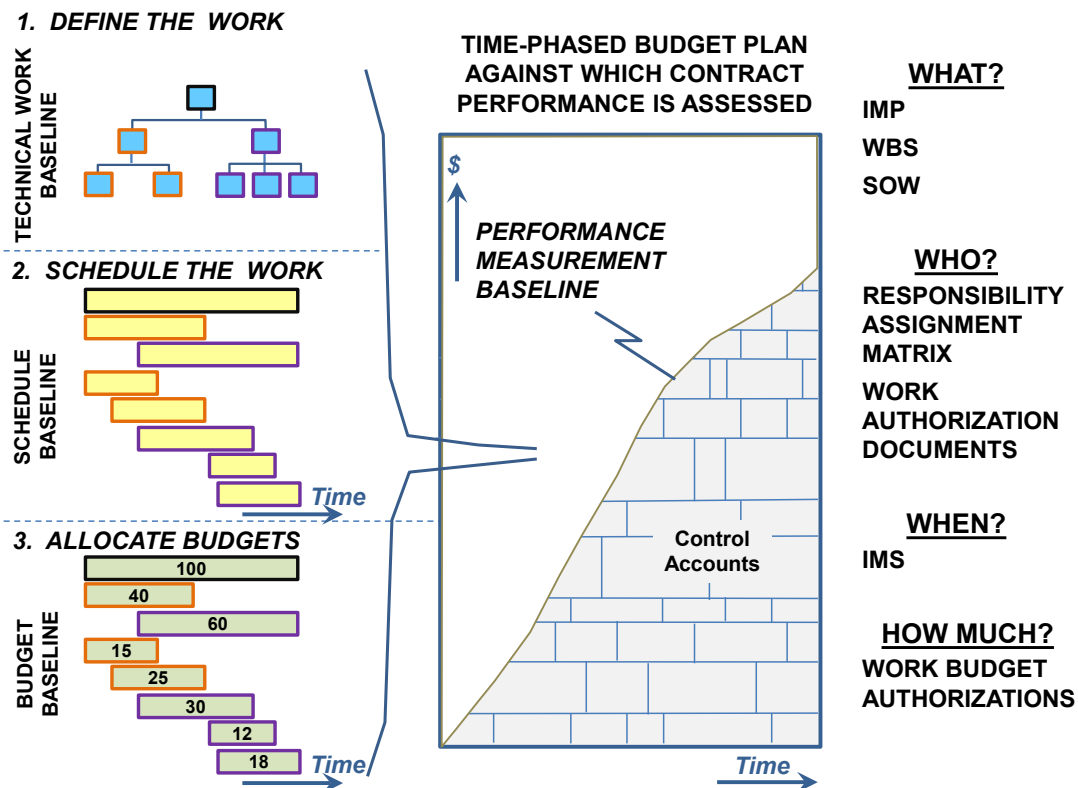


Figure 6-2. IMP/IMS Hierarchy and Content

It may be helpful to view the IMS as a collection of subordinate, interrelated schedules. In alignment with the WBS, the IMS has both a higher-level component, focused on Government

events and activities, and a lower-level component, detailing elements for contracted activities and tasks. Consistent and in alignment with the Government-approved IMP, the IMS is baselined after approval of the contractor(s)' schedules at the Integrated Baseline Review (IBR).

For major acquisition programs, the IBR is typically conducted within 6 months after the contract award to facilitate an understanding and agreement of the detail needed to manage the effort. Once the IBR is complete and the baseline IMS is established, the change management process should be implemented to approve subsequent modifications to the IMS. Contractor IMS submissions to the program office should comply with DI-MGMT-81861 (Integrated Program Management Data and Analysis Report), with each submission updated to reflect actual start and actual finish of activities, to date.

Early identification of, and adherence to, critical path tasks is essential to ensure the program remains on track toward achieving schedule and cost goals. The IMS provides linkages between tasks to capture the relationship of predecessor and successor tasks required to initiate or complete major tasks. It facilitates stakeholder communication by establishing expectations and dependencies, particularly for tasks performed by different organizations, and identifies all risk mitigation activities. The IMS helps the PM, systems engineer, and software engineer:

- Identify a baseline for program monitoring, reporting, and control.
- Plan, execute, and track risk mitigation efforts.
- Support resource analysis and leveling, exploration of alternatives, and cost/schedule trade-off studies.
- Provide a roadmap for stakeholders.
- The IMP and IMS Preparation and Use Guide provides additional guidance on developing and implementing these technical planning tools.

For more information, see the Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide (2023).

Schedule Risk Assessments

A Schedule Risk Assessment (SRA) predicts the completion date of a target milestone or program event by assigning a best, worst, and most likely outcome to each task for that event. By quantitatively assigning risk to each event in the baseline schedule and identifying the potential impact of uncertainty in meeting program completion, an SRA can help the PM determine the likelihood of an acquisition program meeting its proposed deadlines by evaluating schedule risks and applying estimated duration ranges. It is a best practice to conduct an SRA annually.

Monte Carlo is one technique to generate multiple runs simulating project progress. It performs an SRA against a baseline program plan for all non-summary, non-milestone tasks (see Figure 6-3). Each simulation run generates a duration for every project activity, given an uncertainty

profile previously defined by the contractor. The quality of the assessment depends on the quality of the input data. Knowledge about the potential impact of these estimation errors should be tracked in the project risk register or within the IMS (see Section 6.1.5, Risk Management Process).

When part of the contract, the DI-MGMT-81861 specifies when SRAs should be performed. Contractors and subcontractors should perform an SRA on their schedule before an IBR, before processing an Over Target Baseline/Over Target Schedule, or as required by the contract. The results from an SRA inform management decisions, support what-if scenarios, and provide input for mitigating risk.

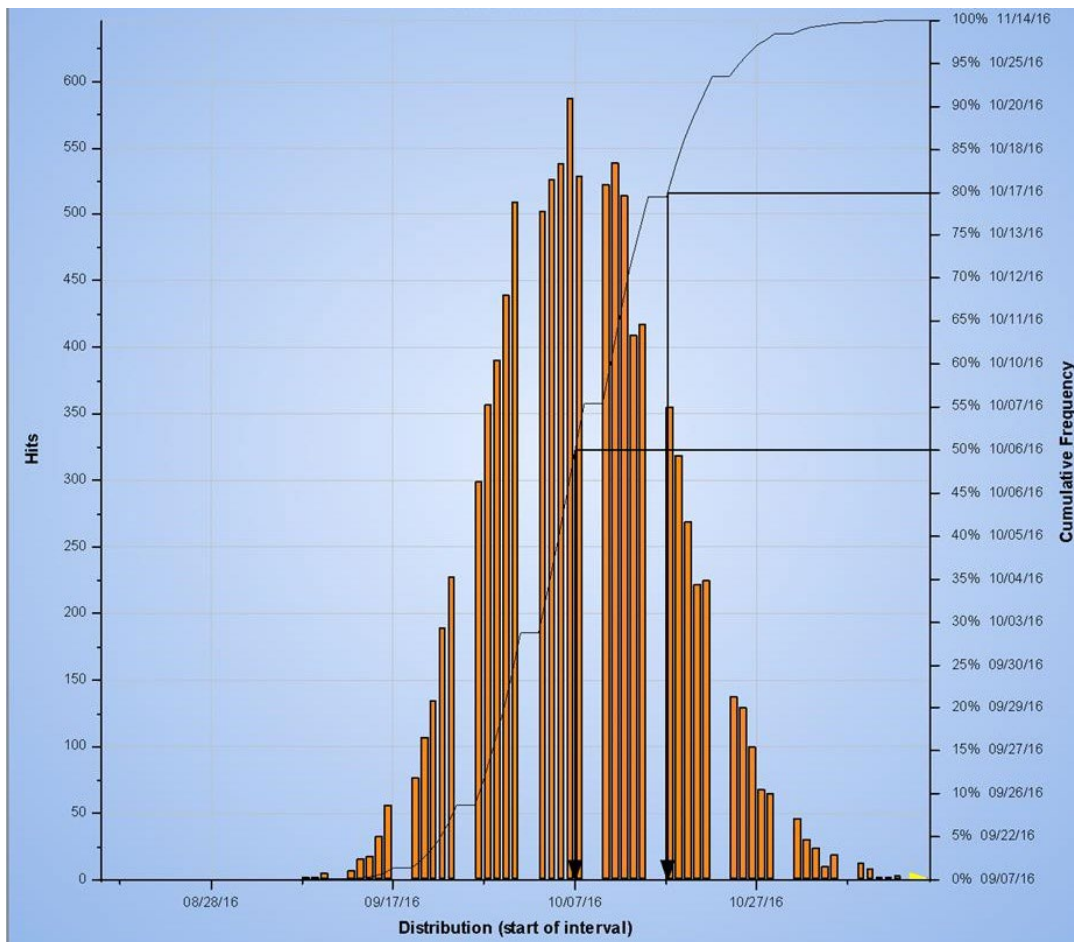


Figure 6-3. Schedule Risk Assessment Histogram

6.1.2 Decision Analysis Process

The Decision Analysis process transforms a broadly stated decision opportunity into a traceable, defensible, and actionable plan. It encompasses one or more discrete analyses at one or more lower (e.g., system element) levels and aggregates them into a higher-level view (e.g., system “scorecard” presentation) relevant to the decision maker and other stakeholders. Decision

analysis can be the central process for formulating, managing, and executing an effective and efficient program at any point in the life cycle.

Decision analysis and associated trade studies should be integrated with, and mutually supportive of, aspects of several SE processes in the early stages of the program, in particular:

- Technical Planning (see Section 6.1.1)
- Technical Assessment (see Section 6.1.3)
- Stakeholder Requirements Definition (see Section 6.2.1)
- Requirements Analysis (see Section 6.2.2)
- Architecture Design (see Section 6.2.3)

A well-executed decision analysis or trade-off analysis helps the PM and the systems engineer understand the impact of various uncertainties, identify one or more course(s) of action that balance competing objectives, and objectively communicate the results to decision makers. As such, it provides the basis for selecting a viable and effective alternative from among many under consideration. This analysis should explicitly reference alignment with RRAB prioritization cycles and JFRC KOP rankings.

Decision analysis applies to technical decisions at all levels, from evaluating top-level architectural concepts to sizing major system elements to selecting small design details. The breadth and depth of the analysis should be scaled to both the scope of the decision and the needs and expectations of the decision maker(s).

Activities and Products

Decision analysis teams generally include a lead analyst with a suite of reasoning tools, SMEs with access to appropriate models and analytical tools, and a representative set of end users and other stakeholders. A robust Decision Analysis process acknowledges that the decision maker has full responsibility, authority, and accountability for the decision at hand.

Decision analysis typically includes the following steps:

- Identifying the problem or issue.
- Reviewing requirements and assumptions to establish the overall decision context.
- Framing/structuring the decision in terms of supporting program/project objectives.
- Identifying methods and tools to be used in the analyses (see Section 3, SE Modernization).
- Developing decision criteria (objectives and measures), criteria weight, and associated rationale.

- Identifying, recording, and tracking assumptions.
- Identifying and defining alternatives to be evaluated (for high-level analyses, these are generally directed, although additional ones may arise during the course of the analysis).
- Analyzing and assessing alternatives against criteria.
- Synthesizing results.
- Analyzing sensitivities.
- Developing decision briefing with action/implementation plan(s).
- Making appropriate recommendation(s) to decision maker as expected/requested.

Sound recommendations and action plans are the principal output of a well-framed and well-executed Decision Analysis process. The ability to drill down quickly from overall trade-space visualizations to detailed analyses that support the synthesized views is particularly useful to decision makers in understanding the basis of observations and conclusions.

6.1.3 Technical Assessment Process

The Technical Assessment process provides a fact-based understanding of the current level of product knowledge, technical maturity, program status, and technical risk by comparing assessment results against defined criteria. These assessment results enable a better understanding of the health and maturity of the program, giving the PM a sound technical basis upon which to make program decisions.

Disciplined technical assessment activities begin early in a system's life cycle by examining the status of development planning activities. During system development, technical assessments provide a basis for tracking development of the system and lower-level system element designs. Disciplined technical assessments support the establishment of the various baselines and achievement of system verification. Technical assessment activities continue into manufacturing and production and continue through O&S to support reliability growth and sustainment engineering efforts.

The PM, systems engineer, software engineer, and technical management team evaluate technical maturity in support of program decisions at event-driven technical reviews and audits (see Section 5, Technical Reviews and Audits) that occur throughout the acquisition life cycle. The PM, systems engineer, and software engineer use various measures and metrics, including TPM and leading indicators, to gauge technical progress against planned goals, objectives, and requirements. (See Technical Performance Measures, below, for more information.)

Technical assessments against agreed-upon measures enable data-driven decisions. Evidence-based evaluations that communicate progress and technical risk are essential for the PM to determine the need for revised program plans or technical risk mitigation actions throughout the acquisition life cycle.

Technical assessment provides:

- An evaluation of the program's technical progress measured against the expected or planned performance for that period of time.
- An objective means of identifying, quantifying, and monitoring a system's technical risks.
- A rigorous method to help define corrective actions that may be needed to address and resolve identified technical risks.

Activities and Products

The PM should ensure that technical assessments routinely occur throughout the life cycle on a reporting timeline that supports forecasting and timely resolution of risks – informing decision makers of technical progress to plan and supporting EVMS. Some elements of technical assessments should be done on a monthly basis to inform programmatic attention, while other assessments may be quarterly or yearly. In all cases, the assessment timelines should allow for tracking trends over time to show stability and impact of corrective actions before major reviews and milestones. The PM should ensure that assessments are appropriately contracted, resourced, and staffed, and that they include appropriate stakeholder and SME participation.

Technical assessment products should form the basis of both the input criteria as well as the output of event-driven criteria for technical reviews and audits (see Section 5, Technical Reviews and Audits). For example, percentage completion of documents/drawings could be entrance criteria for the review, and the output is an objective assessment of technical progress, maturity, and risk. Technical assessments need to be considered as part of all SE processes. All SE processes support activities that contribute to the assessment of program status, technical maturity, and risk in various areas (e.g., schedule, technology, manufacturing, or threat).

The PM should approve the technical assessment products for the program as part of three documents: (1) the performance measurement baseline to capture time-phased measures against the WBS (see Technical Performance Measures); (2) a resource-allocated IMS (see Section 6.1.1); and (3) the SE approach (see Section 1.6) to govern the overall measures and metrics to be collected, update cycle, tasking, control thresholds and expected analysis.

The systems engineer assists the PM in planning and conducting the Technical Assessment process. This assistance may include advising on technical reviews and audits, defining the technical documentation and artifacts that serve as review criteria for each review/audit, and identifying TPMs. Specific activities should include:

- Establish event-driven technical planning.
- Identify appropriate measures and metrics.
- Conduct analyses to assess risks and develop risk mitigation strategies.

- Conduct assessments of technical maturity, process health and stability, and risk to communicate progress to stakeholders and authorities at decision points.
- Propose changes in the technical approach to reduce the program’s technical risks.
- Advise the PM on the program’s technical readiness to proceed to the next phase of effort.
- Include decision maker stakeholders and SMEs as appropriate for reviews and audits.

Inputs to the Technical Assessment process should include approved program plans (e.g., SEP, TEMP, CSS, AS, APB, engineering products (i.e., TPMs, drawings, specifications and reports, prototypes, system elements, and engineering development modules)), and current performance metrics. Outputs may include various reports and findings (e.g., technical review reports, corrective actions, Independent Technical Risk Assessment (ITRA) findings, or test reports).

Technology Readiness Assessments

A Technology Readiness Assessment (TRA) is a systematic, metrics-based process that assesses the maturity of, and the risk associated with, critical technology elements (CTEs) to be used in larger systems. A TRA examines program concepts, technology requirements, and demonstrated technology capabilities. It is conducted by the PM with the assistance of an independent team of SMEs and involves other key players such as the lead systems engineer and CAE or PAE.

A CTE is a new or novel technology on which a program or platform depends to successfully develop a system or to meet an operational threshold. A CTE may be hardware, software, or a process critical to the performance of a larger system or to the fulfillment of a key objective. OUSW(R&E) defines a technology element as “critical” if the system being acquired depends on this technology element to meet operational requirements and if the technology element or its application is either new or novel or in an area that poses major technological risk during detailed design or demonstration.

A TRL is a measurement of a specific CTE’s level of maturity. During a TRA, the evaluators identify and document the CTEs to determine their level of maturity and then assign each CTE a TRL. PMs should conduct knowledge-building TRAs throughout the DoW acquisition life cycle, including in support of major decision points (for MDAPs this would include PDR, Milestone B, and Milestone C). They can also be performed to learn about specific aspects of a technology’s development, to identify risks, or to determine whether a more comprehensive TRA needs to be conducted before an upcoming decision point.

See the Engineering of Defense Systems Guidebook (2022) and the Technology Readiness Assessment Guidebook (2025) for additional information.

Technical Performance Measures

TPMs are the method of collecting and providing information to PMs and systems engineers at routine intervals for decision making. TPMs are measures collected over time for the purpose of seeing trends and forecasting program progress to plan. TPMs encompass the quantifiable attributes of both the system's development processes and status, as well as the system's product performance and maturity. Early in the life cycle, the TPMs may be estimated based on numerous assumptions and modeling and simulation. As the life cycle proceeds, actual demonstrated data replaces estimates and adds to the fidelity of the information. The insight gained can be at any level: the entire system, subsystem elements, enabling system elements, and other contributing mission (e.g., SoS) elements, as well as all of the SE processes and SE disciplines in use across the program.

The goal of having a robust TPM process is the ability for the PM, systems engineer, and senior decision makers to: (1) gain quantifiable insight to technical progress, trends, and risks; (2) empirically forecast the impact on program cost, schedule, and performance; and (3) provide measurable feedback of changes made to program planning or execution to mitigate potentially unfavorable outcomes. In addition, if sufficient margin exists, then TPMs help identify trade space and can be used by PMs to balance cost, schedule, and performance throughout the life cycle. The PM and SE should use TPM data as the basis of evidence to support entrance and exit criteria, incentives, and direction given at technical reviews or milestone decisions. TPMs provide leading indicators of performance deficiencies or system risk.

Activities and Products

TPMs should be identified, tailored, and updated in the SEP to fit the program. As the program progresses through the acquisition cycle, TPMs should be added, updated, or deleted. TPMs should be chosen that will not only confirm the performance of the program in the current phase but also provide leading indicators to future risk and issues in the next phase. In early phases of a program, a program should document a strategy to identify, prioritize, and select TPMs. As the program matures, the program should document in a SEP the actual TPMs to be used. Further TPM guidance is provided in the SEP outline.

TPM Categories and Definitions

Although the specific TPMs used to monitor a program are unique to that program, 16 categories are of concern across all DoW acquisition programs. Having TPMs in each of these core categories is considered best practice for effective technical management. For each of the categories in Table 6-3, the PM and systems engineer should consider at least one TPM to address product and process performance. For some categories, such as "System Performance," there should be multiple TPMs to monitor forecasted performance of each requirement (such as KPPs and KSAs). These TPMs relate to the test community use of CTPs and should be identified as such to focus the test community. The traceability of the TPMs to the core categories should be documented in the SEP.

Table 6-3. Core TPM Category Definitions

Core TPM Category	Description of TPM
Mission Integration Management (System of Systems (SoS) Integration /Interoperability)	Metrics evaluate the stability, maturity and adequacy of external interfaces to understand the risks from/to other programs integrating with the program toward providing the required capability, on-time and within budget. Understand the growth, change and correctness of the definition of external and internal interfaces. Evaluate the integration risks based on the interface maturity. (See SE Guidebook Section 6.2.5, Integration and Section 7.12, Interoperability and Dependencies)
Mission (End-to-End) Performance	Measure of the overall ability of a system to accomplish a mission when used by representative personnel in the environment planned in conjunction with external systems. Metrics should provide an understanding of the projected performance regarding a mission thread achieving the intended mission capability. These may relate to the Critical Operational Issues, criteria, and measures of effectiveness in the operational test agencies
Reliability, Availability and Maintainability (RAM)	Metrics should evaluate the requirements imposed on the system to ensure operationally ready for use when needed, will successfully perform assigned functions and can be economically operated and maintained within the scope of logistics concepts and policies (See Section 7.18, Reliability and Maintainability Engineering).
System Performance	Metrics should evaluate the performance of the system or subsystem elements in achieving critical technical attributes (e.g., weight) that contribute to meeting system requirements. There should be multiple TPMs to monitor forecasted performance of KPPs and KSAs. These are called CTPs by the test community.
Program Protection	System assurance evaluates the safeguarding of the system and the technical data anywhere in the acquisition process, including the technologies being developed, the support systems (e.g., test and simulation equipment) and research data with military applications.
Cybersecurity	Include metrics to evaluate Defense in Depth ; requirement satisfaction vulnerability assessments; STIG compliance. (See Section 7.24, System Security Engineering)
Manufacturing Management	Metrics should evaluate the extent to which the product can be manufactured with relative ease at minimum cost and schedule, and maximum reliability. (See Section 7.14, Manufacturing and Quality)
Manufacturing Quality	System manufacturing quality metrics should track both quality of conformance and quality of design. Quality of conformance is the effectiveness of the design and manufacturing functions in executing the product manufacturing requirements and process specifications while meeting tolerances, process control limits and target yields for a given product group (e.g., defects per quantity produced). (See Section 7.14, Manufacturing and Quality)
Schedule Management	Include metrics to assess both schedule health (e.g., the DCMA 14-point health check), associated completeness of the WBS and the risk register. A healthy, complete and risk-enabled schedule forms the technical basis for the EVMS. Strong schedule metrics are paramount for accurate EVMS data.
Staffing and Personnel Management	Metrics should evaluate the adequacy of the effort, skills, experience and quantity of personnel assigned to the program to meet management objectives throughout the acquisition life cycle.

Core TPM Category	Description of TPM
Resource Management	Metrics should evaluate the adequacy of resources and/or tools (e.g., models, simulations, automated tools, synthetic environments) to support the schedule.
Software Development Management	Metrics should evaluate software development progress against the software development plan. For example, the rate of code generation (lines of code per man-hour). (See Section 3.6, Software Engineering)
Software Quality	Metrics should address software technical performance and quality (e.g., defects, rework) evaluating the software's ability to meet user needs. (See Section 3.6, Software Engineering)
Requirements Management	Evaluate the stability and adequacy of the requirements to provide the required capability, on-time and within budget. Includes the growth, change, completeness and correctness of system requirements. (See Section 6.1.4, Requirements Management Process)
Risk Management	Metrics should include the number of risks open over time or an aggregate of risk exposure (the potential impact to the performance, cost and schedule). (See Section 6.1.5, Risk Management Process)
Test Management	Metrics should include process measures such as the status of decomposition of requirements into discrete test objectives, number of test response variables defined and associated levels/factors as well as system-specific metrics to assess attainment of key CTPs.

TPM Hierarchy

As shown in Figure 6-4, TPMs at the “Management Decisional” level may be allocated or decomposed into supporting details associated with subsystem assemblies along the lines of the WBS or organizational management hierarchies. As examples: a system weight TPM may be allocated to separate subsystem assemblies or a software productivity TPM may be added to effectively manage a high-risk subcontractor’s development efforts.

**Hierarchy of Technical Performance Metrics to support decisions at
different Organizational and WBS levels**
(This hierarchy is applied to each of the core TPMs)

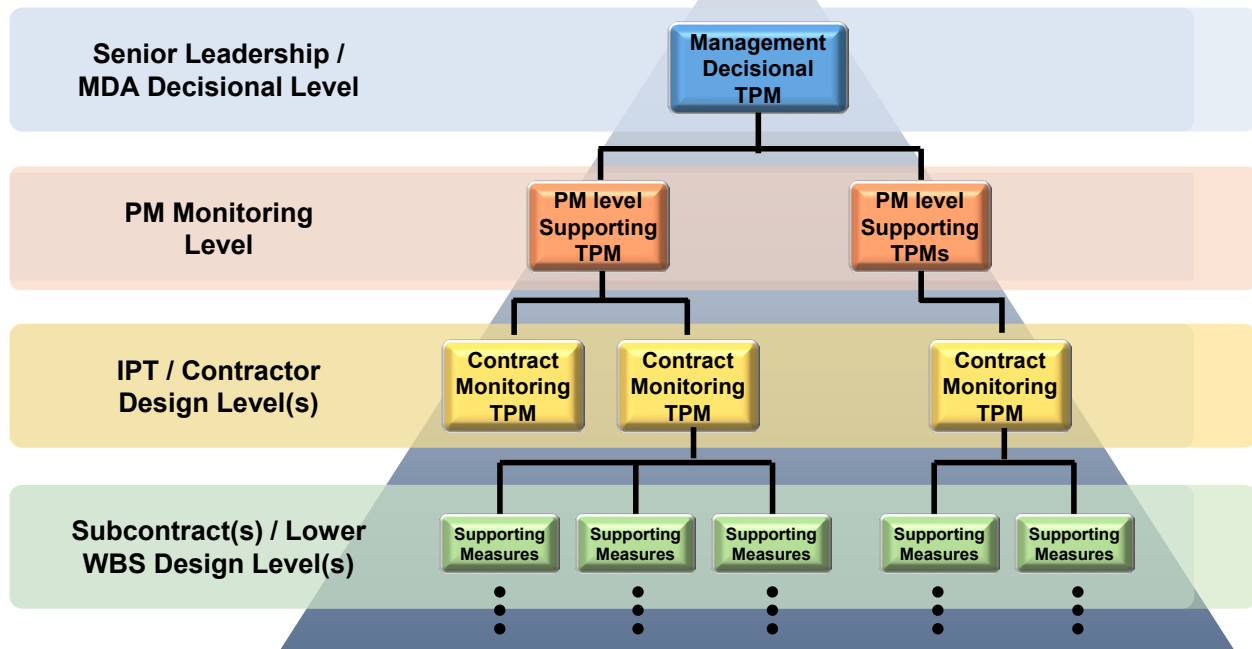


Figure 6-4. Technical Performance Measure Hierarchy

TPM Characteristics

Figure 6-5 depicts the characteristics of a properly defined and monitored TPM to provide early detection or prediction of problems that require management. TPM reporting should be in terms of actual versus planned progress, plotted as a function of time and aligned with key points in the program schedule (e.g., technical reviews). A continuous (historical) plot of planned and actual values for each TPM, along with program planning information, enables assessment of performance trends (i.e., progress-to-plan relationships with respect to both objective and threshold values).

Example of a well-thought-out TPM

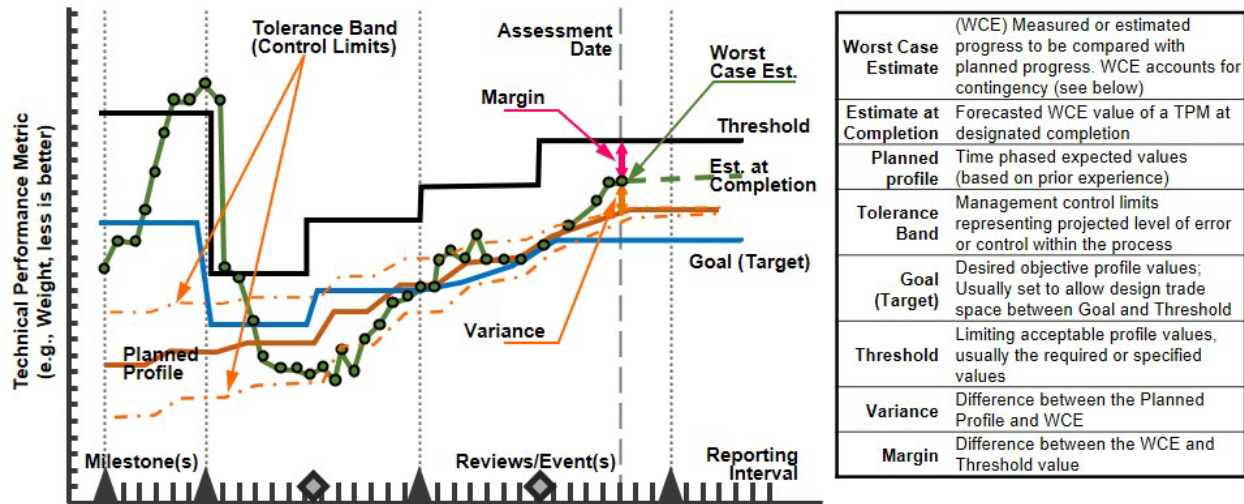


Figure 6-5. Leading Indicators Influence Risk Mitigation Planning

As illustrated in the figure, a good metric includes four attributes:

- **Quantifiable:** The measure is quantifiable with defined criteria and consistent methods for determining a measurement point.
- **Routine:** The interval of measure collections is routine and on a cycle to support timely evaluation of corrective action. The routine enables statistical forecasting of the overall condition by allowing the observation and measurement of change over time.
- **Controlled:** There is a curve of an expected plan, goal, control limits or threshold values over time for the appropriate phase to measure against for status, as well as to determine stability and whether the measure is in control. At a minimum, each review and assessment point should have a planned value.
- **Risk Relevant:** The attribute being measured should be strongly relevant to a program risk, a programmatic decision, a contractual incentive, a key developmental process, or a predictor of required system performance. Strongly suggested are metrics that allow the forecasting of each requirement (such as KPPs and KSAs) as well as known developmental process risks such as software development, cybersecurity, schedule health, requirements stability, and mission integration/interoperability.

To achieve an accurate status, TPM reporting should account for uncertainties such as measurement error and the immaturity of the item being measured. Allotted values for these uncertainties are termed “Contingency” and are used to adjust the Current Best Estimate (CBE) to arrive at a Worst Case Estimate (WCE) for purposes of comparison against the planned profile, thresholds, and goals. For example, if a surrogate item is used to determine a measured value, it would warrant a greater contingency factored into the WCE than if the actual end item were used. Contingency is allocated as part of each WCE data point and typically decreases as

the system and measurements mature, while Margin is not allocated. “Margin” is the amount of growth that can be accommodated while remaining within the threshold (the remainder of threshold minus WCE). Margin is potential trade space available to the PM to potentially offset under-achieving measures.

Figure 6-6 depicts the relationship between contingency, CBE, WCE, threshold, and margin, as well as example criteria of how contingency changes as the system/testing matures.

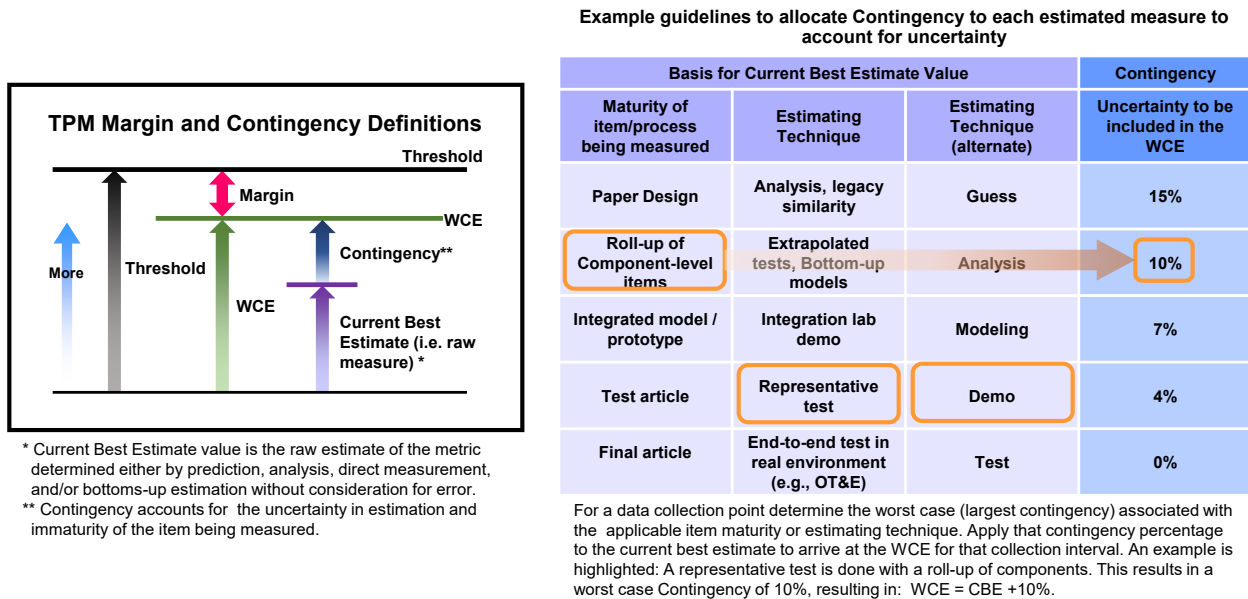


Figure 6-6. TPM Contingency Definitions

6.1.4 Requirements Management Process

Through the Requirements Management process, a program maintains a current and approved set of requirements over the entire acquisition life cycle. This oversight helps ensure delivery of a capability that meets the intended mission performance, as stipulated by the operational user. Service requirements authorities are prioritized annually by the JFRC as KOPs and resourced by the RRAB.

The end-user needs are usually identified in operational terms at the system level during implementation of the Stakeholder Requirements Definition and Requirements Analysis processes (see Sections 6.2.1 and 6.2.2). Through the Requirements Management process, the systems engineer tracks requirement changes and maintains traceability of end-user needs to the system performance specification and, ultimately, the delivered capability. As the system design evolves to lower levels of detail, the systems engineer traces the high-level requirements down to the system elements through the lowest level of the design. The complexity of this process will vary with the complexity of the system being acquired and acquisition pathway, but should always include periodic feedback from the end user.

Requirements management provides bottom-up traceability from any derived lower-level requirement up to the applicable source (system-level requirement) from which it originates. This bidirectional traceability is the key to effective management of system requirements. It enables the development of an analytical understanding of any system-wide effects of changes to requirements for a given system element, updating requirements documentation with rationale and impacts for approved changes. At the same time, bidirectional traceability ensures that approved changes do not create any “orphaned” lower-level requirements (i.e., that all bottom-up relationships to applicable system-level requirements remain valid after the change). Bidirectional traceability also ensures that higher-level requirements are properly flowed to lower-level requirements and system element designs so there are no “childless parent” higher-level requirements (i.e., each high-level requirement is ultimately being addressed by lower-level requirements and system element designs).

Robust requirements management, implemented in synchronization with the program’s CM process (see Section 6.1.6), can help the program avoid or mitigate unintended or unanticipated consequences of changes through rigorous documentation of the system performance specification. Thoughtful analysis and management of requirements can help lay the foundation for system affordability.

Activities and Products

The PM should keep leadership and all stakeholders informed of cost, schedule, and performance impacts associated with requirement changes and requirements growth.

The systems engineer establishes and maintains a Requirements Traceability Matrix (RTM), which captures all the requirements in the system performance specification, their decomposition/derivation and allocation history, and rationale for all entries and changes. The requirements should be:

- Traceable to and from the stated end-user needs.
- Correctly allocated, with potential effects of proposed changes fully investigated, understood, and communicated to the PM.
- Feasibly allocated, i.e., lower-level system elements cannot have the same or wider tolerance bands as those of the higher-level system elements into which they are incorporated.

All affected stakeholders and decision makers should fully understand the effects of proposed changes to requirements at the system or system element level before they accept any changes for incorporation into the design. The RTM provides significant benefits during trade-off analysis activities, since it captures the system-wide effects of proposed changes to established requirements.

In accordance with DoDI 5000.85 for programs in the MCA pathway, CAEs establish Configuration Steering Boards (CSBs), following CDD (or equivalent) validation, for Acquisition Category (ACAT) I programs in development, production, and sustainment. The CSB reviews all requirements changes and any significant technical configuration changes that have the potential to result in cost and schedule impacts to the program. In a continuous effort to reduce TOC, the PM, in consultation with the PAE and requirements sponsor, will identify and propose to the CSB recommended requirements changes, including de-scoping options, that reduce the program cost or moderate requirements needed to respond to any threat developments. These recommended changes will be presented to the CSB with supporting rationale addressing operational implications.

Section 3 SE Modernization contains information about SE tools generally employed in the Requirements Management process. Many commercial software packages are specifically designed for the traceability aspect of Requirements Management, from top-level operational requirements down to the lowest-level system elements in the WBS.

6.1.5 Risk Management Process

The most important decisions to control risk are made early in a program life cycle. During the early phases, the program works with the requirements community to help shape the product concept and requirements. PMs and teams should understand the capabilities under development and perform a detailed analysis to identify the risks. Where necessary, they should prioritize requirements and make trade-offs to meet affordability objectives. Once the concept and requirements are in place, the team determines the basic program structure, the acquisition strategy, and which AAF pathway to use based on the type and level of risks.

Defense programs encounter risks and issues that should be anticipated and addressed on a continuing basis. Risk and issue management are closely related and use similar processes. Opportunity management is complementary to risk management and helps achieve should-cost objectives. Risks, issues, and opportunities may be in areas including, but not limited to, technology, integration, cybersecurity, quality, manufacturing, logistics, requirements, software, test, and reliability. Risk and issue management is an integral part of program planning and execution regardless of the acquisition pathway the program uses to acquire a system, product, or service.

The PM and systems engineer are the program members primarily responsible for leading risk management. A PM should align risk tolerance with organizational capacity to manage risks and allocate resources to the best effect; however, PMs should move away from being highly risk averse at the expense of the timely deployment of needed military capabilities, and toward encouraging innovation and smart risk taking. This also includes failing fast and leveraging iterative learning to adjust approaches (while acknowledging and prioritizing actions to address critical risks to avoid long-term catastrophic failures). An example would be exploring SBIR/STTR technologies for innovative solutions to reduce risk.

Funding instability, resourcing misalignment, or delays in Joint Acceleration Reserve allocations should be captured as explicit risk categories in the RIO process. Technical, programmatic, and business events can develop into risks, issues, or opportunities, each with cost, schedule, or performance consequences as shown in Figure 6-7.

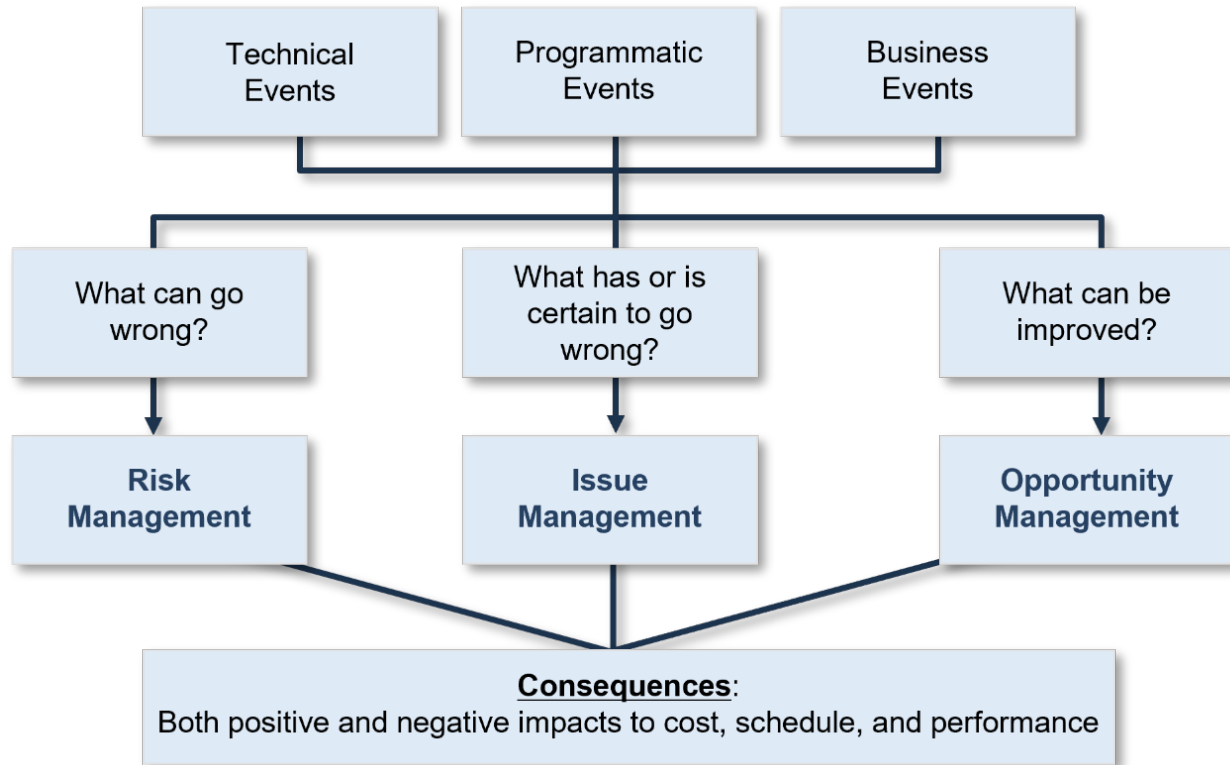


Figure 6-7. Risk, Issues, and Opportunities

Statute (10 USC 4272) requires PMs to document a comprehensive approach for managing and mitigating risk (including technical, cost, and schedule risk) in the AS for MDAPs and major systems. MDAPs and major systems must identify the major sources of risk for each phase and must include consideration of risk mitigation techniques such as prototyping, modeling and simulation, technology demonstration and decision points, and multiple design approaches. In accordance with 10 USC 4272, ITRAs are conducted on all MDAPs before approval of Milestone B and before any decision to enter into LRIP or FRP. Additional guidance on ITRAs can be found on the SE&A website (<https://www.cto.mil/sea>).

The program's risk profile is the dominant consideration in deciding which contract type to pursue. The type of contract, cost-plus or fixed-price, fundamentally will affect the roles and actions of the Government and industry in managing risk. Cost-plus contracts are best suited to situations in which the inherent technical risks are greater (typically during development). Fixed-price development is most appropriate when the requirements are stable and expected to remain unchanged, where technical and technology risks are understood and minimal and the contractor has demonstrated a capability to perform work of the type required.

Systems engineers support the PM in executing a risk management program. The systems engineer's primary concern is with technical risks, issues, and opportunities. Programs are required to summarize the risk management approach and planning activities in the SEP or equivalent. The systems engineer should assess and describe cost and schedule implications of risks, issues and opportunities at technical reviews. Risk mitigation activities should be reflected in the program's IMS and IMP or equivalents.

The PM establishes and typically chairs the Government Risk Management Board (RMB) as a senior group supporting risk management. The RMB usually includes the individuals who represent the various functionalities of the program office, such as program control, the chief engineer, logistics, test, SE, contracting officer as warranted, a user representative, and others depending on the agenda.

The PM may document the risk management process in more detail in a Program Risk Management Process (PRMP) – a best practice. While the processes support risk management, the risk mitigation plans, which focus on reducing individual risks (i.e., the output of the processes), are even more important. As a best practice, the programs may combine their risk, issue, and opportunity plans in a combined RIO document. A good PRMP should:

- Explain the risk management working structure.
- Define an approach to identify, analyze, mitigate, and monitor RIO across the program.
- Document the process to request and allocate resources (personnel, schedule, and budget) to mitigate risks and issues.
- Define the means to monitor the effectiveness of the risk management process.
- Document the processes as they apply to contractors, subcontractors, and teammates.

Separate from the PRMP, as a best practice, the Government and contractor should use a common or electronically compatible tool(s) to collectively identify, analyze, mitigate, and monitor the program's risks, issues, and opportunities. An example of a tool is the Risk Register. Section 7, Design Considerations, provides additional information on identifying and managing risks in different contexts, for example, HSI (Section 7.9), ESOH (Section 7.23), and System Security Engineering (Section 7.24). The associated DoDI 8510.01, "Risk Management Framework for DoD Systems," establishes processes for ensuring confidentiality, integrity and availability for DoW information technology (IT) programs. Programs should consider these specialized risk processes when creating their program risk process.

For additional information on managing RIO, see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (2023).

6.1.6 Configuration Management Process

The CM process establishes and maintains the consistency of a system's functional, performance, and physical attributes with its requirements, design, and operational information and allows technical insight into all levels of the system design throughout the system's life cycle. Effective CM supports the establishment and maintenance of the functional, allocated, and product baseline. Establishing rigorous configuration control enables the successful development, test, production, delivery, and sustainment of the needed capability to the end user.

CM activities support:

- Traceability of designs to requirements.
- Proper identification and documentation of system elements, interfaces, and interdependencies.
- Timely and thorough vetting and disposition of change requests.
- Control and documentation of approved changes to baselines.
- Proper and timely incorporation of verified changes in all affected items and documentation.
- Consistent and appropriate provisions in the ECP and related contract actions.
- Consistency between a product and its design requirements, supporting documentation, and associated production and sustainment systems.
- A complete audit trail of design decisions and modifications.
- Continued assurance of system supportability and interoperability, consistent with the approved acquisition and life cycle sustainment strategies.

CM facilitates the orderly development of a system through establishment of the technical baseline (including the functional, allocated, and product baselines), and the assessment and approval of the baselines at various technical reviews and audits. A baseline is an agreed-upon description of the attributes of a product at a point in time, which serves as a basis for change. Upon approval, the technical baseline documentation is placed under formal configuration control. Through CM, the program identifies, controls, and tracks changes to the technical baseline, ensuring changes occur only after thorough assessments of performance, cost, and schedule impacts, as well as associated risks.

The following baselines are critical to executing CM:

- **Functional Baseline:** Describes the system's performance (functional, interoperability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics. It is directly traceable to the operational requirements contained in the ICD (or equivalent requirements document). The PM establishes Government control of the functional baseline at the SFR and verifies it through FCAs leading up to the system-level FCA or the SVR. Attributes of the functional baseline include:
 - Assessed to be achievable within cost and schedule constraints.
 - Documentation of established interfaces between functional segments.
 - Documented performance requirements traced to (draft) CDD or equivalent requirements.
 - Reflects design considerations and clear linkage in the SoS context.
 - Documented verification requirements.
- **Allocated Baseline:** Describes the functional and interface characteristics for all system elements (allocated and derived from the higher-level product structure hierarchy) and the verification required to demonstrate achievement of those specified characteristics. The allocated baseline for each lower-level system element (hardware and software) is usually established and put under configuration control at the system element PDR. This process is repeated for each system element and culminates in the complete allocated baseline at the system-level PDR. The PM then verifies the allocated baseline at the FCA and/or SVR. Attributes of the allocated baseline include:
 - All system-level functional performance requirements decomposed (or directly allocated) to lower-level specifications (CIs for system elements).
 - Uniquely identified CIs for all system elements at the lowest level of the specification tree.
 - All interfaces, both internal (between element CIs) and external (between the system under development and other systems) documented in Interface Control Documents.
 - Verification requirements to demonstrate achievement of all specified functional performance characteristics (element CI to element CI level and at the system level) documented.
 - Design constraints documented and incorporated into the design.

- **Product Baseline:** Describes the detailed design for production, fielding/deployment, and O&S. The product baseline prescribes all necessary physical (form, fit and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. It is traceable to the system performance requirements contained in the CDD or equivalent. At the CDR, the product baseline is initially established and is referred to as the initial product baseline.

The initial product baseline includes “build-to” specifications for hardware (product, process, material specifications, engineering drawings, and other related data) and software (software module design “code-to” specifications). The initial system element product baseline is established and placed under configuration control at the system element CDR and verified later at the Physical Configuration Audit.

The PM assumes control of the initial product baseline Class I configuration changes, as defined in accordance with the program’s CM plan, from the contractor at completion of the system-level CDR. This does not necessarily mean that the PM takes delivery and acceptance of the TDP. If one or more performers are on contract and competing for a follow-on contract when CDR is conducted, the PM may delay assuming control of the initial product baseline until after down-selection to one contractor. Attributes of the product baseline include:

- RTM is complete.
- The detailed design (hardware and software), including interface descriptions, satisfies the CDD or equivalent and pertinent design considerations.
- Hardware, software, and interface documentation are complete.
- Key product characteristics having the most impact on system performance, assembly, cost, reliability, survivability, cybersecurity, ESOH, and sustainment have been identified.
- Traceability from the design documentation to the system, and to the system-element verification requirements and methods, is complete.
- Manufacturing processes that affect the key characteristics have been identified, and capability to meet design tolerances has been determined.

Activities and Products

The program office and developer share responsibility for planning, implementing, and overseeing the CM process and its supporting activities. The distribution of responsibilities between the program office and the developer varies, based on the acquisition strategy and the life cycle phase.

The PM approves the Configuration Management Plan (CMP) and should ensure adequate resources are allocated to implement CM throughout the life cycle. The PM assesses the impact

of proposed changes to a baseline, approves changes – usually through a CCB (see MIL-HDBK-61B (Configuration Management Guidance) and SAE-GEIA-HB-649 (Configuration Management Standard Implementation Guide) for additional information) – and ensures proper documentation of decisions, rationale, and coordination of changes.

The systems engineer ensures the program has completed CM planning and should document details and activities in the SEP and the supporting CMP (as appropriate). The PM, with the support of the systems engineer, ensures that the CM approach is consistent with the Intellectual Property Strategy (See Section 6.1.7, Technical Data Management Process). The CM process described in the DoW-adopted standard SAE EIA-649, Configuration Management Standard, consists of five interrelated functions that, when collectively applied, allow the program to maintain consistency between product configuration information and the product throughout its life cycle. The five CM functions are:

- Configuration Management Planning and Management
- Configuration Identification
- Configuration Change Management
- Configuration Status Accounting
- Configuration Verification and Audit

In addition, the DoW-adopted standard SAE EIA-649-1, CM Requirements for Defense Contracts, implements the principles outlined in SAE EIA-649 for use by defense organizations and industry partners during all phases of the acquisition life cycle. It makes provisions for innovative implementation and tailoring of specific CM processes to be used by system suppliers, developers, integrators, maintainers, and sustainers.

6.1.7 Technical Data Management Process

The Technical Data Management process provides a framework to acquire, manage, maintain, and ensure access to the technical data and computer software required to manage and support a system throughout the acquisition life cycle (see Section 7.24, System Security Engineering, for information regarding protection of critical program information (CPI)). Key technical data management considerations include understanding and protecting Government and contractor intellectual property and data rights, achieving competition goals, maximizing options for product support, and enabling performance of downstream life cycle functions.

Acquiring the necessary data and data rights, in accordance with MIL-STD-31000, “Technical Data Packages,” for acquisition, upgrades, and management of technical data, provides the following advantages:

- The information necessary to understand and evaluate system designs throughout the life cycle.

- The ability to operate and sustain systems under a variety of changing technical, operational, and programmatic environments.
- The ability to recompute item acquisition, upgrades, and sustainment activities in the interest of achieving cost savings; the lack of technical data or data rights often makes it difficult or impossible to award contracts to anyone other than the original manufacturer, thereby taking away much or all of the Government's ability to reduce TOC.

Activities and Products

The PM, systems engineer, and software engineer, in conjunction with the PSM, should ensure that life cycle requirements for system-related data products and data rights are identified early and appropriate contract provisions are put in place to enable deliveries of these products. Figure 6-8 shows the activities associated with technical data management.

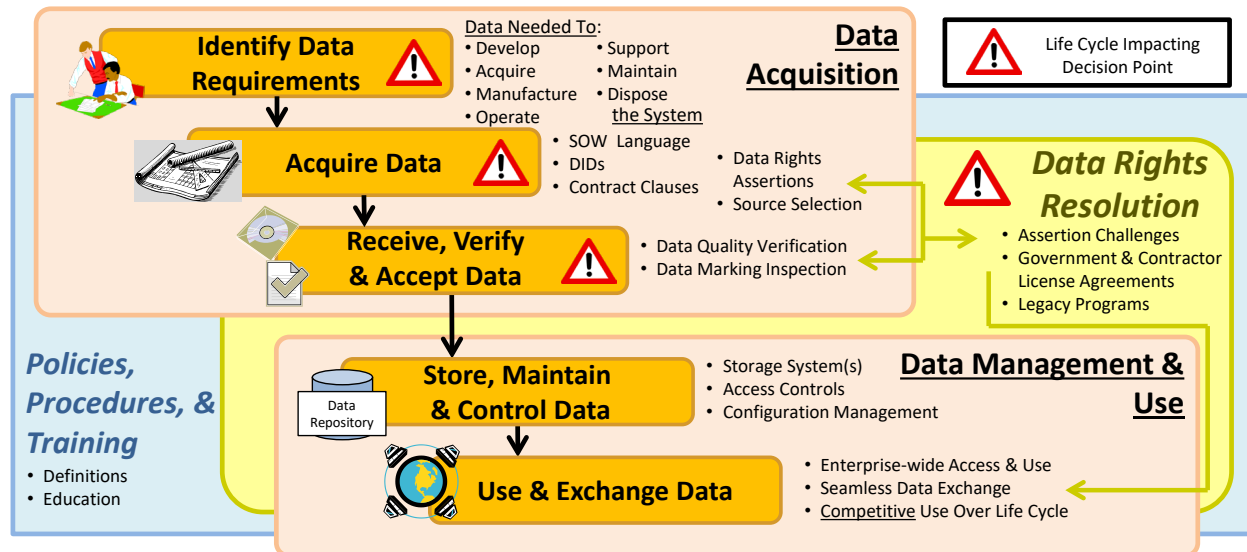


Figure 6-8. Data Management Activities

Following are additional details related to the activities:

- Identify Data Requirements
 - Formulate the program's Intellectual Property (IP) Strategy and technical data management approach, with an emphasis on technical and product data needed to provide support throughout the acquisition life cycle (see Intellectual Property Guidebook for DoD Acquisition (2025)).
 - Consider all opportunities to leverage the system model and WBS structure to capture data rights assertions as the system architecture is being developed and throughout the system life cycle.

- Ensure that data requirements are documented in the IP Strategy; summarized in the AS and presented with the LCSP, or equivalents, during O&S; and submitted before award of the contract for the next life cycle phase.
- Give special attention to acquire or obtain access to data and digital artifacts within the digital ecosystem throughout the program's life cycle, including identifying formats that can be made compatible with Government data systems (program office, T&E, models and simulations, sustainment, etc.).
- Based on the technical baseline, identify assemblies, subassemblies, and parts that are candidates for Government ownership of data rights. Include this information in trade studies, and as input to RFPs.
- Consider not only the immediate, short-term costs of acquiring the needed technical data and data rights but also the long-term cost savings resulting from the ability to compete production and logistics support activities and reduce TOC. Understand that the Government can possess either Government Purpose or Unlimited Rights to use many types of technical data and data rights, at no additional cost, based on the type of technical data and the source of funding used to generate the data (see DoD Open Systems Architecture Contract Guidebook for Program Managers (2013) for more information about data rights).
- Consider any requirements to acquire rights to production and sustainment tooling and facilities, including processes required to use this equipment. Where the Government has acquired rights to specific parts, these rights do not necessarily also convey rights to the equipment or processes used to produce the parts.
- Acquire Data
 - Use explicit contract SOW tasks to require the developer to perform the work that generates the required data and digital artifacts. The content, format, and quality requirements should be specified in the contract.
 - Use current, approved DIDs and CDRLs in each contract to order the delivery of the required technical data, digital artifacts, and computer software.
 - Consider obtaining data through an open business model with emphasis on having open, modular system architectures that can be supported through multiple competitive alternatives. The model may include MOSA as a part of the design methodology supported by an IP strategy, which may be implemented over the life cycle of a product (see Section 3.7, Modular Open Systems Approach).
- Receive, Verify, and Accept Data
 - Ensure verification of content, format, and quality of all required product-related data received from originators.
 - Inspect contractually ordered data deliverables to ensure markings are in accordance with the relevant data rights agreements and Defense Federal Acquisition Regulation

Supplement (DFARS) clauses and contain appropriate distribution statements and/or export control statements.

Caution: *Acceptance of delivered data not marked consistent with the contract can result in the Government “losing” legitimate rights to technical data and can incur significant legal liability on the Government and the individual Government employees. Regaining those rights generally requires costly and time-consuming legal actions.*

- Store, Maintain, and Control Data
 - Budget for and fund the maintenance and upkeep of product data throughout the life cycle.
 - An Integrated Data Environment (IDE) or Product Life Cycle Management (PLM) system allows every activity involved with the program to create, store, access, manipulate, and exchange digital data.
 - To the greatest extent practical, programs should use existing IDE/PLM infrastructure such as repositories operated by Commodity Commands and other organizations. (Program-unique IDEs are discouraged because of the high infrastructure cost; furthermore, multiple IDEs inhibit access, sharing, and reuse of data across programs.)
 - Ensure all changes to the data are made in a timely manner and are documented in the program IDE or PLM system.
- Use and Exchange Data
 - Plan for and establish methods for access and reuse of product data by all personnel and organizations that perform life cycle support activities.

In support of the Government’s requirement for a TDP, the PM also should consider product-related data (e.g., technical manuals, repair instructions, and design/analysis data) to:

- Allow logistics support activities.
- Better enable sustainment engineering.
- Apply, implement, and manage product upgrades.

Contractually deliverable data should be identified and ordered at the specific “data product” level, (e.g., two-dimensional drawings, three-dimensional Computer-Aided Design models, technical manuals). Figure 6-9 provides a notional representation of different types of product-related data.

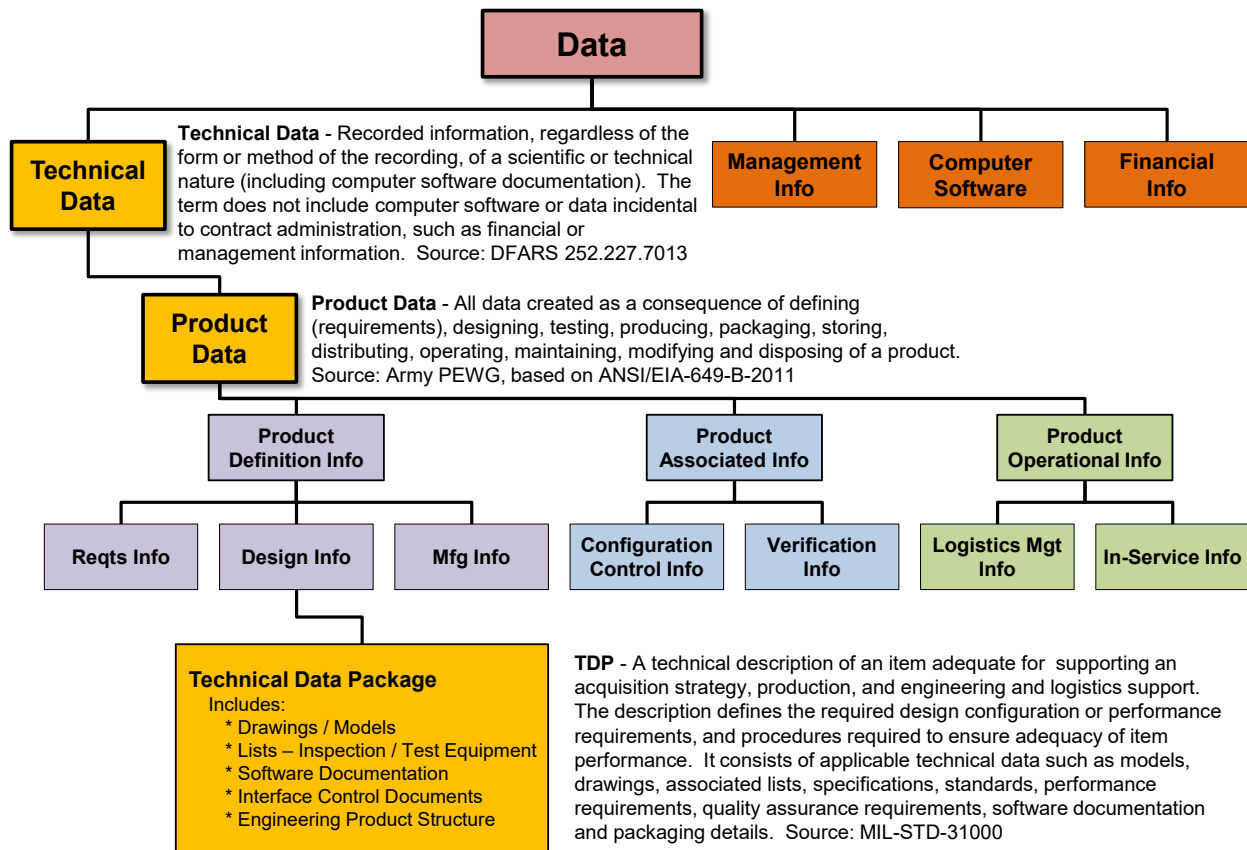


Figure 6-9. Data Taxonomy

Caution: PMs, systems engineers, and software engineers should be aware that terms such as “technical data,” “product data,” and “TDP” are imprecise, not equivalent, and often incorrectly used interchangeably.

Resources for establishing and conducting technical data management activities include but are not limited to:

- DoD Manual 5010.12, Procedures for the Acquisition and Management of Technical Data
- Intellectual Property Guidebook for DoD Acquisition (2025)
- Army Data and Data Rights (D&DR) Guide (2015)
- Army Regulation 25-1 Army Information Technology
- Department of the Army Pamphlet 25-1-1 Army Information Technology Implementation Instructions
- Air Force Product Data Acquisition guidance (requires an Air Force portal account)

- Air Force Technical Data and Computer Software Rights Handbook (Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals 2018)
- Navy Technical Manual SL150-AA-PRO-010/DMP - Data Management Program
- MIL-HDBK-245 (Preparation of Statement of Work)
- MIL-STD-963 (Data Item Descriptions)
- MIL-STD-31000 (Technical Data Packages)

The PM is responsible for protecting system data, whether the data is stored and managed by the Government or by contractors. The DoW policy with regard to data protection, marking, and release can be found in:

- DoDD 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure"
- DoDI 5230.24, "Distribution Statements on Technical Documents"
- DoDM 5400.07, "Freedom of Information Act (FOIA) Program"
- DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)"

Data containing information subject to restrictions are protected in accordance with the appropriate guidance, contract, or agreement. Guidance on distribution statements, restrictive markings and restrictions on use, release, or disclosure of data can be found in the DFARS (Subpart 252.227-7013 and 7014) and DoDI 5230.24.

When digital data are used, the data should display applicable restriction markings, legends, and distribution statements clearly and visibly when the data are first opened or accessed. These safeguards not only ensure Government compliance regarding the use of data but also guarantee and safeguard contractor data delivered to the Government and extend responsibilities of data handling and use to parties who subsequently use the data.

P.L. 107-347, "E-Government Act of 2002" (Sec 208 para (b)), and DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," require that PIA be conducted before developing or purchasing any DoW information system that collects, maintains, uses, or disseminates personally identifiable information about members of the public, Federal personnel, DoW contractors, and in some cases, foreign nationals. Available PIA guidance provides procedures for completing and approving PIAs.

All data deliverables should include distribution statements. Processes should be established to protect all data that contain critical technology information, as well as ensure that limited

distribution data, intellectual property data, or proprietary data are properly handled throughout the life cycle, whether the data are in hard-copy or digital format.

6.1.8 Interface Management Process

The Interface Management process provides a framework to identify, define, manage and ensure compliance with internal and external system interfaces. The process helps ensure that developers capture all internal and external interface requirements and requirements changes in accordance with the program's CMP. Materiel developers also should communicate interface information to their counterparts responsible for affected systems and system elements and should plan for coherent testing to verify expected performance and, ultimately, operational performance.

Systems are composed of system elements and may operate as part of larger SoS. The design, definition, and management of the physical and logical interfaces, both internal (communications between system elements) and external (communications between the human, system and other systems), are critical to program success. Both types of interfaces have become increasingly important, as system complexity has increased, along with the demands for systems to operate in highly interdependent SoS environments. Interfaces play a critical role in all systems and SoS that interact to deliver a collective capability. Complex systems consist of numerous interfaces of various types. When the circumstances reach a point that the number and complexity of interfaces can no longer be managed effectively, poor interface configuration control can result in degraded system performance, affordability, sustainability, and maintainability.

The use of system interface specifications compliant with widely supported and consensus-based standards that exist at the time of the milestone decision enables a modular and open systems approach. Modular, open systems with standardized interfaces facilitate innovation and competition in future technology insertion and refresh efforts for the system. When necessary to use a non-standard interface specification, acquiring the rights to the design as part of the program's Intellectual Property Strategy may be an enabling option. Standards and specifications for interfaces may be found in ASSIST.

Managing interfaces can include developing, deploying, and sustaining key interfaces as separate configurable items. Use of Interface Requirements Specifications and related Interface Control Documents published by DoW organizations gives the Government ownership control of that interface without any corporate licenses needed. This allows the PM, systems engineer, and software engineer to conduct normal system life cycle updates without breaking interoperability with other systems while successfully executing a MOSA. Managing interfaces as separate CM items allows the PM enterprise reuse items and potentially reduces cost.

Explicit management of the definition, development, implementation, and test of internal and external interfaces, including any associated dependencies, helps ensure that systems operate as designed and meet stakeholder expectations throughout the life cycle. The DoW Architecture

Framework and Unified Architecture Framework provide guidance on how to generate operational and system views that describe interface relationships in a manner common across the DoW user community. Interface management should consider programmatic issues (e.g., roles and responsibilities, funding and scheduling) in addition to the technical aspects of SE and integration.

Activities and Products

Interface management is an iterative process: as knowledge of the system and system elements increases during design activities, verifiable lower-level requirements and interfaces are defined and refined. Materiel developers should assess impacts of the originally defined capabilities and interfaces, performance parameter thresholds and objectives and the overall system when defining and modifying interfaces.

The PM, systems engineer, and software engineer should ensure that the program's interface management plan:

- Documents the system's internal and external interfaces and dependencies, and requirement specifications along with technical data and intellectual property right expectations.
- Identifies preferred and discretionary interface standards and their profiles.
- Provides definition of modular system interfaces with the Interface Requirements Specifications necessary to support system operation, interface standards and standards profiles, and other documentation that fully describe the physical and functional interfaces needed to ensure compatibility between interfacing components, systems, and platforms.
- Supports architecture descriptions for how the system and subsystems join together at internal and external interface boundaries leveraging the DoDAF and UAF to form the system and support interoperability, upgradeability, integration, verification, and validation.
- Provides justification for the selection and procedure for upgrading interface standards.
- Describes the certifications and tests applicable to each interface or standard.
- Is consistent with the program's CM plan processes for managing and controlling internal and external interfaces.

The PM, systems engineer, and software engineer should ensure that the developer documents all system interface requirements (see Section 6.1.4, Requirements Management Process), places them under appropriate levels of CM and makes them available to the appropriate stakeholders.

These documented interface requirements serve critical functions at all levels of the system throughout the life cycle, including:

- Developing functional and physical architectures.
- Facilitating competitive bids.
- Enabling integration of systems and lower-level system elements.
- Supporting system maintenance, future enhancements, and upgrades.
- Providing input data for continuous risk management efforts.

The systems engineer responsible for interface management has numerous tasks throughout the life cycle, including:

- Defining and establishing interface specifications.
- Assessing compliance of interfaces among configuration items composing systems or SoS.
- Monitoring the viability and integrity of interfaces within a system.
- Establishing an interface management plan to assess existing and emerging interface standards and profiles, to update interfaces and to abandon obsolete architectures.

The PM should establish an interface control working group (ICWG) composed of appropriate technical representatives from the interfacing activities and other interested participating organizations. The ICWG serves as a forum to develop and provide interface requirements, as well as to focus on detail interface definition and timely resolution of issues. In the SoS environment, external program offices and developers collaborate as members of the ICWG.

6.2 Technical Processes

Whereas the Technical Management Processes provide insight of, and control over, the technical development of a system throughout its life cycle, the Technical Processes are used to design, develop, and analyze the system, system elements and enabling system elements required for integration, test, production, deployment, support, operation, and disposal. The eight Technical Processes discussed in sections 6.2.1 through 6.2.8 provide a framework for ensuring and maintaining traceability between stakeholder requirements, system design, and the eventual delivered capability.

6.2.1 Stakeholder Requirements Definition Process

The Stakeholder Requirements Definition process translates stakeholder capability needs into a set of technical requirements. The process helps ensure each individual stakeholder's requirements, expectations, and perceived constraints are understood from the acquisition perspective. Failing to actively maintain a rigorous Stakeholder Requirements Definition process could result in requirements creep, rework because of misunderstanding of end-user needs, unexpected contract modifications, cost growth, and schedule slip. This should be an iterative

process throughout the program life cycle, working toward incremental product releases, to the maximum extent practicable, that build upon each other and incorporate more frequent user involvement and requirements owner feedback. The objective of this process is to help ensure that stakeholder requirements are feasible, balanced, and fully integrated as more information is learned through requirements analysis.

Stakeholder Requirements Definition bridges the gap between the identification of a materiel need, and the acquisition of a materiel solution, governed by the Warfighting Acquisition System.

The Stakeholder Requirements Definition process complements Requirements Analysis and Architecture Design (see Sections 6.2.2 and 6.2.3). These three processes are recursively applied at each level of the system's specifications and then iteratively within each level throughout development.

The PM, systems engineer, and software engineer are responsible for supporting the Stakeholder Requirements Definition process and should work with the end user to establish and refine operational needs, attributes (e.g., knowledge, skills, abilities, and other attributes of personnel), performance parameters, and constraints documented in program requirements documents.

Stakeholder Requirements Definition activities are performed throughout the acquisition life cycle and include the following:

- Elicit stakeholder capability objectives
 - Identify stakeholders who have an interest in the system and maintain relationships with the stakeholders and their organizations throughout the system's entire life cycle.
 - Elicit capability objectives from the stakeholders about what the system will accomplish and how well.
- Define stakeholder requirements
 - Define the constraints on a system solution.
 - Define the relevant operational environment, missions, including cyberspace, and support scenarios that can be used to analyze the operation of the system (via ME).
 - Define potential requirements that may not have been formally specified by any of the stakeholders.
- Analyze and maintain stakeholder requirements
 - Analyze requirements for specificity, completeness, consistency, measurability, testability, and feasibility.
 - Negotiate modifications with stakeholders to resolve requirement discrepancies.

- Validate, record, and maintain stakeholder requirements throughout the system life cycle.
- Support the Requirements Analysis process to establish and maintain a traceability matrix to document how the system requirements are intended to meet the stakeholder objectives and achieve stakeholder agreements.

6.2.2 Requirements Analysis Process

The Requirements Analysis process results in the decomposition of end-user needs, usually identified in operational terms at the system level during implementation of the Stakeholder Requirements Definition process (see Section 6.2.1), into clear, achievable, and verifiable requirements. As the system design evolves, Requirements Analysis process activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design. The allocated requirements form the basis of contracting language and the system performance specification. The resultant system requirements are addressed at technical reviews and audits throughout the acquisition life cycle and captured in applicable program and SE technical documentation.

The Requirements Analysis process objectives include:

- Link the needs of the end users to the system, system elements, and enabling system elements to be designed and developed.
- Define a system that meets end users' operational mission requirements within specified cost and schedule constraints.
- Provide insight into the interactions among various functions to achieve a set of balanced requirements based on user objectives.

The Requirements Analysis process provides:

- Translation of end-user needs (usually stated in operational terms) to unambiguous, measurable, testable, verifiable, and feasible system performance specification requirements.
- Incorporation of design considerations, including statutory and regulatory constraints (see Section 7, Design Considerations).
- Allocation of requirements from the system-level specification to the lowest-level system elements and enabling system elements.
- Rationale for specification requirements and their decomposition/allocation.
- A mechanism to support trade-off analyses between related requirements to provide maximized mission assurance within cost and schedule constraints.
- A framework for accurate assessment of system performance throughout the life cycle.

The process of defining, deriving, and refining requirements proceeds as follows:

- Analyze user requirements.
- Translate end-user needs into basic functions.
- Develop a quantifiable (qualitative and quantitative) set of performance requirements by defining the functional boundaries of the system in terms of the interactions, behavior, and properties to be provided.
- Define each function that the system is required to perform.
- Define implementation constraints (stakeholder requirements or solution limitations).
- Translate performance requirements into specific system technical design requirements and functions.

The Requirements Analysis process is an iterative activity whereby system requirements are identified, refined, analyzed, and traded to remove deficiencies and minimize the impacts of potential cost drivers to establish an agreed-to set of requirements coordinated with the appropriate stakeholders. Poorly written requirements can lead to significant problems in the areas of schedule, cost, or performance and can thus increase program risk. A well-crafted set of functional and performance requirements can then be translated into design requirements for the total system over its life cycle and can allow stakeholders to assess system performance during execution of the Verification and Validation processes (see Sections 6.2.6 and 6.2.7). Good requirements have the following attributes:

- Necessary
- Unique
- Unambiguous
- Clear and concise
- Complete
- Consistent
- Technically feasible/achievable/obtainable within cost and schedule constraints
- Traceable
- Measurable/quantifiable
- Verifiable (e.g., Testable)
- Able to be validated
- Operationally effective and survivable
- Singular

For more information on writing requirements, see the INCOSE Guide to Writing Requirements.

The Requirements Analysis process ensures that requirements derived from user-specified capability needs are analyzed, decomposed, and functionally detailed across the system design. Early development and definition of requirements using the attributes listed above reduces development time, enables achievement of cost and schedule objectives, and increases the quality of the final system. The Requirements Analysis process encompasses the definition and refinement of the system, system elements, enabling system elements, and associated functional and performance requirements.

The development of the functional baseline is largely a product of the Requirements Analysis process. All requirements are placed under configuration control, tracked, and managed as described in the Requirements Management process and CM process (see Sections 6.1.4 and 6.1.6).

6.2.3 Architecture Design Process

The Architecture Design process is a trade and synthesis method to allow the PM, systems engineer, and software engineer to translate the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions. Through this process, the program establishes the architectural design of candidate solutions that may be found in a system model. It is critical that the Architecture Design process identify the design drivers and driving requirements as early as possible to enable the trades. The alternative design solutions may include hardware, software, and human elements; their enabling system elements; and related internal and external interfaces.

The Architecture Design process, combined with Stakeholder Requirements Definition and Requirements Analysis, provides insights into technical risks early in the acquisition life cycle, allowing for early development of mitigation strategies. Architecture Design is integral to ensuring that multiple well-supported solutions are considered. The Architecture Design process supports analysis of design considerations and enables reasoning about system aspects and attributes such as reliability, maintainability, survivability, sustainability, performance, and TOC.

Architectures and integration strategies should be validated against ME, prototyping, and experimentation results and reference architectures to ensure mission-level interoperability.

Architecture design synthesizes multiple potential solutions from system performance requirements, evaluates those solutions, and eventually describes the system down to the individual system element for implementation. The Architecture Design process is iterative and strives to seek a balance among cost, schedule, performance, and risk that still meets stakeholder needs. The development of the system architecture should adhere to sound SE and should conform to industry best practices and NGSs as applicable. The functional architecture should be part of the functional baseline, and the physical architecture should be part of the allocated and product baselines. The system architecture must be placed under configuration control and

maintained in a robust repository that includes the architecture descriptions and its relationship to each of the baselines as defined as part of the enterprise architecture. CM provides the systems engineer with a means of ensuring consistency of the system architecture definition throughout the acquisition life cycle.

The functional architecture, often called the behavioral architecture, provides the foundation for defining what the system must do through the allocation of functions and subfunctions to hardware/software, databases, facilities, and human operations to achieve its mission. The physical architecture defines the structural elements and their arrangement that provides the “how” for the behavioral architecture.

This distinction between functional and physical is critical in MBSE. The product structure may consist of conceptual design drawings, schematics, or block diagrams that define the system’s form and the arrangement of the system elements and associated interfaces. Creating and maintaining tightly controlled digital models of the functional and physical architecture should be considered as a best practice and ensures consistency in application of the architecture as it evolves through the system development life cycle. The development of the physical architecture is an iterative and recursive process and evolves together with the functional requirements and functional architecture. Development of the physical architecture is complete when the system has been decomposed to the lowest system element (usually the lowest replaceable unit of the support strategy).

The PM may oversee Architecture Design efforts to gain and maintain insights into program schedule and cost drivers for use in the evaluation of alternative architectures, excursions, mitigation approaches, etc.

Key activities in the Architecture Design process include:

- Define System Behavior (Functional Architecture): Develop behavioral models (e.g., SysML Activity, Sequence, State Machine diagrams) that describe the system’s functions.
- Define System Structure (Physical Architecture): Identify and describe the system elements, including design budgets (e.g., weight, reliability) and open system principles.
- Allocate Behavior to Structure: Map the functions from the behavioral architecture to the structural elements of the physical architecture.
- Define and Analyze Interfaces: Based on the allocation, define the data, energy, and matter exchanged between structural elements.
 - Prescribe detailed form, fit, and function characteristics and selected functional characteristics designated to support replacement or reuse of emerging or obsolescent technology to support MOSA implementations in accordance with 10 USC 4401, 4402, and 4403.

- Describe how MOSA is implemented in the system design to enable affordable change, evolutionary acquisition, and interoperability.
- Document and characterize MOSA-related controlling or guiding reference architectures, interface packages, and standards (where applicable) that support the delivery of interfaces, syntax and properties, documentation, and communication implementations (10 USC 4401).

During this process, derived requirements come from solution decisions. It is essential to identify derived requirements, ensure that the requirements are traceable and part of the allocated requirements, and ensure they are placed under configuration control. For each solution alternative, the Decision Analysis process trades off requirements against solution alternatives. For each solution alternative, based on programmatic decisions, certain performance requirements may be emphasized over others.

The essence of this activity is to achieve a balanced and feasible design with acceptable risk that falls within the program design constraints. An integral part of defining and refining the functional and physical architecture is to provide technical support to the market research, especially early in the acquisition life cycle. Systems engineers should analyze whether existing products (commercial or non-developmental items) can meet user performance requirements or whether technologies can realistically be matured within the required time frame. When possible, mature technologies should be used to satisfy end-user needs.

The output of this process is the allocated baseline, which includes the digital artifacts that describe the physical architecture of the system, the specifications that describe the functional and performance requirements for each configuration item, and the interfaces that compose the system. In addition, the WBS and other technical planning artifacts should be updated. The system architecture and the resulting design artifacts should be sufficiently detailed to:

- Confirm the upward and downward traceability of requirements.
- Confirm the interoperability and open system performance requirements.
- Sufficiently define products and processes to support implementation, verification, and validation of the system.
- Establish achievable alternatives to allow stakeholders to make informed decisions.

Confirmation of requirements traceability and the soundness of the selected physical architecture can be accomplished using a cost-effective combination of design modeling and analysis, as applicable.

The result of the Architecture Design process is an architectural design that meets the end-user capability needs shown in the Requirements Management process to have all stated and derived requirements allocated to lower-level system elements and to have the possibility of meeting cost, schedule, and performance objectives. The architectural design, ideally in a digital system

model, must maintain continuous traceability, ensuring that every function and structural element can be traced back to a verified system requirement and, ultimately, to a stakeholder need. The level of detail of the architectural design depends on the complexity of the system and the support strategy. It should be detailed enough to bound the cost and schedule of the delivered system, define the interfaces, assure customers that the requirements can be met, and control the design process down to the lowest removable unit to support operations and sustainment. This architecture design may be documented and found in a program's system model. Once identified, the system architecture is placed under CM.

6.2.4 Implementation Process

The Implementation process is composed of two primary efforts: design and realization. The outputs of the Implementation process include the detailed design, down to the lowest level system elements in the system architecture, and the fabrication and production procedures of forming, joining, and finishing, or coding for software. Depending on technology maturity, the Implementation process may be used to develop, buy, or reuse system elements to render the system. Implementation is integral to systematically increasing maturity, reducing risk, and ensuring the system is ready for the Integration, Verification, and Validation processes (see 6.2.5, 6.2.6, and 6.2.7). The Implementation process provides a system that satisfies specified design and stakeholder performance requirements. As a best practice, the systems engineer should develop an implementation plan that includes implementation procedures, fabrication processes, tools and equipment, implementation tolerances, and verification uncertainties.

Design

Design analysis takes many forms, such as the use of models, simulations, experiments, and prototypes through which competing systems can be assessed. Engineering analysis and trade studies (e.g., threat analysis, functional criticality analysis, technology opportunities, evolved capability assessments) should adequately inform the program's technical strategy and identify system elements for MOSA implementation. Careful decisions regarding the design of system elements can enable the use of open standards and an open systems or modular approach that may allow for resiliency as well as reduce costs and promote competition during development, production, technology refresh, and life cycle extension. Design activities may include:

- Identify and analyze the constraints that the technology and design and realization techniques and approaches impose on the design solution.
- Develop design and implementation prototypes and solutions for the system elements.
- Analyze candidate system element design and implementation solutions and conduct variability studies to identify conflicts and resolution alternatives to ensure system integrity.
- Identify fabrication and quality procedures, and document design assumptions and decisions in the final system elements drawings or TDPs.
- Identify any special tools or processes required to sustain custom, or non-COTS, parts.

Realization

Realization is the process of building the system elements using specified materials and fabrication and production tools/procedures identified during design. Early fabrication and production planning is critical for the successful realization and delivery of the needed capability. System elements are built to the product baseline and should meet quality standards. Realization activities may include:

- Obtain or acquire access to materials and tools required to build system elements.
- Obtain external system elements as applicable.
- Build system elements in accordance with implementation procedures, tolerances, and other applicable policies/requirements.
- Determine system elements functionality against specified product quality characteristics.
- Document production and quality issues and associated corrective actions.
- Deliver implemented system elements for integration and verification.

The outputs of the Implementation process are the physical system elements as identified in the product baseline, including fabrication and production methods.

6.2.5 Integration Process

The Integration process provides a framework to systematically assemble lower-level system elements into successively higher-level system elements, iteratively with verification until the system itself emerges. Integration is essential to increasing system maturity, reducing risk, and preparing the system for transition to the warfighter. Architectures and integration strategies should be validated against MEIA experimentation results and reference architectures to ensure mission-level interoperability.

The PM, with support from the systems engineer, is responsible for planning, managing, and executing the Integration process. Experience has shown that programs that develop an integration plan are more successful. This plan defines the stages during which system elements are successively integrated to form higher-level elements and eventually the finished product. Alternative integration paths should be considered. The integration plan should include a description of the required System Integration Laboratories or other facilities, personnel, test stands, harnesses, testing software, and integration schedule.

The Interface Management process (6.1.8) is critical to the success of the Integration process. Interface control specifications or Interface Control Documents should be confirmed early on and placed under strict configuration control. All of the program's external interfaces and dependencies should be documented in the program's SEP. The SEP Outline requires that all programs with external dependencies or interfaces establish MOAs to formally document

commitments and management procedures. The SEP, updated in each phase, includes a table showing the status of all MOAs.

Integration activities support the Interface Management process by verifying that accurate and effective interface specifications are documented. In parallel, the program should include in the allocated baseline the verification methods for each integration level. The successive integration phases follow the sequence defined in the program's integration plan and lead to a final product ready for V&V.

6.2.6 Verification Process

The Verification process provides the evidence that the system or system element performs its intended functions and meets all performance requirements listed in the system performance specification and functional and allocated baselines. Verification answers the question, "Did you build the system correctly?" Verification is an important risk-reduction activity in the implementation and integration of a system and enables the program to catch defects in system elements before integration at the next level, preventing costly troubleshooting and rework.

The PM, systems engineer, software engineer, and test engineer (e.g., chief developmental tester) manage verification activities and methods as defined in the functional and allocated baselines and review the results of verification. See the T&E Enterprise Guidebook (2022) and DoDI 5000.89 for guidance for managing and coordinating integrated testing activities.

Verification begins during requirements analysis, when top-level stakeholder performance requirements are decomposed and eventually allocated to system elements in the initial system performance specification and interface control specifications. During this process, the program determines how and when each requirement should be verified and the tasks required to do so, as well as the necessary resources (test equipment, range time, personnel, etc.). The resulting verification matrix and supporting documentation become part of the functional and allocated baselines. The program completes verification using any combination of the following methods:

- **Demonstration.** Demonstration is the performance of operations at the system or system element level where visual observations are the primary means of verification. Demonstration is used when quantitative assurance is not required for the verification of the requirements.
- **Examination.** Visual inspection of equipment and evaluation of drawings and other pertinent design data and processes should be used to verify conformance with characteristics such as physical, material, part, and product marking and workmanship.
- **Analysis.** Analysis is the use of recognized analytic techniques (including computer models) to interpret or explain the behavior or performance of the system element. Analysis of test data or review and analysis of design data should be used as appropriate to verify requirements.

- **Test.** Test is an activity designed to provide data on functional features and equipment operation under fully controlled and traceable conditions. The data are subsequently used to evaluate quantitative characteristics.

The program should verify designs at all levels of the physical architecture through a cost-effective combination of these methods, all of which may incorporate modeling and simulation. The program should document verification activities and results among the artifacts for FCAs and the SVR (see Section 5.8, System Verification Review/Functional Configuration Audit). When possible, verification should stress the system, or system elements, under realistic conditions representative of its intended use.

The program should verify the individual system elements provided by the Implementation process through DT&E, acceptance testing, or qualification testing. During the Integration process, the program verifies successively higher-level system elements before allowing the elements to move to the next level of integration. Verification of the system as a whole occurs when integration is complete. As design changes occur, the program should assess each change for potential impact to the qualified baseline. This assessment may result in a need to repeat portions of verification to mitigate risk of performance degradation.

The output of the Verification process is a verified production-representative article with documentation to support Initial OT&E. The SVR provides a determination of the extent to which the system meets the system performance specification.

6.2.7 Validation Process

The Validation process provides the objective evidence that the system capability complies with stakeholder performance requirements, achieving its use in its intended operational environment. Validation answers the question, “Is it the right solution to the problem?” Validation consists of evaluating the operational effectiveness, operational suitability, sustainability, and survivability (including cybersecurity) or lethality of the system or system elements under operationally realistic conditions.

The PM, systems engineer, and software engineer support the Validation process. The chief developmental tester and the operational test agencies and evaluators are responsible for executing the Validation process, which is typically conducted by independent testers as documented in the TEMP (See T&E Enterprise Guidebook (2022)). System end users and other stakeholders typically participate in validation activities. Guidance for managing and coordinating integrated testing activities can be found in the T&E Enterprise Guidebook (2022) and DoDI 5000.89. Using and engaging integrated test teams composed of knowledgeable and experienced Government and industry developmental and operational testers can bring different perspectives and allow for an efficient use of resources.

Validation activities can be conducted in the intended operational environment or on an approved simulated environment. Early program-validation activities assist in the production of

validated CONOPS/OMS/MP, system performance specifications, use cases, functional and physical system architectures, and test cases.

A program should apply validation to the product baseline to ensure the emerging design meets the end-user needs. Models, simulations, mockups, and prototypes may be used in these early activities. They are often combined with the verification activities (see Section 6.2.6).

Aggressive early validation significantly mitigates the risk to the program by identifying operational issues up front when they are easier and less costly to fix. This approach ultimately improves system performance during the final validation activity (e.g., OT&E).

Final validation involves operational testing on a production-representative system in an operationally realistic environment. The product of the Validation process is a validated system and enabling system elements, leading to approval for FRP or a Full Deployment (FD) DR.

6.2.8 Transition Process

The Transition process moves any system element to the next level in the physical architecture. For the end-item system, it is the process to install and deploy the system to the user in the operational environment. The program may need to integrate the end-item system with other systems in the operational environment, honoring the defined external interfaces. In this case, the program should perform the Transition process in conjunction with the Integration process and Interface Management process for a smooth transition.

Early planning for system transition reduces risk and supports smooth delivery and rapid acceptance by the end user. Transition considerations should include, as appropriate, end-user and maintainer requirements; HSI and training; deployability; support tasks; support equipment; and packaging, handling, storage, and transportation (PHS&T). Part of the process is ensuring that each site is properly prepared for the receipt, acceptance, or installation of the system.

The Transition process includes maintenance and supportability activities for the deployed system and enabling system elements, as well as a process for reporting and resolving deficiencies. Sustainment and support planning should be documented in the LCSP, which is required for all acquisition programs and reviewed before Milestone A, B, and C, and FRP DR.

The PM, systems engineer, and PSM oversee all transition plans and activities required to install or deploy the end-item system, and associated enabling system elements, to the operational environment. The systems engineer leads engineering efforts to correct deficiencies found during transition and fielding. PMs should ensure all deliverables, particularly documentation (drawings, tech manuals, etc.), have been received from the contractor and made available to the activity responsible for sustaining the system through disposal.

7 DESIGN CONSIDERATIONS

Design considerations are factors that influence the design, characteristics, or behavior of a system. Design considerations may be mandated by law or regulation, while others are based on decades of experience, lessons learned, and best practices in system development. Some design considerations are concepts that assist trade-offs and should be accommodated or applied to each system or program. Others are constraints, boundaries, or limitations, with values that can sometimes be tailored or negotiated, but which generally represent immovable parts of the trade space. Whether mandated or recommended by best practice, systems engineers should address these factors to increase the likelihood of producing better systems for end users.

The PM, systems engineer, and software engineer should address and document design considerations, including all statutory and regulatory requirements in order to:

- Translate the end-user desired capabilities into a structured system of interrelated design specifications that support delivery of required operational capability.
- Enable trade-offs among the design considerations in support of achieving desired mission effectiveness within cost and schedule constraints.

The design considerations, as documented in the SE approach or SEP, should demonstrate critical thinking on the part of the PM, systems engineer, and software engineer. According to the SEP Outline, the SEP should include a table of design considerations that are relevant to the program and are an integral part of the design process, including trade-off analyses.

With the understanding that each design consideration is discrete, the PM, systems engineer, and other stakeholders should also view design considerations as an integrated set of variables that can influence one another. The PM, systems engineer, and software engineer should consider them in conjunction with one another to achieve better mission performance and to preclude a stovepipe view during design.

Table 7-1 lists the statutory requirements for the design considerations covered in this chapter, as well as applicable policy, guidance, and standards related to those design considerations. PMs and systems engineers can incorporate the standards into acquisition contracts to support delivery of required operational capability. The table contains several mandatory standards.

The table does not include additional design considerations levied by the Service, the Center, the platform, or the domain. Not all design considerations are equally important or critical to a given program, but all should be examined for relevancy.

Please note that ASSIST contains the most up to date information on standards. It is not possible, in many cases, to list every standard. This table should be used as a starting reference; please visit ASSIST (<https://assist.dla.mil>) to access the most up-to-date and comprehensive information.

Table 7-1. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Accessibility (Section 508 Compliance)	7.1	Section 508 of the Rehabilitation Act (i.e., 29 USC 794d) unless exempt by FAR Subpart 39.204, para (b), "Electronic and Information Technology"	- DoDD 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," Mar 17, 2016 - DoDI 5000.82, "Requirements for The Acquisition of Digital Capabilities" - DoDM 8400.01, "Accessibility of Information and Communications Technology (ICT)," Nov 2017 - FAR 39.204, "Acquisition of Information Technology" - DoDI 5000.95, "Human Systems Integration in Defense Acquisition"	FED-STD-795, "Uniform Federal Accessibility Standards" [Mandatory]
Affordability - SE Trade-Off Analysis	7.2		- DoW 5000.02, "Operation of the Adaptive Acquisition Framework" - DoDI 5000.85, "Major Capability Acquisition"	N/A
Anti-Counterfeiting	7.3	P.L. 112-81 (SEC 818), "Detection and Avoidance of Counterfeit Electronic Parts"	- DoDI 4140.67, "DoD Counterfeit Prevention Policy" - SD-19, "Parts Management Guide," Jan 2024	Search ASSIST for a current listing of government standards and DoW-adopted NGS (e.g., SAE AS5553D). Users are also encouraged to check standards development organizations' (e.g., SAE, ASTM) websites for new anti-counterfeit standards as technologies and test methods continue to evolve.
Commercial-Off-the-Shelf (COTS)	7.4	41 USC 104, "Commercially Available Off-the-Shelf Item" 41 USC 1907, "List of Laws Inapplicable to Procurements"	SD-2, "DoD Acquisitions Buying Commercial Items and Non-developmental Items," Nov 2018	N/A

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
		of Commercially Available Off-the-Shelf Items” • P.L. 103-355 (SEC 8104), “Preference for Acquisition of Commercial Items” • P.L. 104-106 (SEC 357), “Increased Reliance on Private-Sector Sources for Commercial Products and Services”		
Corrosion Prevention and Control (CPC)	7.5	• 10 USC 2228, “Office of Corrosion Policy and Oversight” • 10 USC 4251, “Major Defense Acquisition Programs: Factors to be Considered Before Milestone A approval” • 10 USC 4252, “Major Defense Acquisition Programs: Factors to be Considered Before Milestone B Approval”	• DoDD 5000.01, “The Defense Acquisition System,” Sep 9, 2020 • DoDI 5000.67, “Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure” • DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment, Aug 2022 • DFARS 223.73 “Minimizing the Use of Materials Containing Hexavalent Chromium” • DoDD 4151.18, “Maintenance of Military Materiel,” Aug 31, 2013 • DoDI 5000.91, “Product Support Management for the Adaptive Acquisition Framework” • Product Support Manager Guidebook, May 2022 • Integrated Product Support (IPS) Elements Guidebook, Jan 2024	• MIL-STD-810, “Environmental Engineering Considerations and Laboratory Tests” • MIL-STD-889, “Dissimilar Metals” • MIL-STD-1568, “Materials and Processes for Corrosion Prevention and Control in Aerospace Weapons Systems” • MIL-STD-1587, “Material and Process Requirements for Aerospace Weapons Systems” • NACE SP21412-2020-SSPC-CPC 1-2020, AMPP “Corrosion Prevention and Control Planning” Standard

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Critical Safety Item (CSI)	7.6	• P.L. 108-136 (SEC 802), "Quality Control in Procurement of Aviation Critical Safety Items and Related Services" • P.L. 109-364 (SEC 130), "Quality Control in Procurement of Ship Critical Safety Items and Related Services" • 10 USC 2319(g), "Encouragement of New Competitors"	• DoDM 4140.01, Volume 11, "DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling," Nov 2022 • Aviation Source Approval and Management Handbook, Mar 2011 • SECNAVINST 4140.2, "Management of Aviation Critical Safety Items" Also known as: ○ AFI 20-106 ○ DA Pam 95-9 ○ DLAI 3200.4 ○ DCMA INST CSI (AV) Management of Aviation CSIs • DFARS: ○ 209.270, "Aviation and ship critical safety items" ○ 246.407, "nonconforming supplies or services" ○ 246.504, "Certificate of conformance" ○ 246.370, "Notification of potential safety issues" ○ 252.246-7003, "Notification of potential safety issues" • Aviation Critical Safety Item (CSIs) Management Handbook, JALC, Mar 2011	• N/A

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Demilitarization and Disposal	7.7		- DoDI 4160.28, "Defense Demilitarization: Demilitarization Procedures" - DoDM 4160.28, "Defense Demilitarization: Demilitarization Procedures," Nov 2022 - DoDM 4140.01, Volume 6, "DoD Supply Chain Materiel Management Procedures: Materiel Returns, Retention, And Disposition," Nov 2022 - DoDM 4160.21, "Defense Materiel Disposition: Disposal Guidance and Procedures," Aug 2022	MIL-STD-882, "System Safety" [Mandatory]
Diminishing Manufacturing Sources and Material Shortages (DMSMS)	7.8		- SD-22, "Diminishing Manufacturing Sources and Material Shortages: A Guidebook of Best Practices for Implementing a Robust (DMSMS) Program," Mar 2024 - SD-19, "Parts Management Guide," Jan 2024 - SD-26, "DMSMS and Parts Management Contracting Guide," Jun 2023 - DoDI 4245.15, "Diminishing Manufacturing Sources and Material Shortages Management" - DoDM 4245.15, "Management of Diminishing Manufacturing Sources and Material Shortages," Oct. 2022 - DoDI 5000.85, "Major Capability Acquisition" - DoDI 4140.01, "DoD Supply Chain Materiel Management Policy"	- MIL-STD-11991, "Parts, Materials, and Processes Management" [Mandatory] - SAE STD-0016, "Standard for Preparing a DMSMS Management Plan"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
			DoDM 4140.01, Volume 3 “DoD Supply Chain Materiel Management Procedures: Materiel Sourcing,” Jul 2025	
Human Systems Integration (HSI)	7.9		- DoDD 5000.01, “The Defense Acquisition System,” Sep 9, 2020 - DoWI 5000.02, “Operation of the Adaptive Acquisition Framework” - DoDI 5000.95, “Human Systems Integration in Defense Acquisition” - HSI Guidebook, May 2022	- SAE 6906, “Standard Practice for Human Systems Integration” - SAE 1007, “Habitability domain standard” - SAE 1008, “Standard Practice for Force Protection and Survivability” - SAE 1009, “Design for Maintainer Standard” - SAE 1010, “Manpower and Personnel domain standard” - MIL-STD-1472, “Human Engineering” - MIL-STD-46855, “Human Engineering Requirements for Military Systems, Equipment, and Facilities” - ANSI/HFES 400, “Human Readiness Levels”
Insensitive Munitions (IM)	7.10	10 USC 2389, “Ensuring Safety Regarding Insensitive Munitions”	- DoDD 6055.09E, “Explosives Safety Management (ESM),” Jun 26, 2019 - Secretary of Defense Memorandum, “DoD Policy on Submunition Reliability,” Jan 10, 2001 - USD(AT&L) Memorandum, “Joint Insensitive Munitions Test Standards and Compliance Assessment,” Feb 10, 2010	MIL-STD-2105, “Hazard Assessment Tests for Non-Nuclear Munitions”

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
			• USD(AT&L) Memorandum, "Insensitive Munitions Strategic Plans," Jul 21, 2004 • DoD Acquisition Manager's Handbook for Insensitive Munitions, Nov 2008 • U.S. Navy Insensitive Munitions Handbook • TB 700–2, NAVSEAINST 8020.8B TO 11A-1-47 DLAR 8220.1, "Department of Defense Ammunition and Explosives Hazard Classification Procedures"	
Intelligence (Life Cycle Mission Data Plan (LMDP))	7.11		• DoDD 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," Aug 29, 2017 • DoDI 5000.85, "Major Capability Acquisition" • AAFDID	• N/A
Interoperability and Dependency (I&D)	7.12	• 44 USC 3506, "Federal Agency Responsibilities"	• DoDI 8330.01, "Interoperability of Information Technology, Including National Security Systems" • DoDD 5000.01, "The Defense Acquisition System," Sep 9, 2020 • DoDI 2010.06, "Materiel Interoperability and Standardization with Allies and Coalition Partners" • DoWI 5000.02, "Operation of the Adaptive Acquisition Framework"	• MIL-STD-1760, "Aircraft/Store Electrical Interconnection System"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Item Unique Identification (IUID)	7.13		- DoDI 8320.03, "Unique Identification (UID) Standards for Supporting the DoD Information Enterprise" - DoDI 4151.19, "Serialized Item Management (SIM) for Life-Cycle Management of Materiel" - DoWI 5000.02, "Operation of the Adaptive Acquisition Framework" - DoDI 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property" - DoDI 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property" - DoD Guide to Uniquely Identifying Items, Dec 2014 - DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements, Apr 2007 - DFARS 211.274-2, "Policy for item unique identification" - DFARS 252.211-7003, "Item Unique Identification and Valuation" - DFARS 252.211-7007, "Reporting of Government-Furnished Property"	MIL-STD-130, "Identification Marking of U.S. Military Property" [Mandatory]
Manufacturing and Quality	7.14	P.L. 111-383 (SEC 812), "Management of Manufacturing Risk in Major Defense Acquisition Programs"	- DFARS 207.105, "Contents of written acquisition plans" - DFARS 215.304, "Evaluation factors and significant subfactors" - SD-19, "Parts Management Guide," Jan 2024	- MIL-STD-11991, "Parts, Materials, and Processes Management" [Mandatory] - MIL-STD-31000, "Technical Data Packages" - ISO 9001, "Quality Management Systems – Requirements"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
				• SAE-AS9100, "Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations" • SAE-AS9003, "Inspection and Test Quality Systems Requirements for Aviation, Space, and Defense Organizations" • SAE-AS6500, "Manufacturing Management Program"
Modular Design	7.15	• 10 USC 4201, "Major Defense Acquisition Programs Defined: Definition; Exceptions"	• DoWI 5000.02, "Operation of the Adaptive Acquisition Framework" • DoDM 5010.12, "Procedures for the Acquisition and Management of Technical Data," Aug 2018	• MIL-STD-1553, "Digital Time Division Command/Response Multiplex Data Bus" • MIL-STD-1760, "Aircraft/Store Electrical Interconnection System" • MIL-STD-6017, "Variable Message Format (VMF) Main" • MIL-STD-6040, "U.S. Message Text Format (USMTF) Description"
Operational Energy	7.16	• 10 USC 138c, "Assistant Secretaries of Defense for Operational Energy Plans and Programs"		• N/A

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Packaging, Handling, Storage, and Transportation (PHS&T)	7.17	49 CFR Parts 171-180, "Hazardous Materials Regulations (HMR)"	- DoDI 4540.07, "Operation of the DoD Engineering for Transportability and Deployability Program" - DoD 4145.19-R, "Storage and Materials Handling" - DoDM 4140.27, "DoD Shelf-Life Management Program: Program Administration," Dec 2019	- MIL-STD-129, "Military Marking for Shipment and Storage" [Mandatory] - MIL-STD-2073, "Standard Practice for Military Packaging" [Mandatory] - ASTM-D3951, "Standard Practice for Commercial Packaging" [Mandatory] - MIL-STD-648, "Specialized Shipping Containers" - MIL-STD-1366, "Transportability Criteria" - MIL-STD-3037, "Inspection Criteria for International Organization for Standardization (ISO) Containers and Department of Defense Standard Family of ISO Shelters AMSC" - Please visit ASSIST for a comprehensive list of standards.
Reliability and Maintainability (R&M) Engineering	7.18	10 USC 4328, "Weapon System Design: Sustainment Factors"	- DoD R&M Engineering Management Body of Knowledge, Aug 2018 - RAM-C Rationale Report Outline Guidance, Feb 2017 - RAM-C Rationale Report Outline Guidance Training, June 2018 - Guidance for the Tailoring of R&M Engineering Data, April 2016 - SD-19, "Parts Management Guide," Jan 2024	- GEIA-STD-0009, "Reliability Program Standard for System Design, Development, and Manufacturing" - IEEE Standard 1633-2016, "IEEE Recommended Practice on Software Reliability"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
Spectrum Management	7.19	• 47 USC 305, “Telecommunications: Government Owned Stations” • 47 USC 901 - 904, “Telecommunications: § 901. Definitions; Findings; Policy § 902. Establishment; Assigned Functions § 903. Spectrum Management Activities § 904. General Administrative Provisions” • P.L. 102-538 (SEC 104), “National Telecommunications and Information Administration Organization Act”	• DoDI 3222.03, “DoD Electromagnetic Environmental Effects (E3) Program” • DoDI 4650.01, “Policy and Procedures for Management and Use of the Electromagnetic Spectrum” • DoWI 5000.02, “Operation of the Adaptive Acquisition Framework” • AR 5-12, “Army Use of the Electromagnetic Spectrum” • AFI 33-118, “Electromagnetic Spectrum Management” • SECNAVINST 2400.1 and 2400.2, “Electromagnetic Spectrum Policy and Management” • OPNAVINST 2400.20, “Electromagnetic Environmental Effects and Spectrum Supportability Policy and Management”	• MIL-STD-461, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment” • MIL-STD-464, “Electromagnetic Environmental Effects Requirements for Systems”
Standardization	7.20	• 10 USC 2451-2457, “Defense Supply Management”	• DoDI 4120.24, “Defense Standardization Program” • DoDM 4120.24, Defense Standardization (DSP) Procedures, Oct 2018 • Visit DSP website (https://www.dsp.dla.mil) for access to Standardization-related guidance documents (SDs)	• MIL-STD-11991, “Parts, Materials, and Processes Management” [Mandatory] • Please visit ASSIST for a comprehensive list of standards.
Supportability	7.21		• DoDD 5000.01, “The Defense Acquisition System,” Sep 9, 2020 • DoWI 5000.02, “Operation of the Adaptive Acquisition Framework”	• MIL-STD-11991, “Parts, Materials, and Processes Management” [Mandatory] • SAE-GEIA-STD-0007, “Logistics Product Data”

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
			- DoDI 4151.22, "Condition-Based Maintenance Plus for Materiel Maintenance" - DoDM 4151.25, "Reliability Centered Maintenance (RCM)," Jun 2011 - SD-19, "Parts Management Guide," Jan 2024 - MIL-HDBK-502, "Product Support Analysis," Apr 2025 - SD-22, "Diminishing Manufacturing Sources & Material Shortages (DMSMS) Guidebook," Mar 2024	SAE-TA-STD-0017, "Product Support Analysis"
Survivability (including CBRN)	7.22	P.L. 108-375 (SEC 1053), "Survivability of Critical Systems Exposed to Chemical or Biological Contamination"	- DoDI 3150.09, "The Chemical, Biological, Radiological, and Nuclear Survivability Policy" - DoWI 5000.02, "Operation of the Adaptive Acquisition Framework" - DoDI 5000.89, "Test and Evaluation" - DoDI 5000.95, "Human Systems Integration, See Force Protection and Survivability domain" - DoDM 5000.103, "Cyber DT&E" - DoD Cyber T&E Guidebook, v3.0, June 2025	- STANAG-4521, "Chemical, Biological, Radiological and Nuclear (CBRN) Contamination Survivability Factors in the Design, Testing and Acceptance of Military Equipment - AEP-7" [Mandatory] - MIL-STD-461, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" - MIL-STD-464, "Electromagnetic Environmental Effects Requirements for Systems" - MIL-STD-810, "Environmental Engineering Considerations and Laboratory Tests" - MIL-STD-1766, "Nuclear Hardness and Survivability Program Requirements for ICBM Weapon Systems"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
				• MIL-STD-3023, "High-Altitude Electromagnetic Pulse (HEMP) Protection for Military Aircraft" • MIL-STD-3056, "Design Criteria for Chemical, Biological, and Radiological System Contamination Survivability" • MIL-STD-4023, "High-Altitude Electromagnetic Pulse (HEMP) Protection for Military Surface Ships" • MIL-STD 2169, "High Altitude Electromagnetic Pulse (HEMP) Environment Standard" • MIL-STD 3065, "Satellite System Nuclear Survivability Protection Standard (SSNS-P)" • MIL-STD 3053, "Satellite Systems Natural and Nuclear Environments (SSNS-E)" • MIL-STD 3054, "Comprehensive Atmospheric Nuclear Environment Standard (CANES)" • MIL-STD 188-125-1, "HEMP Protection Fixed Facilities" • MIL-STD 188-125-2, "High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions – Part 2 - Transportable Systems"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
				- MIL-HDBK 533, "Satellite Systems Nuclear Survivability Design/Verification Handbook" - MIL-HDBK 423, "HEMP Protection for Fixed and Transportable Ground-Based C4I Facilities, Vol 1 Fixed Facilities"
System Safety (including Environment, Safety, and Occupational Health (ESOH))	7.23	42 USC 4321, "Congressional Declaration of Purpose" 42 USC 4331, "Congressional Declaration of National Environmental Policy" - EO 12114, "Environmental Effects Abroad of Major Federal Actions"	- DoDD 5000.01, "The Defense Acquisition System" - DoWI 5000.02, "Operation of the Adaptive Acquisition Framework" - DoDI 5000.85, "Major Capability Acquisition" - DoDI 5000.88, "Engineering of Defense Systems" - DoDI 5000.69, "Joint Services Weapon and Laser System Safety Review Processes" - DoDD 3000.09, "Autonomy in Weapon Systems," May 8, 2017 - DoDD 5137.02, "Under Secretary of Defense for Research and Engineering," Jul 15, 2020 - DoDI 4715.18, "Emerging Chemicals (ECS) of Environmental Concern" - DoDD 4715.21, "Improving Military Installation and Critical Resources Resilience," Aug 1, 2025 - DFARS 223.73, "Minimizing the Use of Materials Containing Hexavalent Chromium"	- MIL-STD-882, "DoD Standard Practice, System Safety" [Mandatory] - MIL-STD-1425, "Safety Design Requirements for Military Lasers and Associated Support Equipment" - NASA-STD-8719.14, "Process for Limiting Orbital Debris" - NAS 411, "Hazardous Materials Management Program" - NAS 411-1, "Hazardous Materials Target List"

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
			• MIL-STD 882, “DoD Standard Practice System Safety” • FAR 23.2, “Energy and Water Efficiency and Renewable Energy” • FAR 23.4, “Use of Recovered Materials and Biobased Products” • FAR 23.7, “Contracting for Environmentally Preferable Products and Services” • FAR 23.8, “Ozone-Depleting Substances and Greenhouse Gases” • Joint Software System Safety Engineering Handbook, Aug 2010 • Software System Safety, Implementation Process and Tasks Supporting MIL-STD-882, Joint Services – Software Safety Authorities (JS-SSA), Mar 2018 • Unmanned System Safety Engineering Precepts Guide for DoD Acquisition, Aug 2021	
System Security Engineering (SSE)	7.24	• 10 USC 2358, “Research and Development Projects”	• DoDI 5000.02 “Operation of the Adaptive Acquisition Framework” • DoDI 5000.83, “Technology and Program Protection to Maintain Technological Advantage” • DoDI 5200.39, “Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)”	• NIST SP 800-37: A complete guide to the risk management framework • NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations • NIST SP 800-160 Vol 1 & 2: Engineering Trustworthy Secure Systems

7. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance	Standards
			• DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)” • DoDI 8582.01, “Security Of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information” • Program Protection Plan Outline and Guidance, 2025 • DoDM 5000.103, “Cyber DT&E” • CJCSI 6510.01F: Information Assurance (IA) and Support to Computer Network Defense (CND) • DoDI 8500.01: Cybersecurity • DoD Cyber T&E Guidebook, v3.0, June 2025 • Technology and Program Protection Guidebook, 2022	

7.1 Accessibility (Section 508 Compliance)

DoW electronic and information technology (E&IT) systems must comply with Section 508 of the Rehabilitation Act (i.e., 29 USC 794d), unless exempt under FAR (Subpart 39.204, para (b), “Exceptions”) as a military system or National Security System. Compliance with Section 508 provides access by Federal employees with disabilities and the public to information and data that able-bodied persons can access through E&IT systems. Section 508 should be considered as a design requirement, addressed at each technical review and stated in the AS and SEP, or equivalent documentation.

PMs should ensure Section 508 compliance, unless exempt, while systems engineers are responsible for implementation through use of standards and compliant tools and products.

Resources to aid programs in complying are in Table 7-2. Additional information on accessibility is found in DoDI 5000.82, “Acquisition of Information Technology (IT),” and DoDM 8400.01, “Accessibility of Information and Communications Technology (ICT).”

Table 7-2. Links to Section 508 Government Resources

Description of Section 508 Government Resource	URL as of 2025
Section 508 technical standards	http://www.access-board.gov/508.htm
Federal rules for Section 508 implementation hosted by General Services Administration (GSA) include: • Roles and responsibilities of procurement officials and engineers • 508 best practices • Products and techniques	https://www.section508.gov/
The “Buy Accessible System” GSA site has free tools and guides for conduct of Section 508-compliant acquisitions as well as on-line training and help desk	https://www.buyaccessible.gov/
Department of Health and Human Services has: • Checklists • Code library • Test tools	http://www.hhs.gov/ found by searching on "section 508"
Department of Justice home page for Americans with Disabilities Act (ADA) has Federal laws and pending legislation	https://www.ada.gov/
Department of Veteran Affairs reports on Section 508 products and tools and tracks user comments	http://www.section508.va.gov/

7.2 Affordability – Systems Engineering Trade-Off Analyses

Affordability is a determination that the Life Cycle Cost (LCC) of an acquisition program is in consonance with the long-range investment and force structure plans of the DoW or individual

DoW components. SE trade-off analyses for affordability, a special application of the Decision Analysis process (see Section 6.1.2), should:

- Support the establishment of realistic affordability caps as documented in the program's APB, or equivalent documentation.
- Serve as inputs for the will-cost estimate and should-cost targets, including related should-cost initiatives.
- Enable continuous monitoring of program life cycle costs with respect to affordability caps across the system life cycle.

The SE trade-offs are conducted among cost, schedule, and performance objectives to ensure the program is affordable. The PM should identify the design performance points that are the focus of trade-off analyses to establish cost and schedule trade space. The PM presents the results of the trade-off analyses at program milestone/technical reviews, showing how the system's life cycle cost varies as a function of system requirements, major design parameters, and schedule. The results are used to identify cost and affordability drivers and to demonstrate how the cost-effective design point is established for the system.

7.3 Anti-Counterfeiting

An increasing threat of counterfeit (and fraudulent) parts in the global marketplace could affect every component of the program from COTS assemblies to military-unique systems. Preventing counterfeit parts from entering the supply chain reduces cost and negative impacts to program schedule and system performance. DoDI 4140.67, "DoD Counterfeit Prevention Policy," provides direction for anti-counterfeit measures for DoW weapon and information systems acquisition and sustainment to prevent the introduction of counterfeit materiel.

Counterfeit parts are pervasive in various supply chains and therefore have become a significant threat to the defense supply chain. Counterfeiters' motives are primarily greed (profit) or malicious intent. Counterfeits may appear at all phases of the life cycle, making it necessary for the PM, systems engineer, and PSM to plan for prevention, detection, remediation, reporting, and restitution activities from the beginning of the life cycle to disposal and demilitarization.

In order to properly assess the risks of counterfeit products, the PM needs to be aware that anti-counterfeit activities have relationships, as described in Table 7-3.

Table 7-3. Anti-Counterfeit Design Considerations Relationships

Design Consideration	Relationship
Commercial-Off-the-Shelf (COTS)	The Government and its industry agents have little to no visibility into the supply chains that create COTS products. Implications of this lack of visibility into the supply chain include counterfeit vulnerabilities and counterfeit parts being more readily available.
Corrosion Prevention and Control (CPC)	Counterfeits, by their nature, may have been falsely certified. In addition, if the counterfeit is a compound/material or component (e.g., gaskets, ground wires) intended to prevent or reduce corrosion, then effects of wear may appear sooner than predicted and the impacts to the system may be worse than expected or catastrophic.
Critical Safety Items (CSI)	From an anti-counterfeiting risk-based approach, CSIs should be more carefully scrutinized to ensure no counterfeits infiltrate the supply chain.
Cybersecurity	Cybersecurity in the supply chain cannot be viewed as an IT problem only. Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security, and many other functions across the enterprise and require a coordinated effort to address (NIST, Cyber Supply Chain Best Practices).
Demilitarization and Disposal	An excellent source for counterfeiters to obtain parts that can be turned into “used sold as new” parts (fraudulently certified as new).
Diminishing Manufacturing Sources and Material Shortages (DMSMS)	As systems age and the trustworthy sources for the piece parts dry up, counterfeiters increasingly take advantage of the situation by offering a source for hard-to-find parts.
Environment, Safety, and Occupational Health (ESOH)	Several examples of counterfeit materials that can increase ESOH risks include false R-134, a refrigerant that produces explosive by-products; fire extinguishers compressed with air; and faulty smoke detectors. Furthermore, Restriction of Hazardous Substances (RoHS) (2002/95/EC) has led to increased numbers of counterfeits, where a lead-free (Pb-free) microcircuit is sold as having tin-lead (SnPb) leads.
Item Unique Identification (IUID)	Successful implementation of IUID could reduce the ability of counterfeiters to introduce parts into supply. Conversely, IUID may provide a false sense of security if it can be duplicated by counterfeiters.
Manufacturing and Quality (M&Q)	M&Q can be severely degraded if supply is contaminated with counterfeits.
Modular Design (Modular Open Systems Approach (MOSA))	MOSA could provide a means to quickly certify a newer, more available part for use in systems, thus reducing the impact of DMSMS. Conversely, it could also result in more part numbers (equivalents) being introduced into supply, thus increasing the likelihood of counterfeit intrusion.
Reliability and Maintainability (R&M) Engineering	Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the authentic part.
Supportability	Increased failure rates resulting from counterfeits can have a negative impact on supportability and might drive the wrong problem-resolution behaviors and increase sustainment costs.
System Security Engineering (SSE)	SSE implements anti-counterfeit protection measures as part of a comprehensive plan to protect CPI and mission-critical functions and components (see T&PP Guidebook (2022)).

During development of the SEP and PPP, the PM, systems engineer, and PSM should consider these relationships and develop plans to address the threat.

7.4 Commercial-Off-the-Shelf

The use of COTS items, including Non-Developmental Items (NDIs), can provide significant opportunities for efficiencies during system development but also can introduce certain issues that should be considered and mitigated if the program is to realize the expected benefits.

The primary benefits of using COTS components in system design are to:

- Reduce development time.
- Allow faster insertion of new technology.
- Lower life cycle costs by taking advantage of the more readily available and up-to-date commercial industrial base.

However, regardless of the extent to which a system is made up of commercial items, the PM, systems engineer, and software engineer still develop, integrate, test, evaluate, deliver, sustain, and manage the overall system.

Concerns with using COTS products are:

- Subtle differences in product use can significantly affect system effectiveness, suitability, and survivability for achieving mission needs, HSI, ESOH, cybersecurity, reliability, and durability. More detailed analyses are required to understand trade-offs for implementing NDI/COTS solutions, to determine the impact of design considerations and communicate any associated risks to the PM.
 - Example: The graphical user interface design may not completely support user tasks or the TAD, which can cause an increased training burden, inefficient workarounds, and improper use of the system by the user, leading to human error and system or mission failures.
- If integration requires a “modified COTS product,” meaning a COTS product may not be designed for many military environments (which, by definition, is not a COTS product under 41 USC 104, but is allowed under 41 USC 1907), then the program may lose the ability to use the vendor’s subsequent product upgrades or to find a suitable replacement for the product from other commercial sources.
- The vendors can embed proprietary functions into COTS products, limiting supply sources.
- Vendors do not have to provide design information and often restrict purchasers from reverse engineering their intellectual property.

- Licensing agreements vary and can be restrictive while limiting the vendor's liability for merchantability for intended purposes.
- Supply chain risk management of COTS items is limited by the vendor, who is under no obligation to the purchaser to provide such information.
- Incorporating COTS products places constraints on the rest of the design and reduces trade space; functionality, interfaces, and reliability and maintainability characteristics are embedded in the choice of a COTS system element.
- If the COTS vendor stops manufacturing a product or changes the configuration drastically, the program may have difficulty finding suitable replacements or alternatives and may need to maintain different configurations of a single product.
- The program needs to understand the "pedigree" of the qualified vendors for the COTS product and the pedigree of the vendor suppliers.

The marketplace drives COTS product definition, application, and evolution. COTS products presume a flexible architecture and often depend on product releases that are designed to be used "as is" to meet general business needs and not a specific organization's needs. The commercial product life cycle is usually much shorter than the equivalent military product life cycle. Programs should consider the potential availability of suitable replacement or alternative items throughout the longer, military life cycle, and should monitor the commercial marketplace through market research activities and ongoing alignment of business and Technical Processes. This necessary activity imposes additional cost, schedule, and performance risks for which the acquisition community should plan. COTS products should be evaluated to meet all performance and reliability requirements during all environmental conditions and service life requirements specified by the intended application requirements documents.

P.L. 103-355 (Section 8104) and P.L. 104-106 (Section 357) both endorse the use of COTS products by the Federal Government but have slightly different definitions, with the latter allowing for modifications to COTS products.

The systems engineer should ensure open system design, identification, and mitigation of HSI, ESOH, and security risks, survivable technology insertion, or refresh throughout the projected system life cycle.

The PM, systems engineer, and software engineer should consider the following when evaluating use of COTS products:

- The intended product-use environment and the extent to which this environment differs from (or is similar to) the commercial-use environment.
- Integration, documentation, security, HSI, ESOH, hardware/software integrity, reliability risk, survivability, program protection, and corrosion susceptibility/risk.

- Planning for life cycle activities (including sustainment, supply chain risks, DMSMS, and disposal).
- Developing relationships with vendors, Foreign Ownership, Control, and Influence (FOCI) (see Defense Security Service for the latest policy regarding COTS products from FOCI sources).
- Supportability, if product modifications are made or if vendor or marketplace changes occur.
- T&E of COTS items (including early identification of screening, functionality testing and usability assessments) (See T&E Enterprise Guidebook (2022)).
- Protecting intellectual property rights by being aware of pertinent intellectual property rights issues associated with commercial items acquisitions, especially with the acquisition of commercial software products. When acquiring intellectual property license rights, the acquisition community should consider the core principles described in the DoW guide: “Intellectual Property: Navigating through Commercial Waters.”
- Ability to modify or interface COTS software with other software even if Government-generated or owned.
- Ability to have insight into CM, and the features and functions of upgrades and changes.
- Ability to instrument or test aspects of COTS products.

7.5 Corrosion Prevention and Control

The corrosion of military equipment and facilities costs the DoW approximately \$20 billion annually. In addition, corrosion degrades system availability, safety, and ESOH factors. Therefore, acquisition officials should fully consider CPC as early as possible in the acquisition life cycle and should implement appropriate strategies to minimize the life cycle impact.

Sound CPC planning reduces life cycle costs, improves maintainability and availability, and enhances ESOH compliance. The Association for Materials Protection and Performance (AMPP) Corrosion Prevention and Control Planning Industry Standard (SSPC-CPC-1/NACE-21412-2020) and the DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment (MS&E) (OUSD(A&S) 2022, i.e., CPC Planning Guidebook) helps PMs, systems engineers, PSMs, and other program staff understand the key elements of CPC planning in order to develop and execute a comprehensive CPC approach.

DoDI 5000.67, DoDI 5000.91, and DoDD 4151.18 require CPC planning and execution for all acquisition programs across the life cycle. The PM is responsible for identifying and evaluating corrosion considerations throughout the acquisition and sustainment phases to reduce, control, or mitigate corrosion. The PM and lead systems engineer should conduct CPC planning, ensure corrosion control requirements are included in the system design and verified as part of test and acceptance programs, and include CPC management and design considerations in the SEP and

LCSP, or equivalent documentation. Product support planning should be developed based on understanding the CPC risks inherent in the system design in order to develop appropriate corrosion maintenance strategies to meet sustainment and operational availability requirements.

Good CPC planning and execution includes, but is not limited to, the following elements:

- Engaging corrosion expertise relevant to the system and its operating environment early and throughout the life cycle.
- Examining legacy systems for corrosion-prone designs and possible corrosion-design improvements.
- Documenting alternative material and process assessments that offer increased corrosion protection.
- Including CPC as a consideration in trade studies involving cost, useful service life, and effectiveness.
- Incorporating CPC requirements, plans, specification, standards, and criteria into relevant contractual documentation for all equipment and facilities.
- Including CPC in Integrated Product Support Element (IPSE) development and evaluation, including facilities (see T&E Enterprise Guidebook (2022)).
- Identifying planning, resourcing, and acquisition of corrosion-related features for longevity, lowest TOC, and sustained system effectiveness.
- Retaining access to CPC resources throughout the life cycle.

All designated ACAT programs are required to conduct CPC planning across their life cycle. Refer to the DoD Corrosion Prevention and Control Planning Guidebook for MS&E for more information.

In addition to the SEP and LCSP, CPC planning and execution for all ACAT programs should be reflected in other program documents, including, but not limited to:

- AS
- TEMP
- RFP and contract
- Program schedule – IMP/IMS
- Funding/budget
- PESHE (i.e., DFARS (Subpart 223.73, Minimizing the Use of Hexavalent Chromium))
- System finish/process specification (add to the SOW and as a DID to the CDRL)

- Contractor CPC Plan (add to the SOW/Statement of Objectives/Performance Work Statement and as a DID to the CDRL)
- System performance specifications

In the contract and RFP, CPC planning and execution should be addressed in the management and technical content of each contract/RFP section and subsection, including, but not limited to, the SOW, IMP/IMS, CDRL, DID, and system performance specifications (see Section 4.6, Systems Engineering Role in Contracting, and the DoD Corrosion Prevention and Control Planning Guidebook for MS&E).

7.6 Critical Safety Item

A CSI is a part, assembly, software, or piece of support equipment whose failure could cause loss of life, permanent disability or major injury, loss of a system, or significant equipment damage. Special attention should be placed on CSIs to prevent the potential catastrophic or critical consequences of failure. Significant problems occurred when DoW purchased CSIs from suppliers with limited knowledge of the item's design intent, application, failure modes, failure effects, or failure implications.

The purpose of CSI analysis is to ensure that PMs for DoW acquisition programs who enter into contracts involving CSIs do so only with resources approved by the Design Control Activity (DCA). The DCA is defined by law as the systems command of a Military Department. The DCA is responsible for the airworthiness or seaworthiness certification of the system in which a CSI is used.

The intent of CSI laws, policies, regulations, and guidance is to reduce the likelihood and consequence of failure by mitigating receipt of defective, suspect, improperly documented, unapproved, and fraudulent parts having catastrophic potential. These statutory requirements are contained in P.L. 108-136 (Section 802), enacted to address aviation CSIs, and P.L. 109-364 (Section 130), enacted to address ship CSIs, embedded in 10 USC 2319. The statute addresses three areas:

- Establish that the DCA is responsible for processes concerning the management and identification of CSIs used in procurement, modification repair, and overhaul of aviation and ship systems.
- Require that DoW work only with sources approved by the DCA for contracts involving CSIs.
- Require that CSI deliveries and services performed meet all technical and quality requirements established by the DCA.

CSI policies and guidance ensure that items of supply that are most critical to operational safety are rigorously managed and controlled in terms of:

- Supplier capability
- Conformance to technical requirements
- Controls on changes or deviations
- Inspection, installation, maintenance, and repair requirements

DoDM 4140.01, Volume 11, establishes top-level procedures for the management of aviation CSIs. The Joint Aeronautical Commanders Group (JACG) issued the Aviation Critical Safety Items (CSI) Management Handbook (2011). This guidance establishes standard user-level operating practices for aviation CSIs across the Services, the DLA, the DCMA, and other Federal agencies. Appendix I of the Aviation CSI Management Handbook is a joint Military Service/Defense Agency instruction on “Management of Aviation Critical Safety Items” issued on January 25, 2006. This instruction (SECNAVINST 4140.2, AFI 20-106, DA Pam 95-9, DLAI 3200.4, and DCMA INST CSI (AV)) addresses requirements for identifying, acquiring, ensuring quality of, managing, and disposing of aviation CSIs. Similar policies and guidance are being developed or revised to address ship CSIs as defined by public law.

The DFARS was amended to implement the contractual aspects regarding aviation CSIs. Comparable DFARS amendments are being developed to address ship CSIs. DFARS (Subpart 209.270) states that the DCA is responsible for:

- Identifying items that meet aviation CSI criteria
- Approving qualification requirements
- Qualifying suppliers

This supplement states that the contracting activity contracts for aviation CSIs only with suppliers approved by the DCA. PMs should coordinate with the contracting activity to ensure they contract for aviation CSIs only with suppliers approved by the DCA and that nonconforming aviation CSIs are to be accepted only with the DCA’s approval, as required by DFARS (Subpart 246.407). DFARS (Subpart 246.407) was amended to state that DCA authority can be delegated for minor nonconformance. DFARS (Subpart 246.504) requires DCA concurrence before certificates of conformance are issued to accept aviation CSIs.

Because the developer may uncover problems with products after items are delivered, DFARS (Subpart 246.371) and DFARS (Subpart 252.246-7003) require the developer to notify the procuring and contracting officers within 72 hours after discovering or obtaining credible information that a delivered CSI may have discrepancies that affect safety. PMs should coordinate with the contracting authority to be kept aware of materiel recalls and shortfalls that may impact production rates and sustainment.

The CSI list evolves as the design, production processes, and supportability analyses mature. PMs identify and document CSIs during design and development to influence critical downstream processes, such as initial provisioning, supply support, and manufacturing planning to ensure adequate management of CSIs throughout a system's O&S phase.

For programs in the MCA pathway, the PM should ensure that the allocated baseline established at the PDR includes an initial list of proposed CSIs and a proposed process for selecting and approving CSIs, and that it addresses the critical characteristics of those items. Before the CDR, the program office, with support from the DCA and developer/original equipment manufacturers, should ensure there is a clear understanding of CSI processes, terms, and criteria. The initial product baseline, established at CDR, should have 100 percent of drawings completed for the CSIs. Throughout LRIP (if applicable), conduct of the PCA and establishment of the product baseline, the program should update the CSI list and review it to ensure the list reflects the delivered system. Before the FRP/FD DR, a final CSI list should be documented and approved by the DCA.

7.7 Demilitarization and Disposal

The incorporation of demilitarization (DEMIL) and disposal requirements into the initial system design is critical to ensure compliance with:

- All DoW DEMIL and disposal policies.
- All legal and regulatory requirements and policies relating to safety (including explosive safety), security, and the environment.

PMs and PSMs should ensure, as an essential part of SE, that DEMIL and disposal requirements are incorporated in system design to minimize DoW's liabilities, reduce costs, and protect CPI and technology. For programs in the MCA pathway, this includes integrating DEMIL and disposal into the allocated baseline approved at the PDR and refining DEMIL and disposal requirements in the initial product baseline at the CDR. DEMIL and disposal requirements are included in the program's SEP, LCSP, or equivalent documentation, and contract(s). For munitions programs, DEMIL and disposal documentation need to be in place before the start of DT&E.

DEMIL eliminates functional capabilities and inherent military design features from both serviceable and unserviceable DoW materiel. It is the act of destroying the military offensive or defensive advantages inherent in certain types of equipment or material. DEMIL may include mutilation, scrapping, melting, burning, or alteration designed to prevent the further use of this equipment and material for its originally intended military or lethal purpose. Systems engineers integrate DEMIL considerations into system design to recover critical materials and protect assets, information, and technologies from uncontrolled or unwanted release and disruption or reverse engineering. PMs should ensure the DEMIL of materiel is accomplished in accordance with DoDI 4160.28, "Defense Demilitarization: Demilitarization Procedures."

Disposal is the process of reusing, transferring, donating, selling, or destroying excess surplus and foreign excess property. Disposal first ensures adequate screening is accomplished to satisfy all valid DoW and other U.S. Government agency needs. After assurances that Government needs for surplus DoW property are met, the materiel disposition process:

- Permits authorized transfer or donation to Government or non-Government entities.
- Obligates DoW to obtain the best-available monetary return to the Government for property sold.

PMs ensure disposal is accomplished in accordance with DoDI 4140.01 and DoDM 4160.21-M, Volume 1, Defense Materiel Disposition: Disposal Guidance and Procedures.

The program's plan for DEMIL and disposal of DoW excess and surplus property protects the environment and personnel and minimizes the need for abandonment or destruction. During system design, the systems engineer supports the PM's plans for the system's demilitarization and disposal, through the identification and documentation of hazards and Hazardous Materials (HAZMAT) related to the system, using MIL-STD-882, System Safety. Early, balanced analyses of ESOH hazards relative to the system's design enable the PM to make informed decisions based on alternatives and provide a clear understanding of trade-offs and consequences, both near term and over the system's life cycle.

7.8 Diminishing Manufacturing Sources and Material Shortages

DMSMS is the loss, or impending loss, of manufacturers or suppliers of items, raw materials, or software. DMSMS-generated shortages in the ongoing production capability or life cycle support of a system or shortages in any training, support, or test equipment already in the field can endanger mission effectiveness. While DMSMS issues can be caused by many factors, their occurrence is inevitable.

The PM, the PSM, and systems engineer should develop a technology management strategy for maintaining insight into technology trends and internal product changes by the manufacturer and test the effects of those changes on the system when necessary. This insight into technology trends could result in seamless upgrade paths for technologies and system elements and provide a timetable for replacing system elements to improve supportability even if those system elements are not obsolete. The PM, PSM, and systems engineer should incorporate the technology management strategy into design activities and ensure the program's intellectual property strategy attains the appropriate technical data (e.g., indented bills of material or parts lists) as best practices to reduce DMSMS cost and readiness impacts throughout the life cycle.

A DMSMS resilient design both delays the occurrence of DMSMS issues and increases the likelihood of low-cost resolutions being available. The systems engineer should be aware of and consider DMSMS resilience during system design. Following are several practices the program should consider promoting DMSMS resilience:

- Avoid selecting technology and components that are near the end of their functional life.
- During the design process, proactively assess the risk of parts obsolescence while selecting parts.
- When feasible, use a MOSA to enable technology insertion/refreshment more easily than with design-specific approaches.
- Proactively monitor supplier bases to prevent designing in obsolescence; participate in cooperative reporting forums, such as the Government-Industry Data Exchange Program, to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities, and equipment.
- Proactively monitor potential availability problems to resolve them before they cause an impact in performance readiness or spending.

In addition, by using MIL-STD-11991 (General Standard for Parts, Materials, and Processes), the program can enhance the reliability of the system and mitigate DMSMS.

Useful resources for additional guidance include the following:

- SD-19, Parts Management Guide
- SD-22, Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook
- SD-26, DMSMS and Parts Management Contracting Guide
- DoDI 5000.85, “Major Capability Acquisition”
- DoDI 4245.15, “Diminishing Manufacturing Sources and Material Shortages Management”
- DoDM 4245.15, “Management of Diminishing Manufacturing Sources and Material Shortages”
- DoDI 4140.01, “DoD Supply Chain Materiel Management Policy”
- DoDM 4140.01, Volume 3 “DoD Supply Chain Materiel Management Procedures: Materiel Sourcing”

7.9 Human Systems Integration

SE addresses the three major elements of each system: hardware, software, and human. SE integrates human capability considerations with the other specialty engineering disciplines to achieve total system performance requirements by factoring into the system design the capabilities and limitations of the human operators, maintainers, and support personnel (i.e., users). Within the SE process, HSI involves both the technical and program management efforts

that provide integrated and comprehensive analysis, design, and assessment of human performance requirements, concepts, and resources for the seven HSI domains. HSI supports enhanced operational effectiveness, optimal system design, and reduction in TOC.

The HSI effort assists the PM (i.e., Component Capability Developer) and systems engineer to minimize ownership costs and ensure the system is built to accommodate the human performance characteristics of users who operate, maintain, and support the total system. The total system includes not only the mission equipment but also the users, training and training devices, and operational and support infrastructure.

DoDI 5000.02 describes planning considerations for seven HSI domains. DoDI 5000.95 (2022), further states:

Component capability developer or program manager will:

- a. Plan for and implement an HSI program from initial user requirements through the program life cycle to system disposal, appropriate to the system's acquisition pathway.
- b. Perform, document, and manage program and systems human-centered design considerations and readiness risks through trade-off analyses among the HSI domains. The trade-off analyses will ensure human performance data systematically informs and facilitates total system performance in both materiel and non-materiel solutions during SE activities.
- c. Ensure that DoW Component HSI SMEs and HSI practitioners are engaged with working groups tasked with the development and review of program documents.

The DoW Component capability developer or program manager should formulate a comprehensive HSI program using an appropriate strategy to ensure HSI-related and human performance requirements are achieved. The program will consist of risk management, engineering, analysis, and human-centered design activities, in accordance with DoDI 5000.02. The HSI Guidebook (2022) covers HSI activities throughout concept development, design, test, production, deployment, operational use, and disposal and addresses HSI domain activities, trade-offs, and the integration of HSI with SE and logistics. Execution of HSI activities should be tailored to the unique acquisition program.

The PM is responsible for integrating the recommended elements to establish an effective HSI program (see HSI Guidebook (2022)). The PM, systems engineer, and software engineer should use SAE 6906 to conduct best practice of HSI on the program. Throughout the acquisition life cycle, the systems engineer should apply HSI design criteria, principles, and practices described in MIL-STD-1472 (Human Engineering) and MIL-STD-46855 (Human Engineering Requirements for Military Systems, Equipment and Facilities).

The systems engineer supports the PM by leading HSI efforts. The systems engineer should work with the manpower, personnel, training, safety and occupational health, habitability, force protection, and (personnel and system) survivability (FP&S) and HF (Human Factors Engineering) SMEs to develop the HSI program effort aligned to the SE process. The systems engineer translates and integrates those human capability and limitations (i.e., constraints) considerations, as contained in the capabilities documents, into quantifiable system requirements. Requirements for conducting HSI efforts should be specified for inclusion in the SOW and contract in accordance with SAE 6906. HSI should also be addressed in the SEP, specifications, TEMP, SDP, LCSP, and other equivalent program documentation. The SEP Outline requires that HSI be addressed as a Specialty Engineering discipline. The SEP, or equivalent, should address the following:

- Human aspects of architectures and interface control as appropriate.
- HSI staffing, resources, activities, tools, and schedules.
- HSI risk and issue management and tracking.
- HSI working group hierarchy and relationship with other SE IPTs and working groups.
- HSI related TPMs.
- HSI entrance and exit criteria for SE technical reviews.

In the conduct of SE technical reviews, emphasis is placed on assessing the following HSI attributes:

- HSI requirements based on a top-down requirements analysis (including allocating an optimal crew concept and allocating system functions to automation and human performance).
- Position descriptions based on functions for crew position, including duties, jobs, responsibilities, and levels of authority.
- HSI inputs to acquisition documents and specifications.
- HSI risk assessment and mitigation plans, identifying factors that affect manpower, human effectiveness, workload, survivability, and safety.

See also the HSI Guidebook (2022) and the WarU Acquisition Knowledge Matrix (<https://www.waru.edu/acquisition-knowledge-matrix>).

7.10 Insensitive Munitions

The term “Insensitive Munitions” (IM) implies that unanticipated stimuli will not produce an explosive yield, in accordance with MIL-STD-2105 (Hazard Assessment Tests for Non-Nuclear Munitions). IM minimizes the probability of inadvertent initiation and the severity of subsequent collateral damage to weapon platforms, logistic systems, and personnel when munitions are

subjected to unanticipated stimuli during manufacture, handling, storage, transport, deployment, or disposal, or because of accidents or action by an adversary.

IM is a component of explosives ordnance safety described in 10 USC 2389, which specifies that it is the responsibility of DoW to ensure IM under development or procurement are safe, to the extent practicable, throughout development and fielding when subjected to unplanned stimuli, (e.g., electro-magnetic interference, vibration, or shock). The PM, systems engineer, and software engineer for munitions programs and other energetic devices (such as ordnance, warheads, bombs, and rocket motors) and munitions handling, storage, and transport programs have an overriding responsibility to address safety aspects of their programs in trade studies, design reviews, milestone reviews, and in program requirements documents.

The PM, systems engineer, and software engineer for munitions programs, regardless of acquisition pathway or ACAT level, should consider safety a priority when performing trade studies or making program decisions. The PM and cognizant technical staff should coordinate IM/Hazard Classification (HC) test plans with the Service IM/HC testing review organizations. The Service organizations should coordinate the IM/HC with the Joint Services Insensitive Munitions Technical Panel, Joint Service Hazard classifiers, and the DoW Explosives Safety Board, which is chartered by DoDD 6055.09E, “Explosives Safety Management.” Aspects of IM also apply to nuclear weapons but are not addressed here.

The primary document to address IM is the Insensitive Munitions Strategic Plan (IMSP). The DoD Standard Operating Procedure for IMSP and the Plan of Action and Milestones (POA&M), defined by Joint Business Rules, March 2011, define the content of the IMSP, which spans the Future Years Defense Program and includes currently funded as well as unfunded requirements. The DoD Acquisition Manager’s Handbook for Insensitive Munitions contains the above-referenced documents and appendices for each Service’s policy and review board process.

The IMSP is the primary program output required by USD for Acquisition and Sustainment and the Joint Staff to provide evidence that the program is in compliance with all applicable laws and regulations. Both the Component-level and DoW-level IM review organizations can provide additional guidance and can assess the adequacy of the IMSP. In addition to the IMSP, the AS, SEP, TEMP (or equivalent documents), Risk Management Plan, and other program requirements documents address aspects of explosives ordnance safety, including IM.

7.11 Intelligence (Life Cycle Mission Data Plan)

In collaboration with the intelligence community and the operational sponsor(s), the PM, with support from the systems engineer and chief developmental tester, is responsible for planning, identifying, documenting, communicating, and programming for life cycle IMD (intelligence mission data) support (see Figure 7-1 and DoDD 5250.01).

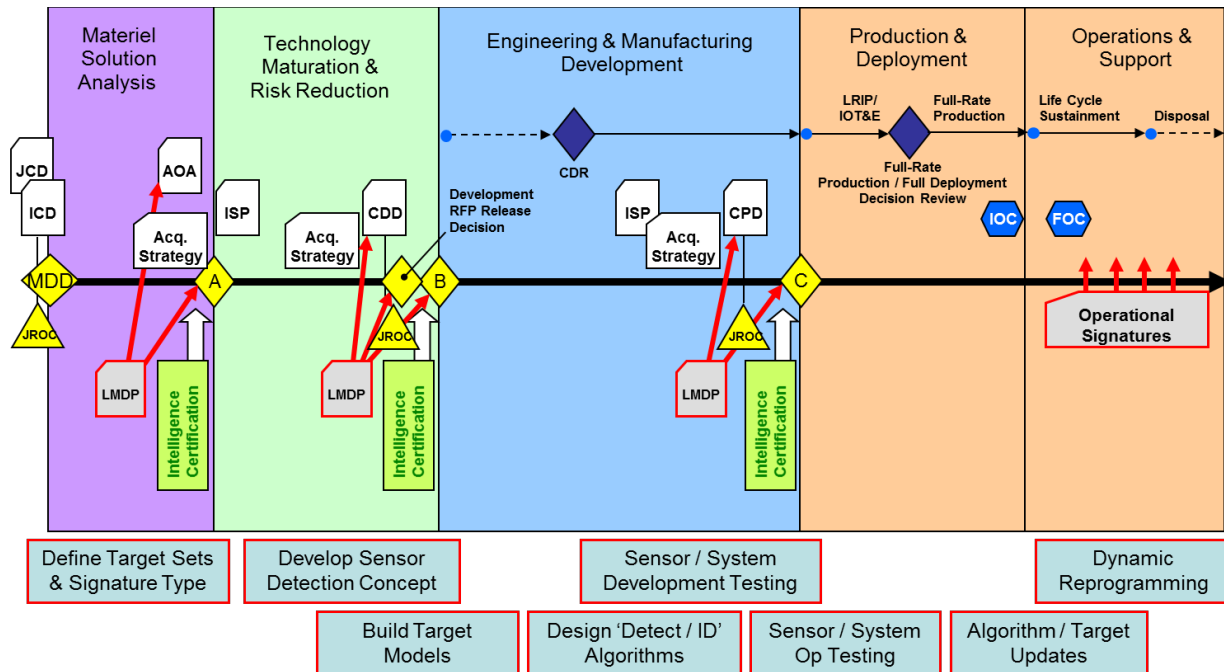


Figure 7-1. Intelligence Mission Data Life Cycle Timeline (MCA Pathway)

Modern weapon systems depend on a variety of scientific and technical intelligence products throughout every stage of their life cycle, so programs must plan for IMD support, which informs design and development trade-offs, risk assessments, and decisions. Similarly, it is critical for programs to communicate IMD requirements to the DoW intelligence community that supplies the necessary intelligence data.

Modern weapon systems are often intended to operate in threat and target environments throughout the world in multiple domains. System design decisions, development trade-offs, and advanced technology insertion may be optimized, thereby creating sensitivities to changes in adversary capabilities in the threat and target environments. Critical intelligence parameters (CIP) represent key performance thresholds of foreign threat systems, which, if exceeded, could compromise the mission effectiveness of the system in development. Therefore, these CIPs (for example, radar cross-section, armor type, or thickness or acoustic characteristics) should be identified and communicated to the Intelligence Community for tracking and immediate notification if breached.

To address threats as they emerge and change over the program's life cycle, the PM, systems engineer, system security engineer, and software engineer should continuously engage with stakeholders to identify how threats are expected to evolve and use this information to ensure the system architecture is flexible to the maximum extent practicable so system updates can be made efficiently and effectively to address these threats. See the Intelligence Support to the Adaptive Acquisition Framework (ISTA AF) Guidebook (2023) (Intelligence Support Guidebook (2023)) for more information on CIPs.

Intelligence life cycle mission data planning is necessary to effectively:

- Derive functional baseline requirements and life cycle IMD requirements necessary to identify, define, and refine sensors, algorithms, and intelligence data needs and trade-offs.
- Design, develop, test, and evaluate IMD-dependent sensors, algorithms, systems, processes, and interfaces.
- Conduct effectiveness analyses and risk assessments.
- Identify and acquire threat and target parameters that support digital modeling and simulation (see Section 3.2, Models and Simulations).
- Develop TPMs to inform T&E.
- Inform decision making and science and technology investments for identifying IMD production and collection requirements.
- Assess system capability and limitations.
- Ensure system flexibility and agility in response to a dynamic threat and target environment.

The Intelligence Support Guidebook (2023) provides key linkages to the system performance specification (sometimes called the SRD), SEP, and TEMP, or equivalent documentation. These three products are directly affected by IMD requirements.

7.12 Interoperability and Dependencies

Almost all DoW systems operate in an SoS context relying upon other systems to provide desired user capabilities – making it vital that interoperability needs and external dependencies are identified early and incorporated into system requirements. When identifying system requirements, it is critical to consider the operational and SoS context. These include, but are not limited to, physical requirements (size, power limits, etc.), electronic requirements (signature, interference, etc.), and information exchange/management (network, bandwidth, information needs, data format, secure transmission, etc.). These system requirements also include interdependencies with other systems. For efficiency, systems often rely on service provided by other systems or on reuse of system elements developed by other programs. Interoperability assessments should be validated by MEIA mission thread experimentation to ensure cross-service and mission-area integration.

Interoperability is the requirement that the program's system interact with other systems through transport of information, energy, or matter. For example, an air-launched missile is required to be interoperable with its delivery platform(s). Information is exchanged. A mechanical interface secures the missile until launch and so on. Usually, interoperability involves external interfaces (see Section 6.1.8, Interface Management Process) and is essential for the creation of SoS. Every

system is required to be certified interoperable before it is fielded. The Joint Interoperability Test Command is responsible for this certification.

Dependencies are relationships between different programs that cause one program to rely on another program's actions or products to successfully meet its requirements. As examples, a ship development program may require prototypes of mission modules being developed by another program during developmental testing, or a weapon may depend on new sensor capabilities provided by another system. The program depends on the mission module or sensor program to enable it to meet its testing schedule. A schedule issue could occur if the needed prototypes are not available in time for the tests. A performance issue could occur if the designs of the two systems do not support the needed end-to-end capability.

The common element linking I&D is the need for cooperation and coordination between separate programs. Two common ways to meet this need are MOAs and invited attendance at program technical reviews and other technical meetings. MOAs are agreements between programs that specify expectations as to performance, resources, management and schedules. Interchange between engineers and managers at technical meetings opens lines of communication, which permits risk identification and early mitigation.

The PM is responsible for ensuring that the operational and SoS context for the system are well understood. The PM is also responsible for establishing required MOAs and managing relationships with other programs.

The systems engineer is responsible for ensuring all I&D impacts are analyzed and coordinated with the appropriate internal/external stakeholders and translated into system requirements and design considerations.

Analysis conducted for the SoS contexts for the system – where the system is dependent on other systems and where the system needs to interact with other systems – enables translation of I&D into system requirements. I&D requirements call for collaborative implementation approaches with external organizations, including identification, management, and control of key interfaces. Areas of dependency and interoperability should be reviewed for risks to the program and plans made to manage and mitigate those risks. This review includes system interdependencies (e.g., a weapon may depend on new sensor capabilities provided by another system) and information exchanges with other systems required to support mission capabilities. For efficiency, systems may rely on system elements developed by others for functionality, either through services (e.g., weather information) provided by other systems or through reuse of system elements (e.g., engines, radios) developed by other programs. The systems engineer analyzes these contexts to identify system requirements and risks, including actions needed by external parties (e.g., other systems or infrastructure) for the system to meet user requirements.

Additional DoW policy and guidance regarding I&D, summarized below, seek to ensure systems work effectively with other systems:

- DoDI 8330.01, and 44 USC 3506: Interoperability of IT and National Security System (NSS) acquisition programs is required to comply with these sources.
- DoDD 5000.01, Section 1.2: “Joint concepts, standardization, and integrated architectures will be used to the maximum extent possible to characterize the exchange of data, information, materiel, and services to and from systems, units, and platforms to assure all systems effectively and securely interoperate with other U.S. forces and coalition partner systems.”
- DoDI 2010.06: Programs should pursue opportunities throughout the acquisition life cycle to enhance international cooperation and improve interoperability with allies and partners.

7.13 Item Unique Identification

IUID is a systematic process to distinguish one item globally and unambiguously from all the other items that DoW buys or owns. IUID-enabled Serialized Item Management (SIM) provides a capability that allows DoW to locate, control, value, and manage its assets throughout the life cycle. A robust SIM program provides tools and processes to assist informed decision making to achieve better system reliability and readiness at reduced TOC. IUID-enabled SIM provides DoW with a standard methodology to:

- Consistently capture the value of all individual items it buys or owns.
- Trace these items during their use.
- Combat counterfeiting of parts.
- Associate valuable business intelligence to an item throughout its life cycle via automatic identification technology and connections to automated information systems.

PMs and PSMs should budget, plan for, and implement IUID-enabled SIM as an integral activity within MIL-STD-130 (Identification Marking of U.S. Military Property) requisite item identification processes to identify and track applicable major end items and configuration-controlled items. IUID implemented in accordance with DoDI 8320.04 and IUID Implementation Plans are required for all milestone decisions as directed by the Milestone Document Identification. IUID-specific design considerations are required in the SEP or equivalent document. SIM planning and implementation required by DoDI 4151.19 are addressed in the LCSP or equivalent document.

The systems engineer considers what to mark and how to incorporate the IUID mark within MIL-STD-130 item-marking requirements when formulating design decisions. In addition, the systems engineer considers where product and maintenance information reside and how the life

cycle data are used within the CM and product support systems – including new and legacy information systems.

The DoD Guide to Uniquely Identifying Items (2014) provides guidance on implementing IUID intended for use by DoW contractors and their suppliers, who put unique item identifier marks on new items during production, as directed in the contract.

7.14 Manufacturing and Quality

M&Q management share some common characteristics. All programs must develop and then execute their M&Q plans and strategies, including attention to producibility. The Government develops a Manufacturing Strategy and a Quality Strategy. The contractor develops a Manufacturing Plan and a Quality Plan. M&Q considerations begin early and continue throughout the acquisition process, regardless of acquisition pathway.

The contractor should be required to develop and implement a Manufacturing Management System (MMS) and a QMS. PMOs should not dictate in the contract specific MMS or QMS, but these systems should share common elements or framework with industry best practices.

A Manufacturing Management Program describes the proven manufacturing management practices. The industry standard for Manufacturing Management is SAE AS6500, “Manufacturing Management Program.” The Government’s implementation of SAE AS6500 is detailed in MIL-HDBK-896, “Manufacturing Management Program Guide.” The PMO team should identify the appropriate contract manufacturing requirements.

- A Manufacturing Strategy should be tied to the program’s acquisition strategy and should focus on how the resources of the manufacturing system can be used to support critical business and technical objectives. A business strategy may be to use an existing facility with standard, stable processes to reduce costs and risks.
- A Manufacturing Plan addresses, in detail, how the company and manufacturing facility will meet contract requirements and deliver the product as requested. The plan should be linked to the WBS and Bill of Materials and describe steps necessary fabricate and assemble the end item.

Quality Management describes the proven quality management practices. Example industry standards for Quality Management are SAE AS9100, Quality Management Systems, and ISO 9001, Quality Management Systems Requirements. A QMS includes all the functions involved in the determination and achievement of quality. The PMO team should identify the appropriate quality requirements per FAR 46 Quality Assurance and 52 Contract Provisions.

- A Quality Strategy should be tied to the program's acquisition strategy and should focus on how the resources of the quality system can be used to support critical business and technical objectives. A strategy may be to use Lean/Six Sigma as a way to identify and evaluate contractors and later incentivize contractors to reduce costs and risks.
- A Quality Plan should address, in detail, how the company and facility will meet contract requirements and deliver the product as requested. The plan should be linked to fabrication and assembly, and how in-process and end-item inspection will lead to lower costs and better reliability.

For more information on quality strategies and plans, see the Early Manufacturing and Quality Engineering Guide (2022).

Producibility is a design accomplishment for the relative ease of manufacturing. Like manufacturing and other system design functions, producibility is integral to delivering capability to the warfighter effectively and efficiently. Producible designs are lower risk, more cost-effective, and repeatable, which enhances product reliability and supportability. Producibility should be assessed at both a product and enterprise (i.e., organizational, prime contractor facility) level. The PM should implement producibility engineering and planning efforts early and should continuously assess the integrated processes and resources needed to successfully achieve producibility.

To assess producibility on a product level, both the product and its manufacturing processes should be assessed. Manufacturing processes should be monitored and controlled, through measurement, to ensure that they can repeatedly produce accurate, high-quality products, which helps the program meet objectives for limiting process variability to a tolerable range (see DoD Producibility and Manufacturability Engineering Guide (2024)).

Manufacturing feasibility, processes, and risk should be assessed early and continuously through the acquisition life cycle in all acquisition programs. To ensure integration of manufacturing readiness and risk as part of design activities, the focus should be on manufacturing process reliability and producibility, and system risk reduction. Additional guidance on assessing manufacturing risks can be found in the Manufacturing Readiness Level Deskbook (2025).

PMs should use existing manufacturing processes whenever practical to support low-risk manufacturing. When the design requires new manufacturing capability, the PM may need to consider new manufacturing technologies or process flexibility (e.g., rate and configuration insensitivity), which introduces risk. See DFARS (Subpart 207.105 – Contents of Written Acquisition Plans) for specific guidance on manufacturing actions planned by the PM to execute the approach established in the AS and to guide contractual implementation.

PMs will ensure part and component suppliers are qualified in accordance with DoDM 4120.24, Enclosure 14. This involves a systematic assessment of a potential supplier to ensure that the supplier can meet the organization's contractual requirements. This can include a production part

approval process, where it is determined whether all customer engineering requirements are understood by the supplier and that the supplier has the potential to produce products consistently meeting these requirements. Another key aspect is whether acceptable materials are being used by the supplier to avoid unexpected fabrication and test issues (i.e., use of hazardous or sole source materials).

PMs should be interested in three broad risk areas from an industrial base perspective that go beyond classical supply chain considerations: Capability to Produce (one unit), Capacity to Produce (all units required over the life of the program), and Financial Stability (the company will endure long enough to complete all production) at rate and on schedule. When the DoW is in danger of losing industrial capabilities because a supplier (plant, industry, company, etc.) is going out of business, merging with another company, or being bought out, the program should perform an Industrial Capability Analysis (see also DoD Producibility and Manufacturability Engineering Guide (2024)).

More information on manufacturing management, quality management, producibility, specific M&Q activities throughout the acquisition life cycle, assessing manufacturing readiness and risk, and assessing industrial capabilities is available at the SE&A M&Q web page (<https://www.cto.mil/sea/mq/>).

7.15 Modular Design

Modular design allows for modifications to systems, recombination of existing capabilities and upgrade of system elements, to enable competition, innovation, rapidly responding to a changing environment, etc. (see also Section 3.7, Modular Open Systems Approach). Designing for modularity is a technical principle for implementing MOSA and is a complementary piece to the open system practices in contracting. The major tenet of a modular design strategy is to develop loosely coupled modules that can be decoupled, separated, or rearranged in a major system platform. In addition, major system components developed under the program or outside the program can be integrated into the program. MOSA implementation should support rapid capability insertion, and competitive sourcing across mission teams. It should avoid vendor lock. Modular architectures should enable iterative experimentation cycles.

When designing for modularity, the system should be appropriately partitioned into discrete, scalable, self-contained functional elements by decomposing and decoupling the functions of a system. This functional partitioning results in elements that can be composed into modules that can be reconfigured or even replaced. Accurately isolating functionality during the design process simplifies development, maintenance, changes, and upgrades. Separating the system into major functions and elements, which work together across defined interfaces for which the program can verify conformance, supports a modular architecture. The standard interfaces allow the individual architecture elements to evolve separately and with minimal impact to other elements in the systems.

Acquisition programs implementing a modular design provide flexible system designs, which allow for the replacement or recombination of subsystems and components. Programs should describe how the system design considers the evolution of requirements identified in the capability documents. In addition, program management needs to understand the expected benefit from modular design as part of implementing a MOSA strategy. Understanding the benefit helps the program choose the right enabling elements (standards, contract clauses, engineering tools, etc.). MOSA benefits are usually categorized into six areas, which often overlap: risk reduction, cost savings/cost avoidance; increased competition; enhanced interoperability; application of innovative elements; and ability to realize technology upgrade opportunities easily.

PMs should understand both the positive and negative outcomes from implementing a modular design and should determine if the realization of a particular benefit outweighs the potential negative consequence. When scoping where the system should implement modular design, the PM, systems engineer, and software engineer should consider multiple factors, such as anticipated DMSMS issues, technical innovation, preplanned product improvements to meet performance, etc. These circumstances will vary across systems. Systems engineers should conduct design trades to support the PM in deciding where to implement modularity into the system design, including how to organize system components, where to put interfaces, and which interface specifications and standards, where suitable, to select. MOSA-enabling standards are identified and accessible in ASSIST.

7.16 Operational Energy

Focusing on energy as an explicit design consideration and SE category is crucial for reducing the Joint Force's dependence on energy logistics and improving its effectiveness, mobility, and resilience against emerging threats and operational challenges.

The PM, systems engineer, and software engineer should generate informed choices that appropriately balance the Energy KPP (as required by 10 USC 2911) alongside other system KPPs, and consistent with the threshold and objective values of the energy relevant requirements for the system. The Energy KPP includes, but is not limited to, addressing fuel and electric power demand/supply/storage optimization in capability solutions, with regard to the logistical supply of energy to the warfighter and the subsequent demands placed on the force to provide and protect critical energy supplies.

Systems Engineers should incorporate energy supportability and associated risks in design, technology and material consideration into the system trade space along with other performance issues so that oppressive energy impacts to operational effectiveness and logistics needs are not inadvertently introduced in the attempt to achieve other performance goals (e.g., survivability, lethality). These considerations should inform the development of validated requirements, performance specifications, and design specifications to address energy driven operational and supportability requirements for a system, including impacts from sub-systems and components.

Conflict between interdependent energy requirements and other KPPs or KSAs should be adjudicated before finalization of requirements and system specifications.

Operational energy issues include:

- How the system and combat unit refuel/recharge/produce and store power in the battlespace, as well as how often refueling/recharging/producing are required in an operational scenario.
- How refueling/recharging/power production and storage requirements might constrain forces (limit their freedom of action, on-station time, signature, etc.).
- How the adversary might delay, disrupt, or defeat the energy logistics of the system.
- Force protection for refueling/recharging/power production and storage that will need to be diverted from combat missions.

When evaluating solutions to increase energy operational effectiveness and supportability, systems engineers should assess opportunities for solutions drawn from energy innovation efforts including those developed by industry or through government-funded efforts such as Operational Energy Capability Improvement Fund, Operational Energy Prototyping Fund, or other energy-related DoW research and development efforts. Design choices should prioritize the use of standardized energy components and interfaces to reduce integration risk, simplify supply chains, and accelerate production timelines. PMs should have incentives to favor solutions that can be sourced from multiple vendors, preparing the industrial base for surge production.

PMs and systems engineers should include capabilities for monitoring energy use and performance in design solutions to support sustainment, modifications, and future planning efforts. Systems engineers should consider the ability of operators and planners to use the monitoring capability to access and assess energy use data to inform mission planning and operations of the system.

The Operational Energy Strategy provides the PM, systems engineer, and software engineer with additional insight into the issue of Operational Energy in the acquisition life cycle. The results of the sustainability analysis (see Section 4.4, Sustainability Analysis) can also be used to inform energy analyses.

Establishing the Energy Allocation

Systems engineers should establish an Energy Allocation by assessing energy demand and supply requirements of individual sub-systems, components, and operational functions. The Energy Allocation is not an accounting exercise, but instead a critical design analysis that provides flexibility needed to streamline development and rapidly insert new capabilities in the future without exceeding the overall energy capacity of the system.

- The Energy Allocation is the assignment of energy supply and demand targets to the specific components and subcomponents of a system based on anticipated mission requirements.
- The Energy Allocation will begin with total system requirements, which will be allocated down through subsystems to the lowest appropriate energy using or producing component.
- PMs will aggregate the energy allocation for the entire system across different concepts of employment to ensure energy supportability across different operational scenarios.

The Energy Allocation should be established across the WBS to define the projected energy use across the lifespan of a system, which includes system modernization.

Verification of Energy Requirements

During Test and Evaluation, the systems engineer should coordinate with developmental and operational testers verifying that the energy performance of a system meets the energy requirements (e.g., Energy KPP) and is aligned with the Energy Allocation. Systems engineers should employ modeling, simulation, and system testing when conducting the verification of energy performance and allocation. Energy evaluations during Test and Evaluation should also support the development of a Utilization baseline based on projected operational scenarios.

Establishing the Energy Utilization Baseline

Using the data collected from all operationally representative testing—including contractor T&E, DT&E, and OT&E—PMs and lead systems engineers in coordination with the PSM should establish an Energy Utilization Baseline against which the PM can monitor and assess the system's energy use over the life of the program. The Energy Utilization Baseline reflects the system's energy use across a range of operational missions to enable an understanding of actual energy production and consumption of the entire system.

Systems engineers determine this Energy Utilization Baseline by estimating actual energy use according to data collected from the energy monitoring of the system during operationally representative testing (contractor T&E, DT&E, OT&E). The Energy Utilization Baseline should be based on realistic operational employment of the system and provides a suitable departure point to assess trends over the life of the program. PMs should consider the variability of energy use across the mission profiles and the mission environments related to the system. The Energy Utilization Baseline should be used over the life of the program to assess changes in energy performance and identify risks to operational supportability.

7.17 Packaging, Handling, Storage, and Transportation

The program team employs PHS&T principles and methods to ensure the necessary equipment reaches the warfighter while minimizing risk of damage to the equipment during handling, storage, and transportation – frequently in highly challenging and corrosive operational environments.

Thorough PHS&T requirements promote supportability and sustainability of major end items, reparable system elements, and supporting test equipment. PHS&T focuses on transportation, handling, and storage (short- and long-term) constraints on performance resulting from driving size, weight, parts robustness, and shelf life.

PMs, PSMs, systems engineers, and software engineers should ensure PHS&T is addressed during the requirements analysis process, and validated throughout each phase of the SE development of the system. All PHS&T requirements should be verified before entering the P&D phase, as this phase will require the implementation of PHS&T for a system delivery to the warfighter during LRIP. DoDI 4540.07 identifies specifics regarding PHS&T as related to SE of systems acquisitions. In addition, the following documents address PHS&T:

- MIL-STD-2073 (Standard Practice for Military Packaging)
- MIL-STD-129 (Military Marking for Shipment and Storage)
- ASTM-D3951, Standard Practice for Commercial Packaging
- DoDM 4140.27, Volume 1 (DoD Shelf-Life Management Program: Program Administration)
- DTR 4500.9-R, Defense Transportation Regulation
- 49 CFR Parts 171-180, Transportation

ASSIST contains the most up-to-date information on standards.

7.18 Reliability and Maintainability Engineering

The purpose of R&M engineering (Maintainability includes Built-in-Test) is to influence system design in order to increase mission capability and availability and decrease logistics burden and cost over a system's life cycle. Properly planned, R&M engineering reduces TOC and schedule risks by preventing or identifying R&M deficiencies early in development. This early action results in increased acquisition efficiency and higher success rates during operational testing and must be executed early in the development phase of acquisition. The R&M of systems supports availability and the readiness for the systems to perform as designed. Maintenance returns a system to its original reliability.

PMs implement a comprehensive R&M engineering program as an integral part of the SE process. The systems engineer should understand that R&M parameters have an impact on the

system's performance, availability, logistics supportability, and TOC. 10 USC 4328 further emphasizes sustainment factors, particularly those affected by the design, in the development of a weapon system. To ensure a successful R&M engineering program, the systems engineer should at a minimum integrate the following activities across the program's engineering organization and processes:

- Providing adequate R&M staffing, resources, and funding.
- Ensuring R&M engineering is fully integrated into SE activities, IPTs, engineering processes, the digital representation of the system being developed, and other activities (i.e., Logistics, T&E, and SS). A best practice is to develop an R&M engineering program plan to ensure that this integration occurs.
- Ensuring specifications contain realistic quantitative R&M requirements translated from the requirements documents (e.g., ICD, CDD, or equivalent). Note: The initial requirements document (e.g., ICD or equivalent) may not contain quantitative user threshold requirements. The draft CDD (or equivalent) is the first opportunity to review the sustainment requirement (such as a KPP) and supporting R&M requirements (such as KSAs). A RAM-C analysis is conducted to determine if they are valid and feasible (see RAM-C Rationale Report Outline Guidance). Once they are determined to be valid and feasible, the R&M threshold requirements are then translated to design specification requirements and may be allocated to subsystems.
- Ensuring that R&M engineering activities and deliverables in the RFP are appropriate for the program phase and product type. For ACAT Is and IIs, R&M requirements must be included in the TMRR, EMD, and Production solicitations, per 10 USC 4328.
- Including (for ACAT Is and IIs) in the contract and in the process for source selection clearly defined and measurable R&M requirements and engineering activities, per 10 USC 4328.
- Using incentive fees and penalties (as appropriate) to promote achieving design specification requirements for R&M in all EMD and production solicitations and contracts, per 10 USC 4328. The contract should describe the data collection methods to measure R&M requirements and to base determinations of contractor performance during EMD and production, and the collected R&M data should be shared, or available within the digital ecosystem, with appropriate contractor and U.S. Government organizations to the maximum extent practicable.
- Ensuring that R&M DIDs that will be placed on contract are appropriately tailored (see Guidance for Tailoring R&M Engineering Data).
- Integrating R&M engineering activities and reliability growth planning curve(s) in the SEP at Milestones A and B and at the Development RFP Release Decision Point.
- Planning verification methods for each R&M requirement.

- Ensuring the verification methods for each R&M requirement are described in the TEMP, along with a reliability growth planning curve.
- Planning for system and system element reliability growth (i.e., Highly Accelerated Life Test, Accelerated Life Test or conventional reliability growth tests for newly developed equipment).
- Ensuring data from R&M analyses, demonstrations, and tests are properly used to influence life cycle product support planning, availability assessments, cost estimating and other related program analyses.
- Identifying and tracking R&M risks and TPMs.
- Assessing R&M status during program technical reviews.
- Including consideration of R&M in all configuration changes and trade-off analyses.

Regardless of acquisition pathway, the PM, systems engineer, and software engineer work to properly align the applicable R&M Engineering activities needed to reduce program risk. The R&M Engineering Management Body of Knowledge (OUSW(R&E) SE&A website (<https://www.cto.mil/sea>)) should be used as a starting point to assess appropriate activities needed to deliver capability that is reliable, maintainable, and supportable. Detailed considerations for applying each of the activities within a pathway are provided in the Engineering of Defense Systems Guidebook (2022).

7.19 Spectrum Management

Warfighters use spectrum-dependent systems for communications, sensors (i.e., radar), navigation beacons, jammers, homing devices, anti-Improvised Explosive Devices, and other purposes. Often emitters are in physical proximity to each other and to civilian devices that should not be disrupted by military signals. Spectrum-dependent developers should be aware of the enemy electronic order of battle and countermeasures and should plan accordingly. Devices (including commercial items) that do not account for countermeasures may have vulnerabilities in hostile environments.

Spectrum management requirements are needed for all spectrum-dependent systems. Any system that uses an antenna or a platform that mounts such systems is a spectrum-dependent system. If a platform obtains a spectrum-dependent system as GFE, the platform PM is responsible for ensuring that the GFE PM has obtained the needed permissions. Both programs are required to submit a Spectrum Supportability Risk Assessment (SSRA). The platform SSRA can reference the GFE SSRA but may have to expand upon it regarding host-nation features or other information not contained in the GFE-level SSRA. The systems engineer should be aware of the worldwide rules for spectrum management and the need to obtain host-nation permission for each transmitter and frequency assignment.

PMs need to ensure that spectrum access is adequate and that it is granted in the Continental United States (CONUS) and wherever else the equipment is deployed. Both the SSRA and DD Form 1494 are required for each milestone (see DoDI 4650.01). The SSRA is used within the DoW as the basis for assessing the feasibility of building and fielding equipment that operate within assigned frequency bands and identifying potential de-confliction situations. The DD-1494, Application for Equipment Frequency Allocation, has four stages, which reflect the increasing maturity of available spectrum information during development. The DD-1494 form is submitted to National Telecommunications and Information Administration (NTIA) for approval of spectrum allocation, without which emitters cannot operate within CONUS, and to the International Telecommunications Union for satellites. The NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook) chapter 3 addresses international treaty aspects of the spectrum, and chapter 4 addresses frequency allocations.

The systems engineer has a lead role in defining spectrum needs, throughput and power requirements, and other attributes of the signals in space (outside the antenna – not in the transmission device) and the antenna characteristics and platform mounting details, as well as the safety aspects of emitters with regard to the Hazards of Electromagnetic Radiation to Ordnance, Personnel, and Fuel. The systems engineer should be aware that portions of the spectrum previously assigned to DoW or other Federal users are being sold for commercial use. Thus, previously approved DD-1494 can be revoked, requiring modifications to designs and even to fielded equipment. Similarly, host nations can alter prior agreements, as commercial applications encroach upon previously available spectrum.

Each nation reserves the right to control emitters operating within its territory; thus, host-nation agreements are essential in support of deployment. PMs, systems engineers, and software engineers of platforms that mount multiple emitters and receivers need to obtain spectrum access for each emitter and ensure that those emitters and receivers do not produce mutual interference or interact with ordnance (see DoDI 3222.03, MIL-STD-461 (Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment), MIL-STD-464 (Electromagnetic Environmental Effects Requirements for Systems), MIL-HDBK-235-1 (Military Operational Electromagnetic Environment Profiles Part 1D General Guidance), MIL-HDBK-237 (Electromagnetic Environmental Effects and Spectrum Supportability Guidance for the Acquisition Process), MIL-HDBK-240 series (Electromagnetic Environmental Effects to Ordnance), and “Joint Services Guide for Development of a Spectrum Supportability Risk Assessment”).

The Defense Information Systems Agency (DISA), Defense Spectrum Organization provides spectrum support and planning for the DoW. See Figure 7-2 for spectrum activities by acquisition phase. This figure summarizes the requirements of DoDI 4650.01.

	A	B	C	FRPI FD	
Defense Acquisition Life Cycle Phase	Materiel Solution Analysis	Technology Maturation & Risk Reduction	Engineering & Manufacturing Development	Production & Deployment	Operations & Support
Spectrum Supportability Risk Assessment (SSRA)	Prepare SSRA	Update SSRA	Update SSRA	Update SSRA	Update SSRA for mission and technical changes
DD-1494, Application for Equipment Frequency Allocation	Stage 1 (Conceptual)	Stage 2 (Experimental)	Stage 3 (Developmental) NTIA approval needed before transmission tests	Stage 4 (Operational) NTIA approval needed before deployment or when changes occur	
Program Management, Systems Engineering, and Testers Electromagnetic Environmental Effects (E3) Tasks	E3 assessment for SSRA	Update E3 assessment for SSRA	Update E3 assessment for SSRA	Update E3 assessment for SSRA	Resolve interference
	Define EME and E3 requirements (i.e., frequency bands, throughout, power, operational areas, etc.)	Update EME; Prepare E3 inputs to ISP, TEMP, and acquisition documents; Address at PDR	E3 and EME inputs to TEMP and ISP; HERO, HERP, HERF, TEMPEST, and EMI address at CDR; DT&E transmission tests after Stage 3 approval	Conduct OT&E tests including E3 tests IAW TEMP; E3 assessment report	Deployed support
	Consider host nation (HN) constraints	Obtain HN comments via SMO	Begin HN discussions via SMO	Obtain HN approval before deployment	Maintain HN approval

CDR – Critical Design Review Decision Point
 DT&E – Developmental Test and Evaluation
 E3 – Electromagnetic Environmental Effects
 EME – Electromagnetic Environment
 EMI – Electromagnetic Interference
 ISP – Information Support Plan

HERF – Hazard of Electromagnetic Radiation on Fuel
 HERO – Hazard of Electromagnetic Radiation on Ordnance
 HERP – Hazard of Electromagnetic Radiation on Personnel
 HN – Host Nation
 IAW – In Accordance With
 NTIA – National Telecommunications and Information Administration

OT&E – Operational Test and Evaluation
 PDR – Preliminary Design Review
 SMO – Spectrum Management Office
 SSRA – Spectrum Supportability Risk Assessment
 T&E – Test and Evaluation
 TEMP – Test and Evaluation Master Plan

Figure 7-2. Spectrum-Related Activities by MCA Life Cycle Phase

7.20 Standardization

Standardization supports the achievement of compatibility, interchangeability, commonality, and interoperability of parts and processes with U.S. forces and our allies, promotes safety, provides for life cycle sustainment, and allows for rapid, cost-effective technology insertion through use of system interfaces compliant with widely supported and consensus-based standards and modular open systems. Standardization is an enabling tool to provide the warfighter with systems and equipment that are interoperable, reliable, sustainable, and affordable, contributing to improved HSI. Standardization also plays a role in defining SE best practices and processes.

The PM balances the decision to use international standardization agreements, NGS, practices, products, parts, processes, interfaces, and methods with required capabilities, operational environment, technology feasibility and growth and cost-effectiveness.

DoDM 4120.24 provides processes on standardization considerations, how to document standardization decisions, and a discussion of the tailoring of standardization documents. It also provides references to resources for the standardization process. Defense standardization products and information are published in ASSIST (<https://assist.dla.mil>), including defense specifications and standards, U.S. ratified international standardization agreements, and adoption notices for NGSs.

DoDM 4245.15 specifies that DoW Component heads use guidance in Defense Standardization Program Office Standardization Documents SD-22 and SD-19 to implement best practices for DMSMS management.

Parts management is a SE discipline for *selecting* parts and assemblies of parts, while accounting for the materials and processes used to manufacture them, throughout all phases of a system's (or equipment's) life cycle from initial design through disposal. Part selection considerations include performance, cost, quality, qualification, reliability, maintainability, supportability, standardization, technology features and life-cycle stage, manufacturing processes and producibility, DMSMS risk, system security, cyber weaknesses and vulnerabilities, hardware and software assurance, supply chain risk, susceptibility to counterfeiting, unauthorized tampering, and use of HAZMAT.

Disciplined parts management has generally been recognized as a contributor to the long-term success of any system. Selecting the right parts is fundamental to achieving many engineering and manufacturing objectives, influencing cost, schedule, and performance. Parts management processes improve operational readiness and reduce life-cycle costs by promoting the use of common, widely available, reliable parts

MIL-STD-11991 (General Standard for Parts, Materials, and Processes) and the SD-19 Parts Management Guide indicate that program offices should apply standardization processes to:

- Improve parts commonality.
- Reduce TOCs.
- Reduce proliferation of parts.
- Promote the use of parts with acceptable performance, quality, and reliability.

The systems engineer is responsible for:

- Conducting a risk assessment to identify the level and extent of parts selection oversight to be performed by the Government.
- Developing a program office Parts Management Plan.
- Implementing parts management contractual requirements.
- Approving contractor submitted Parts Management Plans.

- Verifying and validating contractor parts management processes to ensure that selected parts meet their allocated requirements.

7.21 Supportability

Supportability refers to the inherent characteristics of the system and the enabling system elements that allow effective and efficient sustainment (including maintenance and other support functions) throughout the system's life cycle. By addressing supportability as part of the system design, the PM, through the systems engineer and PSM, ensures the system reaches initial operational capability with the required enabling system elements in place. The benefits to the program are:

- Cost savings
- Fielding of a more affordable logistics infrastructure
- Improved Materiel and Operational Availability
- Reduced footprint

Supportability analysis is an iterative activity conducted during the system's development and is used by the PM and PSM to define the system's support strategy. It includes sustainment-related should-cost management and risk and opportunity management efforts across the life cycle. Supportability analysis begins in stakeholder requirements definition, as part of the analysis of alternatives, and continues through the design, T&E, production, and deployment activities and phases of the system. The supportability analysis and the resultant product support package mature in parallel with the evolution of the design and should be documented in an integrated data or decision environment, preferably a digital ecosystem.

Early consideration of supportability needs during Requirements Analysis, Architecture Design, and Implementation processes are critical to ensure the delivered capability is operationally effective, suitable, survivable, sustainable, and affordable. The system baseline should incorporate inherent supportability characteristics and should include the design of the enabling support infrastructure. Details can be found in DoDI 5000.91, but typical product support considerations are listed in Table 7-4.

Table 7-4. Product Support Considerations

Product Support Element	Typical Considerations
Manpower and Personnel	Specifically support personnel for installation, checkout sustaining support and maintenance
Training and Training Support	For the system operators and maintenance personnel
Supply Support	Including repairable and non-repairable spares, consumables, and special supplies
Support Equipment	Including tools, condition and state monitoring, diagnostic and checkout special test, and calibration equipment
Computer Resources	Operating systems and software supporting logistics functions and associated infrastructure
Packaging, Handling, Storage, and Transportation (PHS&T)	Special provisions, containers, and transportation needs
Facilities and Infrastructure	Including facilities to support logistics and sustainment actions at all levels
Technical Data	Including system installation and checkout procedures; operating and maintenance instructions and records; alteration and modification instructions, parts list, bill of materials, digital artifacts, etc.
Usage and Maintenance Data	Including data acquisition, movement, storage, and analytic capability to support life cycle support decisions

The PM is responsible for approving life cycle trades throughout the acquisition process. To ensure the design incorporates life cycle supportability, the program should involve logisticians and HSI practitioners and end users early in the Stakeholder Requirements Definition process to develop a performance-based product support strategy (including maintenance, servicing, and calibration requirements). The RCM analysis and Conditioned Based Maintenance Plus (see DoD 4151.22-M and DoDI 4151.22) initiatives enable the performance of maintenance based on evidence of need as provided by RCM analysis and other enabling processes and technologies.

RCM, as defined in DoD 4151.22-M, is a systematic approach for analyzing the system or system element functions and potential failures to identify and define preventive or scheduled maintenance tasks for an equipment end item. Tasks may be preventive, predictive, or proactive in nature. RCM results provide operational availability with an acceptable level of risk in an efficient and cost-effective manner.

In addition, the PSM and systems engineer should ensure that supportability analysis activities are documented in the SEP and the LCSP, or equivalent documentation, and that the supportability design requirements are documented in the functional baseline. The results of the supportability analysis activities including the servicing, calibration, corrective and preventive maintenance requirements are also summarized in the LCSP. (The LCSP outline calls out specific supportability related phase and milestone expectations.)

The systems engineer, working with the PSM and PM, identifies and mitigates the supportability life cycle cost drivers to ensure the system is affordable across the life cycle. This includes

identifying factors that drive the program's life cycle costs and Sustainment requirement (such as a KPP or KSA) to establish affordable and achievable goals and caps (see Section 7.2, Affordability – Systems Engineering Trade-Off Analyses). Once the goals are established the focus turns to the specific metrics driving the O&S cost and Sustainment requirements that can be directly influenced by the design. These drivers are then decomposed into functional and allocated requirements that can be directly traced to the cost targets and the Operational Availability (Ao) and Materiel Availability (A_M) (see Product Support Manager Guidebook (2022)). The cost-benefit analysis, jointly conducted by the systems engineer and PSM within the supportability analysis process, provides insight into supportability drivers and includes the impact of resources on readiness. Engineering analyses (i.e., FMECA; supportability analysis predictions; and diagnostics architecture) provide critical data to impact the design for supportability and to influence the product support package.

7.22 Survivability

A system with a balanced survivability approach maximizes operational crew and personnel safety while satisfying mission effectiveness and operational readiness requirements.

Survivability is the capability of a system (i.e., system survivability) and its crew (i.e., personnel survivability) to avoid or withstand a hostile environment without losing the ability to accomplish its designated mission.

PMs and systems engineers should consider all aspects of survivability including reducing a system's likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability and countermeasures as well as reducing the vulnerability of the system and its occupants if hit by hostile fire by placement of armor around crew and critical components and ensuring redundancy of those critical components. In addition to survivability considerations from traditional kinetic fires, the PM, systems engineer, and software engineer may need to consider the system and crew's ability to survive and operate in:

- Manmade and natural environmental conditions described in MIL-STD-810 (Environmental Engineering Considerations and Laboratory Tests) (sand and dust, vibration, shock, immersion, salt fog etc.).
- Electromagnetic environments described in MIL-STD-461 (Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment), MIL-STD-464 (Electromagnetic Environmental Effects Requirements for Systems) and MIL-STD-188-125 (High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based Facilities Performing Critical, Time-Urgent Mission).
- Chemical, biological, and radiological environments described in MIL-STD-3056 (Design Criteria for Chemical, Biological, and Radiological System Contamination Survivability).

- Nuclear effects environments (including high-altitude electromagnetic pulse) described in MIL-STD-2169 and the Defense Threat Reduction Agency's Nuclear Survivability Program Guidebook (DTRA-TR-14-71).
- Cyber environments described in DoDI 8500.01 and the Cyber Survivability Endorsement Implementation Guide. Cybersecurity and cyber resilience requirements should be part of the prototyping system survivability requirements to achieve true cyber survivability. By addressing both protection from threats and the ability to recover and maintain mission-critical functions during and after adverse events, the need for redesign can be reduced, ensuring systems remain robust against evolving threats.

PMs, systems engineers, and software engineers should consider cyber-survivability because of the reliance on networked information in today's battlefield.

Additional considerations include designing for damage tolerance and rapid system reconstruction (reparability) to maximize wartime availability and sortie rates. The PM, systems engineer, and software engineer should consider all these aspects of system and crew survivability and, if necessary, perform trades to balance survivability, performance, cost, and risk. The PM should document the formal risk acceptance process used.

Unless waived by the MDA, mission-critical systems, including crew, regardless of acquisition category, should be survivable to the threat levels anticipated in their projected operating environment as portrayed in their platform-specific Validated On-line Life Cycle Threat Report (see AAFDID) and Intelligence Support Guidebook (2023).

The System Survivability requirement (such as a KPP) is intended to ensure the system, rather than the system occupants or other personnel, maintains its mission capabilities as defined in the CONOPS. System Survivability should be assessed from three objective criteria: Susceptibility, Vulnerability, and Recoverability. Susceptibility is the degree to which a device, piece of equipment, or system is open to effective attack as a result of one or more inherent weaknesses. Susceptibility is a function of operational tactics, countermeasures, probability of an enemy threat, etc. Vulnerability refers to the characteristics of a system that cause it to suffer a definite degradation (loss or reduction of capability to perform the designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (manmade) or natural (e.g., lightning, solar storms) hostile environment. Recoverability refers to the characteristics of a system's resiliency to support the function necessary for mission success despite hostile action or under adverse conditions.

The Force Protection requirement (such as a KPP) is intended to ensure protection of occupants, users, or other personnel who may be adversely affected by the system or threats to the system. Although the Force Protection requirement may include many of the same attributes as those that contribute to System Survivability, the intent of the Force Protection requirement is to emphasize protecting system occupants or other personnel rather than protecting the system itself.

Protection requirements for Force Protection are generally higher than those in System Survivability.

Proper design and testing ensure that the system and crew can withstand manmade hostile environments without the crew suffering acute chronic illness, disability, or death. The PM, supported by the systems engineer, should fully assess system and crew survivability against anticipated threats throughout the system life cycle. The goal of survivability is to:

- Provide mission assurance while maximizing warfighter safety (or minimizing their exposure to threats).
- Incorporate balanced survivability, with consideration to the use of signature reduction with countermeasures.
- Incorporate susceptibility reduction features that prevent or reduce engagement of threat weapons.
- Provide mission planning and dynamic situational awareness features.

If the system or program has been designated by the Director, Operational Test and Evaluation (DOT&E), for live-fire test and evaluation (LFT&E) oversight, the PM should integrate T&E to address crew survivability issues into the LFT&E program supporting the Secretary of Defense LFT&E Report to Congress.

If the system or program has been designated a CBRN mission-critical system, the PM must address CBRN survivability, in accordance with DoDI 3150.09, The CBRN Survivability Policy. The PM should ensure that progress toward CBRN survivability requirements is documented in the applicable Service CBRN mission-critical report. For each CBRN Mission Critical System entry, identify the intended operating environment(s), CBRN survivability requirements, and an assessment on compliance with each CBRN survivability requirement. Identify if it has been made CBR contamination-survivable, nuclear-survivable, or CBRN-survivable, and identify test infrastructure gaps and limitations. In addition, identify survivability limitations and plans for achieving CBRN survivability. Also identify deficiencies caused by CBRN survivability limitations.

For all systems that may operate in a CBRN environment, the systems engineer should describe in the SEP, or equivalent document, how the system design incorporates the CBRN survivability requirements and how progress toward these requirements is tracked and documented over the acquisition life cycle (e.g., Nuclear/Electromagnetic Pulse Hardness Maintenance/Hardness Surveillance and Chemical, Biological, and Radiological Preventative Maintenance Checks and Services). The plan for demonstrating system survivability will be documented in the SEP. The plan to evaluate system survivability will be documented in the TEMP, or equivalent document.

7.23 System Safety

SS is an important element of SE that provides a standard, generic method for identifying, classifying, and mitigating hazards. DoDI 5000.02 requires the establishment of a safety and risk management program to ensure program cost, schedule, and performance objectives are achieved, and to communicate the process for managing program uncertainty and safety risks that must be eliminated or controlled or can be accepted. DoDI 5000.88 requires programs to include SS in the SE approach in accordance with MIL-STD-882. MIL-STD-882 reinforces integration of other functional disciplines into SE to improve the consistency of hazard management practices across programs.

DoW expands the objective and use of the SS methodology to integrate risk management into the overall SE process. MIL-STD-882 defines System Safety Management (SSM) as *“All plans and actions taken to identify hazards; assess and mitigate associated risks; and track, control, accept, and document risks encountered in the design, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and infrastructure.”* SSM describes general engineering requirements and design criteria for safety risk management during system design and development. It identifies safety risk management requirements, including procedures, for test, O&S, and disposal. MIL-STD-882 provides a matrix and defines probability and severity criteria to categorize risks. Before exposing people, equipment, or the environment to known system-related hazards, the risks must be accepted by the appropriate authority as defined in DoDI 5000.02. According to the instruction, the system configuration and associated documentation that supports the formal risk acceptance decision must be provided to the Government for retention through the life of the system.

MIL-STD-882 covers hazards as they apply to systems, products, equipment, and infrastructure, including both hardware and software, throughout design, development, test, production, use, and disposal. Hazards, control measures, and risks as they apply to autonomy, artificial intelligence, and unmanned systems, including autonomous weapon systems, need to be assessed as part of the SS process. The SS engineering program identifies safety certification such as the Airworthiness Release, Fuze Safety Reviews, Hazard of Electromagnetic Radiation to Ordnance Classification and Certification, Energetic Material Qualification, HC, Ignition Safety Review, Health Hazard Assessment, Joint Weapon Safety, and service specific reviews and assessments.

Additional guidance is provided in the following areas (see also SE&A System Safety Engineering web page):

- **Environment, Safety, and Occupational Health** – ESOH analyses are an integral, ongoing part of the SE process throughout the life cycle. Programs use the SS methodology in MIL-STD-882 to manage their ESOH considerations as an integral part of the program’s overall SE process.
- **Software System Safety** – Programs document a strategy for the SS engineering program including SSS in accordance with MIL-STD-882. The standard provides a

structured, yet flexible and tailorable, framework for the assessments of software contribution to system risk. In addition to the standard, guidance within the DoD Joint Software Systems Safety Engineering Handbook and the Joint Services-Software Safety Authorities Implementation Guide provides a structured and tailorable framework for the assessment of software contribution to system risk.

- **Hazard Tracking System** – A closed-loop HTS should be employed to document, track, and maintain hardware and software related hazards and their associated risks data.
- **SS in SE Process** – The PM and the systems engineer should ensure SS is addressed during material solutions analysis or equivalent phase by identifying inherent hazard risks and developing criteria to define objectives for the SS engineering program.
- **SS System Design Requirements** – The systems engineer should derive SS design requirements and include them in capability documents, technical specifications, solicitations, and contracts.
- **SS in Program Documents** – The systems engineer and the SS SMEs document the program's plan to integrate SS into the SE process, incorporating SS as a mandatory design, test, sustainment, and disposal consideration in the SEP or equivalent. The PESHE and the National Environmental Protection Act (NEPA)/EO 12114 Compliance Schedule are used to document the results of the program's implementation of their Environmental and Occupational Health planning.
- **SS Risk Management** – The PM is responsible for ensuring the appropriate management level accepts SS risks before exposing people, equipment, or the environment to those risks.
- **Hazardous Materials Management** - HAZMAT management is an integral part of the risk management effort within the program's SE process. The PM and systems engineer assess and document the risks for each combination of h and application.
- **Safety Release for Testing** – The PM with the user and the T&E community, provides safety releases, to the developmental and operational testers before any test exposing personnel to ESOH hazards.
- **Safety Confirmation** – The PM with the user and the T&E community, ensures a Safety Confirmation (SC) is provided as a formal document that provides the material developer and the decision maker with the test agency's safety findings and conclusions and that states whether the specified safety requirements have been met.
- **Sustainable Procurement Program** – Programs should follow the policy and procedures identified in the DoD Sustainable Procurement Program in order to enhance and sustain mission readiness over the system life cycle, reduce reliance on resources and reduce the DoW footprint.

7.24 System Security Engineering

SSE activities allow for identification and incorporation of security design and process requirements into risk identification and management in the requirements trade space.

SSE is an element of SE that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. The SSE process should ensure that cybersecurity system attributes are included in the requirements documents. Program Protection is the Department's integrating process for mitigating and managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion (see T&PP Guidebook (2022)), battlefield loss and unauthorized or inadvertent disclosure throughout the acquisition life cycle.

The Program Protection processes capture SSE analysis in the system requirements and design documents and SSE verification in the test plans, procedures and results documents. SSE analysis should leverage threat assessments, vulnerability analyses, criticality analyses, and risk mitigation strategies to inform cybersecurity and cyber resilience requirements. These results should include attributes such as resilience (prevent, mitigate, recover, adapt) and protecting confidentiality, integrity, and availability, ensuring requirements are defined, measurable, and traceable in requirements documents. The PPP (see T&PP Guidebook (2022)) documents the comprehensive approach to SSE analysis and the associated results.

In accordance with the DoD Cyber Developmental Test and Evaluation (DT&E) Guidebook, Version 3.0, June 2025, cyber testing is not a single event but a continuous, iterative process of Planning, with recurring T&E events following the Prepare, Execute, Evaluate, and Report process. This process begins early in the life cycle to inform design and continues through sustainment to address evolving threats. By integrating this iterative approach with SSE activities, programs can ensure cybersecurity measures remain effective and adaptable to the dynamic nature of the cyber threat landscape.

SSE analysis results should be captured in the PPP, provided at each technical review and audit (see T&PP Guidebook (2022)) and incorporated into the technical review assessment criteria as well as the functional, allocated and product baselines. For programs in the Major Capability Acquisition pathway, the PPP is approved by the MDA at each milestone decision review and at the FRP/FD decision, with a draft PPP (as defined in the AAFDID and DoDI 5000.83) due at the Development RFP Release Decision Point. For programs using other pathways in the AAF, a PPP or equivalent documentation is maintained as a best practice.

SSE analysis should be used to update the technical baselines before each technical review and key knowledge point throughout the life cycle. It should also inform the development and release of each RFP (see T&PP Guidebook (2022)) by incorporating SSE process requirements and the system security requirements into the appropriate solicitation documentation.

The PM is responsible for employing SSE practices and preparing a PPP to guide the program's efforts and the actions of others. The systems engineer and/or system security engineer is responsible for ensuring a balanced set of security requirements, designs, testing and risk management are incorporated and addressed in their respective trade spaces. The systems engineer and/or system security engineer is responsible for leading and facilitating cross-discipline teams to conduct the SSE analysis necessary for development of the PPP, or equivalent documentation. The cross-discipline interactions reach beyond the SSE community to the test and logistics communities. The T&PP Guidebook (2022) further details the program protection roles and responsibilities.

To address SSE as a design consideration, the systems engineer and systems security engineer should ensure the system architecture and design address how the system:

- Manages access to, and use of, the system and system resources.
- Is configured to minimize exposure of vulnerabilities that could impact the mission through techniques such as design choice, component choice, STIGs and patch management in the development environment (including integration and T&E), in production and throughout sustainment.
- Is structured to protect and preserve system functions or resources, e.g., through segmentation, separation, isolation, or partitioning.
- Monitors, detects, and responds to security anomalies.
- Maintains priority system functions under adverse conditions.
- Interfaces with DoW Information Network or other external security services.
- Prevents, mitigates, adapts, and recovers from cyberspace attacks and events, based on current cyberspace threats validated by the intelligence community.
- Is designed to be operationally resilient, as per the DoDI 8500.01 and Cyber Survivability Endorsement Implementation Guide.

The early and frequent consideration of SSE principles throughout the program life cycle reduces rework and expense resulting from late-to-need security requirements (e.g., anti-tamper, exportability features, supply chain risk management, secure design, defense-in-depth and cybersecurity implementation).

MBCRAs are required per DoDI 5000.89, with minimum requirements outlined in DoDM 5000.103. MBCRAs should be performed early and updated periodically as cyberspace threats and system designs evolve. These assessments must be collaborative, involving operational users, developers, engineers, and cyberspace threat emulation (testers).

Threat assessments should inform risk assessments, and criticality analysis should leverage the Program Protection Plan (PPP) to confirm systems can perform critical functions under representative threats. SSE activities, such as identifying critical data flows, assessing mission impacts from data compromise, and characterizing the cyberspace attack surface (e.g., reviewing system diagrams, vulnerabilities, and adversary tactics), are essential to MBCRAs. All of these activities should be tied to requirements and drive changes in the SE process throughout the life cycle.

ACRONYMS

AAF	Adaptive Acquisition Framework
AAFDID	Adaptive Acquisition Framework Document Identification Tool
ACAT	Acquisition Category
AIA	Aerospace Industries Association
APB	Acquisition Program Baseline
API	Application Programming Interface
AS	Acquisition Strategy
ASR	Alternative Systems Review
CAE	Component Acquisition Executive
CAI	Critical Application Item
CARD	Cost Analysis Requirements Description
CBE	Current Best Estimate
CBRN	Chemical, Biological, Radiological and Nuclear
CCB	Configuration Control Board
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI	Configuration Item
CI/CD	Continuous Integration and Continuous Delivery
CIP	Critical Intelligence Parameter
CM	Configuration Management
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CPC	Corrosion Prevention and Control
CPI	Critical Program Information
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
CSI	Critical Safety Item
CSS	Cybersecurity Strategy
CTE	Critical Technology Element
CTP	Critical Technical Parameter
DA	Decision Authority
DCA	Design Control Activity

DCMA	Defense Contract Management Agency
DE	Digital Engineering
DEMIL	Demilitarization
DevSecOps	Development, Security, and Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DID	Data Item Description
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DoD	Department of Defense
DoW	Department of War
DT&E	Developmental Test and Evaluation
ECP	Engineering Change Proposal
EMD	Engineering and Manufacturing Development
EO	Executive Order
ESOH	Environment, Safety, and Occupational Health
EVMS	Earned Value Management System
FCA	Functional Configuration Audit
FD	Full Deployment
FMECA	Failure Mode, Effects and Criticality Analysis
FOCI	Foreign Ownership, Control, and Influence
FOS	Family of Systems
FP&S	Force Protection and Survivability
FRP	Full-Rate Production
FUR	Failure Utilization Ratio
GAO	Government Accountability Office
GFE	Government-Furnished Equipment
HAZMAT	Hazardous Material
HC	Hazard Classification
HSI	Human Systems Integration
HTS	Hazard Tracking System
ICD	Initial Capabilities Document
ICE	Independent Cost Estimate
ICWG	Interface Control Working Group
I&D	Interoperability and Dependency
IDE	Integrated Data Environment
IEEE	Institute of Electrical and Electronics Engineers
IM	Insensitive Munitions

IMD	Intelligence Mission Data
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
INCOSE	International Council on Systems Engineering
IPT	Integrated Product Team
ISO	International Organization for Standardization
IT	Information Technology
ITRA	Independent Technical Risk Assessment
IUID	Item Unique Identification
IV&V	Independent Verification and Validation
KOP	Key Operational Problem
KPP	Key Performance Parameter
KSA	Key System Attribute
LCA	Life Cycle Assessment
LCSP	Life Cycle Sustainment Plan
LFT&E	Live-Fire Test and Evaluation
LRIP	Low-Rate Initial Production
LVI	Learning Velocity Index
MBCRA	Mission-Based Cyber Risk Assessment
MBSE	Model-Based Systems Engineering
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
ME	Mission Engineering
MEIA	Mission Engineering and Integration Activity
MOA	Memorandum of Agreement
MOSA	Modular Open Systems Approach
MOU	Memorandum of Understanding
MP	Mission Profile
MTTD	Mean Time from Test to Decision
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NDIA	National Defense Industrial Association
NEPA	National Environmental Protection Act
NGS	Non-Government Standard
NIST	National Institute of Standards and Technology

NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OMS	Operational Mode Summary
O&S	Operations and Support
OT&E	Operational Test and Evaluation
PAE	Portfolio Acquisition Executive
PCA	Physical Configuration Audit
P&D	Production and Deployment
PDR	Preliminary Design Review
PESHE	Programmatic Environment, Safety, and Occupational Health Evaluation
PHS&T	Packaging, Handling, Storage, and Transportation
PLM	Product Life Cycle Management
PM	Program Manager
PMO	Program Management Office
PPBE	Planning, Programming, and Budgeting Execution
PPP	Program Protection Plan
PRMP	Program Risk Management Process
PRR	Production Readiness Review
PSM	Product Support Manager
QMS	Quality Management System
RAM-C	Reliability, Availability, Maintainability, and Cost Rationale
RCM	Reliability Centered Maintenance
RFP	Request for Proposal
RIO	Risk, Issue, and Opportunity
R&M	Reliability and Maintainability
RMB	Risk Management Board
RRAB	Requirements and Resourcing Alignment Board
RTM	Requirements Traceability Matrix
SAE	Society of Automotive Engineers
SDP	Software Development Plan
SE	Systems Engineering
SE&A	Systems Engineering and Architecture
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SFR	System Functional Review
SME	Subject Matter Expert

SoS	System of Systems
SOW	Statement of Work
SRA	Schedule Risk Assessment
SRD	System Requirements Document
SRR	System Requirements Review
SS	System Safety
SSE	System Security Engineering
SSM	System Safety Management
SSRA	Spectrum Supportability Risk Assessment
SSS	Software System Safety
STIG	Security Technical Implementation Guide
SVR	System Verification Review
SWE	Software Engineering
TAD	Target Audience Description
TDP	Technical Data Package
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TOC	Total Ownership Cost
TPM	Technical Performance Measure
TPMM	Technical Performance Measures and Metrics
T&PP	Technology and Program Protection
TRA	Technology Readiness Assessment
TRR	Test Readiness Review
USW(A&S)	Under Secretary of War for Acquisition and Sustainment
USW(R&E)	Under Secretary of War for Research and Engineering
VE	Value Engineering
VECP	Value Engineering Change Proposal
VEP	Value Engineering Proposal
V&V	Verification and Validation
VV&A	Verification, Validation, and Accreditation
WAS	Warfighting Acquisition System
WBS	Work Breakdown Structure
WCE	Worst Case Estimate
WIPT	Working-Level Integrated Product Team

REFERENCES

U.S. Code (USC).

<https://uscode.house.gov/>

10 USC § 138c, Assistant Secretaries of Defense

10 USC § 2228, Authorization of appropriations

10 USC § 2319, Encouragement of new competitors

10 USC § 2358, Research and development projects

10 USC § 2389, Ensuring safety regarding insensitive munitions

10 USC § 2430, Major defense acquisition system defined

10 USC § 2451, Defense supply management

10 USC § 2452, Duties of Secretary of Defense

10 USC § 2453 Supply Catalog: distribution and use

10 USC § 2454 Supply catalog: new or obsolete items

10 USC § 2455, Repealed. P.L. 101-501, div A, title XIII, § 1322(a)(9), November 5, 1990, 104 Stat. 1671

10 USC § 2456, Coordination with General Services Administration

10 USC § 2457, Standardization of equipment with North Atlantic Treaty Organization members

10 USC § 4201, Major defense acquisition programs: definition; exceptions

10 USC § 4251, Major defense acquisition programs: factors to be considered before Milestone A approval

10 USC § 4252, Major defense acquisition programs: factors to be considered before Milestone B approval

10 USC § 4272, Independent technical risk assessments

10 USC § 4328, Weapon system design: sustainment factors

10 USC § 4401, Requirement for MOSA in major defense acquisition programs; definitions

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

15 USC § 272, Establishment, functions, and activities

29 USC § 794d, Electronic and information technology (Section 508 of the Rehabilitation Act)

41 USC § 104, Commercially available off-the-shelf item

- 41 USC § 1711, Value engineering
- 41 USC § 1907, List of laws inapplicable to procurements of commercially available off-the-shelf items
- 42 USC § 4321, Congressional declaration of purpose
- 44 USC § 3506, Federal agency responsibilities
- 47 USC § 305, Government owned stations
- 47 USC § 901, Establishment of agency Chief Financial Officers
- 47 USC § 902, Establishment; assigned functions
- 47 USC § 903, Spectrum management activities
- 47 USC § 904, General administrative provisions

- A Guide to DoD Program Management Business Processes. Fort Belvoir, Va.: Defense Systems Management College, Defense Acquisition University (DAU), April 29, 2022.
<https://aaf.dau.edu/storage/2023/09/A-Guide-to-DoD-Program-Management-Business-Processes.pdf>

- A Guide to Program Management Knowledge, Skills, and Practices. Fort Belvoir, Va.: Defense Systems Management College, DAU, April 29, 2022.
https://us-east1-menlo-inspect.menlosecurity.com/safeview-fileserv/tc_download/dcd2d689d12dfb27b7d07eb6c00462877012fea45ae11d129bf3279892f691b8/?&cid=N1FAA31F08E50&rid=34a8cf6f6c54dfcc1aab06286ecd6515&cl=od_menlo1b&file_url=https%3A%2F%2Fwww.dmi-ida.org%2Fdownload-pdf%2Fpdf%2FA-Guide-to-Program-Management-Knowledge-Skills-and-Practices.pdf&type=original

- “Accessibility Requirements Tool.” GSA. Retrieved August 11, 2021, from:
<https://www.buyaccessible.gov/>

- Acquiring and Enforcing the Government’s Rights in Technical Data and Computer Software under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals (aka Air Force Technical Data and Computer Software Rights Handbook). 9th Edition. Office of the Staff Judge Advocate, Space and Missile Systems Center (SMC), October 2018.
<https://www.dau.edu/sites/default/files/Migrated/ToolAttachments/Technical-Data-and-Computer-Software-Rights-Handbook.pdf>

- Acquisition Knowledge Matrix. Warfighting Acquisition University (WarU).
<https://www.waru.edu/acquisition-knowledge-matrix>

- Acquisition Program Technical Certifications Summary. Office of the Under Secretary for Defense for Research and Engineering (OUSD(R&E)), July 2024.
<https://www.cto.mil/wp-content/uploads/2024/08/AcqTechCert-Summary-July2024.v2.pdf>

- Acquisition Strategy Outline. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, April 20, 2011.
<https://www.cto.mil/wp-content/uploads/2023/06/Acq-Strat-Outline-2011.pdf>

- Adaptive Acquisition Framework Document Identification Tool (AAFDID), August 19, 2021.
<https://www.dau.edu/blogs/adaptive-acquisition-framework-document-identification-tool>
- Air Force Technical Data and Computer Software Rights Handbook. *See* Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals.
- Air Force Instruction 33-118, "Electromagnetic Spectrum Management," July 18, 2005.
<http://www.e-publishing.af.mil>
- Air Force Product Data Acquisition (PDAQ) guidance.
<https://www.dau.edu/artifact/air-force-product-data-acquisition-pdaq-site>
- Allied Ordnance Publication (AOP) 52. NATO Standard. Guidance on Software Safety Design and Assessment of Munitions-Related Computing Systems. Edition B, Version 1. NATO Standardization Office (NSO), November 2016.
<https://www.cto.mil/wp-content/uploads/2025/08/AOP-52-EDB-V1E.pdf>
- ANSI/HFES 400-2021 Human Readiness Level Scale in the System Development Process, Human Factors and Ergonomics Society, 2021.
- Army Data and Data Rights (D&DR) Guide: A Reference for Planning and Performing Data Acquisition and Data Management Activities Throughout the DoD Life Cycle 1st Edition. U.S. Army Product Data & Engineering Working Group, August 2015.
https://www.acq.osd.mil/asda/dpc/cp/policy/docs/pa/Army_Data_and_Data_Rights_Guide_1st_Edition_4_Aug_2015.pdf
- Army Regulation 5-12, "Army Use of the Electromagnetic Spectrum." Headquarters Department of the Army, Washington, D.C. February 8, 2020.
- Army Regulation 25-1, "Army Information Technology." Headquarters Department of the Army, Washington, D.C. July 15, 2019.
https://home.army.mil/benning/1617/4369/7221/ARN37510-AR_25-1-001-WEB-3.pdf
- ASSIST. <https://assist.dla.mil/>
- ASTM-D3951-18, "Standard Practice for Commercial Packaging." ASTM International, October 4, 2023.
<https://store.astm.org/d3951-18.html>
- Aviation Critical Safety Item Management Handbook. Joint Aeronautical Commanders Group (JACG), NAVAIR Public Release 11-515, March 16, 2011.
https://us-east1-menlo-inspect.menlosecurity.com/safeview-fileserv/tc_download/39e210e0f818244cbb20cb4a3a5c559716c085e62ff2a9ba8c3a00e8e6925882/?&cid=N46476B6A4906&rid=d3f123f2e71ec1c998b6a7edcaf9f384&cl=od_menlo_1b&file_url=http%3A%2F%2Feveryspec.com%2FUSN%2FNAVAIR%2Fdownload.php%3Fspec%3DJALC_AVIATION_CSI_MGMT_HDBK_16MAR2011.055725.pdf&type=original
- "Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, ISO/IEC/IEEE 24748-7, and ISO/IEC/IEEE 24748-8) on Contracts for Department of Defense Acquisition Programs." Office of the Deputy Assistant Secretary of Defense for Systems Engineering, April 2017.

Charlock, P.G., and R.E. Fenton, “System-of-Systems (SoS) Enterprise Systems for Information-Intensive Organizations,” *Systems Engineering* 4(4) (2001), pages 242-261.

Code of Federal Regulations (CFR) Title 49: Transportation. Parts 171-180. Office of the Federal Register.

<https://www.ecfr.gov/current/title-49>

CPC Planning Guidebook. *See* DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment (MS&E)

DA Pam 95-9, “Management of Aviation Critical Safety Items.” Also identified as SECNAVINST 4140.2, AF120-06, DLAI 3200.4, DCMA INST CSI (AV). Departments of the Army, Navy, the Defense Logistics Agency, and Defense Contract Management Agency, January 25, 2006. https://static.e-publishing.af.mil/production/1/af_a4/publication/afi20-106_ip/afi20-106_ip.pdf

DD Form 1494. Application for Equipment Frequency Allocation.

<https://www.dau.edu/sites/default/files/Migrated/CopDocuments/DD%20FORM%201494.pdf>

Defense Acquisition University (DAU). CLE 009, System Safety in Systems Engineering. Continuous Learning Module.

<https://www.dau.edu/courses/cle-009>

Defense Acquisition University (DAU). “Milestone Document Identifier,” (n.d.). [Retrieved August 7, 2025]

<https://www.dau.edu/blogs/milestone-document-identification-mdid-tool>

Defense Counterintelligence and Security Agency (DCSA) website. [Accessed August 11, 2021.]

<https://www.dcsa.mil/>

Defense Federal Acquisition Regulation Supplement (DFARS).

<https://www.acquisition.gov/dfars>

DFARS, Subpart 207.105, “Contents of Written Acquisition Plans,” October 30, 2023.

DFARS, Subpart 209.270, “Aviation and ship critical safety items,” August 19, 2011.

DFARS, Subpart 211.274-2, “Using and Maintaining Requirements Documents, General,” October 1, 2020.

DFARS, Subpart 215.304, “Source Selection, Evaluation factors and significant subfactors,” December 31, 2019.

DFARS, Subpart 223.73, “Minimizing the Use of Materials Containing Hexavalent Chromium,” May 20, 2021.

DFARS, Subpart 246.371, “Contract Clauses, Notification of potential safety issues,” June 25, 2013.

DFARS, Subpart 246.407, “Government Contract Quality Assurance, Nonconforming supplies or services,” October 1, 2020.

- DFARS, Subpart 246.504, “Quality Assurance, Certificate of conformance,” January 10, 2008.
- DFARS, Subpart 252.211-7003, “Item Unique Identification and Valuation,” October 1, 2020.
- DFARS, Subpart 252.211-7007, “Reporting of Government-Furnished Property,” October 1, 2020.
- DFARS Subpart 252.227-7013, “Rights in Technical Data—Other Than Commercial Products and Commercial Services,” October 24, 2025.
- DFARS Subpart 252.227-7014, “Rights in Other Than Commercial Computer Software and Other Than Commercial Computer Software Documentation,” October 24, 2025.
- DFARS, Subpart 252.246-7003, “Notification of Potential Safety Issues,” December 21, 2018.
- Defense Standardization Program (DSP). Defense Standardization Program Office (DSPO). <https://www.dsp.dla.mil>
- Defense Technical Risk Assessment Methodology (DTRAM), Version 6.4. OUSD(R&E), May 2023.
- Defense Threat Reduction Agency Nuclear Survivability Program Guidebook (DTRA-TR-14-71). 2014.
- Department of the Army Pamphlet 25-1-1 “Army Information Technology Implementation Instructions,” July 15, 2019.
https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36806-PAM_25-1-1-001-WEB-3.pdf
- Digital Engineering, Modeling and Simulation (DEM&S). Website. Office of Systems Engineering and Architecture.
<https://www.cto.mil/sea/DEMS>
- Digital Engineering, Modeling and Simulation (DEM&S) Glossary. Office of Systems Engineering and Architecture.
<https://www.de-bok.org/glossary>
- DI-MGMT-81861, Integrated Program Management Data and Analysis Report (IPMDAR). Data Item Description. Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) Acquisition Data and Analytics, August 30, 2021.
<https://assist.dla.mil/>
- DoD 4145.19-R, “Storage and Warehousing Facilities and Services,” July 1978.
<https://apps.dtic.mil/sti/pdfs/ADA267900.pdf>
- DoD Acquisition Manager’s Handbook for Insensitive Munitions, Revision 4, Naval Ordnance Safety & Security Activity (NOSSA), December 2018.
- DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment (MS&E). OUSD(A&S), August 29, 2022.

- DoD Cybersecurity Test and Evaluation Guidebook v.3.0. OUSD(R&E), Advanced Capabilities, Developmental Test and Evaluation and Prototyping, June 2025.
<https://www.cto.mil/wp-content/uploads/2025/07/Cyber-DTE-Guidebook-V3-June2025.pdf>
- DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, June 27, 2023.
https://media.defense.gov/2023/nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf
- DoD Digital Engineering Fundamentals, Department of Defense Digital Engineering Working Group, 2022.
<https://www.cto.mil/wp-content/uploads/2023/06/Dig-Eng-Fundamentals-2022.pdf>
- DoD Directives Home. DoD Executive Services Directorate.
<https://www.esd.whs.mil/DD/>
- DoD Directive 4151.18, “DoD Maintenance of Military Materiel.” OUSD(A&S), August 30, 2020.
- DoD Directive 4715.21, “Improving Military Installation Resilience.” August 1, 2025.
- DoD Directive 5000.01, “The Defense Acquisition System.” OUSD(A&S), July 28, 2022.
- DoD Directive 5135.02, “Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)),” July 15, 2020.
- DoD Directive 5137.02, “Under Secretary of Defense for Research and Engineering (USD(R&E)),” July 15, 2020.
- DoD Directive 5230.25, “Withholding of Unclassified Technical Data from Public Disclosure.” OUSD(R&E), October 15, 2018.
- DoD Directive 5250.01, “Management of Intelligence Mission Data (IMD) in DoD Acquisition.” Office of the Under Secretary of Defense for Intelligence (OUSD(I)), August 29, 2017.
- DoD Directive 6055.09E, “Explosives Safety Management (ESM).” OUSD(A&S), November 18, 2016.
- DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise (DoD IE).” Office of the Department of Defense (DoD) Chief Information Officer (CIO), July 27, 2017, as amended.
- DoD Directive 8260.05, “Support of Strategic Analysis (SSA).” Office of Cost Assessment and Program Evaluation, July 7, 2011.
- DoD Earned Value Management System Interpretation Guide (EVMSIG), OUSD(A&S), Office of Acquisition Analytics and Policy, March 14, 2019.
- DoD Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 1.0, 2006.
- DoD Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 2.0, *forthcoming*.

- DoD Guide to Uniquely Identifying Items, Version 3.0, OUSD(AT&L), December 2, 2014.
- DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements, April 20, 2007.
- DoD Instruction 2010.06, “Materiel Interoperability and Standardization with Allies and Coalition Partners.” OUSD(A&S), July 29, 2009, Incorporating Change 1, August 31, 2018.
- DoD Instruction 3150.09, “The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy.” OUSD(A&S), April 8, 2015, Incorporating Change 4, August 12, 2023.
- DoD Instruction 3222.03, “DoD Electromagnetic Environmental Effects (E3) Program,” August 25, 2014, Office of the DoD CIO, Incorporating Change 2, October 10, 2017.
- DoD Instruction 4120.24, “Defense Standardization Program,” OUSD(R&E), March 31, 2022.
- DoD Instruction 4140.01, “DoD Supply Chain Materiel Management Policy.” OUSD(A&S), March 6, 2019, Incorporating Change 1, September 2, 2025
- DoD Instruction 4140.67, “DoD Counterfeit Prevention Policy,” OUSD(A&S), April 26, 2013, Incorporating Change 3, February 2, 2024.
- DoD Instruction 4151.19, “Serialized Item Management (SIM) for Life-Cycle Management of Materiel,” OUSD(A&S), January 9, 2014, Incorporating Change 2, August 31, 2018.
- DoD Instruction 4151.22, “Condition-Based Maintenance Plus for Materiel Maintenance,” OUSD(A&S), August 14, 2020.
- DoD Instruction 4160.28, “DoD Demilitarization Program.” OUSD(A&S), April 7, 2011, Incorporating Change 2, August 30, 2022.
- DoD Instruction 4245.14, “Value Engineering Program.” OUSD(R&E), October 1, 2024.
- DoD Instruction 4245.15, “Diminishing Manufacturing Sources and Material Shortages Management.” OUSD(A&S), November 5, 2020. Incorporating Change 1, September 2, 2025.
- DoD Instruction 4540.07, “Operation of the DoD Engineering for Transportability and Deployability Program.” OUSD(A&S), February 19, 2016, incorporating Change 3, October 30, 2019.
- DoD Instruction 4630.09, “Communications Waveform Management and Standardization.” DoD CIO, November 23, 202050.
- DoD Instruction 4650.01, “Policy and Procedures for Management and Use of the Electromagnetic Spectrum.” Office of the DoD CIO, January 9, 2009, Including Change 1, October 17, 2017.
- DoD Instruction 5000.02, “Operation of the Adaptive Acquisition Framework.” OUSD(A&S), January 23, 2020, Incorporating Change 2, April 8, 2026.
- DoD Instruction 5000.61, “DoD Modeling and Simulation Verification, Validation, and Accreditation.” OUSD(R&E), September 17, 2024.

- DoD Instruction 5000.64, “Accountability and Management of DoD Equipment and Other Accountable Property.” OUSD(A&S), April 27, 2017, Incorporating Change 3, June 10, 2019.
- DoD Instruction 5000.66, “Defense Acquisition Workforce Education, Training, Experience, and Career Development Program.” OUSD(A&S), July 27, 2017, Including Change 3, March 25, 2022.
- DoD Instruction 5000.67, “Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure,” OUSD(A&S), August 31, 2018, as amended.
- DoD Instruction 5000.82, “Requirements for the Acquisition of Digital Capabilities.” Office of the DoD CIO, June 1, 2023.
- DoD Instruction 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” OUSD(R&E), July 20, 2020, Incorporating Change 1, May 21, 2021.
- DoD Instruction 5000.85, “Major Capability Acquisition,” OUSD(A&S), August 6, 2020, Incorporating Change 1, November 4, 2021.
- DoD Instruction 5000.88, “Engineering of Defense Systems,” OUSD(R&E), November 18, 2020.
- DoD Instruction 5000.89, “Test and Evaluation,” OUSD(R&E), November 19, 2020.
- DoD Instruction 5000.91, “Product Support Management for the Adaptive Acquisition Framework, November 4, 2021
- DoD Instruction 5000.95, “Human Systems Integration.” OUSD(R&E), April 1, 2022.
- DoD Instruction 5000.97, “Digital Engineering.” OUSD(R&E), December 21, 2023
- DoD Instruction 5025.13, “DoD Plain Language Program.” Office of the Chief Management Officer of the Department of Defense, January 23, 2020, Incorporating Change 2, February 9, 2024.
- DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI).” Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), October 1, 2020.
- DoD Instruction 5200.39, “Critical Program Information (CPI) Protection Within the Department of Defense,” OUSD(I&S)/ OUSD(R&E), Incorporating Change 3, Effective October 1, 2020.
- DoD Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,” OUSD(I&S)/OUSD(R&E), February 16, 2024.
- DoD Instruction 5205.11, “Management, Administration, and Oversight of DoD Special Access Programs (SAPs),” Office of the Executive Director for Special Access Programs, Incorporating Change 2, February 4, 2020.
- DoD Instruction 5230.24, “Distribution Statements on DoD Technical Information,” OUSD(R&E), January 10, 2023.

- DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance,” Office of the DoD CIO, July 14, 2015, Incorporating Change 1, August 11, 2017.
- DoD Instruction 8320.03, “Unique Identification (UID) Standards for Supporting the DoD Information Enterprise.” OUSD(A&S), Incorporating Change 2, August 31, 2018.
- DoD Instruction 8320.04, “DoD Serially Managed Items of Tangible Personal Property and Item Unique Identification 2.0 Standards.” OUSD(A&S), November 29, 2024.
- DoD Instruction 8330.01, “Interoperability of Information Technology, Including National Security Systems,” Office of the DoD CIO, September 27, 2022.
- DoD Instruction 8500.01, “Cybersecurity,” Office of the DoD CIO, Incorporating Change 1, Effective October 7, 2019.
- DoD Instruction 8510.01, “Risk Management Framework for DoD Systems.” Office of the DoD CIO, July 19, 2022.
- DoD Instruction 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information,” Office of the DoD CIO, December 9, 2019.
- DoD Joint Software Systems Safety Engineering Handbook (JSSSEH). Version 1.0. Joint Software Systems Safety Engineering Working Group, Naval Ordnance Safety and Security Activity. Director of Defense Research and Engineering, August 27, 2010.
<https://www.cto.mil/wp-content/uploads/2023/08/Joint-SW-SSE-2010.pdf>
- DoD Manual 4120.24, “Defense Standardization Program Procedures,” OUSD(R&E), September 24, 2014, Incorporating Change 2, Effective October 15, 2018.
- DoD Manual 4140.01, Volume 3, “DoD Supply Chain Materiel Management Procedures: Materiel Sourcing,” July 2025, as amended.
- DoD Manual 4140.01, Volume 5, “DoD Supply Chain Materiel Management Procedures: Delivery of Materiel.” OUSD(A&S), February 10, 2014.
- DoD Manual 4140.01, Volume 6, “DoD Supply Chain Materiel Management Procedures: Materiel Returns, Retention, and Disposition,” November 2022, as amended.
- DoD Manual 4140.01, Volume 11, “DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling,” OUSD(A&S), March 8, 2017, as amended.
- DoD Manual 4140.27, Volume 1, “DoD Shelf-Life Management Program: Program Administration.” OUSD(A&S), July 6, 2016, as amended.
- DoD Manual 4151.25, “Reliability Centered Maintenance,” OUSD(A&S), February 16, 2024.
- DoD Manual 4160.21, Volume 1, “Defense Materiel Disposition: Disposal Guidance and Procedures.” OUSD(A&S), October 22, 2015, as amended.
- DoD Manual 4160.28, Vol. 1, “Defense Demilitarization: Program Administration.” OUSD(A&S), August 9, 2017, Incorporating Change 3, July 15, 2019.

- DoD Manual 5000.103, “Cyber Developmental Test and Evaluation.” OUSW(R&E), February 26, 2026
- DoD Manual 5010.12, “Procedures for the Acquisition and Management of Technical Data.” OUSD(A&S), November 21, 2025.
- DoD Manual 5400.07, “Freedom of Information Act (FOIA) Program,” Office of the Deputy Chief Management Officer of the Department of Defense, January 25, 2017.
- DoD Manual 8400.01, “Accessibility of Information and Communications Technology (ICT).” Office of the DoD CIO, November 14, 2017, Incorporating Change 1, March 12, 2025.
- DoD Mission Engineering Guide. Version 2.0. OUSD(R&E), Mission Capabilities, October 2023.
https://ac.cto.mil/wp-content/uploads/2023/11/MEG_2_Oct2023.pdf
- DoD Modeling and Simulation Catalog. April 21, 2015.
<https://content.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/modeling-and-simulation/past-events/2015-april/mullen-frank-se-ms-april-2015.ashx>
- DoD Net-Centric Services Strategy. DoD CIO. March 2007.
https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf
- DoD Open Systems Architecture Contract Guidebook for Program Managers, Version 1.1. DoD Open Systems Architecture Data Rights Team, June 2013.
- DoD Operational Energy Strategy: Implementation Plan. Assistant Secretary of Defense for Operational Energy Plans and Programs, DoD, May 2023.
<https://climateandsecurity.org/wp-content/uploads/2024/11/2023-Operational-Energy-Strategy.pdf>
- DoD Producibility and Manufacturability Engineering Guide. Office of the Under Secretary of Defense for Research and Engineering, May 2024.
<https://www.cto.mil/sea/pg> | Manufacturing and Quality
- DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, September 2023, incorporating Change 2.2, December 2023.
<https://www.cto.mil/sea/pg> | Risk Assessments
- DoD Systems Engineering Plan (SEP) Outline, Version 4.1. OUSD(R&E), September 2023.
<https://www.cto.mil/sea/pg> | Engineering Guidance
- DoD Technology Readiness Assessment Guidebook. OUSD(R&E), February 2025.
<https://www.cto.mil/sea/pg> | Engineering Guidance
- DTR 4500.9-R, “Cargo Movement.” In Defense Transportation Regulation (DTR). U.S. Transportation Command.
<https://www.ustranscom.mil/dtr/>

- Early Manufacturing and Quality Engineering Guide. Office of the Under Secretary of Defense for Research and Engineering, 2022.
<https://www.cto.mil/wp-content/uploads/2025/02/EarlyMQEngGuide-15July2022-Cleared.pdf>
- EIA-649-1A, Configuration Management Requirements for Defense Contracts, SAE, August 10, 2020.
- Engineering of Defense Systems Guidebook. OUSD(R&E), February 2022, incorporating change 2, October 2024.
- Executive Order 12114, National Environmental Protection Act (NEPA), Environmental Effects Abroad of Major Federal Actions, January 4, 1979
- Federal Acquisition Regulation (FAR).
<https://www.acquisition.gov/browse/index/far>
- FAR Subpart 23.2, “Energy and Water Efficiency and Renewable Energy.”
- FAR Subpart 23.4, “Use of Recovered Materials and Biobased Products.”
- FAR Subpart 23.7, “Contracting for Environmentally Preferable Products and Services.”
- FAR Subpart 23.8, “Ozone-Depleting Substances and Greenhouse Gases.”
- FAR Subpart 39.204, “Exceptions.”
- FAR Subpart 48.102, “Policies.”
- GAO-12-400SP. “Defense Acquisitions: Assessment of Selected Weapon Programs.” Report to congressional committees. Government Accountability Office (GAO), March 2012.
<https://www.gao.gov/assets/gao-12-400sp.pdf>
- GAO-17-77. “Weapon System Requirements: Detailed Systems Engineering Prior to Product Development Positions Programs for Success.” Report to congressional committees. GAO, November 2016.
<https://www.gao.gov/assets/gao-17-77.pdf>
- Guide to Program Management Business Processes. *See A Guide to...*
- Guide to Program Management Knowledge, Skills and Practices. *See A Guide to...*
- Human Systems Integration Guidebook. OUSD(R&E), 2022, incorporating Change 1, June 2024.
<https://www.cto.mil/wp-content/uploads/2024/07/HSI-Guidebook-C1-2024.pdf>
- IEEE Standard 1633-2016. IEEE Recommended Practice on Software Reliability, January 18, 2017. <https://www.ieee.org/>
- INCOSE Guide to Writing Requirements, July 1, 2023.
- INCOSE (International Council on Systems Engineering). *Systems Engineering Handbook*. 5th edition. Hoboken, N.J.: Wiley and Sons, 2023.

- INCOSE Systems Engineering Competency Framework (SECF). International Council on Systems Engineering (INCOSE) Technical Product Reference INCOSE-TP-2018-002-01-0. INCOSE International Competency Working Group, July 2018.
- Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide. OUSD(R&E), May 2023, incorporating Change 1, October 2024.
<https://www.cto.mil/wp-content/uploads/2024/10/IMP-IMS-Guide-May2023-C1-Oct2024.pdf>
- Intellectual Property Guidebook for DoD Acquisition, OUSD(A&S), April 30, 2025.
- “Intellectual Property: Navigating through Commercial Waters.” Under Secretary for Defense Acquisition Technology and Logistics, October 15, 2001.
- Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook. OUSD(A&S), September 2023.
- ISO/IEC/IEEE 15288, Systems and Software Engineering-System Life Cycle Processes, July 7, 2015.
- ISO/IEC/IEEE 24748-7:2026, Systems and Software Engineering—Life Cycle Management, Part 7: Application of Systems Engineering on Defense Programs.
- ISO/IEC/IEEE 24748-8:2019, Systems and Software Engineering—Life Cycle Management, Part 8: Technical Reviews and Audits on Defense Programs.
- JACG CSI Management Handbook. *See* Aviation Critical Safety Item Management Handbook.
- Joint Services Software Safety Authorities Implementation Guide. *See* Software System Safety Implementation Process and Tasks Supporting MIL-STD-882.
- Life Cycle Sustainment Plan (LCSP) Outline, Version 2.0. Defense Acquisition University, October 13, 2022.
<https://www.dau.edu/tools/life-cycle-sustainment-plan-lcsp-outline>
- Manual of Regulations and Procedures for Federal Radio Frequency Management (“Redbook”). National Telecommunications and Information Administration (NTIA), Department of Commerce, March 6, 2023.
<https://www.ntia.gov/publications/redbook-manual>
- Manufacturing and Quality Engineering. Web page.
<https://www.cto.mil/sea/mq/>
- Manufacturing Readiness Level Deskbook. OSD Manufacturing Technology Program in collaboration with The Joint Service/Industry MRL Working Group, September 2025.
https://www.dodmrl.com/MRL_Deskbook_2025.pdf
- Manufacturing Readiness Levels Guide.
<https://dodmrl.com/>
- Military Handbooks and Standards. ASSIST.
<https://assist.dla.mil/>

- MIL-HDBK-61B, Configuration Management Guidance. August 15, 2025.
- MIL-HDBK-235-1D, Military Operational Electromagnetic Environment Profiles Part 1D General Guidance. Defense Information Systems Agency, October 16, 2024.
- MIL-HDBK-237, Electromagnetic Environmental Effects and Spectrum Supportability Guidance for the Acquisition Process. Defense Information Systems Agency, April 4, 2013.
- MIL-HDBK-240, Hazards of Electromagnetic Radiation to Ordnance Test Guide. Defense Information Systems Agency, November 1, 2002.
- MIL-HDBK-245, Preparation of Statement of Work (SOW). Executive Agent for the Defense Standardization Program, September 21, 2023.
- MIL-HDBK-502, Product Support Analysis. Logistics and Materiel Readiness Directorate, Logistics Data Analysis Center, April 18, 2025.
- MIL-HDBK-539, Digital Engineering and Modeling Practices. OUSW(R&E), March 2026.
- MIL-HDBK-896, Manufacturing Management Program Guide. Air Force Life Cycle Management Center, September 18, 2025.
- MIL-STD-129, “Military Marking for Shipment and Storage.” Army Materiel Command, Packaging, Storage and Containerization Center, February 25, 2023.
- MIL-STD-130, “Identification Marking of U.S. Military Property.” AFMC/A4/10 Directorate of Logistics, Civil Engineering, Force Protection, August 26, 2019.
- MIL-STD-461, “Requirements for the Control of Electromagnetic Interference Characteristics Requirements for Equipment.” Air Force Life Cycle Management Center—Aircraft Systems, December 11, 2015.
- MIL-STD-464, “Electromagnetic Environmental Effects Requirements for Systems.” Air Force Life Cycle Management Center—Aircraft Systems, December 24, 2020.
- MIL-STD-810, “Environmental Engineering Considerations and Laboratory Tests.” Army Test and Evaluation Command, May 18, 2022.
- MIL-STD-881, “Work Breakdown Structures for Defense Materiel Items.” OUSD(A&S) Acquisition Data and Analytics, May 13, 2022.
- MIL-STD-882, “System Safety.” Air Force Materiel Command Safety Office, September 27, 2023.
- MIL-STD-963, “Data Item Descriptions.” Executive Agent for the Defense Standardization Program, November 7, 2019.
- MIL-STD-1472, “Human Engineering.” Naval Sea Systems Command (Ship Systems), September 15, 2020.
- MIL-STD-1546, “Parts, Materials, and Processes Control Program for Space and Launch Vehicles.” Space Systems Command, October 20, 2008.

- MIL-STD-1547, “Electronic Parts, Materials, and Processes for Space and Launch Vehicles.” Space Systems Command, October 20, 2008.
- MIL-STD-11991, “General Standard for Parts, Materials, and Processes.” Executive Agent for the Defense Standardization Program, October 3, 2023.
- MIL-STD-2073, “Standard Practice for Military Packaging.” Naval Air Systems Command, June 27, 2024.
- MIL-STD-2105, “Hazard Assessment Tests for Non-Nuclear Munitions.” Naval Surface Warfare Center Indian Head Division (NSWC IHD), January 6, 2022.
- MIL-STD-31000, “Technical Data Packages.” U.S. Army Combat Capabilities Development Command, Armaments Center, February 3, 2025.
- MIL-STD-3056, “Design Criteria for Chemical, Biological, and Radiological System Contamination Survivability.” Edgewood Chemical Biological Center (ECBC), July 19, 2024.
- MIL-STD-46855, “Human Engineering Requirements for Military Systems, Equipment and Facilities.” Combat Capabilities Development Command, Aviation and Missile Center, September 23, 2025.
- Monje, Andrew. “Guidance for Tailoring R&M Engineering Data.” Office of the Deputy Assistant Secretary of Defense for Systems Engineering, April 2016.
<https://www.cto.mil/sea/rm>
- MOSA Assessment Criteria. OSD(R&E), May 2022.
<https://www.cto.mil/wp-content/uploads/2023/06/MOSA-Assess-2022.pdf>
- National Institute of Standards and Technology (NIST) website.
<https://wwwStandards.gov>
- Navy Technical Manual SL150-AA-PRO-010/DMP. Data Management Program: Operations and Procedures Manual for Contractor-Prepared Data. Revision 2. Naval Sea Systems Command, June 1, 2009.
- NTIA Manual (“Redbook”). *See* Manual of Regulations and Procedures for Federal Radio Frequency Management.
- Office of Management and Budget (OMB) Memorandum, “ ‘Myth-busting 3’ Further Improving Industry Communication with Effective Debriefings.” OMB, January 5, 2017.
- OUSW(R&E) SE&A Website. *See* Systems Engineering and Architecture (SE&A) Website.
- OPNAVINST 2400.20G, “Electromagnetic Environmental Effects and Spectrum Supportability Policy and Management,” January 7, 2021.
- Product Support Business Case Analysis Guidebook, Defense Acquisition University (DAU), June 2024.
- Product Support Manager Guidebook. Defense Acquisition University (DAU), 2022.

- Program Protection Plan Outline and Guidance, Version 1.0. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, July 2011.
- Public Law 82-436, “Defense Cataloging and Standardization Act of 1952,” July 1, 1952.
- Public Law 107-347, “E-Government Act of 2002,” 107th Congress, December 17, 2002.
- RAM-C Rationale Report Outline and Guidance. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, February 2017.
<https://www.cto.mil/wp-content/uploads/2023/06/RAMC-Outline-2017.pdf>
<https://www.cto.mil/sea/pg/> | Reliability and Maintainability Engineering
- RAM-C Rationale Report Outline Guidance Training. Presentation. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, June 26, 2018.
<https://www.cto.mil/sea/pg/> | Reliability and Maintainability Engineering
- Reliability and Maintainability (R&M) Engineering Management Body of Knowledge. Web page. Office of Systems Engineering and Architecture, OUSW(R&E).
<https://www.cto.mil/sea/rm>
- RIO Guide. *See* DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.
- Roedler, Garry, and Dave Walden. INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. 5th Ed. Hoboken, N.J.: Wiley and Sons, 2023.
- SAE 6906, Standard Practice for Human Systems Integration. SAE International, December 12, 2023.
<https://saemobilus.sae.org/standards/sae6906a-standard-practice-human-systems-integration>
- SAE-GEIA-HB-649A, Configuration Management Standard Implementation Guide, March 3, 2016.
- SD-19, Parts Management Guide: A Guidebook of Best Practices for Oversight of Part Selection in Defense Systems. Defense Standardization Program Office, January 2024.
- SD-22, Diminishing Manufacturing Sources and Material Shortages: A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program. Defense Standardization Program Office, March 2024.
- SD-24, Value Engineering: A Guidebook of Best Practices and Tools. OUSD(R&E), February 2025.
<https://www.cto.mil/wp-content/uploads/2025/02/SD-24-VE-Guidebook-25Feb2025-Cleared-1.pdf>
- SD-26, DMSMS and Parts Management Contracting Guide. Defense Standardization Program Office, June 2023.
- SECNAVINST 2400.1, “Electromagnetic Spectrum Policy and Management,” May 20, 2019.
- SECNAVINST 2400.2, “Electromagnetic Environment Policy and Management,” August 2011.

SECNAVINST 4140.2, “Management of Aviation Critical Safety Items.” AFI 20-106. DLAI 3200.4, January 25, 2006.

Secretary of Defense Memorandum, “DoD Policy on Submunition Reliability,” January 10, 2001.

Secretary of War (SecWar) Memorandum, “Reforming the Joint Requirements Process to Accelerate Fielding of Warfighting Capabilities,” November 7, 2025.

Secretary of War (SecWar) Memorandum, “Transforming the Defense Acquisition System into the Warfighting Acquisition System to Accelerate Fielding of Urgently Needed Capabilities to Our Warriors,” November 7, 2025.

Section 104, In Public Law 102-538, “Telecommunications Authorization Act of 1992” October 27 1992.

Section 130, In Public Law 109-364, “John Warner National Defense Authorization Act for Fiscal Year 2007,” October 17, 2006.

Section 357, In Public Law 104-106, “National Defense Authorization Act for Fiscal Year 1996,” February 10, 1996.

Section 800, In Public Law 116-92, “National Defense Authorization Act for Fiscal Year 2020,” December 20, 2019. Section 802, In Public Law 108-136, “National Defense Authorization Act for Fiscal Year 2004,” September 17, 2004.

Section 812, In Public Law 111-383, “Ike Skelton National Defense Authorization Act for Fiscal Year 2011” January 7, 2011.

Section 818, In Public Law 112-81, “National Defense Authorization Act for Fiscal Year 2012,” December 31, 2011.

Section 855, In Public Law 114-328, “National Defense Authorization Act for Fiscal Year 2017,” December 23, 2016.

Section 1054, In Public Law 108-375, “Clarification of definition of major defense acquisition program for certain purposes,” October 28, 2004.

Section 8104, In Public Law 103-355, “Federal Acquisition Streamlining Act of 1994,” October 13, 1994.

SE&A Website. *See* Systems Engineering and Architecture (SE&A) Website.

Shevchenko, Nataliya. “An Introduction to Model-Based Systems Engineering (MBSE).” December 21, 2020.

<https://insights.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/>

Software System Safety Implementation Process and Tasks Supporting MIL-STD-882. Joint Services-Software Safety Authorities (JSSEH), March 14, 2018.

<https://www.cto.mil/wp-content/uploads/2025/08/JSSSEH-Implementation-Guide-2018.pdf>

SoS Systems Engineering and Test & Evaluation: Final Report of the NDIA SE Division SoS SE and T&E Committees. March 2012.

<https://ndia.dtic.mil/wp-content/uploads/2012/system/ttrack214771.pdf>

SSPC-CPC-1/NACE-21412-2020, Corrosion Prevention and Control Planning Industry Standard. Association for Materials Protection and Performance (AMPP).

Sustainability Analysis Guidance: Integrating Sustainability into Acquisition Using Life Cycle Assessment, Version 7. Office of the Assistant Secretary of Defense (Sustainment), June 2020.

Systems Engineering and Architecture (SE&A) Website. OUSW(R&E).

<https://www.cto.mil/sea/>

Defense Standardization Program Office

<https://www.cto.mil/sea/dsp/>

Digital Engineering, Modeling & Simulation

<https://www.cto.mil/sea/DEMS>

Human Systems Integration

<https://www.cto.mil/sea/hsi>

Manufacturing and Quality

<https://www.cto.mil/sea/mq>

Modular Open Systems Approach

<https://www.cto.mil/sea/mosa/>

Policy and Workforce

<https://www.cto.mil/sea/pw/>

Reliability and Maintainability Engineering

<https://www.cto.mil/sea/rm>

SE&A Library: Policy and Guidance

<https://www.cto.mil/sea/pg/>

Software Engineering

<https://www.cto.mil/sea/swe>

Specialty Engineering

<https://www.cto.mil/sea/spe>

Systems Engineering

<https://www.cto.mil/sea/se>

System Safety Engineering

<https://www.cto.mil/sea/sse/>

Value Engineering

<https://www.cto.mil/sea/ve>

Workforce

<https://www.cto.mil/sea/workforce/>

System of Systems Engineering Guidebook. Office of the Under Secretary of War for Research and Engineering (OUSW(R&E)), 2026.

Systems Engineering Research Center (SERC). “Modernizing Systems Engineering for Digital Transformation.” SERC, October 17, 2022.

Systems Engineering Plan (SEP) Outline. *See* DoD Systems Engineering Plan (SEP) Outline.

Technology and Program Protection Guidebook. OUSD(R&E), 2022.

https://aaf.dau.edu/storage/2024/08/TPP_Guidebook.pdf

Technology Readiness Assessment (TRA) Guidebook. OUSD(R&E), February 2025.

<https://www.cto.mil/wp-content/uploads/2025/03/TRA-Guide-Feb2025.v2-Cleared.pdf>

Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Memorandum, “Joint Insensitive Munitions Test Standards and Compliance Assessment,” February 10, 2010.

Under Secretary of War for Acquisition and Sustainment (USW(A&S)) Memorandum, “Establishment of Department-Wide Modular Open Systems Approach Policy and Minimum Expectations,” September 21, 2026.

Unmanned Systems Safety Engineering Precepts Guide for DoD Acquisition. OUSD(R&E), 2021.

<https://www.cto.mil/wp-content/uploads/2023/06/UxS-Precepts-2021.pdf>

U.S. Defense Information Systems Agency and the Defense Spectrum Organization. “Joint Services Guide for Development of a Spectrum Supportability Risk Assessment (SSRA).” Joint Services Software Safety Authorities, September 2011.

<https://www.dau.edu/cop/e3/documents/joint-services-guide-development-ssra>

U.S. Department of Health and Human Services. (n.d.) Retrieved August 11, 2021 from:

<http://www.hhs.gov/>

U.S. Department of Justice Civil Rights Division, “Information and Technical Assistance for the Americans with Disabilities Act,” (n.d.). Retrieved August 11, 2021, from:

<https://www.ada.gov/>

U.S. Department of Veterans Affairs, “VA Section 508,” (n.d.). Retrieved August 11, 2021 from:

<http://www.section508.va.gov/>

Warfighting Acquisition University (WarU) Glossary.

<https://www.waru.edu/glossary>



OFFICE OF SYSTEMS ENGINEERING AND
ARCHITECTURE

OFFICE OF THE UNDER SECRETARY OF WAR
FOR RESEARCH AND ENGINEERING

[HTTPS://WWW.CTO.MIL/SEA](https://www.cto.mil/sea)

1-PRG-01347 - 210-110-210
REVISION 0.0

DEFENSE ACQUISITION
PROGRAM
NOV-19-19

2020-11-19 14:00:00
NOV-19