Systems Engineering Guidebook

February 2022

Office of the Deputy Director for Engineering

Office of the Under Secretary of Defense
for Research and Engineering

Washington, D.C.

Systems Engineering Guidebook

Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd.r-e.comm@mail.mil
https://ac.cto.mil/engineering

Approved by

POSSEHL.STEPHANIE.LYNN.1229383805 Digitally signed by POSSEHL.STEPHANIE.LYNN.1229383805
Date: 2022.02.11 11:22:44 -05'00'

Stephanie L. Possehl
Acting Deputy Director for Engineering
Office of the Under Secretary of Defense for Research and Engineering

Systems Engineering Guidebook Change Record

Date	Change	Rationale

CONTENTS

Figures

Tables

1 INTRODUCTION

The Systems Engineering Guidebook provides guidance and recommended best practices for defense acquisition programs. Much of this information appeared previously in the Defense Acquisition Guidebook (DAG) Chapter 3, Systems Engineering. The DAG has been canceled, and this document is intended to provide interim systems engineering (SE) guidance while the Department of Defense (DoD) is developing new Systems Engineering Modernization policy and guidance. The DoD Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), Deputy Director for Engineering, prepared this guidebook in cooperation with subject matter experts (SMEs) from the Military Services, Defense Agencies, industry, and academia.

This guidebook is intended for Program Managers (PMs) and Systems Engineers and may be tailored for programs in any of the DoD Adaptive Acquisition Framework pathways (DoD Instruction (DoDI) 5000.02). Programs can use the guidebook, along with other acquisition business resources, to plan and execute program SE activities across the system life cycle. The forthcoming Engineering of Defense Systems Guidebook will provide additional guidance on applying SE and other engineering disciplines to each of the acquisition pathways.

1.1 Purpose of Systems Engineering

SE establishes the technical framework for delivering materiel capabilities to the warfighter. It provides the foundation upon which everything else is built and supports program success. SE seeks to ensure the effective development and delivery of capability through the implementation of a balanced approach with respect to cost, schedule, performance, and risk, using integrated, disciplined, and consistent SE 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. GAO Report 17-77 (2016) 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 documented in the Systems Engineering Plan (SEP), identifies the most efficient path to deliver a capability, from identifying user needs and concepts through delivery and sustainment. 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.

In addition, SE

- Supports development of realistic and achievable program performance, schedule, and cost goals as documented in the Joint Capabilities Integration and Development System (JCIDS) documents, Acquisition Program Baseline (APB), and Acquisition Strategy (AS).
- 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 baseline. The final product baseline 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.

This guidebook uses the following terms:

- The "Systems Engineer" refers to the Program Lead Systems Engineer, the Chief Engineer, or Lead Engineer responsible for SE, or to the SE staff responsible for SE processes who plan, conduct, or manage SE activities including design considerations, in the program.
- The "end user" includes the warfighter and other operational users, including support personnel, maintainers, and trainers who use or support the system.
- The "developer" refers to the system prime contractor (including associated subcontractors) or the Government agency responsible for designing and building the system.
- The "design considerations" comprise iterative and recursive management and technical activities, with varying degrees of interdependence, that traverse mission, digital networks, and SE to provide a required capability.

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. 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.

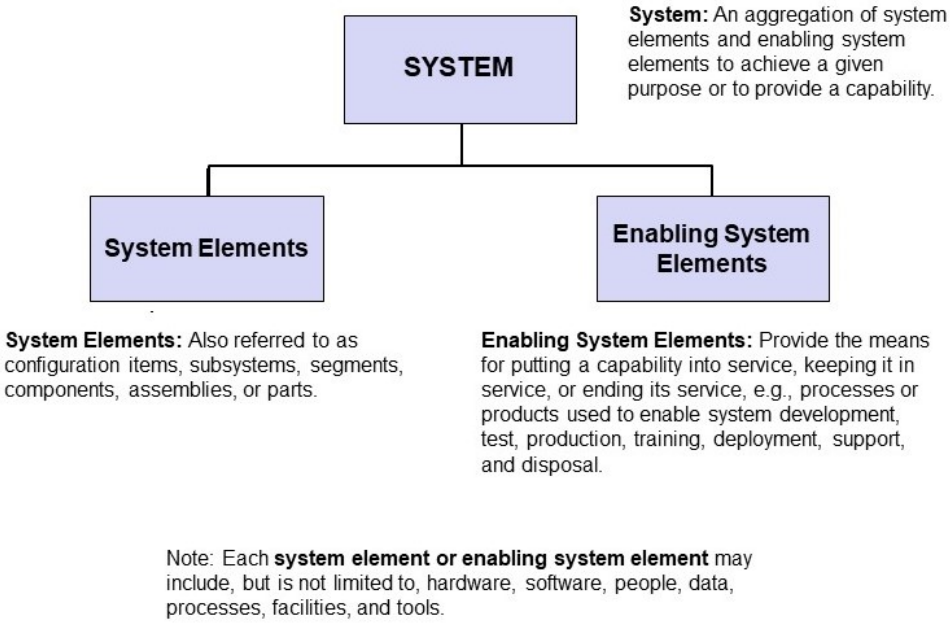


Figure 1-1. The System

SE applies critical thinking to the acquisition of a capability. It is a holistic, integrative discipline, whereby the contributions from across engineering disciplines (e.g., structural engineers, electrical engineers, mechanical designers, software engineers, safety engineers, human factors engineers, reliability engineers) 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 skills, instincts, and critical thinking ability to identify and focus efforts on the activities needed to enhance the overall system effectiveness, suitability, survivability, and sustainability.

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.

Development planning encompasses the engineering analyses and technical planning activities that provide the foundation for informed investment decisions on which path a materiel development decision takes. 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. The PM initiates development planning in advance of the Materiel Development Decision review and transfers the knowledge (documents, tools and related data) to the designated program.

1.3 Systems Engineering Processes

The practice of SE is composed of 16 processes: eight technical management processes and eight technical processes as listed in Figure 1-2 and described in Section 4, Systems Engineering Processes. These 16 processes provide a structured approach to increasing the technical maturity of a system and increasing the likelihood that the capability being developed balances mission performance with cost, schedule, risk, and design constraints.

The eight technical processes include the top-down design processes and bottom-up realization processes that support transformation of operational needs into operational capabilities. The eight technical management processes are implemented across the acquisition life cycle and provide insight and control to assist the PM, Systems Engineer, and Lead Software Engineer to meet performance, schedule, and cost goals.

The SE processes provide a framework that allows the program to structure and conduct its technical efforts to efficiently and effectively deliver a capability to satisfy a validated operational need. To fulfill that purpose, 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 (see Figure 1-2). 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.
- 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, listed at the bottom of Figure 1-2, 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. Taken together, these 16 processes are a systematic approach to provide operational capability to the warfighter while reducing technical and programmatic risk.

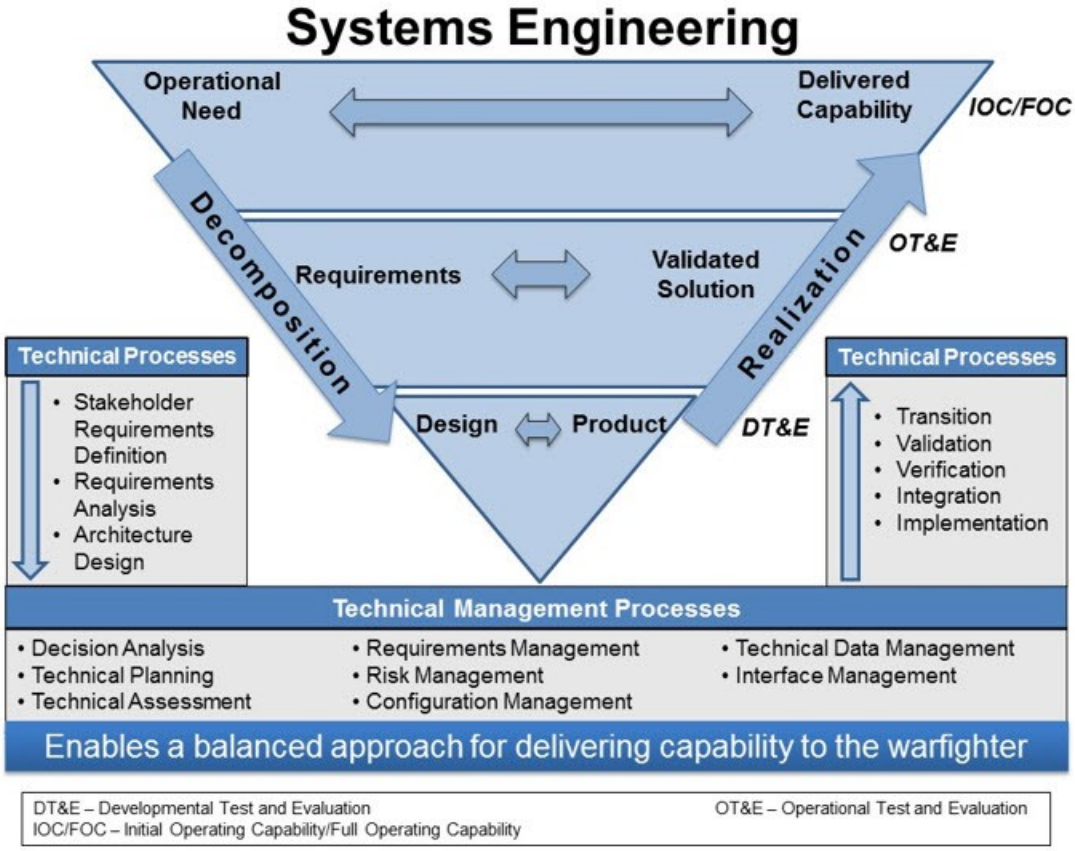


Figure 1-2. Systems Engineering Processes

All organizations performing SE should scale their application of the processes, further described in Section 4, Systems Engineering Processes, 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, adaptive acquisition 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).

1.4 Systems Engineering Policy and Guidance

SE policy and guidance are intended to minimize 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 Lead Software Engineers should know and understand the statutory and regulatory SE mandates. Table 1-1 identifies top-level SE-related policy.

Table 1-1. Systems Engineering-Related Policy

Systems Engineering–Related Policy	Source
DoD Directive 5000.01, The Defense Acquisition System	Office of the Under Secretary of Defense for Acquisition and Sustainment, September 9, 2020
DoD Instruction 5000.02, Operation of the Adaptive Acquisition Framework	Office of the Under Secretary of Defense for Acquisition and Sustainment, January 23, 2020
DoD Directive 5137.02, Under Secretary of Defense for Research and Engineering (USD(R&E))	Office of the Chief Management Officer of the Department of Defense, July 15, 2020
DoD Instruction 5000.88, Engineering of Defense Systems	Office of the Under Secretary of Defense for Research and Engineering, November 18, 2020

Additional SE-related policy and guidance are provided on the DDR&E(AC)/Engineering and Adaptive Acquisition Framework (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, formerly known as Acquisition Streamlining and Standardization Information System, is a web-based application that serves as DoD's official source for standardization documents developed, maintained, and used by DoD.

Programs must comply with DoD policy to receive approval and achieve milestones. DoD 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 are not only allowed but required to 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
- Type of 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 Milestone Decision Authority/Decision Authority (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. DoDI 5000.02 describes six acquisition 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 for more information on these pathways and the expected application for each pathway, highlighting the relevant SE and other engineering activities.).

All program strategy 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 2.2.8 Lessons Learned, Best Practices, Case Studies).

Cybersecurity and operational resilience are critical aspects of SE for all the acquisition pathways. The Systems Engineer should begin focusing on engineering for these aspects early and continuously throughout the program life cycle to ensure engineering designs identify and reduce cybersecurity operational and technical risks to support fielding systems that are capable, effective, and resilient.

1.5 Systems Engineering Plan

The purpose of the SEP is to assist PMs to develop, communicate, and manage the overall SE approach that guides all technical activities of the program. The SEP documents technical risks, performance evolution strategy (including use of a modular open systems approach to the maximum extent practicable), processes, resources, metrics, SE products, organizations, design considerations, and completed and scheduled SE activities. The SEP is a living document that should be updated as needed to reflect the program's evolving SE approach or plans and current

status. In accordance with DoDI 5000.88, Section 1.2.b., a SEP is required for Major Defense Acquisition Programs (MDAPs) and acquisition category (ACAT) II and III programs, unless waived by the SEP approval authority.

In addition, SEP content for MDAPs and ACAT II and III programs can be tailored with approval by the SEP approval authority. SEPs are a recommended best practice for all other defense system development. DoDI 5000.88, Section 3.4.a requires the Lead Systems Engineer, under the direction of the PM, to prepare a SEP to guide the SE activities on the program. PMs should use the SEP Outline to guide preparation of the plan. The SEP Outline identifies the minimum expected content to be addressed. The SEP 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 pathway. The 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).

In an effort to promote a higher probability of mission success, MDAPs should review, tailor, and implement applicable mission assurance concepts and principles when developing their SEP. MDAPs should use resources provided by their Service.

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 documented in the program SEP. DoDI 5000.88, Section 3.4.a identifies the USD(R&E), or designee, as the approval authority for ACAT ID program SEPs. The MDA, or designee, is the approval authority for ACAT IB/IC SEPs. The Component Acquisition Executive (CAE) will designate an approval authority for all other programs. The Engineering of Defense Systems Guidebook provides additional guidance for each of the AAF pathways. DoD Components are required to submit ACAT ID SEPs to the USD(R&E) at least 30 days before the required approval date. For other MDAPs, SEPs should be submitted within 30 days of approval to the designated approval authority, with approved SEPs provided to the USD(R&E) for information purposes. As a best practice, SEP updates should be approved by the Program Executive Office (PEO) 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 SEP.

The SEP 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 SEP 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.

Consistent with the DoDI 5000.88, Section 3.4.a, PMs should include the SEP (either an approved or a draft SEP) 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 acquisition strategy.

Before providing the SEP to the offerors, the PM, Systems Engineer, and Lead Software Engineer should determine whether the document contains sensitive information and, if so, remove this sensitive information from the SEP 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 SEP 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 articulates details of their processes, tools and organization.

As the program's blueprint for the conduct, management, and control of all technical activities, the SEP captures decisions made during the technical planning process and communicates objectives and guidance to program personnel and other stakeholders. The SEP should define the "who, what, when, why, and how" of the SE approach, 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 4, Systems Engineering Processes) to deliver a balanced solution to meet the warfighter's needs. It should identify unique processes, tools, or tailoring of organizational and Government standards, how these processes and tools are integrated, and how products are developed and managed. For instance, the description of the program's risk management approach and the status of top-level technical risk, issues, and opportunities (RIOs), including the mitigation and handling activities, should be documented in the SEP or summarized and referenced in separate planning documentation. As a best practice, the RIOs should be collected monthly and reported to senior leadership stakeholders at least quarterly (see Section 4.1.5 Risk Management Process).
- The event-driven technical review approach based on successful completion of activities as opposed to calendar-based deadlines. Document the plans for conducting each technical review with particular emphasis on the entry and exit criteria and details of the systems engineering technical reviews planned in the program's next acquisition phase. The SEP 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 SEP should include the assumptions made in developing the schedule and the process for conducting schedule risk assessments

(SRAs) and updates. SEPs 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 5.15 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 that ensures the system requirements (including Key Performance Parameters (KPPs) and Key System Attributes (KSAs)) are achievable within cost and schedule constraints. Cybersecurity and operational resilience should be part of the prototyping system survivability requirements to reduce the need for redesign.
- The description of the architecture products that will be developed to better describe and understand the system, including internal and external interfaces. As a best practice, to ensure architectures are properly formulated, the SEP should include a description of mission thread analysis completed to support material 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 5) should be listed in the mandatory tables, with all the associated documentation submitted with each SEP submission.
- The program's strategy for identifying, prioritizing, and selecting the set of TPMs and metrics (TPMM) should provide sufficient insight into the technical progress and program risks. Each measure or metric should have threshold, margin, and contingency values. The values should measure achievement over time and 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, and at least 15 TPMMs should be selected and reported to adequately identify, measure, track, and manage technical and programmatic risks. If the program is developed within a digital engineering ecosystem, stakeholders can access program data and review metrics at will throughout the program's life cycle. The following TPMMs should be considered for inclusion: Risk Management, Schedule Risk, Net Ready KPP, operational resilience, cyber survivability, Number of Class 1 Engineering Change Proposals (ECPs) and Number of Class 2 ECPs. In addition, the program should ensure that each Critical Technical Parameter (CTP) has a corresponding TPM (see Section 4.1.3 Technical Assessment Process).

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 Lead Software Engineer should understand (1) how the system fills the needs for which it was designed, (2) the design considerations (Section 5) 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/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 Lead Software Engineer should define intersystem interfaces using the Interface Control Document(s). In addition to Interface Control Documents, the PM, Systems Engineer, and Lead Software Engineer should also pursue Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with companion programs regarding interfaces, data exchanges, and advance notice of changes interdependencies and schedule (timing) that may affect either program. These agreements are a professional courtesy and 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).

SE is increasingly recognized as key to addressing the evolution of complex SoS. SE principles and tools can be 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 “Federal Enterprise Architecture Framework (FEAF),” January 2013).

This application of SE to address enterprises as complex systems builds on traditional SE activities and expands them to address enterprise challenges. The Systems Engineer can also assist with enterprise strategic planning and enterprise investment analysis. These two additional roles for Systems Engineers at the enterprise level are “shared with the organization’s senior line management, and tend to be more entrepreneurial, business-driven, and economic in nature in comparison to the more technical nature of classical systems engineering," (Source: Charlock, P.G., and R.E. Fenton, “System-of-Systems (SoS) Enterprise Systems for Information-Intensive Organizations,” Systems Engineering, Vol. 4, No. 4 (2001), pages 242-261).

Each DoD Service and Agency, and the Department itself, are examples of enterprises as systems. Such organizations have the challenge of integrating and evolving multiple portfolios of systems often with conflicting sets of objectives, constraints, stakeholders and demands for resources.

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 Specialty Engineering (Reliability and Maintainability (R&M), Manufacturing and Quality (M&Q), Human Systems Integration (HSI), and Safety) design considerations are addressed at the enterprise level. Mission areas, for example, can be viewed as cross-organizational enterprises and also provide critical context for system acquisition. Controlled interfaces with enabling systems in the SoS architecture drive system design. In some cases, enterprise considerations have been articulated as standards 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 Service portfolio of systems and mission area needs.

Most DoD capabilities today are provided by an aggregation of systems often referred to as systems of systems (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 unique capabilities. 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, designed for different purposes but now used to meet new objectives that may not have been defined at the time the systems were deployed.

Both individual systems and SoS conform to the accepted definition of a system in that each consists of parts, relationships, and a whole that is greater than the sum of its parts; however, not all systems are SoS. There are distinct differences between systems and SoS that should be taken into account in the application of SE to SoS (see Table 2-1, adapted from DoD Systems Engineering Guide for Systems of Systems and SoS Systems Engineering and Test & Evaluation: Final Report of the NDIA SE Division SoS SE and T&E Committees).

Table 2-1. Comparing Systems and Systems of Systems

	System	System of Systems (SoS)
Management and Oversight		
Stakeholder Involvement	Clearer set of stakeholders	Two or more levels of stakeholders with mixed, possibly competing interests. The stakeholders represent: 1. the independent and useful systems 2. the aggregation of the independent and useful systems

	System	System of Systems (SoS)
Governance	Aligned program management and funding. Higher levels of governance such as Program Executive Office and Office of the Under Secretary of Defense for Acquisition and Sustainment (internal and external governance)	Added levels of complexity with management and funding for both SoS and systems; No single manager controls all constituent systems in the SoS
Operational Environment		
Operational Focus	Designed and developed to meet operational objectives	Called upon to provide integrated capabilities using systems whose objectives have not been directly derived from current SoS objectives
Implementation		
Acquisition	Aligned to established acquisition process	Multiple system life cycles across acquisition programs, involving legacy systems, systems under development, new developments and technology insertion; stated capability objectives but may not have formal requirements
Test and Evaluation (T&E)	T&E of the system is possible	Testing more challenging because of systems' asynchronous life cycles, independence of constituent systems, and the complexity of all the moving parts; given these challenges, the T&E approach may need to focus on system or subsystem testing in risk areas of the capability and evaluate evidence from SoS level activities or roll-ups of system-level activities
Engineering and Design Considerations		
Boundaries and Interfaces	Focuses on boundaries and interfaces	Focus on identifying systems contributing to SoS objectives and enabling flow of data, control and functionality across and/or between the SoS while balancing needs of systems. The boundaries and interfaces between systems are important, because they serve as a conduit for data transfer
Performance and Behavior	Ability of the system to meet performance objectives	Performance across the SoS that satisfies SoS user capability needs while balancing needs of the systems
Cybersecurity, Operational Resilience	Ability of the system to meet performance objectives in contested cyberspace	Performance across the SoS in contested cyberspace; considerations of zero trust, inherited risk, or inherited defensive capabilities

2.1 Application of Systems Engineering to Systems of Systems

SoS SE deals with planning, analyzing, organizing, and integrating the capabilities of new and existing systems into a SoS capability greater than the sum of the capabilities of its constituent parts. The mix of systems may include existing, partially developed and yet-to-be-designed independent systems.

The DoD Guide to Systems Engineering for Systems of Systems and International Organization for Standards/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288 addresses the application of SE to SoS. The DoD guide

defines four types of SoS (Table 2-2). When a SoS is recognized as a "directed," "acknowledged," or "collaborative" SoS, SE is applied across the constituent systems and is tailored to the characteristics and context of the SoS. With increased efforts to network systems to facilitate information-sharing across the battlespace, most DoD systems also may be viewed as components of a "virtual" SoS. For virtual SoS, DoD net-centric policies and strategies, such as DoD Net-Centric Services Strategy, provide SE guidance regarding SoS contexts where there is an absence of explicit shared objectives or central management. The DoD Mission Engineering Guide (November 2020) can facilitate a way to incorporate human performance needs within SoS Capability delivery.

Table 2-2. Four Types of Systems of Systems

Type	Definition
Directed	Directed systems of systems (SoS) are those in which the SoS is engineered and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the centrally managed purpose
Acknowledged	Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, development, and sustainment approaches. Changes in the systems are based on cooperative agreements between the SoS and the system
Collaborative	In collaborative SoS, the component systems interact more or less voluntarily to fulfill agreed-upon central purposes
Virtual	Virtual SoS lacks a central management authority and a centrally agreed-upon purpose for the SoS. Large-scale behavior emerges-and may be desirable-but this type of SoS relies upon relatively invisible, self-organizing mechanisms to maintain it

2.2 Tools, Techniques, and Lessons Learned

SE tools and techniques support the performance of activities, the development of products, and the completion of specific tasks. SE tools and techniques support the PM, Systems Engineer, and Lead 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 Lead Software Engineer should begin applying SE tools, techniques, and lessons learned during the early stages of program definition to improve efficiency and traceability and to provide a technical framework for managing the system development.

Collaboration tools allow the program office and developer to exchange data and analyses easily. Analytical tools and techniques also can assist in the development and validation of system designs. 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 4.1.7)
- Integration with 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

MDAPs should clearly identify tools in use, define tool interfaces when the Government and developer select different tools to use for the same purpose, and describe how the tools support the program's SE approach.

Table 2-3 lists general capabilities and features of SE tools and the SE processes they might support.

Table 2-3. 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

Systems Engineering Process	Tool Capabilities/Features
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
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 systems of systems • 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 system and system elements performance 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

2.2.1 Models and Simulations

Models and simulations are SE tools used by multiple functional area disciplines. 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 to ensure that the products maintain consistency with the system and external dependencies and provide a comprehensive view of the effort and increase efficiency and confidence throughout the project's life span.

The DoD Modeling and Simulation Glossary defines a model as a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. A simulation is defined as a method for implementing a model over time. Models are essential to aid in understanding project state, complexities, and interdependencies, and to communicate among team members and stakeholders. Simulation provides results, including but not limited to: a means to explore concepts and system characteristics; open up the trade space; facilitate informed decisions; and support training. Perhaps most important, the dynamic nature of simulations can enable us to study the stochastic interactions between different entities (systems, individuals and the environment) in the battlespace that static models cannot.

Models and simulations are key digital tools used to make informed, data-driven decisions throughout all DoD activities, regardless of whether or not an engineering approach is recognized or used. Models and simulation results form a digital record of the effort's activities, phases, and baseline information in decision making.

DoD users require a capability to accurately simulate multi-domain warfare rapidly and cost-effectively to support analysis and training. Components achieve this by integrating multiple existing simulations representing disparate systems and domains into a simulation environment capable of representing the required operating space. Models, simulations, and simulation results should be reused whenever practical to deliver this capability cost effectively and efficiently. This is a great advantage to any user of these capabilities. Reuse can occur across disciplines and across a hierarchy of perspectives that range from an engineering or technical level up to the campaign or strategic level, as long as the model, simulation, or simulation result is appropriate for the reuse.

The DoD reuses many existing models and simulations. To represent large, complex, and multi-domain environments, DoD programs leverage existing Service and Agency built simulations. These simulations are typically custom built for specific uses, such as requirements development, prototyping, algorithm development, verification, performance assessment, testing, and training. Re-use for a different requirement than its intended use requires additional engineering.

In such an environment, integrators need to harmonize many touch points before the environment can be executed accurately. These touch points fall into the following categories:

- Networks and computer environments - This includes Information Assurance approvals for all simulations, middleware and the resulting environment.
- Connectivity and Communications – The protocols and mechanisms used to accurately exchange messages across the simulations.
- Simulation details and models – The underlying assumptions and constraints of the simulations and the models that comprise that simulation must be compatible or able to be made compatible.

Today the simulation integration process addressing these touch points is largely done manually during the set-up for integration events. This manual process is expensive and time consuming. Furthermore, the integration can result in unintended "lock-in" of otherwise variable features, such as weather and terrain, that restrict the value of the model or simulation in many applications. Whether programs modify or develop models and simulations, they should always update the accompanying documentation to allow others to understand what is "under the hood" regarding the integrated environment touch points.

An option for development or modification is federating existing models and simulations, using interoperability standards among suitable models or simulations to create the needed capability. Generally, a federation is a system of interacting models, simulations, and supporting infrastructure based on a common understanding of the objects portrayed in the system. Analysts and developers use simulation federations to achieve some specific objective. Users should consider how to leverage models and simulations and to what degree they are interoperable throughout their life cycles.

Roles, Responsibilities, and Activities

To make effective and appropriate use of models and simulations, the model and simulation support to any effort should be planned and should be:

- Scoped to the purpose/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;
- Integrated into the effort's technical planning (e.g., WBS, schedules, budgets, etc.);
- Appropriately resourced, including a properly skilled workforce;
- Within agreement or contractual requirements;
- Considered to be part of the authoritative source of truth underpinning the effort;

- Supported by regular reviews and management of artifacts and stakeholders' changing needs; and
- 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;
- Developed and documented, including metadata and widely supported and consensus-based standards (if available and suitable), to maximize opportunity for reuse and repurposing;
- Properly managed and controlled as part of the authoritative source of truth; and
- 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.

2.2.2 Digital Engineering

Outside of DoD, digital transformation has been implemented across a range of industries to drive affordability, agility, quality, and efficiency. Advancements in digital technologies are unleashing innovations that provide an opportunity to transform the engineering practice. Digital Engineering (DE) is the DoD's initiative to transform the way it conceives, designs, develops, delivers, operates, and sustains complex systems in a formidable and changing threat environment.

Across the full life cycle of both emerging and legacy systems, DE tools and techniques afford new and improved ways of developing, acquiring, and sustaining capabilities across a program's full life cycle. The overall goal is to harness the power of digital computing to move DoD programs away from traditional, monolithic, paper-driven processes and into a world of increasing numbers of virtual artifacts, greater automation of processes and fewer manual transactions. Successful adoption of DE practices also brings with it technical, cultural, and programmatic changes as well. The overall goal is to embrace advances in all aspects of digital computing across the project life cycle to bring improved capabilities to the warfighter in a timelier and more iterative manner.

DoD'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 *DoD Digital Engineering Strategy,* https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf)).

DoD Definition of Digital Engineering

The DoD Digital Engineering Strategy 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." The strategy describes the relationship to SE as "digital engineering updates traditional SE practices to take advantage of computational technology, modeling, analytics, and data sciences. As evidenced across the Services and industry, digital engineering is a necessary practice to support acquisition in an environment of increasing global challenges and dynamic threat environments."

Basic Goals of Digital Engineering

The DoD DE Strategy comprises five distinct goals, as depicted in Figure 2-1.

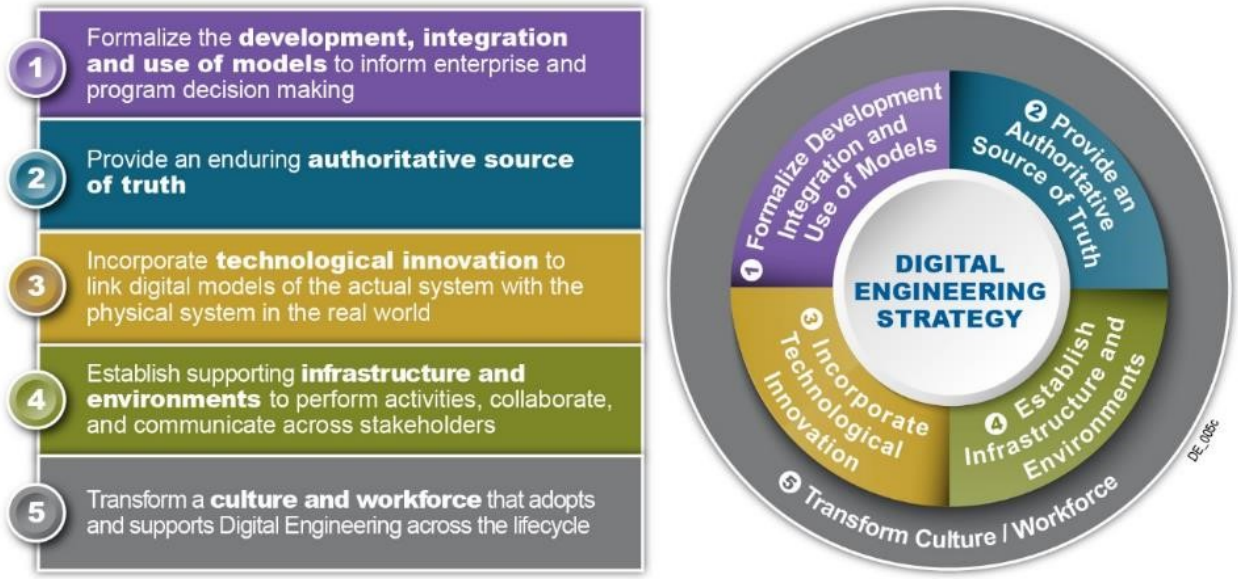


Figure 2-1. Five Goals of DoD's Digital Engineering Strategy

Goal #1: *Formalize the development, integration, and use of models to inform enterprise and program decision making.*

The first goal is at the heart of existing model-based approaches. The National Defense Industrial Association defined *model-based engineering* as an approach to engineering in which models: (1) are used as an integral part of the technical baseline; (2) evolve throughout the project life cycle; (3) are integrated across project disciplines; and (4) can be shared or reused across projects, which encompasses Government and industry stakeholders.

These elements are part of the basis for digital engineering because models are powerful tools that can provide a rich representation of a system, phenomenon, entity, or process. In early phases of the life cycle, models enable the exploration of the system in a virtual environment before it is actually built. Progressing to later phases, high-fidelity physics and engineering models can become indistinguishable from their physical counterparts. These models provide a mechanism to analyze, characterize, simulate, and visualize a range of systems, processes, and phenomena across disciplines. If kept current with the project under development, they also provide the most current record of the project design.

DE extends beyond traditional model-based approaches that typically focus on a particular activity or aspect (e.g., model-based design, digital model-based manufacturing, model-based testing, model-based manufacturing, model-based X) of the life cycle. From model-based systems engineering (MBSE), the focus is on formal systems modeling across the life cycle, regardless of the activity being performed. The vision for DE is to encompass the broad spectrum of models as a continuum across the life cycle of activities.

Goal #2: *Provide an enduring authoritative source of truth.*

The second goal ensures there is an authoritative source of truth for stakeholders across organizations and locations to access, manage, analyze, use, and distribute models. This goal builds on Goal #1 in which the authoritative source is assembled from a collection of digital models. It shifts the primary means of communication from static, disconnected documents toward digital models and data.

Goal #3: *Incorporate technological innovation to improve the engineering practice.*

Goal #3 extends beyond traditional model-based approaches to incorporate technological innovations that enable a digitally connected end-to-end enterprise. Models are central to advancements in digital technologies that will provide revolutionary capabilities. As the pace of technology continues to evolve, this goal intends to take advantage and incorporate technological innovations as they become available to improve the engineering practice.

Goal #4: *Establish a supporting infrastructure and environments to perform activities, collaborate, and communicate across stakeholders.*

The DoD's expectation for the fourth goal is to evolve and interoperate between DE computing infrastructures and environments to support all of the preceding goals. Currently, a wide range of organization and program-specific infrastructures and environments exist to execute DoD missions. They are complex and costly to manage, control, secure, and support because their use varies on an activity-by-activity basis. As such, the DoD plans to advance its infrastructures and environments toward a more consolidated, collaborative trusted environment that delivers capabilities that keep pace with technology, enhance cybersecurity and intellectual property protections, and improve information sharing across stakeholders.

Goal #5: *Transform a culture and workforce that adopt and support digital engineering across the life cycle.*

To succeed at DE, organizations need to implement deliberate efforts in culture and workforce that support digital approaches. DE changes the methods for prototyping, experimenting, and testing solutions virtually before they are delivered to the customer (e.g., warfighter). Using an authoritative source of truth, moving from documents to models, and creating digital methods, processes, and tools all require a change in the way the engineering community operates. DE includes impacts to related business functions such as contracts, legal requirements, and finance. In addition, the shift to DE is intended to enable Government and industry to share digital models more readily.

Benefits of Digital Engineering

The vision driving the adoption of DE is to "modernize how the Department designs, develop, delivers, operates, and sustains systems." The expected benefits include

- "Informed decision making and greater insight through increased transparency
- Enhanced communication
- Increased understanding for greater flexibility and adaptability in design
- Increased confidence that the capability will perform as expected
- Increased efficiency in engineering and acquisition practices" (The *DoD Digital Engineering Strategy* (https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf))

Project/Program Office Digital Engineering Roles, Responsibilities, and Activities

The extent to which any project/program office will need to embrace DE will be driven by multiple factors that include but are not limited to the following:

- Where the development is in its life cycle
- What digital engineering investments the program made during prior stages of the life cycle
- If an acquisition program, which of the adaptive acquisition framework pathways of the new DoD Instruction 5000.02 policy
- The respective organization's experience and lessons learned in implementing DE within similar or adjacent projects or programs (e.g., organizationally adjacent; functionally adjacent)
- What are the remaining activities to be performed (e.g., design, testing, sustainment, retirement, reuse, etc.)

Other Considerations for Implementing Digital Engineering

Models and simulations are DE enablers that help capture data and inform decisions throughout a project's life cycle. The goals of the DoD DE Strategy are to "promote the use of digital representations and components and the use of digital artifacts as a technical means of communication across a diverse set of stakeholders." Activities embracing DE depend upon a well-defined plan for what models and simulations are needed at various way points along the life cycle. The opposite is not true, however. A project does not need to fully embrace a DE approach to be able to make good use of models and simulations throughout its life cycle.

A project that adopts a DE approach is embarking on a journey into a new and evolving way of doing business. The various tools and techniques needed for success typically require the use of leading-edge engineering practices where certain benefits are expected but not given. DE adoption is rapidly growing, is endorsed at senior levels of the Department and is widely supported at the program level to provide insights and guidance.

Each organization has developed its own approach and structure for promulgating and managing the increased use of DE within key projects. In addition, the Services/Agencies together with the Office of the Secretary of Defense (OSD) formed a DoD Digital Engineering Working Group (DEWG) chartered with addressing the critical challenges (referred to as "pain points") to implement DE more broadly, as well as develop solutions to address these pain points. In 2020, the DEWG was restructured to a more collaborative and action-oriented community focused on DE implementation. The initial cross-Department activities were divided into six tiger teams, each with a Service lead. The tasks of the tiger teams are to develop products that are needed to implement DE across the DoD enterprise

The initial efforts focused on the following challenges:

- Enterprise data management to ensure authoritative data and models are widely available or accessible
- Technical solutions to provide collaborative, agile, secure, interoperable, and responsive digital ecosystems
- Cybersecurity protection to data, networks and hosting environments while managing access controls, data at rest, spillage control and exfiltration mitigation
- Useful and shared examples of incremental DE/MBSE implementation and execution
- Uniform and common understanding of what a Digital Engineering Body of Knowledge (DEBoK) should be and what it should contain. There needs to be a structured, shared knowledge base that is accessible to the DoD-wide engineering community
- The National Defense Authorization Act (NDAA) for FY20, Section 231 (Public Law 116-92) directs the Secretary of Defense to establish a DE capability to support automated approaches for testing, evaluation, and deployment throughout the defense acquisition process

2.2.3 Mission Engineering

Overview

The FY17 NDAA, Section 855 directed the Secretary of Defense to develop Mission Integration Management (MIM) to use mission-based information to inform concept, technology, requirements, and systems development. Acting on this direction, the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) established Mission Engineering (ME) 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 provides a quantifiable basis to inform technical and budgetary planning decisions on potential solutions to fulfill mission capability gaps, and to synergize mission concepts, system requirements, technologies, and budgets.

ME is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects. ME is a process through which DoD 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 studies and analyses evaluate capability solutions, enhanced capabilities, technologies, system inter-dependencies, and architectures to close mission gaps. They also inform the acquisition and operational communities with reference architectures to better guide technology development, prototypes, experiments, and SoS portfolio management to achieve reference missions and meet warfighter needs.

The ME analytical process is 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.

The ME process is codified in the OUSD(R&E) Mission Engineering Guide available on the DDR&E(AC)/Engineering website. This guide establishes best practices for the Department in conducting mission-focused, threat-informed analyses. These practices enable practitioners to prioritize and pursue materiel and non-materiel solutions to critical warfighting challenges.

The ME Guide defines consistent terminology, analytic steps, documentation, and expected outputs to enable reuse and sharing of results. The ME Guide is intended to promote critical thinking, share best practices, and provide a sound foundation for mission-thread analysis, architecture development and evaluation, SoS engineering, and modeling and simulation.

The ME Guide establishes the following steps for Mission Engineering: (1) Problem Statement, encapsulating key questions, suspected capability gaps, current and planned technologies, and operational concepts; (2) Mission Characterization, describing well-defined scenarios, vignettes, rules of engagement and concepts of operation, assumptions, and threats; (3) Mission Metrics, including quantifiable measures of effectiveness, linked to decomposed mission capability requirements; (4) Design of Analysis, defining mission threads (effects chains/kill chains) for each trial/modeling run, defined trial approaches to be evaluated, models, data, and analytical products, including as-is and to-be architectures; (5) Analysis/Modeling, capturing mission effectiveness, sensitivity analysis, Monte Carlo, parameterization, cost trades, and confidence level; and (6) Documented Conclusions (reports to senior leadership and decision makers to influence investment strategies and milestones).

Objectives

The goal of ME is to strengthen the extended linkage between development activities and mission capability, helping to highlight how trades in the intersecting roadmaps of emerging concepts, contributing technologies, system requirements, system development, and SoS operations and their budgets will result in mission success in future scenarios and conflicts. The idea is to better synchronize across Joint Staff activities, R&E efforts, acquisition and sustainment, and budgetary planning. ME informs technology modernization, prototyping, and experimentation. ME informs future Joint Warfare Capabilities and informs the Joint Requirements Oversight Council (JROC) and the Services to help shape realistic requirements. ME informs high-priority technology prototyping in support of the Service's Rapid Capability Offices or the Defense Advanced Research Projects Agency (DARPA), and resources the modernization initiatives that help mature those technological solutions. ME informs Joint Staff and the Combatant Commands (CCMDs) as to Joint Capability Technology Demonstration (JCTD) programs and rapid fielding efforts.

ME also supports programs of record by looking at (1) cross-cutting/joint missions; (2) modular, upgradable constructs and standards; and (3) ensuring consistency in cross-cutting capabilities, such as cybersecurity and software. ME products provide mission integration analysis to inform acquisition pathway decisions; support Independent Technical Risk Assessments (described in other sections of this guidebook); advise on needs of test and evaluation (T&E); inform roadmaps for transitioning technology through the rapid acquisition process; and advise on the pursuit of appropriate acquisition pathways.

These products inform decisions early in the acquisition process, before a Materiel Development Decision (MDD), for example by assessing Mission Return on Investment (ROI), or the ratio of one metric/measure to another metric/measure. Mission ROI evaluates the efficiency to achieve success to one or more different measures of effectiveness (e.g., the number of targets destroyed versus the number of assets expended). ROI ratios are especially useful to help resolve cost-benefit efficacy based on type and number of weapons used and the (amortized) cost of each. ME analyses inform the Planning, Programming, and Budgeting Execution (PPBE) process by helping (in concert with Cost Assessment and Program Evaluation (CAPE) and the Services) to establish cost-type ROIs to inform acquisition or technology investment strategies and the selection of cost-appropriate acquisition pathways, either as materiel or non-materiel solutions.

2.2.4 Software Engineering

Software is critical to national security, an integral part of every DoD 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 Software Engineering (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 DoD 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. By adopting commercial best practices, such as an Agile/Development, Security, and Operations (DevSecOps) software development, with modern tool stacks, skilled personnel, the Department can work to deliver new software capabilities to the warfighter in days or weeks rather than months or years. Such findings have resulted in valuable changes in public law, acquisition policy, and workforce development. The most recent and significant acquisition policy change in DoD was the establishment of the AAF and DoDI 5000.87, “Operation of the Software

Acquisition Pathway." The AAF and policy was established 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 DoD 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, continuous integration, and CI/CD have proven successful in a competitive industrial marketplace and should be adopted in DoD. 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 PEO and Service leads, modernize workforce competencies, and establish a culture that unifies previous "silo" activities such as development, safety, security, test, and sustainment into a CI/CD process.

The mission engineering problem, questions, and threats mentioned in the prior section drive the need for more robust software solutions and the use of revolutionary technologies like DevSecOps, which enable innovation through AI, machine learning, high-performance cloud native computing, big data analysis, advanced algorithms with predictive analytics, digital twinning, complex data modeling, network architectures, distributed systems, and sensor networks.

DevSecOps is an organizational SWE culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). DevSecOps is the Department's preferred approach for software development, and adopting DevSecOps is the primary focus area for delivering secure resilient code. Figure 2-2 shows the DevSecOps continuous software development process with security embedded (not bolted on) throughout the continuous process. Advancing cybersecurity and resilience in DoD DevSecOps pipelines should be part of all DoD SWE team processes, which will also enable the ability to execute a continuous Authority to Operate process.

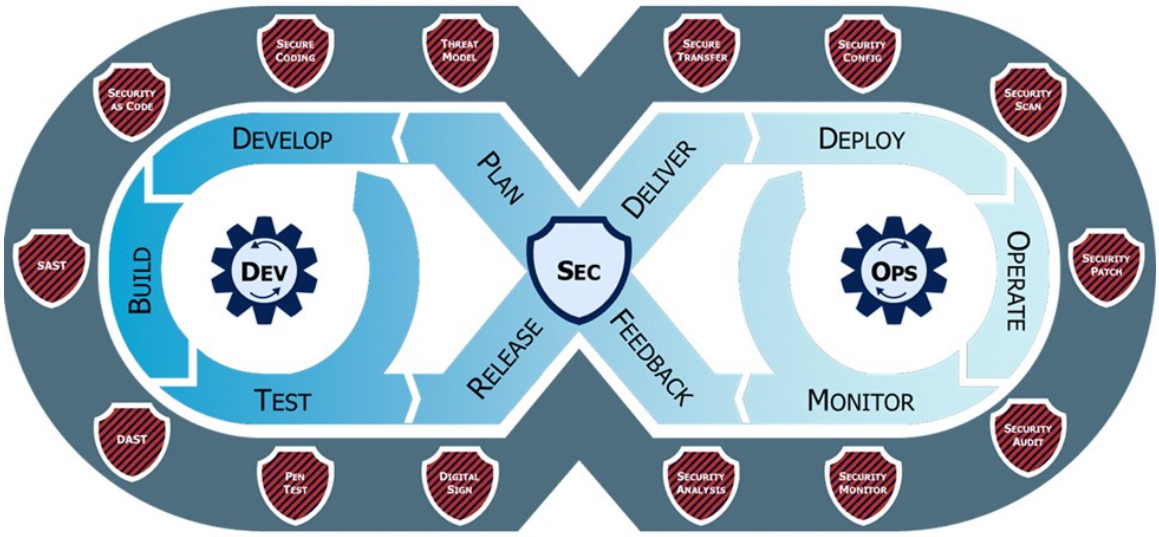


Figure 2-2. DoD DevSecOps Process for Continuous Integration and Continuous Deployment

The Department should use DevSecOps to increase systems engineering rigor in areas including infrastructure-as-code, automated continuous integration, and delivery pipelines, to improve a PMO's software activities. Software development activities should employ automation across all aspects of the software factory and project management components to eliminate tedious, manual steps to the maximum degree practicable, enabling higher velocity, consistency, and overall better quality software components. An automated, continuous integration pipeline should include static code analysis tools to flag programming errors, bugs, stylistic errors, limiting hardware properties, and suspicious constructs to enable continuous feedback and continuous learning. The PMO should enhance digital engineering, establish and curate a digital twin, use model-based software, and use systems engineering with automated tool sets to test, validate, and simulate alternative designs and design changes.

A detailed overview of DevSecOps can be found on the DoD Chief Information Officer DevSecOps Reference Design website along with other guides (https://dodcio.defense.gov/Library/).

2.2.5 Modular Open Systems Approach

Modular Open Systems Approach (MOSA) is an acquisition and design strategy consisting of a technical architecture that uses system interfaces compliant with widely supported and consensus-based standards (if available and suitable) and supports a modular, loosely coupled and highly cohesive system structure that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation. This modular open architecture includes publishing of key interfaces within the system and relevant

design disclosure. MOSA involves adopting an open business model with transparent business practices, allowing for collaborative innovation among participants across the enterprise, shared risk, maximized reuse of assets, and reduced total ownership cost (TOC). The combination of open systems architecture and an open business model permits the acquisition of systems that are modular and interoperable, allowing for system elements to be added, modified, replaced, removed, or supported by different vendors throughout the life cycle in order to afford opportunities for enhanced competition and innovation. MOSA is not an end result sought by the warfighter or end-item user; it is an approach to system design that can enable additional characteristics in the end item.

DoD identifies the primary benefits of MOSA as:

- Increased interoperability, including SoS interoperability and mission integration
- Enhanced competition
- Facilitation of technology refresh and evolutionary upgrades
- Increased innovation
- Potential cost savings or cost avoidance
- Reduced time to field capability to the warfighter

MOSA benefits PMs by using a general set of principles to help manage system complexity by breaking up complex systems into discrete pieces, which can then communicate with one another through well-defined interfaces. In this way, MOSA is broadly defined and inclusive of a variety of tools and practices.

Acquisition programs adopting MOSA may benefit from:

- Reduced life cycle costs without sacrificing capability
- Reduced reliance on single-source vendors (“vendor lock”)
- Shortened program acquisition timeline
- Enhanced rapid and agile development
- Accelerated transition from science and technology into acquisition owing to modular insertion
- Increased ability and flexibility to retrofit/upgrade system elements for new/evolving capability
- Enhanced incremental approach to capabilities
- Increased competition and innovation
- Enhanced ability to create security structures within a design to reduce security risk

MOSA may also benefit warfighters by:

- Reducing operator learning curves by using systems that have similar functions and are operated in similar ways, thereby reducing costs
- Increasing interchangeability
- Reducing support and sustainment costs

Although a PM may employ MOSA to achieve some or all of these benefits, the methods the PM's staff uses, and the associated business implications, can vary widely and may drive different techniques and additional responsibilities into programs. The implementation strategy should consider impacts to the program and to the system's performance (e.g., its effectiveness and feasibility). These factors underpin the Department's policy for MOSA in acquisition.

DoDI 5000.88, Section 3.7.a. direct PMs to evaluate and implement MOSA where feasible and cost-effective. MDAPs that receive Milestone A or B approval after January 1, 2019 are required to be designed and developed with a modular open systems approach to the maximum extent practicable, pursuant to 10 U.S.C. 2446a and DoDI 5000.02, Enc 3, sec. 14. The overarching business case for DoD is increasing the level of competition by enabling small and large businesses to participate in competition for new or upgraded capabilities. Programs should develop a business model, documenting the strategy for use of MOSA and associated data rights.

The DoD Open Systems Architecture Contract Guidebook for Program Managers contains guidance regarding contract language programs should use to acquire data rights in support of a program's MOSA strategy. Additional information and supporting details amplifying each aspect of MOSA are available on the DDRE(AC)/Engineering website.

The PM should:

- Establish supportive requirements; business practices; and technology development, acquisition, T&E, and product support strategies for effective development of open systems.
- Ensure data deliverables support the Intellectual Property Strategy (see Acquisition Strategy template) and secure the necessary data rights to support and sustain the system.
- Map modular open systems strategy and functional architecture to Statement of Work (SOW) requirements, Data Item Descriptions (DIDs) and Contract Data Requirements List (CDRL) items consistently across the enterprise.
- Ensure compliance.
- Consider including MOSA as one of the evaluation criteria for contract proposals.

- Determine the appropriateness of MOSA by considering software constraints, security requirements, and procedures, availability and cost of data rights, life cycle affordability and reliability of widely supported and consensus-based standards, as well as other relevant factors such as environmental constraints (e.g., temperature, humidity) and Environment, Safety, and Occupational Health (ESOH) considerations.

The Systems Engineer should:

- Employ an overall plan for MOSA that supports the system functional architecture and uses prescribed USD(R&E) business case analyses.
- Ensure the system functional architecture is structured to accommodate Open Systems Architecture (OSA) where feasible because of the high potential for reduced risk and cost.
- Assess performance.
- Balance current implementation of MOSA with performance and evolving technology at the physical level; MOSA establishes a technical baseline that may support modular architecture, but formally constrains the interfaces between modules where interfaces close to current performance limits may quickly become obsolete.
- Evaluate the technical appropriateness of MOSA by considering software constraints, security requirements and procedures, availability and cost of data rights, life cycle affordability and reliability of widely supported and consensus-based standards, as well as other relevant factors, such as environmental constraints (e.g., temperature, humidity) and ESOH considerations.

Open systems benefits may not be realized without deliberate planning and guidance at the PEO level. Reuse may be challenging if open systems and software on other systems (even other open systems) are not developed and modularized in a common fashion. As an example, an aviation platform may develop an Automatic Dependent Surveillance-Broadcast (ADS-B) software application that is MOSA conformant, but that application may never be reused by a sister platform that may have its ADS-B and tactical air navigation software combined in a single module.

For MDAPs that use a MOSA, the program may not receive Milestone B approval under 10 USC 2366b until the MDA determines in writing that:

- The program incorporates clearly defined major system interfaces between the major system platform and major system components, between major system components, and between major system platforms;
- Such major system interfaces are consistent with the widely supported and consensus-based standards that exist at the time of the milestone decision, unless such standards are unavailable or unsuitable for particular major system interfaces; and

- The Government has arranged to obtain appropriate and necessary intellectual property rights with respect to such major system interfaces upon completion of the development of the major system platform.

In the case of an MDAP that does not use a MOSA, the MDA is required to determine in the writing that the use of a MOSA is not practicable.

Modular open system designs, developed from the system architecture, should be analyzed at each design review because there is a link between MOSA and the level and type of technical data, computer software, and data rights the Government needs for life cycle support. In many cases weapon systems using MOSA system elements can have increased opportunities for competitive sourcing during the life cycle sustainment, and a correspondingly lesser need for detailed design data and associated data rights. This benefit enables an incremental approach to capability adaptation in MOSA-enabled systems and is a benefit of the modularity originally specified in the functional architecture.

The Analysis of Alternatives (AoA) for an MDAP should include considerations of each alternative's use of a MOSA. As the solution matures and evolves before Milestone A, the PM and Systems Engineer should continue to assess the MOSA strategy. The engineering trade analyses conducted in advance of Milestone B help determine which system elements can be adapted to MOSA in order to reduce program cost and development time lines. Correct application of MOSA principles and practices results in modular system elements having well-defined functions and system interfaces compliant with widely supported and consensus-based standards. Threat analyses, functional criticality analyses, technology opportunities, and evolved capability assessments are examples of assessments against the functional architecture to determine which system elements should be MOSA-enabled.

When these system elements require an upgrade, replacement should be competitive, faster, and cheaper because the MOSA-enabled system elements are modular. Because system functional architecture maps from the higher-level enterprise architecture, engineering trade analyses and assessments supporting MOSA should be completed and MOSA-enabled system elements specified, before contracts are let for technology development of those system elements. The MDA for an MDAP that uses a MOSA shall ensure that a request for proposal for the Engineering and Manufacturing Development (EMD) or Production and Deployment (P&D) phase of the program shall describe the MOSA and the minimum set of major system components that must be included in the design of the MDAP, in accordance with 10 USC 2446b. Successful implementation of MOSA approaches requires the synchronized acquisition of data rights for modular open systems and interfacing architecture elements. These data rights are initially structured to support acquisition of modular open system designs but also should address life cycle support.

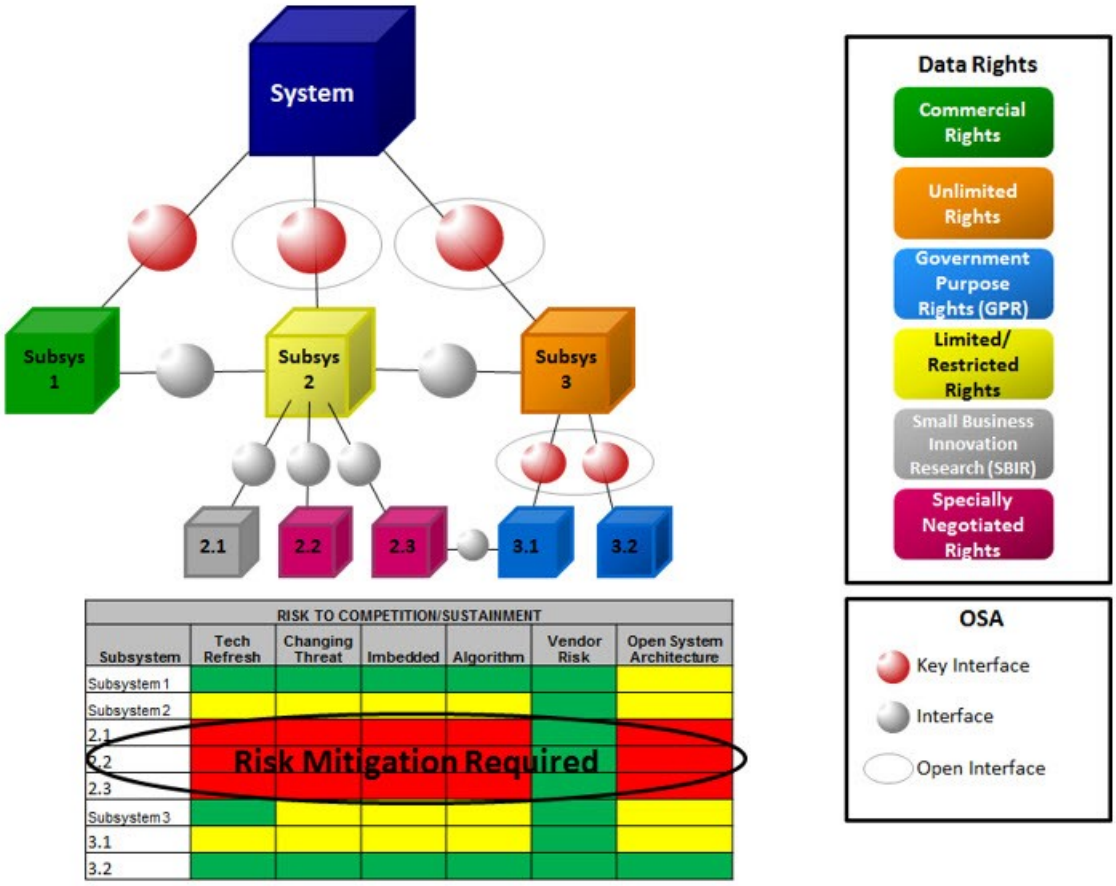


Figure 2-3. Sample MOSA and Data Rights Analysis

Figure 2-3 depicts an example architectural approach for mapping and assessing which system element interfaces can be open, how associated risk is ascertained, and how to visualize the impact to interfaces with other system elements. The figure presents a top-level system view of the MOSA characteristics of system elements. Not all interfaces need to be open at any one level of the design, only those that are required to meet anticipated incremental capability updates, changes in threat or technology insertion. A system view such as this includes a record of the data rights that are required to enable the planned MOSA design. Programs determine the level of data rights required for each MOSA-enabled system in order to assert the requisite contract requirements to obtain them. The data rights strategy should ensure that enterprise-level data rights flow to system elements and that they support the system architecture. Levels of data rights are described in Appendix 9 of the Open Systems Architecture Contract Guidebook.

Successfully implementing a MOSA strategy results in the identification of required technical data and software deliverables necessary to field and maintain weapon systems and their logistics support. The Acquisition Strategy should be updated throughout the system's life cycle to reflect changes in the MOSA approach resulting from technology and software evolutionary developments. In accordance with DoDI 5000.85, sec. 3C.3.a.(5) for a MDAP that uses a MOSA, the program's Acquisition Strategy should:

- Clearly describe the MOSA to be used for the program.
- Differentiate between the major system platform and major system components being developed under the program, as well as major system components developed outside the program that will be integrated into the MDAP.
- Clearly describe the evolution of major system components that are anticipated to be added, removed, or replaced in subsequent increments.
- Identify additional major system components that may be added later in the life cycle of the major system platform.
- Clearly describe how intellectual property and related issues, such as technical data deliverables, that are necessary to support a modular open system approach, will be addressed.
- Clearly describe the approach to systems integration and systems-level configuration management to ensure the system can operate in the applicable cyber threat environment.

The SEP team should update the SEP to reflect the MOSA-related updates and modifications employed throughout the system and its system elements.

The SE team should consider including the following MOSA-related data deliverables in the SEP, as applicable:

- Open Systems Management Plan (DI-MGMT-82099)
- Software Development Plans (SDPs) (DI-IPSC-81427)
- Software Development Status Reports (DI-MCCR-80459)
- Software Development Summary Reports (DI-MCCR-80902)
- Software Design Descriptions (DI-IPSC-81435)
- Hardware Development Plans and Hardware Design Descriptions

The PM should maintain an Open Systems Management Plan. The plan describes the offeror's approach for:

- OSA, modularity, and open design
- Inter-system element dependencies
- Design information documentation
- Technology insertion
- Life cycle sustainability
- Interface design and management

- Treatment of proprietary or vendor-unique elements
- Reuse of preexisting items, including all commercial-off-the-shelf/non-developmental item (COTS/NDI) system elements, their functionality, and proposed function in the system
- Copies of license agreements related to the use of COTS/NDI system elements for Government approval

The Open Systems Management Plan should also include a statement explaining why each COTS/NDI system element was selected for use.

Program products typically used in making decisions regarding MOSA include:

- System Requirements
- AS
- PPP
- AoA
- Enterprise Architecture

Modular open systems approaches and requirements should be addressed at design reviews, e.g., System Requirements Review (SRR), Preliminary Design Review (PDR) and Critical Design Review (CDR).

See DoDM 5010.12-M for data deliverables, and DoDM 4120.24 for DoD procedures pertaining to development and distribution of defense specifications and standards, e.g., MOSA-enabling standards, DIDs. PMs, Systems Engineers, and Lead Software Engineers should use ASSIST, formerly known as Acquisition Streamlining and Standardization Information System, to gain access to data item deliverables (e.g., DIDs), MOSA-enabling standards, and other defense standardization documents (e.g., MIL-STD-188, MIL-STD-1472, STANAG-5616) that may be appropriate for each program.

2.2.6 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, have fewer impacts on human health and the environment, and thus have a lower

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 make systems more affordable and improve the accuracy of life cycle cost estimates.

"Sustainability" differs from "sustainment" in that it relates to the use of resources, and the associated impacts and costs over the system's life cycle. In contrast, sustainment is more concerned with the end user's ability to operate and maintain a system once it is in inventory and deployed. Both aspects need to be addressed in the design process.

Executive Order (E.O.) 13693, "Planning for Federal Sustainability in the Next Decade," dated March 25, 2015, establishes an integrated Federal Government strategy for sustainability. As required by the E.O., DoD generated a Strategic Sustainability Performance Plan (SSPP), which is updated annually. The SSPP identifies DoD goals for efficiency and reductions in energy, water, solid waste, and use of hazardous chemicals and materials.

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 DoD) and external (to society) by monetizing the impacts.

A sustainability analysis can support numerous acquisition activities, including:

- AoA to compare conceptual alternatives.
- 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 HSI contribution to sustainability analyses should include LCSP updates, informing operational supportability analysis, and should include collecting and analyzing field feedback and corrective actions.

The Streamlined Life Cycle Assessment Process for Sustainability in DoD Acquisitions 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.

2.2.7 Value Engineering

PMs use Value Engineering (VE) across the life cycle for supplies and services, including those for major systems, and construction. 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 performance, reliability, quality, and safety. VE is performed to eliminate or modify any element that significantly contributes to the overall cost without adding commensurate value to the overall function.

VE is one of many tools used for increasing value to the warfighter; it focuses on functions (purpose or use of a "program, project, system," etc.) to achieve best value. The Components implement VE to improve military worth or reduce acquisition and ownership costs wherever it is advantageous. VE policy is provided through DoDI 4245.14, "Value Engineering (VE) Program," which implements 41 U.S.C. 1711 and Office of Management and Budget (OMB) Circular No. A-131, "Value Engineering".

SD-24, "Value Engineering: A Guidebook of Best Practices and Tools" provides details on VE activities, Value Engineering Proposals (VEPs) and Value Engineering Change Proposals (VECPs), and the application of VE.

PMs perform VE by:

- Scoping the issue, improvement targets, and evaluation factors
- Identifying specific areas/functions for evaluation
- Collecting and analyzing data
- Exploring alternative approaches
- Developing and presenting specific recommendations
- Implementing directed changes

VE consists of two parts: VEP and VECPs. VEPs are developed and submitted by individual employees or contractors under contract to provide VE services or studies. VECPs are submitted under the VE clause of a contract.

FAR (Subpart 48.102, para (a)) requires the contracting activity including VE provisions in appropriate supply, service, architect-engineer, and construction contracts and the DoD to provide contractors a fair share of the savings on accepted VECPs.

PMs, Systems Engineers, and Lead Software Engineers should encourage the development and submittal of VEPs and VECPs and consider applying VE 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

Additional resources available to the PM, Systems Engineer, and Lead Software Engineer to learn more about VE include the Defense Acquisition University Continuous Learning Module, CLE001, "Value Engineering". For examples of potential areas in which VEPs and VECPs may provide a benefit, see SD-24 Chapter 2, "Opportunities of VE Application," and Chapter 3, "VE over a System's Life Cycle."

2.2.8 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 Lead 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 Lead Software Engineers judiciously select and tailor successful practices or strategies from analogous programs/systems and tailor them to meet current program needs.

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 Lead Software Engineers should be aware that standards are not ad hoc requirements developed by a single engineer or program office.

The ASSIST database is the official source for defense specifications and standards and DoD-adopted Non-Government Standards (NGS). In many cases, DoD uses NGS, as required in 15 USC 272 Notes "Utilization of Consensus Technical Standards by Federal Agencies" and implemented in 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 Global Information Grid (GIG) Technical Guidance Federation (previously known as 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 DoD, 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 Lead 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)
- Government Accountability Office (GAO) reports
- DoD Systems Engineering Community of Practice websites
- Defense Standardization Program Office
- Other departments and agencies such as National Aeronautics and Space Administration, Department of Energy or National Institute of Standards and Technology (NIST)
- Professional organizations such as the International Council on Systems Engineering or the Institute of Electrical and Electronics Engineers
- Industry organizations such as National Defense Industrial Association 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 Lead 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 Lead 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 Lead Software Engineers should consider using this data as a form of process improvement feedback, or as evidence for proposing policy and guidance changes.

2.3 Engineering Resources

Organizing and staffing the SE organization and providing supporting resources and tools are critical tasks that merit attention from both the PM, Systems Engineer, and Lead 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 Lead Software Engineer are an integrated part of the program planning and execution activities. In accordance with DoDI 5000.66, this planning includes ensuring that program offices for MDAP programs will have a qualified Chief Engineer/Lead Systems Engineer with key leadership position criteria defined in DoDI 5000.66.

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 SEP describes the SE organizations of both the Government program office and, when available, the developer organization.

2.3.1 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:

- Ensuring proper level of governance is applied.
- Ensuring processes are followed and reporting is in compliance with plans.
- Interfacing with the end users and developers to determine changes in operational requirements or concepts of operations that may affect the development of the desired capability.

- Ensuring coordinated development and updating of acquisition strategy documents (e.g., AS), program plans (e.g., SEP, PPP (including the Cybersecurity Strategy (CSS)), TEMP, LCSP), and cost and budget documents.
- 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 professional.
- Integrating all aspects of the program office, including business processes relating to program management, SE, test and program control.
- Integrating cyber test personnel early to assist with engineering, cyber requirements scoping in the design, and scoping affordable, relevant cyber T&E.
- Ensuring all necessary MOU/MOAs 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 configuration management plan and ensuring adequate resources are allocated for implementing configuration management throughout the life cycle.
- Reviewing/approving ECP requests and determining the path forward required by any baseline changes.
- Ensuring contracting activities are coordinated with the program systems engineering team.
- Approving the contractor SEMP; ensuring consistency between the program SEP 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 digital engineering SE 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.
- 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 SEP 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 configuration management.
- Supporting the PM in configuration management activities.
- Identifying and mitigating the program's technical risks, which include
    - Integration risks
    - Engineering risks
    - Critical technology risks assessed in the Technology Readiness Assessment (TRA) (MDAPs only)
    - Manufacturing Readiness Assessments (MRAs)
    - Program protection risks throughout the life cycle
- 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 and appropriate engineers.
- Supporting updates to the TEMP and LCSP when appropriate.

- Developing models and simulations to support design analysis, validation and verification activities, mission engineering 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 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 Lead Software Engineer focus on the transformation of required operational and sustainment needs into a system design capability. 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 programs under USD(R&E) oversight, Systems Engineers will be included on the T&E WIPT. 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 SEP. The PM and the Systems Engineer work closely with the Chief Developmental Tester to facilitate coordinated verification and validation activities.

2.3.2 Stakeholders

The PM has the critical role of approving an SE approach 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. 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
- Security Manager, Cybersecurity Engineer, or System Security Engineer Chief Developmental Tester
- Operational test organization
- Certification and accreditation authorities
- Maintainers and logisticians (materiel readiness and sustainment)
- Intelligence Community
- Trainers
- Budget and cost analysts
- Contracting officers and associated staff
- Environment, safety, and occupational health (ESOH) staff
- Contractors who manufacture, test, deploy, or support the capability under development
- Companion programs

2.3.3 Integrated Product Teams

An effective SE organization is typically structured as one or more IPTs. 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(ies) to the end user. In developing the program office and SE organizational structure, the PM, Systems Engineer, and Lead 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 vs. 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 configuration management is executed, etc. In some cases, the PM, Systems Engineer, and Lead Software Engineer may organize multiple IPTs to align with the major products in the program's WBS. 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. A best practice is to establish a Cyber IPT or working group early in the SE life cycle to ensure cyber engineering is integral to all SE processes. For example, performing early and iterative updates for mission-based cyber risk assessments with operational users, developers, engineers, and cyberspace threat emulation (testers) consistently enhances the design and trade-off efforts during the SE process.

For MDAPs, the PM ensures that the program office interfaces with the SE WIPT (a multidisciplinary team responsible for the planning and execution of SE) to address DoD leadership concerns and interests. The SE WIPT is chartered by the PM and is usually chaired by the Systems Engineer. For MDAPs, the SE WIPT should include representation from OUSD(R&E) and the Component Acquisition Executive's organization, both Government and developer IPT leads from the program, the PEO Systems Engineer, and the developer Systems Engineer. Additional information about IPTs can be found in the PM Guidebooks (forthcoming) and HSI Guidebook (forthcoming).

2.3.4 Automated Tools

Automated tools, such as those for requirements management, risk management, schedule management, and architecture development, as well as tools needed to design a capability within a digital engineering ecosystem, can be used by the PM, Systems Engineer, and Lead 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

digital engineering ecosystem. Ideally, the tools should have some degree of interoperability among them (e.g., the requirements management tools linked to the scheduling tool events to verify the requirements). Optimally, the tools used by the PMO and all the stakeholders should be interoperable with the tools used by the vendor.

2.4 Certifications

Certifications provide a formal acknowledgment by an approval authority that a system or program meets specific requirements. Certifications, in many cases, are based on statute or regulations and drive SE planning (i.e., a program may not be able to test or deploy the capability without certain certifications). 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 Safety Confirmations and Safety Certifications need to be provided for Materiel Releases. Also, HSI domain considerations are assessed and documented including risk assessments and control measures impacting manpower, human effectiveness, workload, training, survivability, and safety of personnel. HSI assessments are used to support Safety Confirmations and Safety Certifications. 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 can be a lengthy process. As a result, the PM should ensure that the time necessary to obtain any required certification is factored into technical planning. The PM should include HSI considerations in T&E, certification, and system safety (SS) processes. By planning for the activities required to achieve the necessary certifications, the PM, Systems Engineer, and Lead Software Engineer can ensure that development of the system continues uninterrupted while the program meets all system certification requirements. Early planning allows the Systems Engineer and technical team to begin interacting with certification authorities, which sets the foundation for communication throughout the development of the system.

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.

A non-exhaustive list of certifications is available on the DDR&E(AC)/Engineering website. Furthermore, PMs, Systems Engineers, and Lead Software Engineers should consult both Joint and Service-specific domain experts to determine other certifications that may be required.

2.5 Systems Engineering Role in Contracting

The Systems Engineer should participate in developing program contract tasks to ensure that the appropriate technical activities are contained and properly scoped in the contract. Proper 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. Often contracting activities may appear to be primarily programmatic in nature (e.g., acquisition strategy development, writing requests for proposal, performing market research, developing the CDRL) but, in fact, they reflect technical planning and should be influenced by the desired 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. Also, designing for continuous testability of cybersecurity and operational resilience (i.e. digital representations, system integration labs) requires the contract to articulate the requirement.

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. In accordance with Section 2443 of Title 10, U.S.C., for ACAT I (MDAPs) and II (Major Systems) weapon systems designs, the PM shall include in the contract and in the process for source selection clearly defined and measurable R&M requirements and engineering activities. Incentive fees and penalties such as award fee may be tied to program performance (e.g., R&M) evaluated during technical reviews, or more frequently the incentive or penalty is tied to the completion of a technical review. Incentives can also serve to motivate the contractor to deliver a system that is resilient and survivable in contested cyberspace, as demonstrated through product acceptance cyber T&E by a National Security Agency certified Red Team. If that is the case, the developer may have a strong incentive to call the review complete as soon as possible. The Systems Engineer and PM 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.

Another area to which incentives are tied is the Earned Value Management System (EVMS). The PM should ensure that the EVMS, tied to any incentive, measures the quality and technical maturity of technical work products instead of just the quantity of work. If contracts include earned value (EV) incentives, the criteria should be stated clearly and should be based on technical performance. EV incentives should be linked quantitatively with:

- TPM
- Progress against requirements
- Development maturity
- Exit criteria of life cycle phases
- Significant work packages and work products

The PM should make it a priority to engage with industry to clarify Government expectations and ensure a common understanding of the capability desired, need dates, risks, complexity, and scope. Access to current market information is critical for the program office as it defines requirements for acquisition programs. As they develop acquisition strategies, contracting officers should seek opportunities for small businesses, and negotiate contract terms. The best source of this information is usually found within industry partners. The OMB memo, "Myth-busting 3: Further Improving Industry Communication with Effective Debriefings" addresses productive interactions between federal agencies and industry partners. These interactions are strongly encouraged to ensure the Government understands the marketplace and can award a contract or order for an effective solution at a reasonable price. Early, frequent engagement with industry is especially important for complex, high-risk procurements, including (but not limited to) those for large information technology (IT) projects. PMs should develop ways to remove unnecessary barriers to reasonable communication and develop vendor communication plans, consistent with existing law and regulation, which promote responsible exchanges.

The program office uses a Request for Information to communicate expectations and plans, including the expected business rhythm for contract execution. This communication ensures the offerors have an opportunity to provide a tight linkage across the IMP, WBS, IMS, risk and opportunity management, and cost in their proposals. Early industry engagement opportunities include pre-solicitation notices, industry days, and other market research venues.

Before releasing the RFP, the program office should develop and mature the performance and functional specifications that need to be included in the RFP. The RFP and supporting technical documentation define the Government's expectations in terms of the performance and functional specifications, program planning, program process, risks, and assumptions. The RFP also should direct potential offerors to structure their approach to reflect the Government's expectations.

In support of the PM, the Systems Engineer should ensure that technical documents accurately communicate the Government's requirements including mandatory design, build, test, certification, approval, and acceptance criteria. Well-articulated and defined CDRLS are intended to ensure the vendor successfully implements the appropriate design considerations. The developer is made aware of all required processes and objective quality evidence (OQE) to be produced, including processes leading to certification, approval, and acceptance using predetermined OQE. In addition, the PM should consider providing all offerors with the PPP, the IMP and top-level schedule (with internal and external dependencies), expected business rhythm, current risk assessments, and the SEP (either an approved or a draft SEP) as part of the RFP. Consistent with DoDI 5000.88, Section 3.4.a, the SEP may be applied as guidance or as a compliance document depending on the maturity of the plan and the acquisition strategy. Before providing the SEP to the offerors, the PM, Systems Engineer, and Lead Software Engineer should determine if the document contains sensitive information and, if so, remove this sensitive information from the SEP before attaching it to the RFP.

In an effort to promote a higher probability of mission success, MDAPs should review, tailor and implement applicable mission assurance concepts and principles when developing their contract requirements. MDAPs should use resources provided by their service.

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. See the "Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 1.0, 2006" for additional guidance on the content and format of RFPs.

Within the RFP development team, the Systems Engineer should be responsible for the technical aspects of the RFP and should perform the following actions:

- Referencing current required operational documentation and system performance specifications.
- Identifying SE process requirements (for example, requirements management, configuration management, manufacturing and quality management, and risk management; see Section 4 Systems Engineering Processes).
- Identifying the systems engineering approach(s) such as digital engineering, model based systems engineering, MOSA, etc.
- Identifying the models and simulations requirements throughout the system's life cycle, including verification requirements and delivery of end items.
- Providing available and appropriate architecture(s) characterizing the system's interoperability requirements.
- Identifying any design considerations including producibility, quality, reliability and maintainability (R&M), survivability, SS, HSI, and security. For ACAT Is and IIs, R&M requirements must be included in the Technology Maturation and Risk Reduction (TMRR), EMD and Production solicitations, per 10 USC 2443.
- Identifying Government-required technical data rights produced by the developer for delivery.
- Listing and describing technical assessment evidence and events, including technical reviews, audits, and certifications and associated entrance/exit criteria.
- Specifying data protection, SoS and system testing and verification requirements.
- Coordinating with Chief Developmental Tester with regard to the T&E requirements.
- Providing a requirements verification traceability database (requirements and test method).
- Specifying meetings and technical documentation (digital artifacts or documentation) between the program office and the developer.

- Conducting a review of the deliverables (what data, what format (digital artifacts or documents), level of detail, data rights, and when needed) and buying only what is needed in concert with should-cost goals.
- Leading or supporting the technical evaluation during source selection, including providing inputs to the development of source selection criteria.
- Performing SRAs as part of the source selection evaluation process.
- Supporting the Independent Management Review (Peer Review) of the RFP before release.
- Identifying external or SoS interfaces and ensuring the technical interface requirement and task scope are unambiguous to the offerors.
- Identifying requirements for the protection of critical program information (CPI) and mission-critical functions and components.
- Providing a clear description of the minimum technical requirements used to determine the technical acceptability of a proposal.

Table 2-4 contains the typical technical contents of the RFP and the associated Systems Engineer's responsibilities. It should not be considered an exhaustive or mandatory list.

Table 2-4. Typical Technical Contents of an RFP

	Typical Technical Contents	Systems Engineering (SE) Responsibilities
Section C Description of Work to Be Performed	• Statement of Work (SOW) • System Performance Specification • Operational Documents (Concept of Operations/ Operational Mode Summary/Mission Profile, systems of systems (SoS), Requirements, etc.) • Available and applicable architecture(s) • Engineering processes	• Provide program technical requirements and technical aspects in the SOW • Generate the system performance specification • Identify application of SE processes • Identify appropriate technical specifications and standards
Section H Special Contract Requirements	• Key personnel • Government-furnished equipment (GFE) or information • Diminishing Manufacturing Sources and Material Shortages (DMSMS) management • Parts management plan and associated deliverables • Warranties • Options for delivery of software • Digital Engineering Ecosystem • Award fees	• Include a clear statement of any special contract requirements that are not included in other sections of the uniform contract format • Include a clear statement of the expected software data rights that will be conveyed to the Government for developmental software items

	Typical Technical Contents	Systems Engineering (SE) Responsibilities
Section J Attachments	• Systems Engineering Plan (SEP) • Program Work Breakdown Structure (WBS) • Integrated Master Plan (IMP) • Top-level program schedule • Contract Data Requirements List (CDRL) • Contract security classification specification • Data rights attachment	• Support development of WBS, IMP, top-level program schedule, CDRL and Contract Security Specification • Ensure that sufficient time is allotted to develop high-quality specifications and plans before releasing the Request for Proposals (RFP)
Section K Representations, Certifications, and Other Statements	• Data rights	• Identify provisions that require representations, certifications or the submission of other information by offerors • Consider including a provision requiring offerors to identify any technical data or computer software the offeror proposes to deliver to the Government after award with less than unlimited rights
Section L Instructions on Content and Structure of RFP Response	• Systems engineering solution • Systems engineering management processes • Technical baseline management • Technical reviews and audits • Manufacturing and Quality approaches • Risk management processes and known key risk areas • Mandatory (i.e., statute- and regulation-driven) and advised design considerations • Technical organization • Technical data required for a Streamlined Life Cycle Assessment	• Adequately define the offeror's design • Provide technical background and context for the offeror's solution • Describe the offeror's SE technical and management processes • Provide consistency across the SOW and system performance specifications • Demonstrate alignment with Government processes • Include a statement in the RFP that the vendor will include a draft Software Development Plan as part of their proposal
Section M Source Selection Evaluation Factors	• Technical: technical solution, supporting data, performance specification • Management: SOW, Contractor Systems Engineering Management Plan (SEMP), Integrated Master Schedule (IMS), risks and opportunity management plans • Environmental objectives (when appropriate) • Manufacturing readiness • Quality or product assurance • Past performance • Price or cost to the Government	• Define technical evaluation factors and provide SE specific evaluation criteria used to assess proposals • Participate on or lead the technical evaluation team • Provide technical personnel to participate on each evaluation factor team (e.g., management, past performance, cost) • Provide consistency across the SOW and system performance specifications • Evaluate RFP responses against technical requirements, threshold requirements, management (e.g., SEMP, WBS, and program schedule), and consistency across the proposal (e.g.,

	Typical Technical Contents	Systems Engineering (SE) Responsibilities
	• Extent offeror’s rights in the data rights attachment meet Government’s needs	link between WBS, program schedule, risks, and cost) • Identify and assess the technical risks and opportunities for each proposal, including schedule risks and related risk and opportunity handling plans • Define clearly, in both the Source Selection Plan and Section M, the minimum technical requirements that will be used to determine the technical acceptability of the proposal if using the Lowest Price Technically Acceptable (LPTA) source selection method (see FAR (Subpart 15.101-2)). • At a minimum, include three evaluation factors relating to the offeror's software development approach, experience and process

3 TECHNICAL REVIEWS AND AUDITS

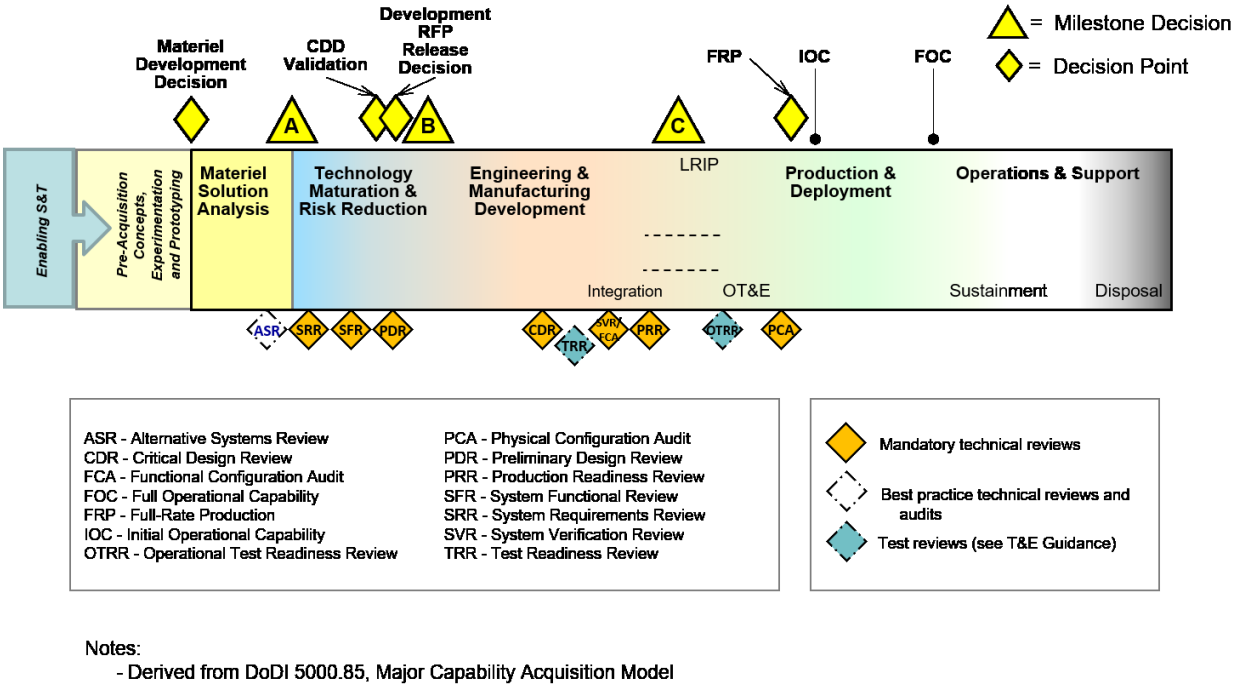
For DoD systems development, a properly tailored series of technical reviews and audits provide key points throughout the system development to evaluate significant achievements and assess technical maturity and risk. DoDI 5000.85 and the Adaptive Acquisition Framework Document Identification Tool (AAFDIT) identify the statutory and regulatory requirements for acquisition programs. Regardless of acquisition pathway, the PM, Systems Engineer, and Lead Software Engineer work to properly align the applicable technical reviews to support knowledge-based milestone decisions that streamline the acquisition life cycle and save precious taxpayer dollars. Technical reviews and audits allow the PM, Systems Engineer, and Lead 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 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 impacted by the extent to which the program adopts a DE approach (as described more fully in Section 2.2.2, Digital Engineering). As mentioned there, DoD'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 lifecycle 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 impact "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 an associated authoritative source 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 elsewise.

Technical reviews of program progress should be event driven and conducted when the system under development meets the review entrance criteria as documented in the SEP. An associated activity is to identify technical risks associated with achieving entrance criteria at each of these points (see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs). SE is an event-driven process based on successful completion of key events as opposed to arbitrary calendar dates. As such, the SEP should clarify the timing of events in relation to other SE and program events. While the initial SEP and IMS have the expected occurrence in the time of various milestones (such as overall system CDR), the plan should be updated to reflect changes to the actual timing of SE activities, reviews and decisions.

Figure 3-1 provides the end-to-end perspective and the integration of SE technical reviews and audits across all AAF pathways. Technical reviews should be tailored appropriately for other acquisition pathways.



Notes:
- Derived from DoDI 5000.85, Major Capability Acquisition Model

Figure 3-1. 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 satisfy operational requirements established in capability requirements documents.
- Providing a framework for interaction with the JCIDS and 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 study on Assessments of Selected Weapons 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 SEP. These policy and guidance documents provide a starting point for the PM, Systems Engineer, and Lead Software Engineer to develop the program's unique set of technical reviews and audits. Tailoring is expected to best suit the program objectives (see Section 1.4). The 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 (including the functional, allocated and product 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
- Program technical plans and schedules, which also inform the APB
- Contracting activity
- M&Q 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 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 systems engineering technical reviews and audits. See Technology and Program Protection (T&PP) Guidebook (forthcoming) Section 5 for system security engineering (SSE) criteria for each technical review and audit.

Roles and Responsibilities

For each technical review, a technical review chair is identified and is responsible for evaluating products and determining the criteria are met and action items are closed. The Service chooses the technical review chair, who could be the PM, Systems Engineer, or other subject matter expert selected according to the Service's guidance. This guidance may identify roles and responsibilities associated with technical reviews and audits. It also 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 in the SEP.

The following notional duties and responsibilities associated with the PM, Systems Engineer, and Lead Software Engineer should be considered in the absence of specific Service or lower level (e.g., System Command or PEO) guidance:

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 SEP 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 5000.85.
- Controlling the configuration of each baseline and convening configuration steering boards when user requirement changes are warranted. This can lead to an unscheduled gateway into the Functional Capabilities Board (FCB) and JCIDS process not identified in Figure 3-1 above.

The Systems Engineer is typically responsible for:

- 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 SEP, carefully tailoring each event to satisfy program objectives and SEP outline guidance associated with the minimum technical reviews and audits.
- Ensuring the plan is event based with pre-established review criteria and entrance and exit criteria for each event, informed by the knowledge point objectives for the specific program and acquisition pathway.
- 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
- Coordinating with Chief Development Tester to provide at each technical review: Developmental Test and Evaluation (DT&E) activities to-date, planned activities, assessments to-date and risk areas.
- 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.
- Coordinating with the appointed technical review chairperson on the technical review plans and supporting execution of the technical reviews.
- Assigning responsibilities for closure actions and recommending to the chairperson and PM when a system technical review should be considered complete (Figure 3-2).

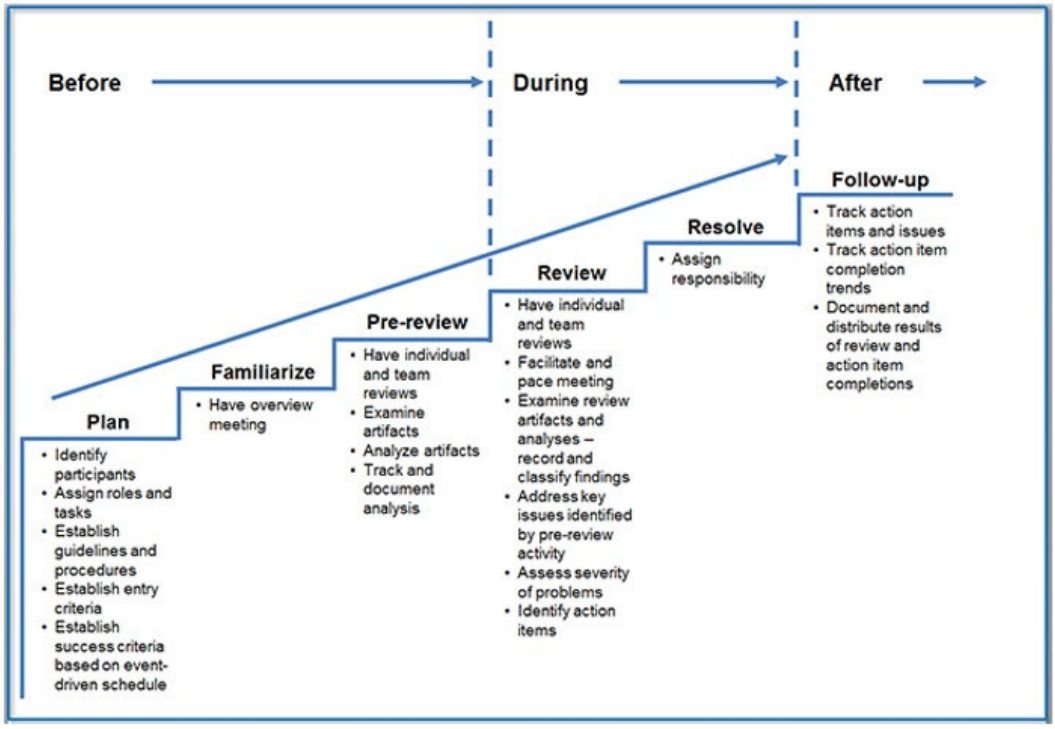


Figure 3-2. Technical Review Process

The PM, Systems Engineer, and Lead Software Engineer should identify key stakeholders who have an interest or role in the review, which may include:

- Technical review chairperson
- PEO
- 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
- Deputy Director, Engineering
- Service Technical Leadership such as chief engineers
- SMEs

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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs" as a resource. Instructions for how DoD military and civilian employees can access the IEEE 15288.2 via ASSIST are located on the DDR&E(AC)/Engineering website. If a PMO chooses to use IEEE 15288.2, additional guidance for implementing the DoD-adopted systems engineering standard on acquisition programs contracts can be found in the Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on Contracts for Department of Defense Acquisition Programs guidance document. When comparing this section on technical reviews and audits to IEEE 15288.2 keep in mind:

- The Alternative Systems Review (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 (forthcoming).
- With the exception of TRR, this chapter addresses all technical reviews and audits in clauses 5 and 6 of IEEE 15288.2. 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.

3.1 Alternative Systems Review

The ASR supports communication between the end user and acquisition community and leads to a draft 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 Lead 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 the AoA is complete and after a preferred materiel solution is selected by the lead Service or Component but before the FCB review. This timing allows the focus of the ASR to be on the preferred materiel solution rather than on all the alternatives, and allows for some post-AoA technical analysis to be completed and inform the FCB deliberations.

- The AoA results are an input to the ASR. The AoA 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 the AoA is complete, 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 should be available as an input to the ASR. It should have been available for use in the AoA and can then be used to support development of missions and operational scenarios to evaluate the preferred materiel solution.

Table 3-1 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". This is a best practice review.

Table 3-1. ASR Products and Criteria

Product	Alternative Systems Review (ASR) Criteria
Refined Joint Requirements	• Joint context and initial Concept of Operations/Operational Mode Summary/Mission Profile (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 system of systems (SoS) context • Required related solutions and supporting references (Initial Capabilities Document and Capability Development Document) identified • Joint refined thresholds and objectives initially stated as broad measures of effectiveness, performance, and suitability (e.g., Key Performance Parameters, Key System Attributes, 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 Analysis of Alternatives • 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 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/system safety analysis for preferred solution(s) complete • Human systems integration 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.

3.2 System Requirements Review

The SRR is a multi-disciplined technical review to ensure that the developer understands the system requirements and is ready to proceed with the initial system design.

A SRR or System Functional Review (SFR) is mandatory per DoDI 5000.88, Section 3.5.a. 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 ensure performance requirements are traceable to 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 includes competing contractual efforts during the 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 SEP.

Roles and Responsibilities

The unique PM responsibilities associated with an SRR include:

- Approving, funding, and staffing the SRR as planned in the SEP 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 SE Master Plan, IMS and IMP.
- 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 (see JCIDS Manual (requires Common Access Card (CAC) to access website).
- 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.
- Ensuring plans to proceed to SFR allow for contingencies.
- Ensuring all interface are documented for the SoS and included in the performance specification.

Inputs and Review Criteria

Figure 3-1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle. The SRR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP.

Table 3-2 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 their action items closed. This is also an opportunity to assess whether technical requirements from all acquisition documentation (e.g., PPP, TEMP, Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report) are flowed 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". This is a best practice review.

Table 3-2. SRR Products and Criteria

Product	System Requirements Review (SRR) Criteria
Cost Estimate	• Preliminary Cost Analysis Requirements Description 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 completed
System Performance Specification	• Contractor clearly demonstrates an understanding of the system requirements consistent with the Initial Capabilities Document (ICD) and draft Capability Development Document (CDD) • 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 (forthcoming)) • 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. reliability and maintainability (R&M) requirements) have been reviewed and included in the overall system design (See Section 5) • Sustainment requirements have been reviewed and included in the overall system design HSI Guidebook (forthcoming).) • 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, the Statement of Work (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 Systems Engineering Management Plan 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 • Adequate processes and metrics are in place for the program to succeed

Product	System Requirements Review (SRR) Criteria
	• 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 • System safety (SS), occupational, and, health hazards, and force protection and survivability (FP&S) domain (i.e. HSI/FP&S) considerations have been reviewed and mitigating courses of action have been allocated within the overall system design • Hazards have been reviewed as part of the Mission-Based Cyber Risk Assessments 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 Technology Maturation and Risk Reduction (TMRR) phase (See Chief Developmental Tester in T&E Enterprise Guidebook (forthcoming)) • Government and contractor configuration management (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 digital engineering ecosystem has begun and is captured in the Systems Engineering Plan and in other appropriate program plans. • The manufacturing and production strategy is complete and adequate • Integrated Master Schedule 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 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.

3.3 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 Functional Configuration Audits (FCAs) leading up to the system-level FCA or the System Verification Review (SVR). For additional information, see Section 4.1.6, Configuration Management Process.

An SRR or SFR is mandatory per DoDI 5000.88, Section 3.5.a. 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 (including cyber survivability and operational resilience requirements).
- 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 SEP 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.
- 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 traceable (both directions) between requirements in the draft CDD, including KPPs, KSAs, other system attributes, and the system performance specification (see CJCSI 5123.01 JCIDS).
- 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.

Table 3-3 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs." This is a best practice review.

Table 3-3. SFR Products and Criteria

Product	System Functional Review (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) Capability Development Document (CDD) requirements and reflecting clear linkage to the system of system (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 System Verification Review/Functional Configuration Audit
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 human systems integration and environment, safety, and occupational health mitigation measure requirements, at levels that warrant continued engineering development • Updated Mission-Based Cyber Risk Assessment
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 reliability and maintainability (R&M) plans specified in the Statement of Work 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.

3.4 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 and 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 4.1.6, Configuration Management Process).

The PDR is mandatory per DoDI 5000.88, Section 3.5.a. The timing of the review should consider the following:

- For all AAF pathway programs that are classified as MDAPs, 10 U.S.C. 2366b requires the MDA certify all MDAPs at Milestone B. This certification 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 DoD 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, 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.
- 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 IAW 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, documenting all assumptions and rationale needed to support an accurate cost estimate for the APB; 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 10 USC 2366b certification required 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, contributing to trade-off analyses. Depending upon the nature/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 and the PM, Systems Engineer, and Lead Software Engineer should update relevant program plans.

Roles and Responsibilities

The PM, Systems Engineer, and Lead 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 Lead 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.

Though many Service systems commands or PEOs define the roles and responsibilities of the PM, Systems Engineer, and Lead 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 CDR in applicable contract documents including the SEMP, IMS, and IMP.
- Ensuring the SEP includes SMEs to participate in each review.
- Reviewing and approving trade-off analyses with SMEs to address design decisions or AoAs.
- 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 (e.g., HSI, reliability and maintainability, corrosion, SS, survivability, and ESOH considerations).

- 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.) Monitor and control 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 3-4 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". The PDR is a mandatory technical review.

Table 3-4. PDR Products and Criteria

Product	Preliminary Design Review (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 Cost Analysis Requirements Description (CARD) 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 Test and Evaluation Master Plan (TEMP) accounts for risks (e.g., system safety (SS) risks assessments) with a mitigation plan; necessary integration and test resources are documented within the TEMP and current availability align with the program Integrated Master Schedule (IMS) (SE coordinates with the Chief Developmental Tester in this area; refer to T&E Enterprise Guidebook (forthcoming)) • Human systems integration (HSI) and environment, safety, and occupational health (ESOH) risks are known and being mitigated • Risks are at an acceptable level to continue with detailed design • Unique software risks identified/assessed and mitigation plans developed and implemented • Updated Mission-Based Cyber Risk Assessment, 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 5.11 Intelligence (Life Cycle Mission Data Plan)

Product	Preliminary Design Review (PDR) Criteria
Technical Baseline Documentation/Digital Artifacts (Allocated)	• Capability Development Document (CDD) is validated per CJCSI 5123.01 • Analysis of system performance is complete and assessed to meet requirements • Preliminary design satisfies design considerations (see Section4.2.2 Requirements Analysis Process) • Producibility assessments of key technologies are complete • Preliminary system-level design is producible and assessed to be within the production budget • 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, etc.) 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 Requirement Specifications (IRSs), 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 configuration management • 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., Statement of Work (SOW), Systems Engineering Plan (SEP), approved Systems Engineering Plan (SEMP), and system performance specification) have been satisfied • Technical plans documented in the SEP and any additional plans for appropriate design considerations (e.g. reliability and maintainability (R&M), cybersecurity, ESOH, manufacturing, HSI)

Product	Preliminary Design Review (PDR) Criteria
	• 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 Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) • Program is properly staffed • Stakeholders are able to access needed data within the digital engineering ecosystem to make informed decisions • Adequate processes and metrics are in place for the program to succeed • Program schedule, as depicted in the updated IMS (See Section 4.1.1) 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 • Life Cycle Sustainment Plan (LCSP) 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, reuse, and other software-related issues are completed • Software development process is defined in a baselined SDP and reflected in the IMP and IMS • 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 plans (hardware and software) and documents schedule and resource implications associated with the T&E program • Update the Program Protection Plan 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

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.
- 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 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) is updated and reflects the design in the allocated baseline.
- The LCSP is updated to reflect development efforts and schedules.

Preliminary Design Review (PDR) Assessment

A system-level PDR assessment is required for MDAPs per 10 USC 2366b and DoDI 5000.88, Section 3.5.a. 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. In compliance with DoDI 5000.88, Section 3.5.a, the USD(R&E) conducts PDR assessments on ACAT ID programs, and the CAE is responsible for the conduct of PDR assessments on ACAT IC programs. In support of this, MDAP PMs are required to invite the USD(R&E) and the CAE to their PDRs and make the PDR artifacts available.

USD(R&E) reviews the conduct of the program's PDR, including system element-level reviews as appropriate, and provides the MDA with an assessment of the following:

- The conduct and adequacy of the PDR including 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 KPP, KSA and TPM thresholds and the proposed corrective actions to address any performance gaps, as appropriate.
- Key systems engineering design considerations.

3.5 Critical Design Review

The CDR, mandatory for MDAPs per DoDI 5000.88, Section 3.5.a, 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 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 has reached the necessary level of maturity to start coding, 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. 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. 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).

In accordance with DoDI 5000.88, Section 3.4.b, the PM assumes control of the initial product baseline at the completion of the system level CDR 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 (for more information, see Section 5.1.6. Configuration Management Process).

Roles and Responsibilities

The Systems Engineer documents the approach for the CDR in the SEP. 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 Lead 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 Lead 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.

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.
- 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; 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 (e.g., HSI, reliability and maintainability, corrosion, SS, and ESOH considerations).
- 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," suggests a best practice is to achieve design stability at the system-level CDR. A general rule is that 75 to 90 percent of (manufacturing quality) 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 with regard to 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 review criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP.

Table 3-5 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". The CDR is a mandatory technical review.

Table 3-5. CDR Products and Criteria

Product	Critical Design Review (CDR) Criteria
Cost Estimate	• Updated Independent Cost Estimate (ICE) and Cost Analysis Requirements Description (CARD) 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 is complete and consistent • Key product characteristics having the most impact on total system performance, assembly, cost, reliability and sustainment, or environment, safety, and occupational health (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 software coding to proceed with proper configuration management • Assessment of the technical effort and design indicates potential for operational test and evaluation (OT&E) success (operationally effective, suitable, survivable) (See T&E Enterprise Guidebook (forthcoming).) • 100% of critical safety items (CSIs) and critical application items (CAIs) have completed drawings, specifications and instructions

Product	Critical Design Review (CDR) Criteria
	• Failure Mode, Effects, and Criticality Analysis (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 human systems integration (HSI) requirements (see HSI Guidebook (forthcoming)) • 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 • Verification (developmental test and evaluation) assessment to date is consistent with the initial product baseline and indicates the potential for test and evaluation (T&E) success (see Test and Evaluation Master Plan (TEMP) and Chief Developmental Tester in T&E Enterprise Guidebook (forthcoming).)
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 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 Integrated Master Schedule (IMS) (Systems Engineer coordinates with Chief Developmental Tester in this area; see T&E Enterprise Guidebook (forthcoming).) • Design consideration risks are known and being mitigated • 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; refer to Section 5.12. Intelligence (Life Cycle Mission Data Plan) • An updated Mission-Based Risk Assessment is completed and identified unacceptable risks mitigated
Technical Plans	• Preliminary Design Review (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., Statement of Work (SOW), Systems Engineering Plan (SEP), approved Systems Engineering Management Plan (SEMP), and system performance specification) have been satisfied • Reliability and maintainability (R&M) technical plans have been updated (individual and as part of the Government's SEP and the contractor's SEMP)

Product	Critical Design Review (CDR) Criteria
	• Adequate processes and metrics are in place for the program to succeed • Program schedule as depicted in the updated IMS (see Section 4.1.1) 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 • Life Cycle Sustainment Plan (LCSP), including updates on program sustainment development efforts and schedules based on current budgets, T&E results and firm supportability design features, is approved • Program Protection Plan is updated when critical design activities result in new program scope, design, threats, vulnerabilities, or protection needs • Cybersecurity Strategy (CSS) and Security Assessment Plan 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.
- Updated CARD (or CARD-like document) 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, 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.

Critical Design Review (CDR) Assessment

A system-level CDR assessment is required for MDAPs. This assessment informs the MDA of the technical risks and the program's readiness to proceed. In compliance with DoDI 5000.88, Section 3.5.a, the USD(R&E) is directed to conduct CDR assessments on ACAT ID programs; and the CAE is to conduct CDR assessments on ACAT IB and IC programs. In support of this policy direction, MDAP PMs are required to invite USD(R&E) and CAE to their CDRs and make the CDR artifacts available.

USD(R&E) 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 KPP, KSA, and TPM thresholds and the proposed corrective actions to address any performance gaps, as appropriate.
- Key systems engineering design considerations.

3.6 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-61 (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 Operational Test and Evaluation (OT&E). Verification of system performance is later accomplished on a production system.

An SVR/FCA is mandatory per DoDI 5000.88, Section 3.5.a. 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 (forthcoming).)
- 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 Production Readiness Review (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 4.1.6 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 configuration items (CIs) and software CIs have achieved the requirements in their specifications.
- Verifying that cybersecurity controls have been implemented as defined in the Security Technical Implementation Guides (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 Physical Configuration Audit (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 3-6 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". This is a best practice review.

Table 3-6. SVR/FCA Products and Criteria

Product	System Verification Review (SVR)/Functional Configuration Audie (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 operational test and evaluation (OT&E) • Reliability and maintainability (R&M) performance meets the contractual specification requirements • Capability Development Document (CDD) R&M requirements are likely to be met.
Risk Assessment	• Identified and documented risks (including human systems integration (HSI), cybersecurity, and environment, safety, and occupational health (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.

3.7 Production Readiness Review

The PRR, mandatory per DoDI 5000.88, Section 3.5.a., 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 Engineering and Manufacturing 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 Physical Configuration Audit (PCA) 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, quality management system, and production planning (i.e., 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 4.1.6 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 3-7 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 IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs". This is a best practice review**.**

Table 3-7. 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 diminishing manufacturing sources and material shortages (DMSMS) risks • Human systems integration (HSI) and environment, safety, and occupational health (ESOH) risks are known and mitigated • Cybersecurity vulnerabilities, threats, and risks are known and mitigated
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

Product	PRR Criteria
	• 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 Low-Rate Initial Production (LRIP) and Full-Rate Production (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 reliability and maintainability (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 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 6.18. Producibility, Quality, and Manufacturing Readiness.

Outputs and Products

The Technical Review Chair determines when the review is complete. Results of the PRR and associated Manufacturing Readiness Assessments (MRAs) are typically documented in a written report or out-brief. 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.

3.8 Physical Configuration Audit

The Physical Configuration Audit (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-61 (Configuration Management Guidance).

The PCA is an event-driven technical assessment that typically occurs during the Production and Deployment (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 testing 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, quality management system and production planning (i.e., 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 4.1.6 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 operations and support 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 (FOC).
- Ensuring plans to get to FOC 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. The PCA is conducted when these criteria are considered to be met.

Table 3-8 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. IEEE 15288.2 "Standard for Technical Reviews and Audits on Defense Programs" is a resource for preparing the audit. This is a best practice audit.

Table 3-8. PCA Products and Criteria

Product	Physical Configuration Audit (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 operational test and evaluation (OT&E)
Risk Assessment	• Risks are identified and documented at levels low enough to continue with Full-Rate Production (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 reliability and maintainability (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.

4 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.

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 (CTI) about DoD 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 use for their program.

As mentioned in Section 4, Technical Reviews and Audits, regardless of acquisition pathway, the ability to conduct needed, supporting analyses can be profoundly impacted by the extent to which the program adopts a digital engineering approach (as described more fully in Section 3.1.2, Digital Engineering). This will not impact "what" systems engineering processes need to be followed, but, as with technical reviews and audits, it can have a profound and revolutionary impact upon "how" these processes are conducted. A well-defined and instantiated digital ecosystem will typically have wide applicability and impact in support of the eight technical processes, such as requirements analysis and architecture design.

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 (e.g., R&M, Safety, HSI, Manufacturing and Quality) and program costs and schedules.
- Able to operate in complex system-of-systems (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. The following subsections, as indicated in Table 4-1, discuss the SE processes in more detail.

Table 4-1. Systems Engineering Processes

Technical Management Processes	Technical Processes
Technical Planning (Section 4.1.1)	Stakeholder Requirements Definition (Section 4.2.1.)
Decision Analysis (Section 4.1.2)	Requirements Analysis (Section 4.2.2)
Technical Assessment (Section 4.1.3)	Architecture Design (Section 4.2.3)
Requirements Management (Section 4.1.4)	Implementation (Section 4.2.4)
Risk Management (Section 4.1.5)	Integration (Section 4.2.5)
Configuration Management (Section 4.1.6)	Verification (Section 4.2.6)
Technical Data Management (Section 4.1.7)	Validation (Section 4.2.7)
Interface Management (Section 4.1.8.)	Transition (Section 4.2.8)

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
- IEEE 15288.1, Standard for 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, utilization, support, and retirement. It is supported by a Government-initiated NGS, IEEE 15288.1, which expands on the SE life cycle processes of ISO/IEC/IEEE 15288 with additional detail specific to DoD acquisition projects. IEEE 15288.1 also adds requirements for SE outputs and the attributes (criteria) for each process.

DoD has adopted both ISO/IEC/IEEE 15288 and IEEE 15288.1. 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 DoD 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 15288.1, additional guidance for implementing the DoD-adopted systems engineering standards on acquisition programs contracts can be found in the Best Practices for Using Systems Engineering Standards (ISO/IEC/IEEE 15288, IEEE 15288.1, and IEEE 15288.2) on Contracts for Department of Defense Acquisition Programs guidance document. Instructions for how DoD military and civilian employees can access the IEEE 15288.1 via ASSIST are located on the DDRE(AC)/Engineering website.

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. Figure 4-1 depicts how the SE Guidebook SE processes/activities map to the ISO/IEC/IEEE 15288 processes. The figure does not cover the ISO/IEC/IEEE 15288 Agreement and Organizational project-enabling

processes because those apply to commercial system development and are outside the scope of DoD acquisition.

	DoD SE Processes (DAG section)	ISO/IEC/IEEE 15288 Processes (Clause)
TECHNICAL MGMT PROCESSES	Technical Planning (4.1.1)	Project Planning (6.3.1)
	Decision Analysis (4.1.2)	Decision Management (6.3.3)
	Technical Assessment (4.1.3)	Project Assessment and Control (6.3.2)
		Measurement (6.3.7)
	Requirements Management (4.1.4)*	System Requirements Definition (6.4.3)
	Risk Management (4.1.5)	Risk Management (6.3.4)
	Configuration Management (4.1.6)	Configuration Management (6.3.5)
	Technical Data Management (4.1.7)	Information Management (6.3.6)
	Interface Management (4.1.8)	Architecture Definition (6.4.4)
	Covered by Section 5.14.4 Manufacturing and Quality and PM Guidebooks	Quality Assurance (6.3.8)
TECHNICAL PROCESSES	*Covered by Sections 2 System Level Considerations and 2.2.3 Mission Engineering*	Business or Mission Analysis (6.4.1)
	Stakeholder Requirements Definition (4.2.1)	Stakeholder Needs and Requirements Definition (6.4.2)
	Requirements Analysis (4.2.2)*	System Requirements Definition (6.4.3)
	Architecture Design (4.2.3)	Architecture Definition (6.4.4)
	Implementation (4.2.4)	Design Definition (6.4.5)
		Implementation (6.4.7)
	Covered throughout Sections 3.2 SE Activities in the Life-cycle and 5s Design Considerations	System Analysis (6.4.6)
	Integration (4.2.5)	Integration (6.4.8)
	Verification (4.2.6)	Verification (6.4.9)
	Validation (4.2.7)	Validation (6.4.11)
	Transition (4.2.8)	Transition (6.4.10)
	Covered by Life Cycle Sustainment Guidebook	Operation (6.4.12)
	Covered by Life Cycle Sustainment Guidebook	Maintenance (6.4.13)
	Covered by Section 5.7 Demilitarization and Disposal and Life Cycle Sustainment Guidebook	Disposal (6.4.14)

*Requirements Management and Requirements Analysis processes are covered by ISO/IEC/IEEE 15288 – System Requirements Definition

Figure 4-1. SE Processes/Activities Mapped to ISO/IEC/IEEE 15288 SE Processes

Roles, Responsibilities, and Activities

The PM, Systems Engineer, and Lead 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 Lead 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 4-2 is a representation of how much effort programs typically focus on each of the SE processes throughout the Major Capability Acquisition (MCA) life cycle. The PM, Systems Engineer, and Lead Software Engineer should apply appropriate resources with the requisite skill sets to ensure successful execution of each process.

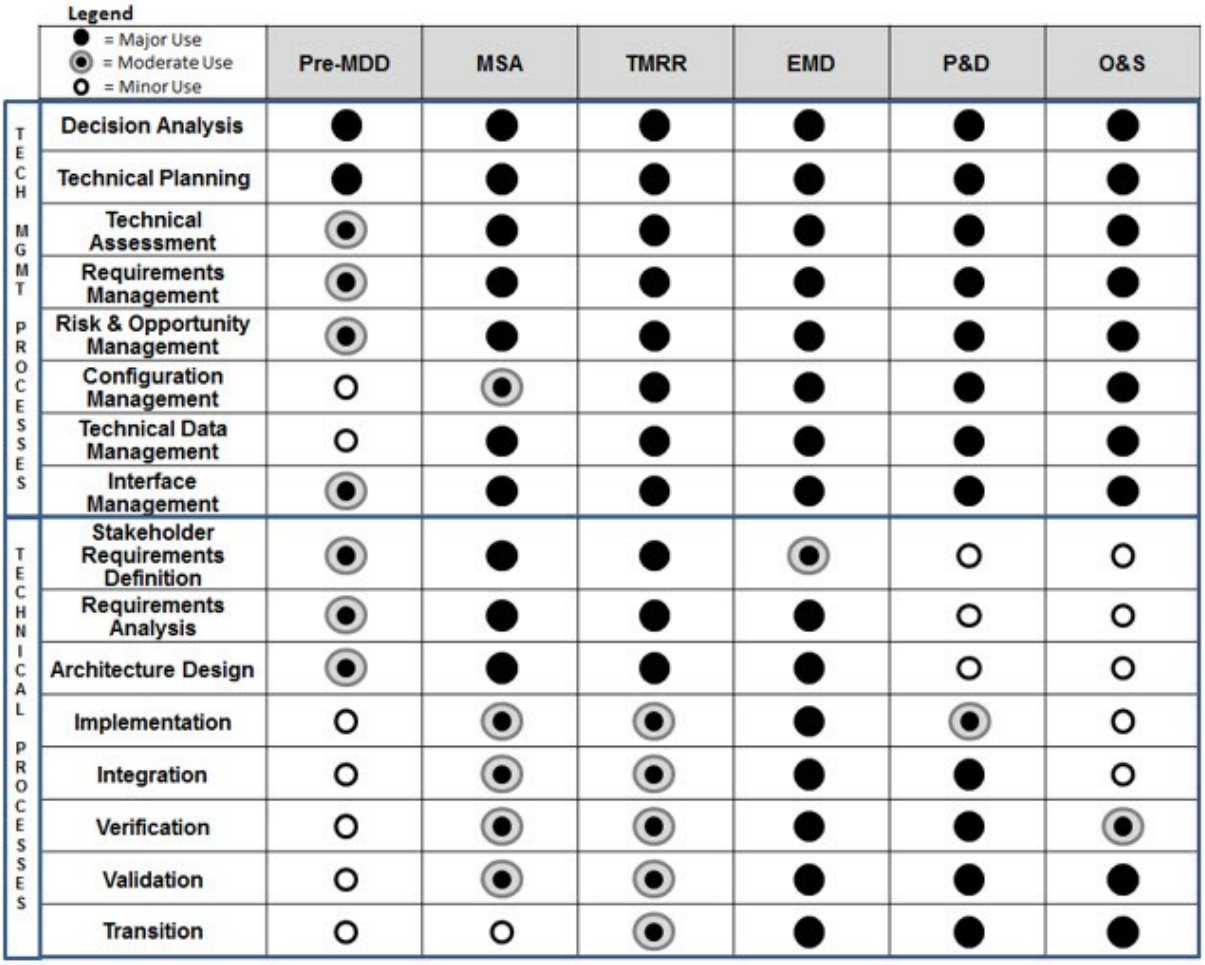


Figure 4-2. Notional Emphasis of Systems Engineering Processes throughout the Major Capability Acquisition Life Cycle

4.1 Technical Management Processes

DoD 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 4.1.1 through 4.1.8 describe the technical management processes.

4.1.1 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 inputs to program planning and life cycle cost estimates. Technical planning provides the PM, Systems Engineer, and Lead 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.
- A foundation for risk identification and management (see Section 4.1.5 Risk Management Process).
- Quantitative measures supporting the Technical Assessment process (see Section 4.1.3) identifies system maturity.
- An accurately constructed and resourced IMS supporting the assignment of Earned Value.

The resulting program cost estimates and risk assessments are essential to support milestone decisions, if applicable, and to establish the plan for accomplishing work against which contract performance is measured and enable mandatory program certifications as well as independent technical assessments (e.g., 10 USC 2366a or 10 USC 2366b).

Technical planning includes the program's plan for technical reviews and audits (see Section 3). 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 re-planning.

The PM, Systems Engineer, and Lead 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 Materiel Development Decision. Technical planning leverages the CONOPS/OMS/MP and mission analysis. The CONOPS/OMS/MP is a document consistent with the validated/approved capability requirements document, including the 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 all 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 Lead Software Engineer should consistently look for root cause(s) and implement corrective actions in order to enable programmatic and technical success. Modifications to the SE processes and SEP may be required because of root cause and corrective action analysis and implementation.

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 developer's SEMP.
- Providing technical inputs and ensuring SEP alignment to other program plans (AS, TEMP, LCSP, DoD Security Requirements Guides (SRGs) and DoD STIGs, and Programmatic Environment, Safety and Occupational Health Evaluation (PESHE).

Technical Planning should reflect the context of the organization and comply with all applicable policies. The PM, Systems Engineer, and Lead 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:

- Defining the scope and objectives of the technical effort and including the performance evolution of system capabilities.
- Identifying constraints and risks.
- Establishing roles and responsibilities.
- Dividing the program scope and objective into discrete elements.
- Identifying technical reviews and audits as well as their timing.
- Establishing schedules and costs.
- Preparing or updating planning documentation.
- Scaling SE processes based on the scope and complexity of the program/system.
- Identifying areas for potential tailoring (including rationale) for MDA approval.

Key factors that the Systems Engineer should consider when accomplishing technical planning include:

- Capability needs (requirements, gaps, threats, operational context, CONOPS/OMS/MP, Target Audience Description).
- 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 systems engineering 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 (forthcoming) 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:

- WBS (see Section 4.1.1) – a framework for specifying program objectives.
- IMP (see Section 4.1.1) – an event-based plan consisting of a hierarchy of program events that need to be accomplished.
- IMS (see Section 4.1.1) – 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 Lead Software Engineer in the Technical Planning process can be found at the DDRE(AC)/Engineering website.

Work Breakdown Structure

The WBS represents the decomposition of both 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). MIL-STD-881 shall be used as required by the mandatory DI-MGMT-81861 (Integrated Program Management Data and Analysis Report (IPMDAR)).

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 should also 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 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 digital engineering systems engineering approach, thought to the level of data access needed is necessary and may be at an even 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, and whenever it is revised, traceability to the previous version needs to be maintained.

The WBS displays and defines the program and product, or products, to be developed and/or produced and provides a common thread for the EVMS, the IMP and the IMS to better understand and 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 PM Guidebooks (forthcoming).

Planning program tasks by WBS element serves as the basis for mapping development of the technical baseline and aids 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 Lead 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 current 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 SOW, WBS, IMP events and acquisition milestones.

Figure 4-3 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 Lead 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.

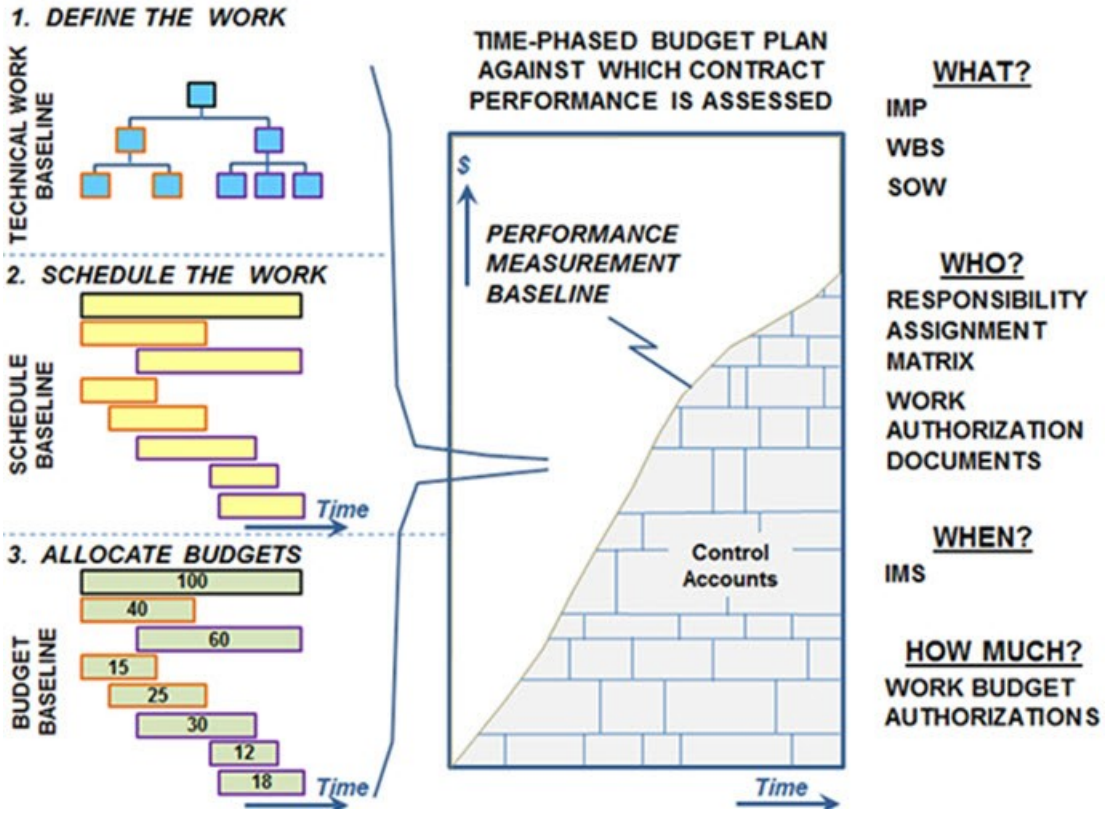


Figure 4-3. IMP/IMS Hierarchy and Content

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 (IPMDAR)), 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 Lead 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 Integrated Master Schedule Preparation and Use Guide provides additional guidance on developing and implementing these technical planning tools.

Schedule Risk Assessments

An 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 used 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 4-4). 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 4.1.5 Risk Management Process).

When part of the contract, the DI-MGMT-81861 (Integrated Program Management Data and Analysis Report (IPMDAR)) 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.

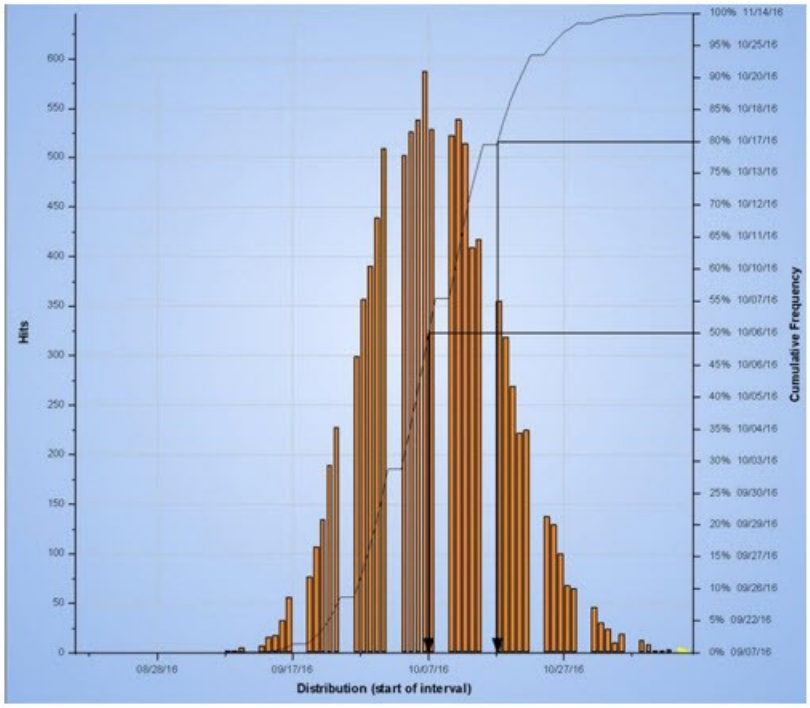


Figure 4-4. Schedule Risk Assessment Histogram

4.1.2 Decision Analysis Process

The Decision Analysis process transforms a broadly stated decision opportunity into a traceable, defendable 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 4.1.1)
- Technical Assessment (see Section 4.1.3)
- Stakeholder Requirements Definition (see Section 4.2.1)
- Requirements Analysis (see Section 4.2.2)
- Architecture Design (see Section 4.2.3)

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.

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 2.2 Tools, Techniques and Lessons Learned).
- 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.

4.1.3 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. These activities begin by examining the status of development planning activities and efforts early in the program life. 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 operations and support to support reliability growth and sustainment engineering efforts.

The PM, Systems Engineer, and technical management team evaluate technical maturity in support of program decisions at event-driven technical reviews and audits (see Section 3 Technical Reviews and Audits) that occur throughout the acquisition life cycle. The PM, Systems Engineer, and Lead 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/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 correction actions before major reviews and milestones. The PM should ensure that assessments are appropriately contracted, resourced and staffed, and include appropriate stakeholder and subject matter expert 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 3 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, and/or threat).

The PM should approve the Technical Assessment products for the program as part of three documents: (1) the performance measurement baseline (PMB) to capture time-phased measures against the WBS (see Technical Performance Measures); (2) a resource-allocated IMS (see Section 4.1.1); and (3) the SEP (see Section 1.5) 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 TPMMs. Specific activities should include:

- Establishing event-driven technical planning.
- Identifying appropriate measures and metrics.
- Conducting analyses to assess risks and develop risk mitigation strategies.
- Conducting assessments of technical maturity, process health and stability and risk to communicate progress to stakeholders and authorities at decision points.
- Proposing changes in the technical approach to reduce the program's technical risks.
- Advising the PM on the program's technical readiness to proceed to the next phase of effort.
- Including 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 TRA is a systematic, metrics-based technical assessment process that assesses the maturity of, and the risk associated with, critical technologies to be used in MDAPs. It is conducted by the PM with the assistance of an independent team of SMEs.

PMs of MDAPs should conduct knowledge-building TRAs throughout the DoD acquisition life cycle, including at PDR, CDR, and Milestone C. These assessments should include the reassessment of all elements of the system design to identify any new critical technology elements and their associated technology readiness levels as a result of any system design changes or new knowledge obtained during the engineering and manufacturing development

phase. See the Engineering of Defense Systems Guidebook and the DoD Technology Readiness Assessment (TRA) Guidance for additional information.

Technical Performance Measures

TPMMs 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, sub-system 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 level of 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/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 both 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 for identifying, prioritizing and selecting 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, there are 15 categories that are of concern within the Department across all DoD 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 4-2, 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 KPP and each KSA. This specific set of TPM's 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 4-2 addresses the organization of the core TPM categories as well as their definitions.

Table 4-2. Core Technical Performance Measure Category Definitions

Core Technical Performance Measure (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 5.2.5. Integration and Section 6.12. 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 5.18 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 Key Performance Parameters and Key System Attributes. These are called Critical Technical Parameters (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 application and techniques for the detect, protect and react paradigm; and controls performance of Security Technical Implementation Guides.
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 5.14 Manufacturing and Quality)
Manufacturing Quality	System manufacturing quality metrics should track both quality of conformance and quality of design. Quality of conformances 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 5.14 Manufacturing and Quality)

Core Technical Performance Measure (TPM) Category	Description of TPM
Schedule Management	Include metrics to assess both schedule health (e.g., the Defense Contract Management Agency 14-point health check), associated completeness of the Work Breakdown Structure and the risk register. A healthy, complete and risk-enabled schedule forms the technical basis for the Earned Value Management System (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.
Resource Management	Metrics should evaluate the adequacy of resources and/or tools (e.g., models, simulations, automated tools, synthetic environments) to support the schedule. See also Table 5-7: Product Support Considerations.
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 2.2.4 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 2.2.4 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 4.1.4 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 4.1.5 Risk Management Process)
Test Management	Metrics should include measures of the stability of the verification and validation process (e.g., number of test points, development of test vignettes and test readiness).

TPM Hierarchy

As shown in Figure 4-5, TPMs at the Management Decisional level may be allocated or decomposed into supporting details associated with subsystem assemblies along the lines of the WBS and/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.

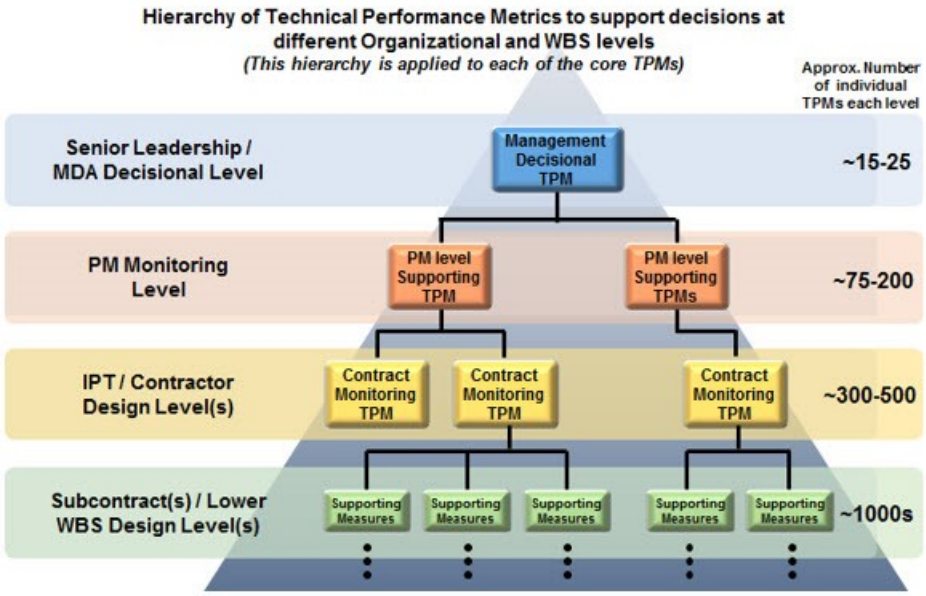


Figure 4-5. TPM Hierarchy

TPM Characteristics

Figure 4-6 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). As illustrated in the figure, there are four attributes of a good metric:

- The measure is quantifiable with defined criteria and consistent methods for determining a measurement point.
- The interval of measure collections is routine and on a cycle to support timely evaluation of corrective action and enable statistical forecasting and the overall condition by observing the change of the measured attribute over time.
- There is a curve of an expected plan, goal, control limits or threshold values over time for the appropriate phase to measure against as-to status, as well as to determine stability, and if the measure is in control. At a minimum, each review and assessment point should have a planned value.
- 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 KPP and KSA as well as known developmental process risks such as software development, cybersecurity, schedule health, requirements stability and mission integration/interoperability.

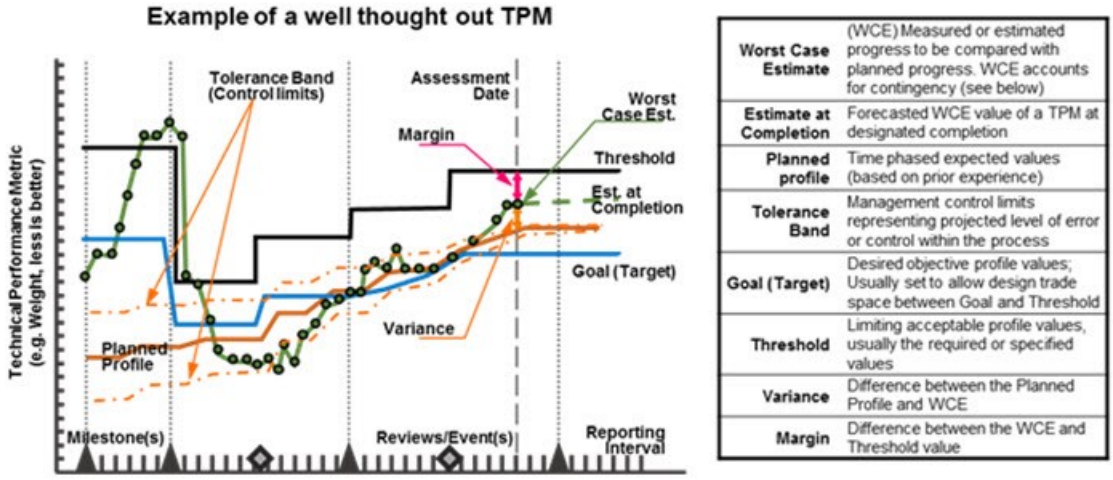
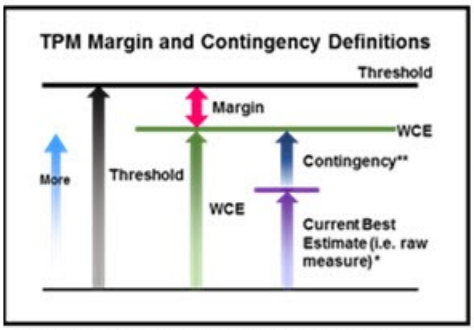


Figure 4-6. Leading Indicators Influence Risk Mitigation Planning

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 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 still 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 4-7 depicts the relationship between Contingency, CBE, WCE, Threshold and Margin, as well as example criteria of how contingency changes as the system/testing matures.



* Current Best Estimate value is the raw estimate of the metric determined either by prediction, analysis, direct measurement, and/or bottoms-up estimation without consideration for error.
** Contingency accounts for the uncertainty in estimation and immaturity of the item being measured.

Example guidelines to allocate Contingency to each estimated measure to account for uncertainty

Basis for Current Best Estimate Value			Contingency
Maturity of item/process being measured	Estimating Technique	Estimating Technique (alternate)	Uncertainty to be included in the WCE
Paper Design	Analysis, legacy similarity	Guess	15%
Roll-up of Component-level items	Extrapolated tests, Bottom-up models	Analysis	10%
Integrated model / prototype	Integration lab demo	Modeling	7%
Test article	Representative test	Demo	4%
Final article	End-to-end test in real environment (e.g., OT&E)	Test	0%

For a data collection point determine the worst case (largest contingency) associated with the applicable item maturity or estimating technique. Apply that contingency percentage to the current best estimate to arrive at the WCE for that collection interval. An example is highlighted: A representative test is done with a roll-up of components. This results in a worst case Contingency of 10%, resulting in: WCE = CBE +10%

Figure 4-7. TPM Contingency Definitions

4.1.4 Requirements Management Process

The Requirements Management process maintains a current and approved set of requirements over the entire acquisition life cycle. This helps ensure delivery of a capability that meets the intended mission performance, as stipulated by the operational user.

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 Section 4.2.1 Stakeholder Requirements Definition Process and 4.2.2 Requirements Analysis Process, respectively). 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.

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 bi-directional 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, bi-directional 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). Bi-directional traceability also ensures that higher-level requirements are properly flowed to lower-level requirements and system element designs so that 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 Configuration Management process (see Section 4.1.6 Configuration Management Process), 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, para 3C.3.e, CAEs establish Configuration Steering Boards (CSB), following CDD validation, for 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 PEO and requirements sponsor, will identify and propose to the CSB recommended requirements changes, including de-scoping options, that reduce the program cost and/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 2.2 Tools, Techniques and Lessons Learned contains information about SE tools generally employed in the Requirements Management process. There are many commercial software packages specifically designed for the traceability aspect of Requirements

Management, from top-level operational requirements down to the lowest-level system elements in the WBS.

4.1.5 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, prioritizing requirements and making trade-offs should be accomplished 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. DoDI 5000.85, para 3C.3.d. requires the PM to present top program risks and associated risk mitigation plans at all relevant decision points and milestones. DoDI 5000.85, para 3C.3.d. also specifies risk management techniques the PM is required to consider when developing the acquisition strategy. Technical risk management is addressed in DoDI 5000.88, para 3.4.f.

Technical, programmatic and business events can develop into risks, issues or opportunities, each with cost, schedule or performance consequences as shown in Figure 4-8.

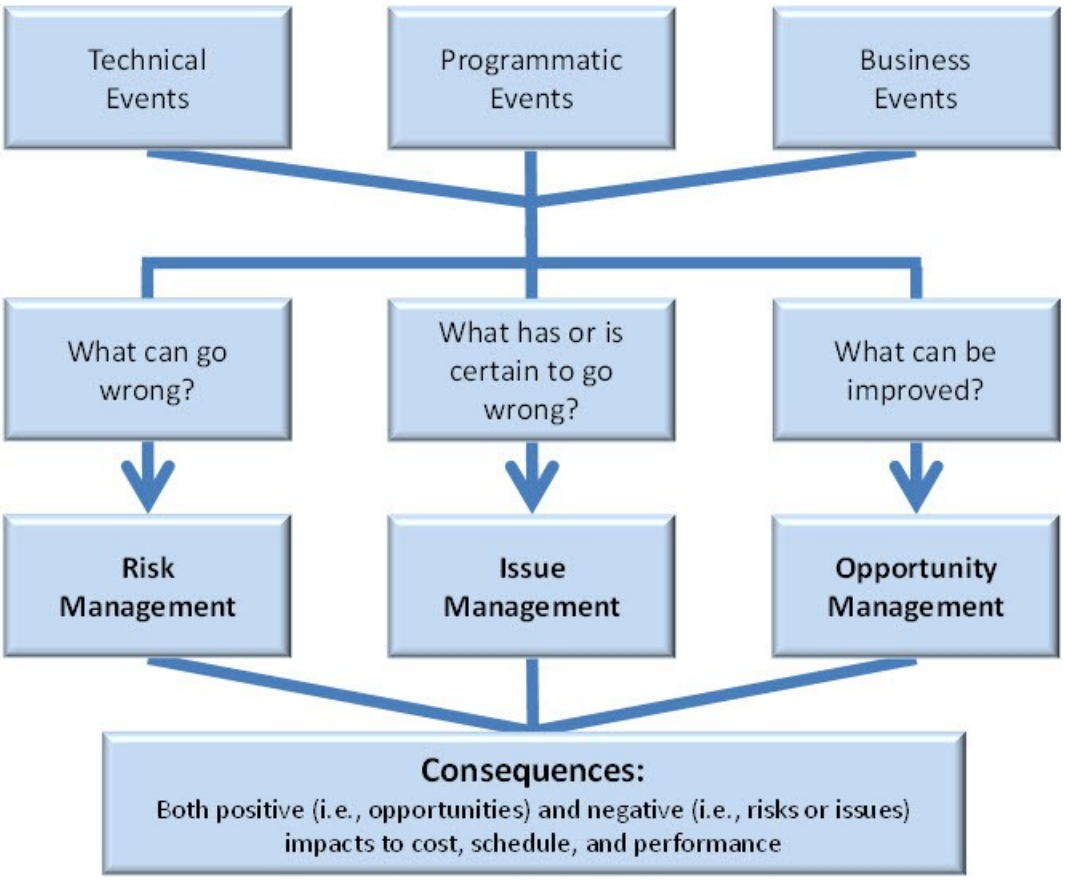


Figure 4-8. Risk, Issues, and Opportunities

Statute 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. Per statute, the approach 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, multiple design approaches and other considerations. In accordance with 10 USC 2448b and DoDI 5000.88, para 3.5.b., ITRAs are conducted on all MDAPs, regardless of AAF pathways, before approval of Milestone A, Milestone B, and any decision to enter into low-rate initial production or full-rate production. Additional information on ITRAs can be found on the DDRE(AC)/Engineering web site.

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. 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.

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 Process (PRP) – 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 PRP should:

- Explain the risk management working structure.
- Define an approach to identify, analyze, mitigate, and monitor risks, issues and opportunities 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 PRP, 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. Other context for risk identification and management can be found in Section 5 Design Considerations. Three specific examples of risk context are HSI, ESOH and program protection. Section 5.9 addresses HSI. Section 5.23.1 addresses ESOH and contains information regarding ESOH-related risk management. Section 5.24 addresses SSE and contains information on identifying and managing program protection risks in the design process. The associated DoDI 8510.01 establishes processes for ensuring confidentiality, integrity and availability for DoD IT programs. Programs should consider these specialized risk processes when creating their program risk process.

For additional information on managing risks, issues and opportunities, see the Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs available on the DDRE(AC)/Engineering web site.

Risk Management

Risks are potential future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance. They are defined by:

- The undesired event and/or condition
- The probability of an undesired event or condition occurring
- The consequences, or impact, of the undesired event, should it occur

Risk planning identifies risks and develops a strategy to mitigate those risks. The risk assessment will help determine where to enter in the life cycle. Whatever the entry point, the solution has to be adequately matured as risks are retired throughout the program's acquisition life cycle.

If technology maturity, manufacturing process maturity, or requirements stability risks exist, the PM should structure a program to enter the life cycle early in the development pathway to conduct technology maturation and risk reduction. Examples of risk reduction activities include:

- Building and testing competitive prototypes in order to validate achievability of the requirements and demonstrating the ability to integrate new technologies into mature architectures.
- Planning knowledge points to converge on results of SE trade-off analysis, which balance cost (affordability), schedule and performance requirements.
- Proposing design to account for complexities of program interdependencies and interfaces.
- Identifying and assessing materials and manufacturing processes the program will require.
- Performing technical reviews through preliminary design to assess problematic requirements and risks that may prevent meeting operational requirements and cost/affordability targets.

If technologies are mature, the integration of components has been demonstrated, and the requirements are stable and achievable, the PM can consider entering directly at system development with acceptable risk. Examples of system development risk reduction activities include:

- Performing technical reviews to finalize the design and verification testing to confirm it meets requirements.
- Performing MRAs to confirm the ability to produce the product.
- Performing development testing, which concentrates early testing on risks so there is adequate time for necessary re-design and re-test.

- Establishing and managing size, weight, power and cooling performance and R&M allocations for all subsystems.

If a materiel solution already exists and requires only military modification or orientation, the PM can structure the program to enter at Milestone C with a small research and development effort to militarize the product. Developmental testing should demonstrate the ability to meet requirements with a stable design. Example production phase risk reduction activities include:

- Conducting a thorough PCA and MRA to verify production does not introduce new risks.
- Identifying and assessing delivery schedule dependencies with external programs/users.
- Addressing risk associated with adapting the product to military needs, follow-on increments, or deferred activities.
- Identifying sustaining engineering needs and design considerations impacts, and funding as appropriate.

Activities and Products

The Risk Management Process encompasses five significant activities: planning, identification, analysis, mitigation and monitoring. PMs are encouraged to apply the fundamentals of the activities presented here to improve the management of their programs. Table 4-3 describes an overview of the focus of each activity and the products that are generally produced from the activity.

Table 4-3. Risk Management Process Activities

Activity	Answers the Question	Products
Risk Planning	*What is the program's risk management process?*	• Program Risk Process • Likelihood and consequence criteria • Risk tools • Tailored program risk training material
Risk Identification	*What can go wrong? Are there emerging risks based on Technical Performance Measure trends or updates?*	• List of potential risk statements in an "If…, then…" construct
Risk Analysis	*What is the likelihood of the undesirable event occurring and the severity of the consequences?*	• Quantified likelihood and consequence ratings, should the risk be realized • Approved risks entered and tracked in a risk register

Activity	Answers the Question	Products
Risk Mitigation	*Should the risk be accepted, avoided, transferred, or controlled? (Various terms are used to describe "Risk Mitigation" including Risk Treatment or Risk Handling.)*	• Acquisition Strategy and Systems Engineering Plan with mitigation activities • Activities entered into Integrated Master Schedule • Burn-down plan with metrics identified to track progress
Risk Monitoring	*How has the risk changed?*	• Status updates of mitigation activities to burn-down plan • Risk register updates • Closure of mitigated risks

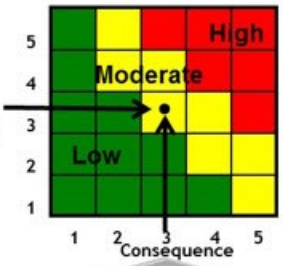
The planning process documents the activities to implement the risk management process. It should address the program's risk management organization (e.g., RMBs and working groups, frequency of meetings and members, etc.), assumptions and use of any risk management tools. The program should address risk training, culture, processes and tools.

Risk identification involves examining the program to identify risks and associated cause(s) that may have negative consequences. While various formal or informal methods can be used to identify risk, all personnel should be encouraged to do so.

Risk statements should contain two elements: the potential event and the associated consequences. If known, the risk statement should include a third element: an existing contributing circumstance (cause) of the risk. If not known, it is a best practice to conduct a root cause analysis. Risk statements should be written to define the potential event that could adversely affect the ability of the program to meet objectives. Using a structured approach for specifying and communicating risk precludes vague and/or inconsistent risk statements. An example method includes a two-part statement in the "if–then" format. See the Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs available on the DDRE(AC)/Engineering web site.

Risk analysis estimates the likelihood of the risk event occurring, coupled with the possible cost, schedule and performance consequences (if the risk is realized) in terms of impact to the program. Risk consequence is measured as a deviation against the program's performance, schedule or cost baseline and should be tailored for the program. PMs should consider the program's performance, schedule and cost thresholds and use these thresholds to set meaningful consequence criteria tailored to their program. Approved risks should then be entered into a risk register and a risk reporting matrix, as shown in Figure 4-9.

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%



Level	Cost			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance/Sustainment		
5	Major impact. 10% or greater increase over APB threshold; or >SD. Management reserve depleted.	Major impact. Budget or unit production cost (e.g., APUC) increasing to a significant Nunn-McCurdy breach, or increase of more than $XX in programmed dollars (POM)	Costs exceed life cycle ownership cost by 10%. Ability to sustain system in jeopardy.	Schedule slip that requires a major schedule re-baselining; precludes program from meeting its APB schedule objectives by more than 6 months; negative float to program completion	Severe degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success; design or supportability margins exceeded; unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4	Significant impact. 5% -<10% increase over APB threshold; or SC-≤SD. Requires use of significant management reserves.	Significant impact. Costs that drive a unit production cost (e.g., APUC) increasing to an APB threshold breach of $C - ≤ $D, or increase of $YY-XX in programmed dollars (POM)	Costs drive increase of more than 2% over program's lifecycle cost estimate, costs drive program to exceed life cycle ownership cost KSA	Significantly impacts ability to meet planned milestones and/or other key dates. Established acquisition decision points or milestones will be delayed, impacting APB schedule objectives by less than 6 months. Slip puts funding at risk; <5% float to major milestones or program completion	Significant degradation impairs ability to meet a KSA; Technical design or supportability margin exhausted in key areas; able to meet one or more mission tasks (defined in mission threads, ConOps, OMS/MP); workarounds required to meet mission objectives
3	Moderate impact. 3% -<5% increase over APB threshold; or $B - ≤ $C, manageable with reserves; inability to meet key cost metrics	Moderate impact. Costs that drive unit production cost (e.g., APUC) increase of $B - ≤ $C, or $ZZ-YY in programmed dollars (POM); inability to meet key cost metrics	Costs drive increase of y - z% over program's lifecycle cost estimate or within 2% of life cycle ownership cost KSA; inability to meet key cost metrics	Minor schedule slip, able to meet key milestones. Total program float decreased by X-Y% with float remaining positive, but nearly consumed; <10% float to major milestones or program completion; inability to meet key schedule metrics	Moderate reduction in technical performance or supportability; unable to meet lower tier attributes (e.g. PAs); planned design or supportability margins reduced; inability to meet key TPMs, CTPs; Workarounds required to achieve mission tasks (defined in mission threads, ConOps, OMS/MP)
2	Minor impact. 1% - <3% increase over APB threshold; or $A- ≤ $B; exceeding cost metrics tripwires	Minor impact. Costs that drive unit production cost (e.g., APUC) increase of $A-≤ $B; or $AA-ZZ in programmed dollars (POM); exceeding cost metrics tripwires	Costs drive increase of x- y% over program's lifecycle cost estimate, exceeding cost metrics tripwires	Able to meet key dates. Total program float decreased by less than X%, with 10% or greater positive float remaining.; exceeding schedule metrics tripwires	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program objectives. Design margins will be reduced, but within limits / tradespace; exceeding key TPMs, CTPs tripwires
1	Minimal impact. <1% increase over APB threshold; or <$A. Costs expected to meet approved funding levels, not projected to increase above thresholds	Minimal impact. Costs that drive APUC increase of ≤ $A ; or less than $AA in programmed dollars (POM). Costs expected to meet approved funding levels, not projected to increase above thresholds	Costs drive increase of ≤lx% over program's lifecycle cost estimate.	Minimal or no schedule impact.	Minimal or no consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires.

Figure 4-9. Risk Reporting Matrix Example

After conducting a risk analysis, the PM should decide whether the risk should be accepted (and monitored), avoided, transferred or controlled. PMs should alert the next level of management when the ability to mitigate a high risk exceeds their authority or resources. Control seeks to reduce risk to an acceptable level in order to minimize potential program impacts. Risk control activities often reduce the likelihood of a risk event occurring, although consequences associated with a risk may be reduced if the program changes the design architecture or addresses binding constraints. Examples of top-level mitigation activities may include:

- System or subsystem competitive or risk reduction prototyping focused on burning down the most critical technical risks (e.g., technology, engineering, and integration).
- Deferring capability to a follow-on increment.
- Establishing events that increase knowledge of whether risks are successfully being abated.
- Limiting the number of critical technologies.
- Developing a realistic program schedule that is "event-" versus "schedule-" driven.
- Identifying off-ramps (i.e., a contingency plan to use mature technology in case technology is not developed successfully to meet critical program performance or schedule) for selected technologies in the IMS.
- Conducting SE trade-off analyses leading up to preliminary design to support finalization of achievable requirements.

After the PM approves the mitigation strategy, the program should systematically track and evaluate the performance of risk mitigation plans against risk burn-down plans as well as assess performance achievement through associated TPMs. The PM should update leaders with the current risk status at least quarterly, before major reviews and whenever there are significant changes.

Programs should integrate risk management with other program management tools. Risk mitigation activities should include assigned resources reflected in the IMP, IMS, and earned value management (EVM) baselines. Programs should use appropriate TPMs and TPMMs to aid in monitoring the progress of mitigation plans.

Managing Cross Program Risks

Internal and external interfaces are significant sources of risk. Interdependent programs may have disconnects regarding resources; hardware and software development schedules; space, weight, power and cooling requirements; immature technologies; testing results; or other areas. Interdependent programs should have a process to manage interfaces and integration risks jointly, share information, and foster a mutually supportive environment.

The following actions aid in managing activities when deploying a new system that depends on programs outside the PEO's portfolio or from another Service:

- CAEs act as or appoint a technical authority within the Service(s) or OSD, who can influence critical interfaces with external programs.
- Develop MOAs between PMs and PEOs to identify and manage critical interfaces.
- Set up an Interface Control Working Group (ICWG) to identify and resolve interface issues.
- Develop and maintain a synchronized schedule.
- Develop an integration plan that tracks interdependent program touch points, identifies risks and institutes a plan to mitigate them.

Issue Management

Issues are unwanted events or conditions with negative effects that have occurred or are certain to occur (probability of one) in the future. Whereas risk management applies resources to lessen the likelihood and/or the consequence of a future event, issue management applies resources to mitigate consequences associated with a realized risk. As risks increase in probability, programs should anticipate their realization, as issues with early plans developed to limit the consequences.

The consequence of an issue should be addressed to prevent impeding program progress. Programs can take advantage of similar practices for identifying, analyzing, mitigating, and monitoring both risks and issues. Programs may evaluate whether a separate issue specific board

is necessary or whether issue management may be executed more effectively and efficiently along with the RMB.

Issue Management encompasses five significant activities as outlined in Table 4-4.

Table 4-4. Issue Management Process Activities

Activity	Answers the Question	Products
Issue Planning	*What is the program's issue management process?*	• Issue management process • Issue management plan
Issue Identification	*What has or will go wrong?*	• Statements of the problems
Issue Analysis	*What is the consequence of the issue?*	• Cost, schedule and performance impacts on the program quantified • Issues entered and tracked in an issue register
Issue Mitigation	*Should the issue be ignored or controlled?*	• Approved courses of action (COA) to address the issue • Activities entered into Integrated Master Schedule • Metrics identified to track progress
Issue Monitoring	*Has the issue changed?*	• Status updates of COA activities • Issue tracking sheet updated • Closure of issue

Approved issues should be analyzed using the program's risk management consequence criteria, and the results entered into an issue tracking register. Unlike risks, no evaluation of issue likelihood is necessary. Issues should be reported in a matrix as in Figure 4-10.

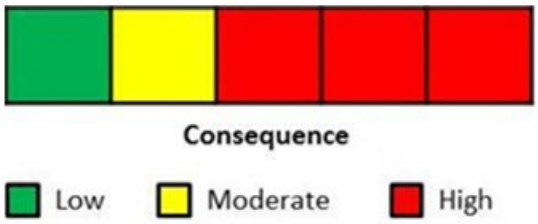


Figure 4-10. Issue Reporting Matrix

The issue management approach should identify problems, assess the severity and urgency of their possible impact on the program and develop associated closure plans. PMs, Systems Engineers, and Lead Software Engineers should develop a course of action, similar to that described in Section 4.1.5 Risk Management, to address and manage program issues with resourced action plans, as appropriate. Mitigation options include ignoring the issue, accepting the consequences without further action based on the results of a cost/schedule/performance business case analysis and controlling the issue by implementing a plan to reduce issue

consequences. Issues should be reviewed during the program office and contractor's regularly scheduled meetings. As with risks, mitigation activities should be included in the program IMS and the tracking register.

Opportunity Management

An opportunity is a potential future benefit to the program's cost, schedule, and/or performance baseline. PMs, Systems Engineers, and Lead Software Engineers should use opportunity management to identify, analyze, manage, and monitor initiatives that can capture these opportunities and achieve should-cost goals.

Opportunity management encompasses the activities as outlined in Table 4-5.

Table 4-5. Opportunity Management Process Activities

Activity	Answers the Question	Products
Opportunity Planning	*What is the program's opportunity management process?*	• Opportunity management process • Opportunity management plan
Opportunity Identification	*What can be improved?*	• Statements of the opportunity
Opportunity Analysis	*What is the business case analysis of the opportunity?*	• Benefits quantified in terms of cost, schedule and performance • Cost and likelihood to achieve benefit understood • Cost-benefit analysis report • Opportunity entered into register
Opportunity Management	*Should the opportunity be pursued, reevaluated or rejected?*	• Allocated resources to pursue opportunity • Activities entered into Integrated Master Schedule • Metrics identified to track progress
Opportunity Monitoring	*How has the opportunity changed?*	• Status updates of management activities • Opportunity tracking sheet updated • Closure of opportunity

Once a capture plan is approved, the program should assign an owner and track it in an opportunity register. The engineering team usually leads or assists with a cost, schedule and performance business case analysis for each potential opportunity. Opportunities with sufficient potential should be evaluated relative to the potential management options of pursue, defer to reevaluate or reject. Programs can also plan parallel on-ramps for research and development activities that might provide opportunities.

The business case analysis should address the potential benefit as well as the resources required and likelihood of achieving the benefit. Management activities should be included in the register and inserted into the program IMS in order to track progress to plan. Once in place, the program office should monitor the plan by collecting actual cost versus planned cost, schedule, performance and benefit information. The potential changes in the opportunity status are tracked, as in Figure 4-11 and management plans adjusted as required.

Opportunity	Likeli-hood	Cost to Implement	Return on Investment					Program Priority	Management Strategy	Owner	Expected Closure
			Monetary			Schedule	Performance				
			RDT&E	Procurement	O&M						
Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades.	Mod	$3.2M			$4M	3 month margin	4% greater lift	#2	Reevaluate - Summarize the mitigation plan	Mr. Bill Smith	March 2017
Opportunity 2: Open Architecture Cockpit	Mod	$2.2M		$8.2M	$6M			#3	Defer	Ms Dana Jones	May 2017
Opportunity 3: Cheaper composite mounting plates	High	$211K		$0.4M	$3.6M	4 months less long-lead time needed	15 lbs less weight	#1	Summarize the mitigation plan to realize the opportunity	Ms. Kim Johnson	January 2017

Figure 4-11. Opportunity Tracking Matrix Example

4.1.6 Configuration Management Process

The Configuration Management 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 configuration management 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.

Configuration Management 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.

Configuration Management facilitates the orderly development of a system through establishment of the technical baseline (including the functional, allocated and product baselines), and their assessment and approval 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 Configuration Management, 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 Configuration Management:

- 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. 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 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 (configuration items (CI) 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 operations and support. 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. 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. In accordance with DoDI 5000.88, the PM will assume 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 select 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 design documentation to system and 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 Configuration Management 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 and should ensure adequate resources are allocated for implementing Configuration Management throughout the life cycle. The PM assesses the impact of proposed changes to a baseline, approves changes – usually through a CCB (see MIL-HDBK-61 (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 Configuration Management planning is complete, and should document details and activities in the program's SEP and the supporting Configuration Management Plan (CMP) (as appropriate). The PM, with the support of the Systems Engineer, ensures that the configuration management approach is consistent with the Intellectual Property Strategy (See Section 4.1.7 Technical Data Management Process). The CM process described in the DoD-adopted standard American National Standards Institute/Electronic Industry Association (ANSI/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 DoD-adopted standard EIA-649-1, Configuration Management Requirements for Defense Contracts, implements the principles outlined in ANSI/EIA-649B 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 configuration management processes to be used by system suppliers, developers, integrators, maintainers and sustainers.

4.1.7 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 5.24 System Security Engineering for

information regarding protection of 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 Military Standard (MIL-STD)-31000, for acquisition, upgrades, and management of technical data provide:

- Information necessary to understand and evaluate system designs throughout the life cycle.
- Ability to operate and sustain systems under a variety of changing technical, operational, and programmatic environments.
- Ability to re-compete item acquisition, upgrades, and sustainment activities in the interest of achieving cost savings; the lack of technical data and/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 Lead 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 4-12 shows the activities associated with Technical Data Management, including:

- Identify Data Requirements
    - Formulate the program's Intellectual Property Strategy and technical data management approach, with an emphasis on technical and product data needed to provide support throughout the acquisition life cycle (see PM Guidebooks (forthcoming) for more information about Data Rights).
    - 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 during Operations and Support (O&S); and submitted before award of the contract for the next life cycle phase.
    - Special attention needs to be given to acquire or access 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 AoAs, 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 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 Data Item Descriptions (DID) and CDRL 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 modular open systems approaches 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 2.2.5 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 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.

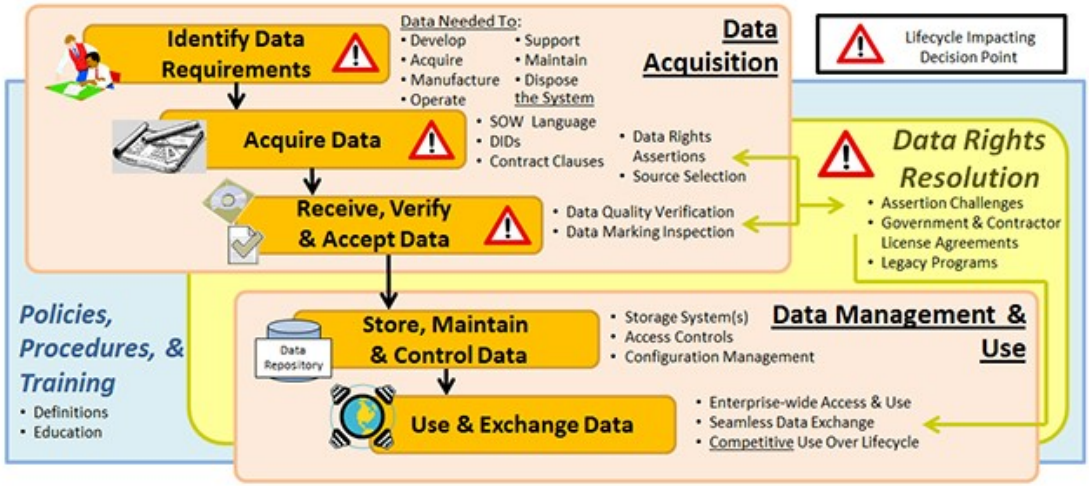


Figure 4-12. Data Management Activities

In support of the Government's requirement for a TDP, the PM should also consider all 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, etc.). Figure 4-13 provides a notional representation of different types of product-related data.

Caution: *PMs, Systems Engineers, and Lead 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 5010.12-M, Procedures for the Acquisition and Management of Technical Data
- Army Data and Data Right (D&DR) Guide
- Army Regulation 25-1 Army Information Technology
- Army Pamphlet 25-1-1 Army Information Technology Implementation Instructions
- Air Force Product Data Acquisition (PDAQ) guidance (following link requires an Air Force portal account)
- Air Force Technical Data and Computer Software Rights Handbook
- 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)

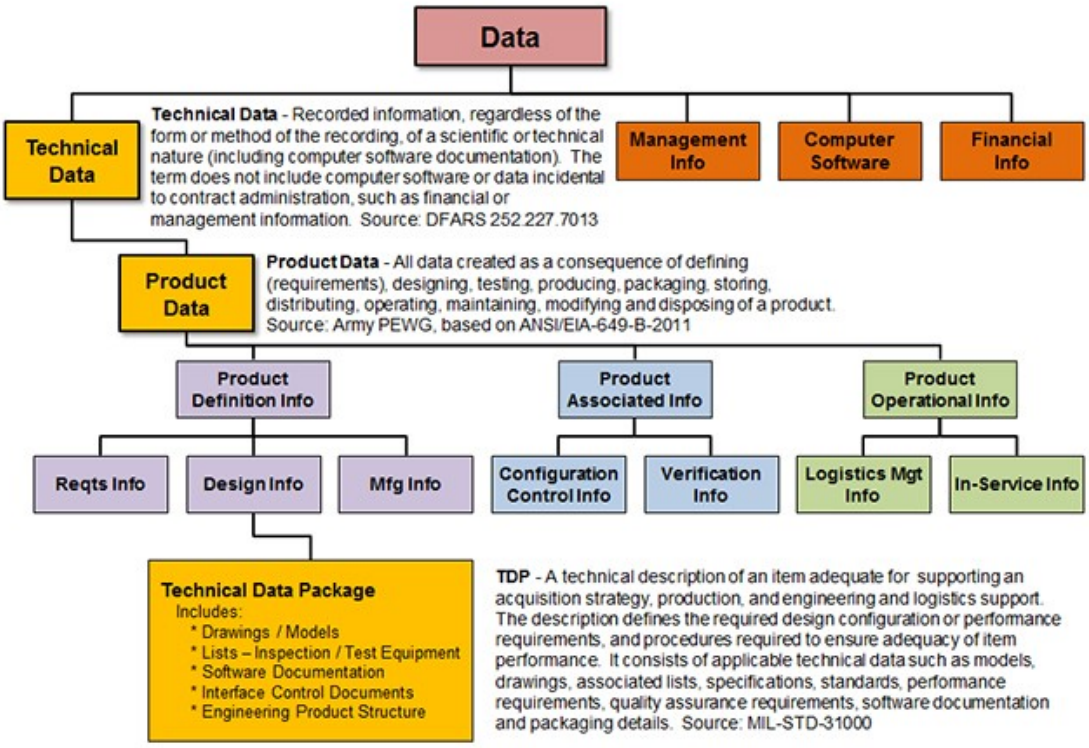


Figure 4-13. Data Taxonomy

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

- DoDD 5230.25
- DoDI 5230.24
- DoDM 5400.07
- DoDI 5200.01

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 (SEC 208 para (b)) and DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance" requires that PIA be conducted before developing or purchasing any DoD information system that collects, maintains, uses or disseminates personally identifiable information about members of the public, federal personnel, DoD 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.

4.1.8 Interface Management Process

The Interface Management process provides a framework to identify, define, manage and ensure compliance with internal and external system interfaces. The Interface Management process helps ensure that developers capture all internal and external interface requirements and requirements changes in accordance with the program's Configuration Management Plan. 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 systems of systems 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 requirement specifications (IRS) and related Interface Control Documents published by DoD organizations gives the Government ownership control of that interface without any corporate licenses needed. This allows the PM, Systems Engineer, and Lead Software Engineer to conduct normal system life cycle updates without breaking interoperability with other systems while successfully executing a MOSA. Managing interfaces as separate configuration management items allows the PM enterprise re-use 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 DoD Architecture Framework (DoDAF) provides guidance on how to generate operational and system views that describe interface relationships in a manner common across the DoD 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 Lead Software Engineer should ensure that the program's interface management plan:

- Documents the system's internal and external interfaces and their requirement specifications.
- Identifies preferred and discretionary interface standards and their profiles.
- 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 configuration management plan.

The PM, Systems Engineer, and Lead Software Engineer should ensure that the developer documents all system interface requirements (see Section 4.1.4 Requirements Management Process), places them under appropriate levels of configuration management 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 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.

4.2 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 4.2.1 through 4.2.8 provide a framework for ensuring and maintaining traceability between stakeholder requirements, systems design and the eventual delivered capability.

4.2.1 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 perform an exhaustive Stakeholder Requirements Definition process could result in significant requirements creep, rework because of misunderstanding of end-user needs, unexpected contract modifications, cost growth and schedule slip. 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, described in the JCIDS CJCSI 5123.01, and the acquisition of a materiel solution, governed by the Defense Acquisition System.

The Stakeholder Requirements Definition process complements Requirements Analysis and Architecture Design (see Section 4.2.2 Requirements Analysis Process and Section 4.2.3 Architecture Design Process, respectively). 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 Lead 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., KSAs; Knowledge, Skills, Abilities and other attributes of personnel), performance parameters and constraints documented in JCIDS documents.

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

- 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 (i.e., mission analysis).
  - 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.

The authoritative source for stakeholder requirements are documents produced via the JCIDS such as the ICD and the CDD. JCIDS analyzes gaps in existing and/or future warfighting operations and provides a process that allows the Joint Requirements Oversight Council to balance joint equities and make informed decisions on validation and prioritization of capability needs.

4.2.2 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 4.2.1 Stakeholder Requirements Definition Process) into clear, achievable and verifiable requirements. As the system design evolves, Requirements Analysis 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:

- Linking the needs of the end users to the system, system elements and enabling system elements to be designed and developed.

- Defining a system that meets end-users' operational mission requirements within specified cost and schedule constraints.
- Providing 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 5 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/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 Section 4.2.6 Verification Process and Section 4.2.7 Validation Process, respectively). Good requirements have the following attributes:

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

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. Requirements Analysis 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 Configuration Management process (see Section 4.1.4 Requirements Management Process and Section 4.1.6 Configuration Management Process, respectively).

4.2.3 Architecture Design Process

The Architecture Design process is a trade and synthesis method to allow the PM, Systems Engineer, and Lead Software Engineer to translate the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions and establishes the architectural design of candidate solutions that may be found in a system model. 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.

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 systems engineering (SE, SSE) and conform to industry standards 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 should be placed under configuration control and maintained in a robust repository that maintains the architecture descriptions and its relationships to each of the baselines. This control provides the Systems Engineer with a means of ensuring consistency of the system architecture definition throughout the acquisition life cycle.

The functional architecture provides the foundation for defining the system architecture through the allocation of functions and sub-functions to hardware/software, databases, facilities and human operations to achieve its mission. The physical architecture consists of one or more product structures, or views, of the physical solution. The product structure may consist of conceptual design drawings, schematics and/or block diagrams that define the system's form and the arrangement of the system elements and associated interfaces.

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). It is critical that this process identify the design drivers and driving requirements as early as possible.

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:

- Analyzing and synthesizing the physical architecture and appropriate allocation.
- Analyzing constraint requirements.
- Identifying and defining physical interfaces and system elements.

- Identifying and defining critical attributes of the physical system elements, including design budgets (e.g., weight, reliability) and open system principles.

During this process, derived requirements come from solution decisions. It is essential to identify derived requirements and ensure that they are traceable and part of the allocated requirements. For each given solution alternative, the Decision Analysis process trades off requirements against given 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 documentation that describes the physical architecture of the system and the specifications that describe the functional and performance requirements for each configuration item, along with the interfaces that compose the system. In addition, WBS and other technical planning documentation are updated. The system architecture and the resulting design documentation 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 should be able to be communicated to the customers and to the design engineers and testers. 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 configuration management.

4.2.4 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/production procedures of forming, joining and finishing, or coding for software. Depending on technology maturity, the Implementation process may 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 Integration, Verification, and Validation. 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

Implementation begins in the Materiel Solution Analysis (MSA) phase, where the AoA informs whether the preferred materiel solution can be developed, bought or reused. This analysis takes many forms, such as the use of models, simulations, experiments and prototypes through which competing systems can be assessed. Careful decisions regarding the design of system elements can enable the use of open (non-proprietary) 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:

- Identifying and analyzing the constraints that the technology and design and realization techniques and approaches impose on the design solution.
- Developing design and implementation prototypes and solutions for the system elements.
- Analyzing candidate system element design and implementation solutions and conducting variability studies to identify conflicts and resolution alternatives to ensure system integrity.
- Identifying fabrication and quality procedures, and documenting design assumptions and decisions in the final system elements drawings or TDPs.
- Identifying 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:

- Obtaining or acquiring access to materials and tools required to build system elements.
- Obtaining external system elements as applicable.
- Building system elements in accordance with implementation procedures, tolerances and applicable HSI and ESOH, security, and privacy.
- Determining system elements functionality against specified product quality characteristics.
- Document production and quality issues and associated corrective actions.
- Delivering implemented system elements for integration and verification.

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

4.2.5 Integration Process

The Integration process provides a framework to systematically assemble lower-level system elements into successively higher-level system elements, iterative 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.

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 Systems Integration Laboratories or other facilities, personnel, test stands, harnesses, testing software, and integration schedule.

The Interface Management process 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 and/or interfaces establish MOAs in order to formally establish 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 verification and validation.

4.2.6 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, thereby preventing costly troubleshooting and rework.

The PM, Systems Engineer, and Lead Software Engineer, in coordination with the Chief Developmental Tester, manage verification activities and methods as defined in the functional and allocated baselines and review the results of verification. Guidance for managing and coordinating integrated testing activities can be found in the T&E Enterprise Guidebook (forthcoming) and in DoDI 5000.89.

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 (i.e., 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/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.

Verify designs at all levels of the physical architecture through a cost-effective combination of these methods, all of which can be aided by modeling and simulation.

Document verification activities and results among the artifacts for FCAs and the SVR (see Section 3.6 System Verification Review/Functional Configuration Audit). When possible, verification should stress the system, or system elements, under realistic conditions representative of its intended use.

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

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

4.2.7 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 Lead 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 (forthcoming)). 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 (forthcoming) and DoDI 5000.89. Using and engaging integrated test teams composed of knowledgeable and experienced Government and industry developmental and operational testers 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. 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 4.2.6 Verification Process). 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.

4.2.8 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 system's 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 Transition 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 its enabling system elements, as well as a process for reporting and resolving deficiencies. Sustainment and support planning be documented in the LCSP, which is required for all acquisition programs and reviewed before Milestones A, B, and C, as well as the 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 (i.e., drawings, tech manuals, etc.), have been received from the contractor and made available to the activity responsible for sustaining the system through disposal.

5 DESIGN CONSIDERATIONS

The PM, Systems Engineer, and Lead 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.
- Incorporate design considerations into the set of system requirements, as some are mandated by laws, regulations, or treaties, while others are mandated by the domain or DoD Component or Agency; these mandates should be incorporated during the Requirements Analysis process to achieve balance across all system requirements.

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. The PM, Systems Engineer, and Lead Software Engineer should show evidence of critical thinking in addressing the design considerations, as documented in the program SEP. According to the SEP Outline, the SEP should include a table of design considerations that are critical 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 Lead Software Engineer should consider them in conjunction with one another, as early as the AoA, to achieve better mission performance and to preclude a stovepipe view during design.

Table 5-1 lists the statutory requirements for the design considerations covered in this chapter, as well as applicable policy and guidance related to those design considerations. PMs and Systems Engineers can incorporate the standards into acquisition contracts to support delivery of required operational capability. The supplemental guidance 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.

Table 5-1. Design Considerations

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance
Accessibility (Section 508 Compliance)	**5.1**	• Section 508 of the Rehabilitation Act (i.e., 29 U.S.C. 794d)	• DoDD 8000.01 • DoDI 5000.82 • DoD 8400.01-M • FAR 39.204
Affordability - SE Trade-Off Analysis	**5.2**		• DoDI 5000.02 • DoDI 5000.85 • DoDI 5000.88
Anti-Counterfeiting	**5.3**	• P.L. 112-81 (SEC 818)	• DoDI 5000.85, Appendix 3D.2 • DoDI 4140.67 • SD-19
Commercial-Off-the-Shelf (COTS)	**5.4**	• 41 USC 104 and 1907 • P.L. 103-355 (SEC 8104) • P.L. 104-106 (SEC 357)	• SD-2
Corrosion Prevention and Control (CPC)	**5.5**	• 10 USC 2228	• DoDD 5000.01, paragraph 1.2.r. • DoDI 5000.85, Appendix 3D.2. • DoDI 5000.88, paragraph 3.7.c. • DoDI 5000.67 • DoD Corrosion Prevention and Control Planning Guidebook • DFARS 223.73
Critical Safety Item (CSI)	**5.6**	• P.L. 108-136 (SEC 802) • P.L. 109-364 (SEC 130) • 10 USC 2319	• DoDM 4140.01, Volume 11 • JACG Aviation CSI Management Handbook • SECNAVINST 4140.2 • AFI 20-106 • DA Pam 95-9 • DLAI 3200.4 • DCMA INST CSI (AV) Management of Aviation CSIs • DFARS 209.270, 246.407, 246.504, 246.371 and 252.246-7003
Demilitarization and Disposal	**5.7**		• DoDI 4160.28 • DoDM 4160.28 • DoDM 4140.01, Encl. 6 • DoDM 4160.21, Volume 1

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance
Diminishing Manufacturing Sources and Material Shortages (DMSMS)	**5.8**		• SD-22 • SD-19 • SD-26 • DoDI 4245 .15 • DoDI 5000.85 • DoDI 4140.01 • DoDM 4140.01, Volume 3
Human Systems Integration (HSI)	**5.9**		• DoDD 5000.01, paragraph 1.2.p. • DoDD 5000.02T/DoDI 5000.PR (forthcoming) • DoDI 5000.88 • HSI Guidebook (forthcoming) • MIL-STD 46855 • MIL-STD-1472
Insensitive Munitions	**510**	• 10 USC 2389	• DoDD 6055.09E • Secretary of Defense Memorandum, "DoD Policy on Submunition Reliability," January 10, 2001 • USD(AT&L) Memorandum, "Joint Insensitive Munitions Test Standards and Compliance Assessment," February 10, 2010 • USD(AT&L) Memorandum, "Insensitive Munitions Strategic Plans," July 21, 2004 • DoD Acquisition Manager's Handbook for Insensitive Munitions, Revision 02, November 2008
Intelligence (Life Cycle Mission Data Plan (LMDP))	**511**		• DoDD 5250.01 • DoDI 5000.85 • AAFDIT
Interoperability and Dependency (I&D)	**5.12**	• 44 USC 3506	• DoDI 8330.01 • DoDD 5000.01 • DoDI 2010.06 • DoDI 5000.02 • CJCSI 5123.01 • JCIDS Manual

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance
Item Unique Identification (IUID)	**5.13**		• DoDI 8320.03 • DoDI 4151.19 • DoDI 5000.88 • DoDI 5000.02 • DoDI 5000.64 • DoDI 8320.04 • DoD Guide to Uniquely Identifying Items, Version 2.5, September 15, 2012 • DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements, April 20, 2007 • DFARS 211.274-2, 252.211-7003, 252.211-7007
Manufacturing and Quality	**5.14**	• P.L. 111-383 (SEC 812)	• DoDI 5000.88 • DFARS 207.105, 215.304 • SD-19
Modular Design	**5.15**	• 10 USC 2430	• DoDI 5000.02 • DoDI 5000.88 • DoD 5010.12-M
Operational Energy	**5.16**	• 10 USC 138c	• CJCSI 5123.01 • JCIDS Manual
Packaging, Handling, Storage, and Transportation (PHS&T)	**5.17**	• 49 CFR Parts 171-180	• DoDI 4540.07 • DoD 4145.19-R • DoD 4140.27-M • DTR 4500.9-R
Reliability and Maintainability (R&M) Engineering	**5.18**		• DoDI 5000.88 • DoD R&M Engineering Management Body of Knowledge • RAM-C Rationale Report Outline Guidance • RAM-C Rationale Report Outline Guidance Training • Guidance for the Tailoring of R&M Engineering Data • SD-19

Design Consideration	Section Number	Statutory Requirement	Policy & Guidance
Spectrum Management	**5.19**	• 47 USC 305 • 47 USC 901 - 904 • P.L. 102-538 (SEC 104)	• DoDI 3222.03 • DoDI 4650.01 • DoDI 5000.02 • DoDI 5000.88 • AR 5-12 • AFI 33-118 • SECNAVINST 2400.1 and 2400.2 • OPNAVINST 2400.20
Standardization	**5.20**	• 10 USC 2451-2457 • P.L. 82-436	• DoDI 4120.24 • DoDM 4120.24 • SD-19
Supportability	**5.21**		• DoDD 5000.01 • DoDI 5000.02 • DoDI 5000.88 • DoDI 4151.22 • DoD 4151.22-M • SD-19 • MIL-HDBK-502 • SD-22
Survivability (including CBRN)	**5.22**	• P.L. 108-375 (SEC 1053)	• DoDI 3150.09 • DoDI 5000.02 • DoDI 5000.89
System Safety (including Environment and Occupational Health (ESOH))	**5.23**	• 42 USC 4321 • EO 12114	• DoDD 5000.01 • DoDI 5000.02 • DoDI 5000.02T • DoDI 5000.85, • DoDI 5000.88 • DoDD 5137.02 • DoDD 4715.21 • DFARS 223.73 • MIL-STD 882 • FAR 23.2, 23.4, 23.7 and 23.8 • JSSSEHB
System Security Engineering (SSE)	**5.24**	• 10 USC 2358	• DoDI 5000.02 • DoDI 5000.83 • DoDI 5200.39 • DoDI 5200.44 • DoDI 8582.01 • Program Protection Plan Outline and Guidance, Version 1.0, July 2011 • DoD Cyber T&E Guidebook, Version 3

5.1 Accessibility (Section 508 Compliance)

All Electronic and Information Technology (E&IT) systems comply with Section 508 of the Rehabilitation Act (i.e., 29 U.S.C. 794d), unless exempt under FAR (Subpart 39.204, para (b)) 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.

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 5-2. Additional information on accessibility is found in DoDI 5000.82 and DoDI 5000.PR, Human Systems Integration in Defense Acquisition (forthcoming).

Table 5-2. Links to Section 508 Government Resources

Description of Link	Active Link
Section 508 technical standards	http://www.access-board.gov/508.htm
Federal rules for Section 508 implementation hosted by General Services Administration(GSA) has: • 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: • Check lists • 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/

5.2 Affordability – Systems Engineering Trade-Off Analyses

Affordability is the degree to which the capability benefits are worth the system's TOC and support DoD strategic goals. SE trade-off analyses for affordability, a special application of the Decision Analysis process (see Section 4.1.2), should:

- Support the establishment of realistic affordability caps as documented in the program's APB.
- 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.

The PM, Systems Engineer, and Lead Software Engineer use the results of SE trade-off analyses for affordability to inform system requirements and ensure that, when taken collectively, the requirements are compelling, affordable, and achievable within the time frame available to the program.

The SE trade-off analyses are executed by a resourced team that consists of a decision maker with full responsibility, authority, and accountability for the trade at hand; a trade-off analyst with a suite of reasoning tools; SMEs with performance models; and a representative set of end users and other stakeholders.

Throughout the system life cycle, the Systems Engineer continuously monitors affordability drivers, identifies opportunities to reduce life cycle costs, and conducts SE trade-off analyses as needed to meet program cost, schedule, and performance requirements.

5.3 Anti-Counterfeiting

An increasing threat of counterfeit (and fraudulent) parts in the global marketplace affects 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 DoD weapon and information systems acquisition and sustainment to prevent the introduction of counterfeit materiel.

Counterfeit parts are becoming 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 5-3.

Table 5-3. 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. (National Institute of Standards and Technology (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	Manufacturing and Quality 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.

Design Consideration	Relationship
Reliability and Maintainability Engineering	Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the "honest" 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 critical program information and mission-critical functions and components (see T&PP Guidebook (forthcoming)).

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

5.4 Commercial-Off-the-Shelf

The use of COTS items, including Non-Developmental Items (NDI), 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 Lead Software Engineer still develop, integrate, test, evaluate, deliver, sustain, and manage the overall system.

Among 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 solution to determine design considerations' impacts and communicate any associated risks to the PM.
    - Example: The graphical user interface design may not completely support user tasks or the Target Audience Description, 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 (SEC 8104) and P.L. 104-106 (SEC 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 Lead 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 (forthcoming)).
- 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 DoD 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 configuration management, and the features and functions of upgrades and changes.
- Ability to instrument or test aspects of COTS products.

5.5 Corrosion Prevention and Control

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

Sound corrosion prevention and control (CPC) planning reduces life cycle costs, improves maintainability and availability, and enhances ESOH compliance. The DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment (MS&E) (i.e., CPC Planning Guidebook) helps PMs, Systems Engineers, PSMs, and other program staff develop and execute a comprehensive CPC approach.

DoDI 5000.85, DoDI 5000.67 and DoDD 4151.18 require CPC planning and execution for all acquisition programs across the life cycle. In accordance with DoDI 5000.88, Section 3.7.c., the PM is responsible for identifying and evaluating corrosion considerations throughout the acquisition and sustainment phases to reduce, control, or mitigate corrosion. The PM, Systems Engineer, and Lead Software 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. DoDI 5000.PS (forthcoming) further integrates CPC planning into sustainment. Product support planning should mitigate the appropriate CPC risks inherent in the system design to meet sustainment 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 throughout the life cycle.
- Examining legacy systems for 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 (forthcoming)).
- 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 Acquisition Category (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
- Programmatic ESOH Evaluation (PESHE) (i.e., DFARS (Subpart 223.73, Minimizing the Use of Hexavalent Chromium))
- System finish/process specification (add to the SOW and as a Data Item Description (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 2.5 Systems Engineering Role in Contracting and the DoD Corrosion Prevention and Control Planning Guidebook for MS&E).

5.6 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 DoD 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 DoD 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 (SEC 802), enacted to address aviation CSIs, and P.L. 109-364 (SEC 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 DoD 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 issued the Aviation Critical Safety Items Management Handbook. This guidance establishes standard user-level operating practices for aviation CSIs across the Services, the Defense Logistics Agency (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. 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 Physical Configuration Audit (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.

5.7 Demilitarization and Disposal

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

- All DoD 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 DoD's liabilities, reduce costs, and protect CPI and technology. 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, and contract(s). For munitions programs, DEMIL and disposal documentation need to be in place before the start of Developmental Test and Evaluation.

DEMIL eliminates functional capabilities and inherent military design features from both serviceable and unserviceable DoD 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, DoD Demilitarization Program.

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 DoD and other U.S. Government agency needs. After assurances that Government needs for surplus DoD property are met, the materiel disposition process:

- Permits authorized transfer or donation to Government or non-Government entities.
- Obligates DoD 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 DoD 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 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.

5.8 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., indentured 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 to promote 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-3018 (Parts Management), 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 Contract Language Guidebook
- DoDI 5000.85 "Major Capability Acquisition"
- DoDI 4245.15, "Diminishing Manufacturing Sources and Material Shortages"
- DoDI 4140.01 "Supply Chain Material Management Policy"
- DoDM 4140.01, Volume 3 "DoD Supply Chain Materiel Management Procedures: Materiel Sourcing"

5.9 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 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.

DoDI 5000.02 describes planning considerations for seven HSI domains. DoDI 5000.02T, Change 7 (April 21, 2020), Enclosure 7 further states: "The PM will plan for and implement HSI beginning early in the acquisition process and throughout the product life cycle. The goal will be to optimize total system performance and TOC, while ensuring that the system is designed, operated, and maintained to effectively provide the user with the ability to complete their mission. PMs will ensure that the DoD Component HSI staff is aware of and engaged with WIPTs tasked with the development and review of program planning documents that reflect HSI and that they inform program decisions." The HSI Guidebook (forthcoming) 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 systems engineering and logistics. Execution of HSI activities should be tailored to the unique acquisition 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 HSI effort assists the 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.

The PM is responsible for integrating the HSI effort into the program (see HSI Guidebook (forthcoming)).

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 and Human Factors Engineering (HFE) stakeholders 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. HSI should also be addressed in the SEP, specifications, TEMP, SDP, LCSP, and other appropriate

program documentation. The SEP Outline requires that HSI be addressed as a design consideration.

Elements of an effective HSI program should (see HSI Guidebook (forthcoming)):

- Provide an optimized operational solution to the warfighters.
- Lead to the development or improvement of all human interfaces.
- Achieve required effectiveness of human performance during system testing, operation, maintenance, support, transport, demilitarization, and disposal.
- Provide HSI input to RFP effort and monitor contractor activities for human performance prototype engineering and testing at component- and system-levels where applicable (and allowable by contract).
- Ensure the demands upon personnel resources, skills, training, and costs are planned and accounted for at every stage in the system life cycle.
- Ensure that overall human performance is within the knowledge, skills, and abilities of the designated operators, maintainers, and users to support mission tasking.
- The SEP should emphasize that the human is an essential element of the system and that human requirements and issues will be addressed in the design. The SEP should establish an HSI IPT or working group within the SE element of the program office to ensure provisions for human performance and accommodation to satisfy system requirements. The SEP should also state that HSI is an inherent component of SE and describe the specific HSI objectives, issues, risks, milestones, activities, products, and schedules. Summarizing the HSI role, planning, risks, and activities in the SEP ensures that HSI receives the required level of visibility and inclusion in the overall SE processes.
- Consistent with the DoDI 5000.02T/DoDI 5000.PR (forthcoming), the SEP 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 systems engineering technical reviews.

In the conduct of systems engineering 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.

HSI domain experts should review the elements of the AoA devoted to HSI considerations (i.e., manpower, personnel, and training). In addition, HSI domain experts should ensure that the preferred solution considers the end user besides just the hardware and software components in the system. Defining the intended end user population through a TAD provides boundary conditions for defining the required human performance parameters.

The Systems Engineer should review HSI requirements and determine if they have been implemented in the system design. HSI requirements should be specified in both the ICD and draft CDD.

SI practitioners and domain-level SMEs (e.g., HFEs) involvement should ensure that the functional baseline is compliant with human factors design guidance, and standards. Human performance and end user requirements should be sufficiently detailed and understood to enable system design to proceed. System requirements should be allocated among hardware, software, and human functions. The HSIP and other related acquisition documents are updated as required.

- HSI design factors should be reviewed and included, where needed, in the overall system design up to this stage. HSI should ensure that safety analysis on Human Machine Interfaces (HMI) was conducted early in the system design, and training burdens are reduced by implementing user-centered design (UCD) methodologies. Software-related products are vetted with the target user population.

Some design decisions leading up to PDR may precipitate discussions with the operational requirements community and consultation with HSI practitioner because they could have an impact on the CDD, contributing to trade-off analyses. CDR determines whether the hardware, human, and software final detail designs are complete. HSI should ensure that the detailed design satisfied known HFE and other HSI requirements.

The HSI practitioner has access to many tools to support the PM and SE, including HSI simulation tools (e.g., for task network modeling or digital human modeling), guidelines and standards, checklists, subjective assessments, and other resources. Models and simulations provide a mechanism to define, visualize, and adjust parameters for human contribution to implementing a DE enterprise. Digital Human Modeling (DHM) provides a digital representation of a human (or set of humans) and a virtual environment that represents the system within which the user needs to fit, see, reach, or otherwise physically interact. Any HSI tool can be used to aid in the application of SE methods and complement the use of SE tools that ensure systems consider human limitations and capabilities across the spectrum of HSI domains, such as:

- Simulations of human-out-of-the-loop that create virtual elements of a future situation characterizing impacts before they are readily available.
- Simulations of human-in-the-loop of hardware and software that are configured to reproduce a set of circumstances or an environment under which a task or activity is performed by an end user.

For access to the HSI body of knowledge online repository, see HSI Guidebook (forthcoming).

5.10 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 DoD 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 Lead 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 JCIDS documents.

The PM, Systems Engineer, and Lead Software Engineer for munitions programs, regardless of 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 (JSIMTP), Joint Service Hazard classifiers, and the DoD 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 Plan (FYDP) 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 Under Secretary of Defense 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 DoD-level IM review organizations can provide additional guidance and can assess the adequacy of the IMSP. In addition to the IMSP, the AoA, AS, SEP, TEMP, Risk Management Plan, and other JCIDS documents called for in CJCSI 5123.01 and the JCIDS Manual (requires Common Access Card (CAC) to access website), address aspects of explosives ordnance safety, including IM.

5.11 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 Intelligence Mission Data (IMD) support (see Figure 5-1 and DoDD 5250.01.)

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, programs communicating IMD requirements to the DoD intelligence community that supplies the necessary intelligence data is critical to achieving system capabilities.

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. In order to address threats as they emerge and change over the program's life cycle, the PM, Systems Engineer, System Security Engineer, and Lead 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 Intelligence Guidebook (forthcoming) for more information on CIPs.

Intelligence life cycle mission data planning is necessary to effectively:

- Derive functional baseline requirements and life cycle Intelligence Mission Data (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 2.2.1 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.

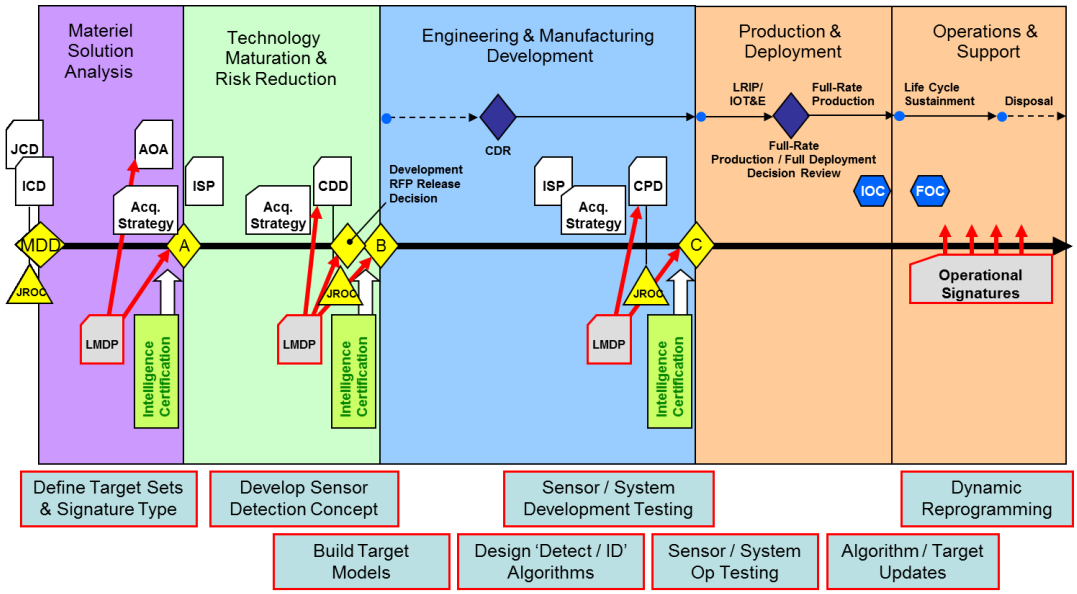


Figure 5-1. Intelligence Mission Data Life Cycle Timeline (MCA Pathway)

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

5.12 Interoperability and Dependencies

Almost all DoD 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 services provided by other systems during operations or reuse of system elements developed by other programs.

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 4.1.8 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 in the course of 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 interoperability and dependencies (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 interoperability and dependency 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 DoD policy and guidance regarding I&D, summarized below, seek to ensure systems work effectively with other systems:

- DoDI 8330.01, CJCSI 5123.01, the JCIDS Manual (requires Common Access Card (CAC) to access website), and 44 USC 3506: Interoperability of IT and National Security System (NSS) acquisition programs are 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.

5.13 Item Unique Identification

Item Unique Identification (IUID) is a systematic process to globally and unambiguously distinguish one item from all the other items that DoD buys or owns. IUID-enabled Serialized Item Management (SIM) provides a capability that allows DoD 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 DoD 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. SIM planning and implementation required by DoDI 4151.19 are addressed in the LCSP.

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 configuration management and product support systems – including new and legacy information systems.

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

5.14 Manufacturing and Quality

Manufacturing and Quality management share some common characteristics. All programs must develop and then execute their manufacturing and quality (M&Q) plans and strategies, including Producibility. The Government develops a Manufacturing Strategy and a Quality Strategy. The contractor develops a Manufacturing Plan and a Quality Plan.

- A Manufacturing Strategy should be tied to the program's acquisition strategy and 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.

Three important parts of execution include:

- The contractor should be required to develop and implement a Manufacturing Management System (MMS) and a Quality Management System (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.
- The program office should include the DCMA as part of team to help support contractor surveillance and oversight.
    - Note: There are 78 Contract Administration Service (CAS) functions that PMOs need to accomplish. Some of these can be partially transferred to DCMA for on-sight performance oversight based on the development and execution of a MOA or MOU. PMOs need to recognize that DCMA resources are limited, thus the MOA/MOU should focus on specific M&Q requirements and negotiate a level of oversight commensurate with risks.
- Assessment of risks and development of risk mitigation strategies.

5.14.1 Manufacturing Management Program

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-896A, "Manufacturing Management Program Guide." The PMO team should identify the appropriate contract manufacturing requirements.

AS6500 and MIL-HDBK-896A address many requirements including:

- Design and Producibility Analysis
- Variability Reduction and Key Characteristics
- Process Capability and Continuous Improvement
- Manufacturing Planning and Control
- Manufacturing Surveillance and Risk Assessments
- Supply Chain Management
- Manufacturing Modeling and Simulation
- Facilities, Tooling, and Test Equipment (Special Tooling, Test, and Inspection Equipment)
- Manufacturing Workforce
- Cost Estimating, Tracking, Management, and Cost Reduction

A Manufacturing Management Program provides a system to promote the timely development, production, and fielding of affordable and capable weapon systems by addressing manufacturing risks and issues throughout the program acquisition cycle. PMs of programs with a manufacturing component should ensure contractors have a robust manufacturing management system.

Manufacturing management is closely linked to the SE process and the SEP in several ways. First, the manufacturing organization should provide representation to the design function and ensure producibility and inspectability are addressed as design considerations. Manufacturing engineers should provide process capability data to the designers and compare proposed tolerances, materials, and assemblies to current capabilities. Typically, a representative from the manufacturing function must coordinate on designs, indicating the design properly takes these considerations into account. Because of this close linkage to SE, manufacturing personnel should:

- Support all design reviews, and systems engineering technical reviews, to ensure the program addresses manufacturing considerations.

- Support the development of the SEP with planned manufacturing management activities. In addition, previous and subsequent phases should be summarized in the SEP.
- Include efficient and cost-effective manufacturing in the SEP, mapping design considerations into contracts.
- Support the identification, tracking, and management of technical risks.

Manufacturing should be a TPM for the program, and the program's strategy for manufacturing should be contained in the program's SEP. Typical TPMs for manufacturing include:

- Capacity Utilization rates
- Overall Operating Efficiency
- Overall Equipment Effectiveness
- Inventory Turns and Accuracy
- On-Time Delivery
- Quality (First Pass Yield, Scrap, Rework and Repair, Cost of Quality, Customer Returns, etc.).

5.14.2 Quality Management Program

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. Quality planning should include the development of a Quality Strategy (Government) and a Quality Plan (contractor).

- A Quality Strategy should be tied to the program's acquisition strategy and 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.

Quality Standards (AS and ISO) that can be used by a program to focus on these specific quality areas of concern:

- First Article Inspection

- Variation Reduction of Key Characteristics
- Non-conformance Documentation
- Qualification Procedure for Aerospace Standard Parts (Supplier Quality)
- Advanced Product Quality Planning and Production Part Approval Process

To ensure consistency in applying quality planning and process control, the program should establish a QMS early, ideally at Milestone A (see PM Guidebooks (forthcoming) for more information on Quality Management). The QMS should be defined and documented in the AS. Quality should be integrated into the AS an SE practice that supports the successful transition of a capability to development, then LRIP, FRP, and delivery of systems to support warfighter missions.

The primary focus of the QMS should be to ensure efficiency in processes. The program team should integrate the QMS with Statistical Process Control to eliminate defects and control variation in production.

The PM, Systems Engineer, and Lead Software Engineer should take into consideration that process capability goes beyond machine capability. The process should include the effects of change in workers, materials, fabrication methods, tooling and equipment, setup, and other conditions. Process capability data should be collected throughout process and product development.

Two more valuable tools to assist in creating quality in design are Six Sigma and Quality Function Deployment. Six Sigma techniques identify and reduce all sources of product variation – machines, materials, methods, measurement system, the environment and the people in the process. Quality Function Deployment is a structured approach to understanding customer requirements and translating them into products that satisfy those needs.

Quality of Design

Quality of Design focuses on the concurrent development of product and manufacturing processes, leading to a producible, testable, sustainable, and affordable product that meets defined requirements. The design phase is critical because product life cycle costs are committed at this point. The QMS should aid the transition from development to production by controlling and reducing life cycle cost by reducing complexities that are often found when quality is not integrated as a function of the design. Therefore, to achieve high-quality (product characteristics meet specification requirements), an end product should be designed so that:

- Processes to produce the end product are in statistical control (uniformity in manufacturing and production).
- Design specifications are aligned with manufacturing process capabilities.

- Functional design integrates producibility requirements (measure of relative ease of manufacturing) with no significant compromises to quality and performance.

The objectives of quality design efforts are to:

- Achieve effective and efficient manufacturing with necessary process controls to meet system requirements.
- Transition to production with no significant manufacturing process and reliability risks that could breach production thresholds for cost and performance.

Quality of Conformance

Quality of Conformance is the degree to which a product or service meets or exceeds its design specifications and is free of defects or other problems that could degrade its performance. The manufacturing, processing, assembling, finishing, and review of the first article and first production units, is where failure or success in the area of quality of conformance is first measured. Any operation that causes the characteristic to be outside of the specified limits will render the configuration of the product different from that which was originally intended, and this could impact cost, schedule, and performance.

5.14.3 Producibility

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.

The PM should ensure that the producibility program focuses on the following five elements to build and maintain a successful producibility system:

1. Establish a producibility infrastructure:
    - Organize for producibility
    - Integrate producibility into the program's risk management program

- Incorporate producibility into the new product strategy
- Employ producibility design guidelines

2. Define manufacturing requirements early along with methods to ensure verification and validation of requirements to be met:
   - Determine Process Capability (Cp and Cpk) and Process Performance (Pp and Ppk) as appropriate
   - Understand and document company and supplier requirements and processes
   - Verify and validate that production processes can and do meet requirements
   - Plan for future process capabilities and performance
3. Address producibility during initial design efforts:
   - Identify design objectives
   - Identify key characteristics of the design
   - Perform trade studies on alternative product and process designs
   - Develop a manufacturing plan
   - Perform complexity analysis
4. Address producibility during detailed design:
   - Address producibility measurements at PDR, CDR, PRR, and FRP DR
   - Optimize manufacturing plans as the design matures
5. Measure producibility processes, products and systems.

Quality and Producibility should be a TPM for the program, and the program's strategy for producibility should be contained in the program's SEP. Planned producibility engineering activities for previous and subsequent phases also should be summarized in the SEP. As a design accomplishment, producibility should be included in the SEP, mapping key design considerations into the RFP and subsequently into the contract.

5.14.4 Manufacturing and Quality Activities

M&Q considerations begin early in the acquisition process and continue through all acquisition phases regardless of acquisition pathway. Table 5-4 should be used as a starting point to assess appropriate activities regardless of pathway. Detailed considerations for each of the pathways are provided in the Engineering of Defense Systems Guidebook. Often M&Q activities are driven by other functional types. For example, the procuring contracting officer in developing the contract and RFP may look to M&Q personnel for Section L and M criteria. Financial personnel may ask M&Q personnel to support Government independent cost estimates, or to evaluate contractor cost proposals, or to monitor production costs. Additional information on required M&Q tasks and activities can be found at https://ac.cto.mil/maq/.

Table 5-4. M&Q Activities by Phase

Acquisition Phase	Typical Manufacturing and Quality (M&Q) Activities
Materiel Solution Analysis (MSA)	• Participate in Analysis of Alternatives (AoA) and provide inputs to the draft Capability Development Document (CDD). • Provide inputs to the draft Acquisition Strategy (AS) and Systems Engineering Plan (SEP), and develop Manufacturing Plan, Manufacturing Strategy, Quality Plan, and Quality Strategy. • Support development of the draft Request for Proposals (RFP), review contractor proposals, and support cost estimating and tracking. • Review and provide inputs to the Life Cycle Sustainment Plan (LCSP), Test and Evaluation Master Plan (TEMP), Integrated Master Plan (IMP) and Integrated Master Schedule (IMS). • Support all program and technical reviews and audits (Alternative System Review (ASR), Manufacturing Readiness Assessment (MRA), and Independent Technical Risk Assessment (ITRA)).
Technology Maturation and Risk Reduction (TMRR)	• Participate in prototyping and design development through the Integrated Product Team (IPT) structure to identify and mitigate M&Q risks in the product to be developed in the next phase. • Inputs to AS, SEP, final CDD, TEMP, LCSP, IMP/IMS, and draft RFP. Develop, implement, and monitor M&Q plans. • Support prototype build and testing; assess manufacturing readiness (Manufacturing Readiness Level (MRL) 6). • Support all program and technical reviews and audits (System Requirements Review (SRR), System Functional Review (SFR), Technology Readiness Assessment (TRA), MRA, ITRA, and Preliminary Design Review (PDR)). • Support development of the draft RFP, review contractor proposals, and support cost estimating and tracking.
Engineering and Manufacturing Development (EMD)	• Participate in trades, manufacturing technology, and design development activities through the IPT structure. • Provide inputs to the AS, SEP, Corrosion Prevention and Control (CPC), LCSP, IMP/IMS, and draft RFP. Develop, implement, and monitor M&Q plans. • Support build/testing and assess manufacturing readiness (MRL 7 and 8). • Support all program and technical reviews and audits (Critical Design Review (CDR), Technology Readiness Review (TRR), TRA, MRA, System Verification Review (SVR)/Functional Configuration Audit (FCA), Production Readiness Review (PRR), ITRA). • Support development of the draft RFP, review contractor proposals; support cost estimating and tracking.
Production and Deployment (P&D)	• Participate in the Configuration Control Board (CCB) process. • Support Low-Rate Initial Production (LRIP) and Full-Rate Production (FRP); assess manufacturing readiness (MRL 9 and 10). • Support Initial and Full Operational Capability (IOC and FOC). • Provide inputs to the LCSP and performance based logistics Plan. Develop, implement, and monitor M&Q plans. • Support development of the draft RFP, review contractor proposals; and support cost estimating and tracking.
Operations and Support (O&S)	• Support FRP decision. • Provide input to AS, SEP, TEMP, LCSP. Develop, implement, and monitor M&Q plans. • Analyze system use data such as deficiency reports, hazard reports, regulatory violations. • Support build and test activities, along with pre-planned product improvement and block updates. • Support development of the draft RFP, review contractor proposals, support cost estimating and tracking.

5.14.5 Assessing Manufacturing Readiness and Risk

The National Defense Authorization Act, Section 812 and DoDI 5000.85 establish policy on the requirement to address manufacturing risks over the entire life cycle of a program.

Manufacturing feasibility, processes, and risk should be assessed early in the MSA phase and continuously through the P&D phase 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.

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. DoDI 5000.88, Section 3.6.c., defines the requirements for manufacturing processes and manufacturing risks. 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. These include:

- Consideration of requirements for efficient manufacture during the design and production of the system.
- The availability of raw materials, special alloys, composite materials, components, tooling, and production test equipment.
- The use of advanced manufacturing technology, processes, and systems.
- The use of contract solicitations that encourage competing offerors to acquire modern technology, production equipment, and production systems (including hardware and software).
- Methods to encourage investment in advanced manufacturing technology, production equipment, and processes.
- During source selection, increased emphasis on the efficiency of production.
- Expanded use of commercial manufacturing processes rather than processes specified by DoD.

Low-risk manufacturing readiness includes early planning and investments in producibility requirements, manufacturing process capabilities, and quality management to ensure effective and efficient manufacturing and transition to production. It also includes assessments of the industrial base. Manufacturing risk is evaluated through MRAs, which are integrated with existing program assessments throughout the acquisition life cycle. The PM should assess manufacturing readiness in the program's earliest phase, and the assessment should be continuous. The PM should report on the program's manufacturing readiness progress/status

during each technical review, Program Support Assessment, or its equivalent, and before each milestone decision.

Successful manufacturing has many dimensions. Industry and Government have identified best practices in the following nine manufacturing risk categories. PMs should use the best practices to assess their programs early and should report on these areas during technical reviews and before acquisition milestones. Implementation of these best practices should be tailored according to product domains, complexity and maturity of critical technologies, manufacturing processes, and specific risks that have been identified throughout the assessment process. These categories should help frame the risk assessment and focus mitigation strategies:

1. Technology and the Industrial Base: assess the capability of the national technology and industrial base to support the design, development, production, operation, uninterrupted maintenance support and eventual disposal (environmental impacts) of the system.
2. Design: assess the maturity and stability of the evolving system design and evaluate any related impact on manufacturing readiness.
3. Cost and Funding: examine the risk associated with reaching manufacturing cost targets.
4. Materials: assess the risks associated with materials (including basic/raw materials, components, semi-finished parts and subassemblies).
5. Process Capability and Control: assess the risks that the manufacturing processes may not reflect the design intent (repeatability and affordability) of key characteristics.
6. Quality Management: assess the risks associated with management efforts to control quality and foster continuous improvement.
7. Manufacturing Workforce (Engineering and Production): assess the required skills, certification requirements, availability, and required number of personnel to support the manufacturing effort.
8. Facilities: assess the capabilities and capacity of key manufacturing facilities (prime, subcontractor, supplier, vendor and maintenance/repair).
9. Manufacturing Management: assess the orchestration of all elements needed to translate the design into an integrated and fielded system (meeting program goals for affordability and availability).

As part of the manufacturing strategy development effort, the PM needs to understand the contractor/vendor business strategy and the impacts to Government risk identification and mitigation efforts, such as the Make/Buy decisions and supply chain risks assessments. Additional guidance on assessing manufacturing risks can be found in the Manufacturing Readiness Levels Guide.

Assessment and mitigation of manufacturing risk should begin as early as possible in a program's acquisition life cycle – including conducting a manufacturing feasibility assessment as part of the AoA.

The PM, Systems Engineer, and Lead Software Engineering technical team should consider the manufacturing readiness and manufacturing-readiness processes of potential contractors and subcontractors as a part of the source selection for major defense acquisition programs (see DFARS Subpart 215.304).

The PM, Systems Engineer, and Lead Software Engineering technical team should assess manufacturing readiness during the acquisition life cycle, as described in Table 5-5.

Table 5-5. Minimum Points (When) to Assess Manufacturing Readiness

Key Manufacturing Readiness Assessment (MRA) Points	Considerations
1. Materiel Solution Analysis (MSA) Phase supporting Milestone A Decision. As part of the Analysis of Alternatives (AoA), manufacturing risks should have been assessed for each of the competing alternatives (see the Manufacturing Readiness Levels Guide for one source of specific assessment factors). Risks for the preferred system concept should be assessed and identified at this point. The overall assessment should consider:	• Assess manufacturing feasibility and capability to produce in a lab environment. • Program critical technologies are ready for the Technology Maturation and Risk Reduction (TMRR) phase • Required investments in manufacturing technology development have been identified • Processes to ensure manufacturability, producibility, and quality are in place and are sufficient to produce prototypes. • Manufacturing risks and mitigation plans are in place for building prototypes. • Cost objectives have been established and manufacturing cost drivers have been identified; draft Key Performance Parameters (KPPs) have been identified as well as any special tooling, facilities, material handling and skills required. • Producibility assessment of the preferred system concept has been completed, and the industrial base capabilities, current state of critical manufacturing processes and potential supply chain sources have all been surveyed.
2. TMRR Phase supporting Milestone B and Development Request for Proposals (RFP) Release Decision. As the program approaches the Development RFP Release Decision and the Milestone B decision, critical technologies and manufacturing processes should have matured sufficiently for 2366b certification and demonstrated in a relevant environment.	• Assess contractor's manufacturing capability to produce in a production-relevant environment. An initial manufacturing approach has been developed. • Manufacturing processes have been defined and characterized, but there are still significant engineering and/or design changes in the system itself; manufacturing processes that have not been defined or that may change as the design matures should be identified. • The program should be nearing acceptance of a preliminary system design. Preliminary design, producibility assessments, and trade studies of technologies and components should have been completed. • Prototype manufacturing processes and technologies, materials, tooling and test equipment, as well as personnel skills have been demonstrated on systems and/or subsystems in a production-relevant environment.

Key Manufacturing Readiness Assessment (MRA) Points	Considerations
	• Cost, yield and rate analyses have been performed to assess how prototype data compare with target objectives, and the program has in place appropriate risk reduction to achieve cost requirements or establish a new baseline, which should include design trades. • Producibility considerations should have shaped system development plans, and the Industrial Base Capabilities assessment (in the Acquisition Strategy for Milestone B) has confirmed the viability of the supplier base.
3 Engineering and Manufacturing Development (EMD) Phase, Critical Design Review (CDR). At the CDR the system should be sufficiently mature to start fabricating, integrating, and testing pre-production articles with acceptable risk. The product baseline describes the detailed design for production, fielding, deployment, operations, and support. The product baseline also prescribes all necessary physical (form, fit and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. Production should be demonstrated in a relevant environment and should consider:	• Assess contractor's manufacturing capability to produce in a production representative environment. An initial manufacturing approach has been developed. • Critical manufacturing processes that affect the product characteristics have been identified, process control plans have been developed, and the capability to meet design tolerances has been determined. • Detailed design is producible and assessed to be within the production budget. • Detailed producibility trade studies using design characteristics and related manufacturing process are completed. Materials and tooling are available to meet the pilot line schedule. • Long-lead procurement plans are in place; supply chain assessments are complete. • Verify configuration control of the initial product baseline as demonstrated by: the completion of build-to documentation for hardware and software configuration items, production models, drawings, software design specifications, materials lists, manufacturing processes, and qualification plans and procedures.
4. EMD Phase, Milestone C. A Production Readiness Review (PRR) identifies the risks of transitioning from development to production. Manufacturing is a function of production; in order to transition to production without significant risk, the program should thoroughly evaluate processes during the PRR. Production should be demonstrated on a pilot line and should consider:	• Assess contractor's manufacturing capability to produce on a pilot line. • The detailed system design is complete and stable to support Low-Rate Initial Production (LRIP). • Technologies are mature and proven in a production environment, and manufacturing and quality processes are capable, in control, and ready for LRIP. • All materials, manpower, tooling, test equipment, and facilities have been proven on pilot lines and are available to meet the planned low-rate production schedule. • Cost and yield and rate analyses are updated with pilot line results. • Known producibility risks pose no significant challenges for LRIP. • Supplier qualification testing and first article inspections have been completed. • Industrial base capabilities assessment for Milestone C has been completed and shows that the supply chain is adequate to support LRIP.
5. Production and Deployment (P&D) Phase, Full-Rate Production (FRP) Decision Review	• Assess LRIP and FRP production environments.

Key Manufacturing Readiness Assessment (MRA) Points	Considerations
(DR). To support FRP, there should be no significant manufacturing process and reliability risks remaining. Manufacturing and production readiness results should be presented that provide objective evidence of manufacturing readiness. The results should include recommendations for mitigating any remaining low (acceptable) risk, based on assessment of manufacturing readiness for FRP, which should include (but not be limited to):	• LRIP learning curves that include tested and applied continuous improvements have been assessed and validated. • Meeting all systems engineering and design requirements. • Evidence of a stable system design demonstrated through successful test and evaluation. • Evidence that materials, parts, manpower, tooling, test equipment, and facilities are available to meet planned production rates. • Evidence that manufacturing processes are capable, in control, and have achieved planned FRP objectives. • Plans are in place for mitigating and monitoring production risks. • LRIP cost targets data have been met; learning curves have been analyzed and used to develop the FRP cost model.

5.14.6 Assessing Industrial Capabilities

DFAR 207.105, Contents of Written Acquisition Plans, provides guidance on manufacturing actions planned by the PM to execute the approach established in the AS and to guide contractual implementation.

Current legislation and policies governing industrial base capabilities are intended to ensure that:

- The industrial needs of acquisition programs are properly addressed.
- The impacts of acquisition programs on industrial capabilities are understood.
- The manufacturing needs of acquisition programs are met.

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).
- Financial Stability (the company will endure long enough to complete all production) at rate and on schedule.

The ability of the industrial base to respond to near-term readiness, or to meet surge and mobilization requirements, has deteriorated as our industrial base continues to shrink. This has diminished the likelihood of competition and contributed to the emergence of production bottlenecks at many points.

Industrial Capability Analysis

When the DoD 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 analysis. The analysis addresses the following issues:

- Ability to cost-effectively design, develop, produce, maintain, support, and restart the program (if necessary)
- When the new production facilities are able to produce certified units
- The approach to making production rate and quantity changes in response to contingency and support objectives
- Critical planning and infrastructure considerations, including prime and sub-tier contractors
- Vulnerable suppliers
- Component obsolescence
- DoD involvement in new and unique capabilities

Industrial Capabilities Planning

Industrial Capabilities Planning should address current and future status of unique manufacturing capabilities. The planning should:

- Assess the adequacy of industrial capabilities to meet acquisition needs. All manufacturing capabilities must be strategically analyzed to ensure that these capabilities are maintained throughout the life of the program.
- Identify all unique items projected to go out of production. For each item, planning should address:
    - Product/technology obsolescence
    - Replacement of life-limited items
    - Regeneration
    - Identify all unique manufacturing capabilities. In addition to identifying unique items, any facilities or corporations that provide unique services or products also need to be identified.

5.15 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 2.2.5). 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, where modules can be decoupled, separated, or even rearranged in a major system platform and major system components developed under the program, as well as major system components developed outside the program that will be integrated into the MDAP. 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 now be composed into modules that can be reconfigured or even replaced.

Acquisition programs implementing a modular design provide flexible system designs, which allow for the replacement or recombination of subsystems and components. Program management needs to understand the expected benefit from modular design as part of implementing a MOSA strategy. This understanding provides guidance to the system realization, on which enabling elements (e.g., standards, contract clauses, engineering tools, etc.) to use. MOSA benefits are usually categorized into six individually useful 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 Lead 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 to select. MOSA-enabling standards are identified and accessible in ASSIST.

5.16 Operational Energy

Emerging threats to the logistic resupply of operational forces, the trend toward ever greater energy demand in the operational forces and increasing costs to operate and resupply energy-intensive systems have all put increasing focus on lowering system and unit energy demand. Reducing the force's dependence on energy logistics can improve the force's mobility and resilience and increase its control over the timing and conditions of the fight. Focusing on energy as an explicit design consideration and SE category is a significant change in practice and thinking that will help manage emerging operational challenges.

The PM, Systems Engineer, and Lead Software Engineer can help lower operational energy by addressing issues associated with the system's energy logistics support and power resupply frequency.

This approach should generate informed choices based on the threshold and objective values of the Energy KPP for the system. For liquid energy-consuming systems, the top-level units of measure for the Energy KPP might be gallons of fuel demanded (consumed) over a defined set of duty cycles or for accomplishing a specified mission goal such as a sortie. These measures may be further decomposed into weight, range, electric power demand, and other relevant measures to inform the necessary SE trade-off analysis. The intended result is a comprehensive set of trade-space choices for industry to consider to deliver solutions that are not only energy efficient but also mission-effective and affordable. See the JCIDS Manual linked at the end of this section for more information on the Operational Energy KPP.

Energy's relationship to performance arises from the operational context in which the system is used. Accordingly, the scenarios that illustrate how the system is used, as part of a unit of maneuver, are essential to understanding the energy supply and demand constraints to be managed. This is essentially the same approach as balancing survivability goals against lethality goals in the engineering trade space. Operational energy issues include:

- How the system and combat unit refuel/recharge in the battlespace scenarios, and how often.
- How this refueling/recharging requirement might constrain our forces (limit their freedom of action, on-station time, signature, etc.).
- How the adversary depicted in the defining scenarios might delay, disrupt, or defeat our forces by interdicting this system's refueling/recharging logistics.
- How much force protection could be diverted from combat missions to protecting these refueling or recharging events when and where required.

Systems Engineers should consider incorporating energy demand in design, technology, materials, and related issues into the system trade space along with other performance issues, so that oppressive energy resupply needs are not inadvertently introduced in the attempt to achieve other performance goals (e.g., survivability, lethality). In practice, this means requirements managers should factor into the system design the necessity of refueling/recharging using the same scenarios used to illustrate other performance requirements, and allowing the adversary a realistic chance to interdict the refueling/recharging effort. Systems Engineers may find it necessary to have a continuing dialogue with the warfighter (the user and requirements manager) to help grasp the operational impact of these issues and depict them in trade-space decisions.

Energy-related engineering analysis should begin early enough to support initial AoA planning following the Materiel Development Decision, and should also be routinely updated to inform any AoA performed later in the life cycle (i.e., in support of block upgrades and modifications).

The following documents provide the PM, Systems Engineer, and Lead Software Engineer with additional insight into the issue of Operational Energy in the acquisition life cycle:

- JCIDS Manual (for the Energy KPP; requires Common Access Card (CAC) to access website)
- Operational Energy Strategy: Implementation Plan

The results of the sustainability analysis (see Section 2.2.6 Sustainability Analysis) can be used to inform energy analyses.

5.17 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, Systems Engineers, and Lead 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 Production and Deployment 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 systems engineering of systems acquisitions. In addition, the following documents address PHS&T:

- MIL-STD-2073-1 (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

5.18 Reliability and Maintainability Engineering

The purpose of R&M engineering (Maintainability includes Built-in-Test (BIT)) 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 can even occur in the development process.

DoDI 5000.88, Section 3.6.b. requires PMs to 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. Title 10, U.S.C., section 2443 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 ICD and CDD. Note: The ICD may not contain quantitative user threshold requirements. The draft CDD is the first opportunity to review the sustainment KPP and supporting R&M 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 KSA 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 2443.
- 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 2443.
- 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 2443. 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 Data Item Descriptions (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 Lead Software Engineer work to properly align the applicable R&M Engineering activities needed to reduce program risk. Table 5-6 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 and in the R&M Engineering Management Body of Knowledge (DDRE(AC)/Engineering website).

Table 5-6. Foundational R&M Activities

Life Cycle Phase	Reliability and Maintainability (R&M) Activities
During System definition the R&M engineer, as part of the program SE team, should:	• Analyze conceptual design approaches and estimate the feasibility with respect to R&M performance capabilities • Perform Analysis of Alternatives (AoA) trade-off studies among R&M, availability and other system performance parameters to arrive at a preferred system alternative. The studies should be performed in conjunction with product support, cost and design personnel, to ensure that user requirements are valid and feasible. • Conduct a Reliability, Availability, Maintainability, and Cost (RAM-C) analysis. For Major Defense Acquisition Programs (MDAPs), prepare a preliminary RAM-C Rationale Report and attach the report to the Systems Engineering Plan (SEP) for Milestone A

Life Cycle Phase	Reliability and Maintainability (R&M) Activities

	• Translate user performance capabilities and requirement thresholds to R&M specification requirements based on the CONOPS/OMS/MP (Concept of Operations/Operational Mode Summary/Mission Profile) failure definitions, and utilization rates
	• Develop an R&M engineering program plan. The plan should address the full life cycle of the program. Planning activities typically commence early in design and continue through operations and support.
	  ○ A properly tailored R&M engineering program ensures that all elements are cost-effectively implemented and properly conducted, evaluated, reported, and integrated in a timely manner for design, analysis, development, testing, and manufacturing.
	  ○ Planning the early stages should include the approach and procedures by which the contractor will ensure compliance with the proposed contractual requirements. The approach should also provide results of R&M design analyses and test results needed to support all major design reviews, program reviews, and milestones. These planning activities should be documented in the appropriate DoD acquisition component program plans and Integrated Master Schedule (IMS).
	• Develop a system reliability growth planning curve and include it in the SEP. Reliability growth curves should be stated in a series of intermediate goals and tracked through fully integrated, system-level test and evaluation events until the reliability threshold is achieved. If a single curve is not adequate to describe overall system reliability, curves for critical subsystems, with rationale for their selection, should be provided
	• Use data from the RAM-C Rationale Report to provide the following for logistics design support:
	  ○ The planning factors and their values used to determine Mean Down Time (MDT) and other maintainability Key System Attributes (KSAs) or additional performance attributes are needed to validate Operational Availability (Ao) and Materiel Availability (Am) and should provide a realistic, definitive, and uniform basis to determine downtime. Failure rate and removal rate estimates, for both corrective and preventive maintenance, to provide a realistic basis for equipment and replaceable unit spares provisioning planning
	• Define contractor R&M engineering activities in the Request for Proposals (RFP) and contract Statement of Work (SOW) for the Technology Maturation and Risk Reduction (TMRR) phase, which should include:
	  ○ Allocations
	  ○ Block diagrams and modeling
	  ○ Predictions
	  ○ Failure Modes, Effects, and Criticality Analysis (FMECA)
	  ○ Subsystem and system-level reliability growth planning activities
	  ○ R&M tests and demonstrations
	  ○ Failure Reporting, Analysis and Corrective Action System (FRACAS)

During preliminary design, the R&M engineer, as part of the program SE team, should:	• Participate in trade studies during requirements analysis and architecture design • Review results of R&M engineering analyses, verification tests, design approach, availability assessments, and maintenance concept optimization to verify conformance to requirements, and to identify potential R&M problem areas

Life Cycle Phase	Reliability and Maintainability (R&M) Activities
	• Contribute to integrated test planning to avoid duplication and afford a more complete utilization of all test data for R&M assessment. Comprehensive test planning should include subsystem reliability growth and maintainability and Built-in Test (BIT) demonstrations as appropriate • Understand schedule and resource constraints, and adjust the reliability growth planning curve based on more mature knowledge points • Integrate R&M engineering analyses with logistics design support in the following areas: requirements and functional analysis; test planning; Reliability-Centered Maintenance (RCM) and Condition-Based Maintenance Plus (CBM+); and refinement of the maintenance concept, including the Level of Repair Analysis (LORA) and maintenance task analysis • Verify that plans have been established for the selection and application criteria of parts, materials and processes to limit reliability risks • Define contractor R&M engineering activities in the RFP and contract SOW during which R&M quantitative requirements and verification methods are incorporated • Update the RAM-C analysis to ensure R&M user requirement thresholds are valid and feasible. For MDAPs, attach the updated RAM-C Rationale Report to the SEP for Milestone B
During detailed design, the R&M engineer, as part of the program SE team, should:	• Perform evaluations to assess R&M status and problems • Update the RAM-C analysis, ensuring the R&M user requirement thresholds are valid and feasible. For MDAPs, attach the updated RAM-C Rationale Report to the SEP for Milestone C • Ensure that the product baseline design and required testing can meet the R&M requirements • Ensure the final FMECA identifies failure modes, and their detection methods, that could result in personnel injury and/or mission loss, and ensure they are mitigated in the design • Ensure that the detailed R&M prediction to assess system potential to meet design requirements is complete • Verify through appropriate subsystem/equipment-level tests the readiness to enter system-level testing at or above the initial reliability established in the reliability growth planning curve in both the SEP and the Test and Evaluation Master Plan (TEMP) • Verify system conformance to specified R&M requirements through appropriate demonstration and test • Implement a FRACAS to ensure feedback of failure data during test and to apply and track corrective actions • Coordinate with the Chief Developmental Tester (T&E Lead) and Operational Test Agencies (OTAs) to ensure that the program office and OTA data collection agree on R&M monitoring and failure definitions, and that R&M and BIT scoring processes are consistent in verification of requirements through all levels of testing • Define contractor R&M engineering activities in the RFP and contract SOW to ensure adequate R&M engineering activities take place during production and the RFP and contract SOW provide adequate consideration of R&M in re-procurements, spares and repair parts. An essential activity during production is the FRACAS process.

Life Cycle Phase	Reliability and Maintainability (R&M) Activities
	• Verify that parts, materials, and processes meet system requirements through the use of a management plan detailing reliability risk considerations and evaluation strategies for the intended service life. Include flow of requirements to subcontractors and suppliers. See MIL-STD-1546 (Parts, Materials, and Processes Control Program for Space and Launch Vehicles) and MIL-STD-1547 (Electronic Parts, Materials, and Processes for Space and Launch Vehicles) and MIL-STD-11991 (General Standard for Parts, Materials, and Processes)
During production or fabrication, assembly, integration, and test (FAIT), the R&M engineer, as part of the programs SE team should:	• Verify initial production control of R&M degradation factors by test and inspection, production data analysis, and supplemental tests • Verify R&M characteristics, maintenance concept, repair policies, Government technical evaluation, and maintenance procedures by T&E • Identify R&M and production-related BIT improvement opportunities via FRACAS and field data assessment • Review Engineering Change Proposals (ECPs), operational mission/deployment changes, and variations for impact on R&M • Update R&M predictions and FMECAs based on production tests, demonstration tests, operational evaluation, and field results and apply them to the models previously developed to assess impacts on maintenance procedures, spares, manpower, packaging design, test equipment, missions, and availability • Verify that parts, materials, and processes management requirements for limiting reliability risk and lessons learned are used during all design change efforts including change proposals, variations, substitutions, product improvement efforts, or any other hardware change effort
During operations and support, the R&M engineer, as part of the program SE team should:	• Assess operational data to determine the adequacy of R&M and BIT characteristics performance; maintenance planning, features and procedures; provisioning plans, test equipment design; and maintenance training • Identify problem areas for correction through ongoing closed-loop FRACAS and field data assessment • Monitor availability rates and respond to negative trends and data anomalies

5.19 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

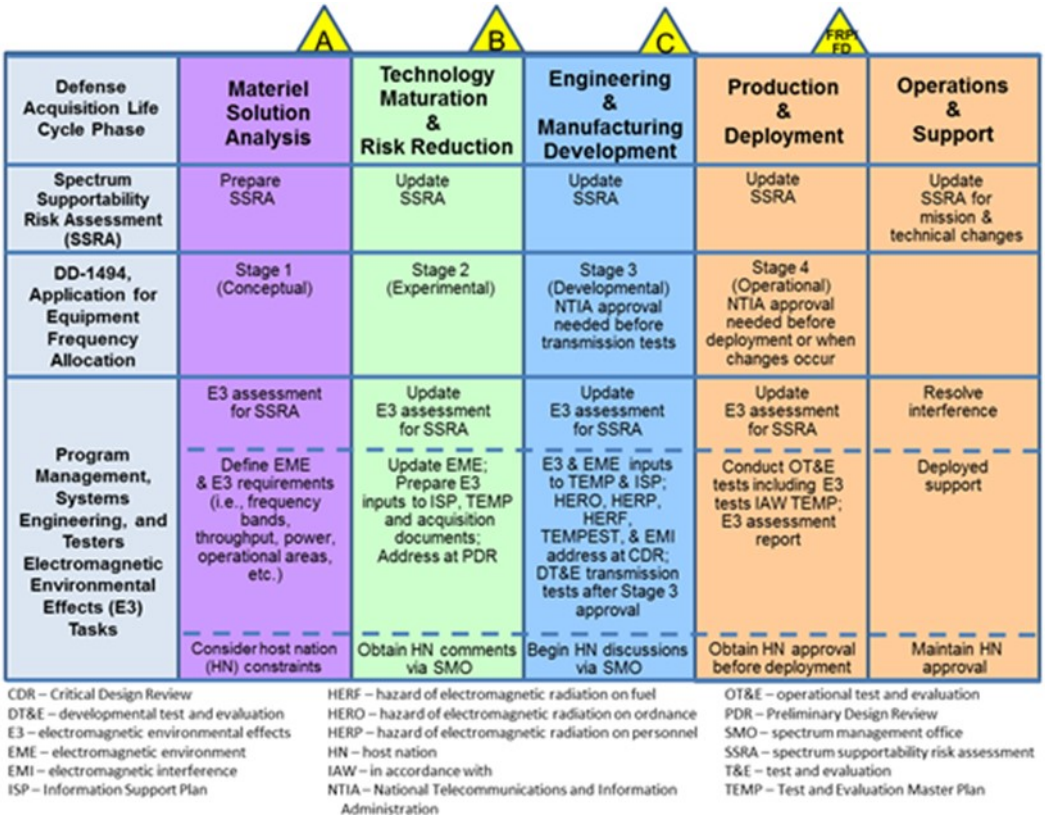
submit a Spectrum Supportability Risk Assessment (SSRA). The platform SSRA can reference the GFE SSRA but may have to expand upon it regarding host-nation features or other information not contained in the GFE-level SSRA. The Systems Engineer should be aware of the worldwide rules for spectrum management 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. The AoA should address spectrum needs as part of concept formulation. Both the SSRA and DD Form 1494 are required for each milestone (see DoDI 4650.01). The SSRA is used within the DoD 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 DoD 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 Lead 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 (Hazards of Electromagnetic Radiation to Ordnance Test Guide), 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 DoD. See Figure 5-2 for spectrum activities by acquisition phase. This figure summarizes the requirements of DoDI 4650.01.



Defense Acquisition Life Cycle Phase	A: Materiel Solution Analysis	B: Technology Maturation & Risk Reduction	C: Engineering & Manufacturing Development	FRP/FD: Production & Deployment	Operations & Support
Spectrum Supportability Risk Assessment (SSRA)	Prepare SSRA	Update SSRA	Update SSRA	Update SSRA	Update SSRA for mission & 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 & E3 requirements (i.e., frequency bands, throughput, power, operational areas, etc.)	Update EME; Prepare E3 inputs to ISP, TEMP and acquisition documents; Address at PDR	E3 & EME inputs to TEMP & ISP; HERO, HERP, HERF, TEMPEST, & 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
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 5-2. Spectrum-Related Activities by Life Cycle Phase

5.20 Standardization

Standardization supports the achievement of commonality and interoperability of parts and processes with United States 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.

DoDI 5000.88, Section 3.6.f requires PMs to use a parts management process for the selection of parts during design to consider the life cycle application stresses, standardization, technology (e.g., new and aging), reliability, maintainability, supportability, life cycle cost, and DMSMS.

Parts management is a standardization design strategy available to PMs. Benefits of parts standardization include:

- Reducing the number of unique or specialized parts used in a system (or across systems).
- Reducing the logistics footprint.
- Lowering life cycle costs.

In addition, parts management can enhance the reliability of the system and mitigate DMSMS issues. MIL-STD-3018 (Parts Management) 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:

- Implementing parts management contractual requirements.
- Approving contractor submitted plans.
- Ensuring parts management objectives are met.

5.21 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 (IOC) 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 AoA, 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.PS (forthcoming) and DoDI 5000.PR (forthcoming) and HSI Guidebook (forthcoming), but typical product support considerations are listed in Table 5-7.

Table 5-7. Product Support Considerations

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, 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 KPP/KSA to establish affordable and achievable goals and caps (see Section 5.2 Affordability – Systems Engineering Trade-Off Analyses, and PM Guidebooks (forthcoming)). Once the goals are established the focus turns to the specific metrics driving the O&S cost and Sustainment KPP/KSAs 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 (A_O) and Materiel Availability (A_M) (see Sustainment Guidebook (forthcoming)). 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.

5.22 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. See the JCIDS manual.

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 Lead 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) (e.g., sand, vibration, shock, immersion, fog, etc.),
- Electromagnetic environments described in MIL-STD-461 (Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment) and MIL-STD-464 (Electromagnetic Environmental Effects Requirements for Systems),
- 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 the Defense Threat Reduction Agency's Nuclear Survivability Program Guidebook (DTRA-TR-14-71), and
- Cyber environments described in DoDI 8500.01 Cybersecurity, JCIDS Cyber Survivability Endorsement Implementation Guide.

PMs, Systems Engineers, and Lead 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 Lead Software Engineer should consider all of 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 AAFDIT) and Intelligence Guidebook (forthcoming).

The System Survivability KPP is intended to ensure the system, rather than the system occupants or other personnel, maintains its mission capabilities as defined in the CONOPS (see JCIDS Manual Enclosure D, Enclosure B, Appendix G, Annex C). 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 in spite of hostile action or under adverse conditions.

The Force Protection 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 (see JCIDS Manual Enclosure D, Appendix B). Although the Force Protection KPP may include many of the same attributes as those that contribute to System Survivability, the intent of the Force Protection KPP 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 test and evaluation (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 Chemical, Biological, Radiological and Nuclear (CBRN) mission-critical system, the PM should 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 all systems that may operate in a CBRN environment, the Systems Engineer should describe in the SEP how the system design incorporates the CBRN survivability requirements and how progress toward these requirements is tracked and documented over the acquisition life cycle.

5.23 System Safety

MIL-STD 882 defines SS as *"The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life cycle."* It defines SS Engineering as *"An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated."*

SS is an important element of SE that provides a standard, generic method for the identifying, classifying, and mitigating hazards. DoDI 5000.88, Section 3.6.e., requires the program to use the SEP to document a strategy for the SS Engineering program 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. 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.

DoD 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, operations and support, 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 shall be accepted by the appropriate authority as defined in DoDI 5000.02. The system configuration and associated documentation that supports the formal risk acceptance decision shall 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 and Joint Weapon Safety reviews and assessments.

5.23.1 Major Capability Acquisition Environment, Safety and Occupational Health

ESOH analyses are an integral, ongoing part of the SE process throughout the life cycle. DoDI 5000.88, Section 3.6.e. requires programs to use the SS methodology in MIL-STD-882 to manage their ESOH considerations as an integral part of the program's overall SE process. This starts with including ESOH management planning in the SEP to cover technology development, and system development activities and continues throughout the system's life cycle.

DoD defines ESOH in MIL-STD-882 as *"the combination of disciplines that encompass the processes and approaches for addressing laws, regulations, EOs, DoD policies, environmental compliance, and hazards associated with environmental impacts, system safety (e.g., platforms, systems, system-of-systems, weapons, explosives, software, ordnance, combat systems), occupational safety and health, hazardous materials management, and pollution prevention."*

The PM uses the SS methodology for the identification, documentation, and management of environmental, occupational and health hazards and their associated risks during the system's development and sustainment. The PM, with support from the Systems Engineer and SS SMEs, eliminates hazards where possible, and manages environmental, occupational, and health hazards risks where hazards cannot be eliminated.

The PM, Systems Engineer and SS SMEs should also identify and integrate environmental, occupational and health hazards requirements into the SE process including, but not limited to, complying with National Environmental Protection Act (NEPA), EO 12114, and applicable environmental quality requirements, which will require assessing the system's operation and maintenance pollutant emissions, prohibiting or strictly controlling the use of banned or restricted hazardous materials, such as hexavalent chrome and ozone-depleting substances. Results of environmental, occupational and health hazards and concerns are documented in the PESHE and their NEPA/EO 12114 Compliance Schedule. The PESHE consists of the environmental, occupational, and health hazard data, hazardous materials management data, and any additional environmental, occupational and health compliance information required to support analyses at test, training, fielding and disposal sites.

5.23.2 Software System Safety

Software System Safety (SSS) is defined in MIL-STD-882 as *"the application of system safety principles to software."* DoDI 5000.88, Section 3.6.e., requires the program to use the SEP to 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. The assessment of risk for software, and consequently software-controlled or software-intensive systems considers the potential risk severity and degree of control the software exercises over the hardware, and dictates the level of rigor (LOR) tasks needed to reduce the risk level. The LOR tasks and analyses specify the depth and breadth of software analysis and verification and validation activities necessary to provide a sufficient level of confidence and safety assurance that a safety significant software function will

perform. The SS and SSS hazard analysis processes and the successful execution of LOR tasks are important elements to increase the confidence that the software will perform as specified to software performance requirements, while reducing the number of contributors to hazards that may exist in the system. All software contributions to system risk are documented in the Hazard Tracking System (HTS).

The Joint Services Software Safety Authorities' "Software System Safety Implementation Process and Tasks Supporting MIL-STD-882" is a concise guide to assist in implementing the SSS information in MIL-STD-882. The Joint Software System Safety Engineering Handbook process descriptions complement MIL-STD-882 for these analyses. Allied Ordnance Publication (AOP) 52, "*Guidance on Software Safety Design and Assessment of Munitions Related Computing Systems*" provides additional guidance on how to conduct required software analyses.

The *Unmanned System Safety Engineering Precepts Guide for DoD Acquisition* is intended to support the development and design of safe Unmanned System (UxS), associated safety significant software, support hardware and firmware, and Service safety reviews. The guide is directed toward UxS SS engineers as well as UxS PMs, systems engineers, system designers, and T&E managers. The precepts are intended to be general, to be complemented by systems specific to a program office. The guide is intended to provide the PM with a point of initiation for precepts that can aid the development of an SS Engineering Program. The guide includes a summary of the three types of safety precepts (e.g. Programmatic, Design, and Operational), an analysis of the major UxS safety concerns, and an assessment of the state of the art of AI and autonomous capabilities, which, when integrated properly, can enable the desired performance of UxS autonomy, human-machine interaction, and command and control.

5.23.3 Hazard Tracking System

A closed-loop HTS is used to document, track, and maintain hardware and software related hazards and their associated risks data. The HTS includes subcontractor, vendor, and supplier hazard tracking data. The minimum data elements for this task for the tracking system are hazard, system, subsystem, applicability, requirements references, system mode, causal factor, effects, mishap, initial risk, event risk, target risk, control measures, hazard status, verification and validation method, acting person(s), record of risk acceptance(s), and hazard management log. The HTS is maintained throughout the system's life- cycle.

The following minimum data for each hazard is included in the HTS identification number; identified hazards (including descriptions); associated mishaps (potential mishaps resulting from the hazard); risk assessments (including the initial, target, and event(s) Risk Assessment Codes (RACs) and risk levels); identified risk mitigation measures; selected (and funded) control measures; hazard status (current RAC and risk level based on any control actions that have been implemented, verified, and validated); verification of risk reductions (i.e., status of assessments of mitigation effectiveness); and risk acceptances (records of each risk acceptance decision

including the names of the risk acceptance authority and user representative(s); and dates of risk acceptance and user concurrence(s)).

5.23.4 SS in SE Process

Early application of SS Engineering contributes to identification and control of potential safety hazards, safer designs, and reduction in overall life cycle cost and avoids reliance on procedural controls. SS considerations start with including SS management planning in the MSA phase, or equivalent phase, after completion of the AoA and before Milestone A activities and continues throughout the system's life cycle.

The PM and the Systems Engineer ensure SS is addressed during MSA or equivalent phase by identifying inherent hazard risks and developing criteria to define objectives for the SS engineering program,

The PM and the Systems Engineer ensure SS is addressed during TMRR or equivalent phase by identifying safety constraints to implement into the development of critical and new technologies. This is critical because the program conducts most of its developmental testing and finalizes a significant portion of the system design during TMRR. During TMRR, the SS SME can provide the most cost-effective SS support to the program by identifying and then eliminating or mitigating hazards and ensuring SS compliance during system testing and design development. The Systems Engineer and SS SMEs document the results of their TMRR. Finally, properly integrating SS in SE requires addressing the following areas:

- Programs should integrate SS activities by incorporating various functional disciplines such as environmental engineers, fire protection engineers, and occupational health professionals to identify hazards and mitigate risks through the SE process.
- Programs should document ESOH management planning in the SEP.
- Programs should continue to conduct assessment of the system and its hazards throughout the system life cycle to address system changes for any potential to alter existing risk levels (even for accepted SS risks) or to add hazards.

5.23.5 SS System Design Requirements

The Systems Engineer identifies the SS requirements applicable to the system throughout its life cycle from statutes, regulations, policies, guidance, design standards and capability documents. From these requirements, the Systems Engineer should derive SS design requirements and include them in capability documents, technical specifications, solicitations, and contracts.

5.23.6 SS in Program Documents

Together the Systems Engineer and the SS SMEs use the SEP to document the program's plan to integrate SS into the SE process, incorporating SS as a mandatory design, test, sustainment, and

disposal consideration. For Environmental and Occupational Health (EOH) considerations, the Programmatic ESOH Evaluation (PESHE) and the NEPA/EO 12114 Compliance Schedule are used to document the results of the program's implementation of their EOH planning. This approach segments required EOH information across the SEP, PESHE, and NEPA/EO 12114 Compliance Schedule to avoid duplication and enhance ESOH integration.

The SEP should include the SS management planning information listed in Table 5-8.

Table 5-8. ESOH Information in SEP

Column Heading in Systems Engineering Plan (SEP) Table 4.6-1	Expected Information (provided or attached)
Cognizant Program Management Office (PMO) Organization	Organizational structure for integrating system safety (SS) and environment, safety, and occupational health (ESOH) (or refer to SEP Table 3.4.4-2)
Certification	Required SS approvals, endorsements, releases, and the designated high and serious risk acceptance user representative(s)
Documentation	SS Management Plan, SS Program Plan, Hazards Analyses, Programmatic ESOH Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule
Contractual Requirements (CDRL#)	SS and environmental and occupational language, SS CDRL items, and ESOH DFARS clauses
Description/Comments	Description of how design minimizes SS risks by summarizing how the program has integrated SS considerations into Systems Engineering processes including the method for tracking hazards and SS risks and mitigation plans throughout the life cycle of system

The Systems Engineer and SS SMEs also provide input to other program documentation such as the: AS, TEMP, LCSP, system performance specifications, solicitations, contracts, and capability documents.

The repository for SS data and information should include, but not be limited to:

- SS Risk Matrices (for hardware and software) used by the program with definitions for severity categories, probability levels, risk levels, and risk acceptance and user-representative concurrence authorities. (*Note:* If a program is using risk matrices other than those required by MIL-STD-882, the program documents the formal Component approval for those alternative matrices in the SS Program Plan.).
- The data for each hazard in the HTS. (*Note*: Providing an electronic copy of the current data from the HTS would satisfy this requirement.).
- In addition to the applicable hazard and risk data, the program should include the following data for each hazardous material, hazardous waste and pollutant associated with the system: the specific uses, locations, quantities and plans for their minimization and/or safe disposal. (providing an electronic copy of the current data from either the

HTS (if it includes this information) or the hazardous materials management data would satisfy this requirement.).

- Environmental impact information not included in the HTS or hazardous materials tracking system needed to support NEPA/EO 12114 compliance activities.

Programs should use the results of the sustainability analysis (see Section 2.2.6 Sustainability Analysis) to inform the hazard analysis.

DoDI 5000.88, Section3.6.e. requires that each program maintain a NEPA/EO 12114 compliance schedule. This schedule includes but is not limited to:

- Each proposed action (e.g., testing or fielding)
- Proponent for each action (i.e., the organization that exercises primary management responsibility for a proposed action or activity)
- Anticipated start date for each action at each specific location
- Anticipated NEPA/EO 12114 document type
- Anticipated start and completion dates for each document
- The document approval authority

The PM should incorporate the NEPA/EO 12114 Compliance Schedule into the program IMS and IMP.

Because actions occurring during technology development and system development may require NEPA/EO 12114 compliance, the program should identify these compliance requirements early in the SEP. DoDI 5000.88, Section 3.6.e. also requires programs to support other organizations NEPA/EO 12114 analyses involving their systems.

5.23.7 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.

- High SS risks require CAE acceptance
- Serious SS risks require PEO-level acceptance
- Medium and Low SS risks require PM acceptance

This means a given SS risk may require multiple risk acceptances as the risk level changes across the life of a system. For example:

- During development, the risk level will change as the program funds and implements identified controls.
- During testing, the risk level may change as a result of test configurations, which differ from the eventual system design.
- During sustainment of a fielded system, the risk level may change as the system ages and as more information about a given risk becomes available.

For joint programs, the SS risk acceptance authorities reside within the lead DoD Component (unless the MDA approves an alternative) and each participating DoD Component provides an appropriate user representative. Joint programs should identify the specific risk acceptance authority and user representative offices in the PESHE. If a joint program uses a MOA to document risk acceptance authority and user representative offices, they should attach the MOA to the PESHE.

The program documents formal risk acceptances in the System Safety Risk Assessment as part of the program record (e.g., HTS). If a risk level increases for a hazard, a new risk acceptance is required before exposing people, equipment or the environment to the increased risk. The program also participates in system-related mishap investigations to assess contributing hazards, risks and mitigations.

DoDI 5000.88, Section 3.6.e. requires programs to report the status of current high and serious SS risks at program reviews and fielding decisions and the status of all SS risks at technical reviews. The purpose of this reporting is to inform the MDA, PEO, PM and end user about trades being made and SS risks that need to be accepted. Each SS risk report includes the following:

- The hazard, potential mishap, initial RAC and risk level
- Mitigation measure(s) and funding status
- Target RAC and risk level
- Current RAC and risk level
- Risk acceptance/user representative concurrence status

In accordance with MIL-STD-882, a risk is never closed nor is the term “residual” risk used. This enables programs to ensure, as their system changes occur over time; they assess those changes for any potential to alter existing risk levels or to add hazards. This also enables a program to determine the potential for eliminating hazards or reducing their risk levels as the program implements system design or operating and maintenance procedure changes.

5.23.8 Hazardous Materials Management

Hazardous Material (HAZMAT) management is an integral part of the risk management effort within the program’s SE process using this Standard's methodology. When HAZMAT, including

any item or substance that, because of its chemical, physical, toxicological, or biological nature, could cause harm to people, equipment, or the environment are designed into the system or used for system operation and maintenance, the PM and Systems Engineer assess and document the risks for each combination of HAZMAT and application. (NOTE: The use of certain HAZMATs in system design can increase life cycle cost and create barriers to Foreign Military Sales.) The Systems Engineer can use the optional Task 108, Hazardous Materials Management Plan, in MIL-STD-882 and/or the AIA National Aerospace Standard (NAS) 411, Hazardous Materials Management Program, as the basis for a program's HAZMAT management. Both Task 108 and NAS 411 require a contractual listing of the HAZMAT, which the program intends to manage. The contractual listing categorizes each listed HAZMAT as Prohibited, Restricted or Tracked. NAS 411-1, Hazardous Material Target List, provides a DoD-AIA agreed-upon baseline listing of HAZMAT for each category to use as the starting point in defining the program's list of HAZMAT. When using either Task 108 or NAS 411, the PM and Systems Engineer should document the following data elements for each listed HAZMAT:

- HAZMAT item or substance name (with Chemical Abstract Services Number if available).
- HAZMAT Category (Prohibited, Restricted or Tracked).
- Special Material Content Code as designated in Federal Logistics Information System (FLIS) Technical Procedures Volume 10.
- The locations, quantities, and usage of each HAZMAT embedded in the system or used during operations and support of the system, with traceability, as applicable, to version specific hardware designs.
- ESOH requirements for demilitarization and disposal.
- Energetic qualification information, as applicable.
- Reasonably anticipated quantities of hazardous waste generated during normal operation and maintenance.
- Reasonably anticipated HAZMAT (whether categorized or not) generated during the system's life cycle (e.g., installation, Government test and evaluation, normal use and maintenance or repair of the system).
- Hazardous emissions/discharges, including those reasonably anticipated in emergency situations.
- Special control, training, handling, Personal Protective Equipment and storage requirements, including provision of required Safety Data Sheets, previously called Material Safety Data Sheets.

The Systems Engineer manages hexavalent chromium usage in systems to balance the requirements for CPC and the procedures in DFARS (Subpart 223.73 - Minimizing the Use of

Hexavalent Chromium). For more information on chemicals/materials of evolving regulatory concern, refer to the DENIX website.

5.23.9 Safety Release for Testing

The PM, in concert with the user and the T&E community, provides safety releases (including formal ESOH risk acceptance in accordance with DoDI 5000.88, Section 3.6.e.), to the developmental and operational testers before any test exposing personnel to ESOH hazards. The safety release addresses each system hazard present during the test and includes formal risk acceptance for each hazard. The program's safety release is in addition to any test range safety release requirements, but it should support test range analyses required for a range-generated test release. Safety releases should be documented as part of the Program Record.

The PM should provide a transmittal letter to the involved test organization with a detailed listing of the system hazards germane to the test that includes the current risk level and documented risk acceptance along with information on all implemented mitigations.

5.23.10 Safety Confirmation

The PM, in concert 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. It includes a risk assessment for hazards not adequately controlled, lists technical or operational limitations, and highlights safety problems requiring further testing. The SC is provided for milestone and materiel release decision reviews, fielding, and equipping.

5.23.11 Sustainable Procurement Program

In an effort to enhance and sustain mission readiness over the system life cycle, reduce reliance on resources and reduce the DoD footprint, programs should follow the policy and procedures identified in the DoD Sustainable Procurement Program (SPP). SPP benefits include:

- Improving mission performance by decreasing life cycle costs and reducing liabilities.
- Reducing impacts to human health and the environment.
- Ensuring availability of chemicals and materials.
- Enhancing installation and national security by reducing dependence on foreign energy sources.
- Contributing to regulatory compliance.
- Increasing potential for Foreign Military Sales.

PMs should implement the applicable SPP procedures in FAR (Subparts 23.2, 23.4, 23.7 and 23.8) to select materials and products that are energy-efficient, water conserving and environmentally preferable. More information on SPP is available on the DENIX website.

5.23.12 Climate Change

In an effort to continuously adapt current and future DoD operations to address the impacts of climate change, and to maintain an effective and efficient U.S. military, DoDD 4715.21 (para 1.2, 2.1, and 2.4) requires programs to integrate climate change considerations, including life cycle analyses, into acquisitions.

Key Resources

- Acquisition Community Connection/ESOH
- Defense Acquisition University Continuous Learning Modules "CLE 009 – ESOH in Systems Engineering" and "CLR 030 - ESOH in JCIDS"
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Federal Acquisition Regulation (FAR)
- Joint Software System Safety Engineering Handbook, August 27, 2010
- MIL-STD-882 with 25 optional Tasks
- Joint Services Software Safety Authorities' "Software System Safety Implementation Process and Tasks Supporting MIL-STD-882
- Allied Ordnance Publication (AOP) 52, Guidance on Software Safety Design and Assessment of Munitions Related Computing Systems
- The Unmanned System Safety Engineering Precepts Guide for DoD Acquisition

5.24 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 systems engineering (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 (forthcoming), Section 3.8), 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. The PPP (see T&PP Guidebook (forthcoming), Sections 3.4 and 3.5) documents the comprehensive approach to SSE analysis and the associated results.

SSE analysis results should be captured in the PPP, provided at each technical review and audit (see T&PP Guidebook (forthcoming), Section 3.4) 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 AAFDIT and DoDI 5000.83, Section 3.4.c.) due at the Development RFP Release Decision Point. For other programs, PPPs are developed and submitted as directed by components for Operation of Middle Tier Acquisition, Urgent Capability Acquisition, and Software Acquisition programs The 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 (forthcoming), Section 5) 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. The cross-discipline interactions reach beyond the SSE community to the test and logistics communities. The T&PP Guidebook (forthcoming), Section 2.3, 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 addresses 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 DoD Information Network or other external security services.

- Prevents, mitigates 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.

The early and frequent consideration of SSE principles reduces re-work 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.). A best practice is to perform Mission-Based Cyber Risk Assessments early, and to update the assessments periodically as cyberspace threats and system design evolves. These assessments should be collaborative and include operational users, developers, engineers, and cyberspace threat emulation (testers).

ACRONYMS

AAF	Adaptive Acquisition Framework
AAFDIT	Adaptive Acquisition Framework Document Identification Tool
AC	Advanced Concepts
ACAT	Acquisition Category
AIA	Aerospace Industries Association
AoA	Analysis of Alternatives
APB	Acquisition Program Baseline
AS	Acquisition Strategy
ASR	Alternative Systems Review
BIT	Built-In-Test
CAC	Common Access Card
CAE	Component Acquisition Executive
CAI	Critical Application Item
CARD	Cost Analysis Requirements Description
CBRN	Chemical, Biological, Radiological and Nuclear
CCB	Configuration Control Board
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI/CD	Continuous Integration/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
CTP	Critical Technical Parameter
DA	Decision Authority
DAG	Defense Acquisition Guidebook
DCMA	Defense Contract Management Agency
DD, ENG	Deputy Director for Engineering
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
DT&E	Developmental Test & Evaluation
DoD	Department of Defense
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
FCB	Functional Capabilities Board
FD	Full Deployment

FMECA	Failure Mode, Effects and Criticality Analysis
FOCI	Foreign Ownership Control, and Influence
FP&S	Force Protection and Survivability
FRP	Full-Rate Production
GAO	Government Accountability Office
GFE	Government Furnished Equipment
HAZMAT	Hazardous Material
HC	Hazard Classification
HFE	Human Factors Engineering
HSI	Human Systems Integration
HTS	Hazard Tracking System
I&D	Interoperability and Dependency
ICD	Initial Capabilities Document
ICE	Independent Cost Estimate
ICWG	Interface Control Working Group
IDE	Integrated Data Environment
IEEE	Institute of Electrical and Electronics Engineers
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 Standards
IT	Information Technology
IUID	Item Unique Identification

JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
KSA	Key System Attribute
LCA	Life Cycle Assessment
LCSP	Life Cycle Sustainment Plan
LOR	Level of Rigor
LRIP	Low-Rate Initial Production
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MOA	Memoranda of Agreement
MOSA	Modular Open Systems Approach
MOU	Memorandum of Understanding
MRA	Manufacturing Readiness Assessment
MP	Mission Profile
MSA	Material Solution Analysis
NASA	National Aeronautics and Space Administration
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
O&S	Operations and Support
OMB	Office of Management and Budget
OMS	Operational Mode Summary

OT&E	Operational Test & Evaluation
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
P&D	Production and Deployment
PEO	Program Executive Office
PESHE	Programmatic ESOH 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
PRP	Program Risk Process
PRR	Production Readiness Review
PSM	Product Support Manager
QMS	Quality Management System
RAC	Risk Assessment Codes
RAM-C	Reliability, Availability, Maintainability, and Cost Rationale
RCM	Reliability Centered Maintenance
R&M	Reliability and Maintainability
RFP	Request for Proposal
RIO	Risk, Issues, and Opportunities
RMB	Risk Management Board
RTM	Requirements Traceability Matrix
SAE	Society of Automotive Engineers

SDP	Software Development Plan
SE	Systems Engineering
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
SPP	Sustainable Procurement Program
SRA	Schedule Risk Assessment
SRD	System Requirements Document
SRR	System Requirements Review
SS	System Safety
SSE	System Security Engineering
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&PP	Technology and Program Protection
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
TRA	Technology Readiness Assessment

TRR	Test Readiness Review
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research and Engineering
VE	Value Engineering
VECP	Value Engineering Change Proposal
VEP	Value Engineering Proposal
VOLT	Validated On-line Life Cycle Threat
WBS	Work Breakdown Structure
WCE	Worst Case Estimate
WIPT	Working-Level Integrated Product Team

REFERENCES

"Accessibility Requirements Tool." GSA. Retrieved August 11, 2021, from: https://www.buyaccessible.gov/

Adaptive Acquisition Framework Document Identification Tool (AAFDIT), forthcoming.

Air Force Instruction 33-118, "Electromagnetic Spectrum Management," July 18, 2005.

Air Force Product Data Acquisition (PDAQ) guidance.

Air Force Technical Data and Computer Software Rights Handbook.

Allied Ordnance Publication (AOP) 52, Guidance on Software Safety Design and Assessment of Munitions Related Computing Systems.

Analysis of Alternatives Guidebook, forthcoming.

Army Data and Data Right (D&DR) Guide 1st Edition, U.S. Army Product Data & Engineering Working Group, August 2015. Available at: https://www.dau.edu/cop/mosa/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/mosa/DAU%20Sponsored%20Documents/Army%20Data%20and%20Data%20Rights%20Guide%201st%20Edition%204%20Aug%202015.pdf&action=default.

Army Regulation 5-12, "Army Use of the Electromagnetic Spectrum," Headquarters Department of the Army, Washington, D.C. February 8, 2005.

ASTM-D3951, "Standard Practice for Commercial Packaging," May 1, 2018.

Aviation Critical Safety Items Management Handbook.

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

Chairman of the Joint Chiefs of Staff Instruction 5123.01H, Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," August 31, 2018.

Chairman of the Joint Chiefs of Staff Joint Capabilities Integration and Development Systems Manual, August 31, 2018.

Charlock, P.G., and R.E. Fenton, "System-of-Systems (SoS) Enterprise Systems for Information-Intensive Organizations," Systems Engineering, Vol. 4, No. 4 (2001), pages 242-261.

CJCSI 5123.01H, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the JCIDS," Aug 31, 2018.

DA Pam 95-9, “Management of Aviation Critical Safety Items,” January 25, 2006.

DD Form 1494. Available at: https://usarmyamis.army.mil/customersupport/dd1494preparationguide.pdf.

Defense Acquisition University, Defense Acquisition Guidebook, Chapter 3, “Systems Engineering,” current edition.

Defense Acquisition University Continuous Learning Modules "CLE 009 – ESOH in Systems Engineering".

Defense Acquisition University, “Milestone Document Identifier,” (n.d.). Retrieved August 11, 2021 from: https://www.dau.edu/mdid/Pages/Default.asp

“DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment.” OUSD(AT&L). Jan 1, 2014.

Defense Counterintelligence and Security Agency (n.d.) Retrieved August 11, 2021, from: https://www.dcsa.mil/

Defense Threat Reduction Agency’s Nuclear Survivability Program Guidebook (DTRA-TR-14-71).

Defense Federal Acquisition Regulation Supplement, Subpart 246.371, “Contract Clauses, Notification of potential safety issues,” June 25, 2013.

Defense Federal Acquisition Regulation Supplement, Subpart 211.274-2, “Using and Maintaining Requirements Documents, General,” Oct. 1, 2020.

Defense Federal Acquisition Regulation Supplement, Subpart 252.211-7003, “Item Unique Identification and Valuation,” Oct. 1, 2020.

Defense Federal Acquisition Regulation Supplement, Subpart 252.211-7007, “Reporting of Government-Furnished Property,” Oct. 1, 2020.

Defense Federal Acquisition Regulation Supplement, Subpart 209.270, “Aviation and ship critical safety items,” Aug. 19, 2011.

Defense Federal Acquisition Regulation Supplement, Subpart 223.73, “Minimizing the Use of Materials Containing Hexavalent Chromium,” May 20, 2021.

Defense Federal Acquisition Regulation Supplement, Subpart 246.407, “Government Contract Quality Assurance, Nonconforming supplies or services,” Oct 1, 2020.

Defense Federal Acquisition Regulation Supplement, Subpart 246.504, “Quality Assurance, Certificate of conformance,” Jan. 10, 2008.

Defense Federal Acquisition Regulation Supplement, Subpart 252.246-7003, "Notification of Potential Safety Issues," December 21, 2018.

Defense Federal Acquisition Regulation Supplement, Subpart 207.105, "Contents of Written Acquisition Plans," [DATE].

Defense Federal Acquisition Regulation Supplement, Subpart 215.304, "Source Selection, Evaluation factors and significant subfactors," December 31, 2019.

Department of the Army Pamphlet 25-1-1 "Army Information Technology Implementation Instructions," July15, 2019. Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN8541_PAM25-1-1_FINAL.pdf.

DI-MGMT-81861, Integrated Program Management Data and Analysis Report (IPMDAR). March 12, 2020.

DoD 4145.19-R, "Storage and Warehousing Facilities and Services," July 1978. Available at: https://biotech.law.lsu.edu/blaw/dodd/corres/pdf/414519r_0678/p414519r.pdf.

DoD 4140.27-M, "Shelf-Life Management Manual." Department of Defense, May 5, 2003.

DoD 5010.12-M, "Procedures for the Acquisition and Management of Technical Data." Office of the Under Secretary of Defense for Acquisition and Sustainment. May 1993, incorporating Change 1, Aug. 31, 2018.

DoD 8400.01-M, "Accessibility of Information and Communications Technology (ICT)," Office of the Chief Information Officer of the Department of Defense November 14, 2017.

DoD Acquisition Manager's Handbook for Insensitive Munitions, Revision 02, November 2008.

DoD Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment (MS&E), January 14, 2014.

DoD Cybersecurity Test and Evaluation Guidebook v.2.0 April 25, 2018, as amended. Version 2.0 available at: https://daytonaero.com/wp-content/uploads/DOD_Cybersecurity-Test-Evaluation-Guidebook-ver-2.0_25-APR-2018.pdf

DoD Directive 4151.18, "Maintenance of Military Materiel," Office of the Under Secretary of Defense for Acquisition and Sustainment, Aug 31, 2018.

DoD Directive 4715.21, "Climate Change Adaptation and Resilience," Jan 14, 2016.

DoD Directive 5000.01, "The Defense Acquisition System," Office of the Under Secretary of Defense for Acquisition and Sustainment, September 9, 2020.

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", Office of the Under Secretary of Defense for Research and Engineering, 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, August 29, 2017.

DoD Directive 6055.09E, "Explosives Safety Management (ESM)," Office of the Under Secretary of Defense for Acquisition and Sustainment, Nov. 18, 2016.

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," Office of the Chief Information Officer of the Department of Defense, March 17, 2016, as amended.

DoD Directive 8260.05, "Support of Strategic Analysis (SSA)," Office of the Cost Assessment and Program Evaluation, July 7, 2011.

DoD Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 1.0, 2006.

DoD Guide to Uniquely Identifying Items, Version 2.5, September 15, 2012.

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," Office of the Under Secretary of Defense for Acquisition and Sustainment, July 29, 2009, Incorporating Change 1, Aug 31, 2018.

DoD Instruction 3150.09, "The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy," Office of the Under Secretary of Defense for Acquisition and Sustainment, April 8, 2015, Incorporating Change 2, Aug 31, 2018.

DoD Instruction 3222.03, "DoD Electromagnetic Environmental Effects (E3) Program," Aug 25, 2014, Office of the Chief Information Officer of the Department of Defense, Incorporating Change 2, Oct. 10, 2017.

DoD Instruction 4140.01, Office of the Under Secretary of Defense for Acquisition and Sustainment, "DoD Supply Chain Materiel Management Policy," March 6, 2019.

DoD Instruction 4120.24, "Defense Standardization Program," Office of the Under Secretary of Defense for Research and Engineering, October 15, 2018.

DoD Instruction 4245.15, "Diminishing Manufacturing Sources and Material Shortages," Office of the Under Secretary of Defense for Acquisition and Sustainment, Nov. 5. 2020.

DoD Instruction 4160.28, "DoD Demilitarization (DEMIL) Program," Office of the Under Secretary of Defense for Acquisition and Sustainment, April 7, 2011, Incorporating Change 2, Aug. 31, 2018.

DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," Office of the Under Secretary of Defense for Acquisition and Sustainment, April 26, 2013, Incorporating Change 3, March 6, 2020.

DoD Instruction 4140.01, "DoD Supply Chain Materiel Management Policy," Office of the Under Secretary of Defense for Acquisition and Sustainment, March 6, 2019.

DoD Instruction 4151.19, "Serialized Item Management (SIM) for Life-Cycle Management of Materiel," Office of the Under Secretary of Defense for Acquisition and Sustainment, Jan. 9, 2014, Incorporating Change 2, Aug. 31, 2018.

DoD Instruction 4245.15, "Diminishing Manufacturing Sources and Material Shortages Management", Office of the Under Secretary of Defense for Acquisition and Sustainment, November 5, 2020.

DoD Instruction 4540.07, "Operation of the DoD Engineering for Transportability and Deployability Program," Office of the Under Secretary of Defense for Acquisition and Sustainment, Feb. 19, 2016, as amended.

DoD Instruction 4151.22, "Condition-Based Maintenance Plus for Materiel Maintenance," Office of the Under Secretary of Defense for Acquisition and Sustainment, Aug. 14, 2020.

DoD Instruction 4630.09, "Communications Waveform Management and Standardization," Office of the Chief Information Officer of the Department of Defense, July 15, 2015, as amended.

DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," Office of the Chief Information Officer of the Department of Defense, January 9, 2009, as amended.

DoD Instruction 5000.PR, "Human Systems Integration", Office of the Under Secretary of Defense for Research and Engineering, forthcoming.

DoD Instruction 5000.PS, "Product Support", Office of the Under Secretary of Defense for Acquisition and Sustainment, forthcoming.

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework", Office of the Under Secretary of Defense for Acquisition and Sustainment, January 23, 2020.

DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," Office of the Under Secretary of Defense for Acquisition and Sustainment, January 7, 2015, as amended.

DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," Office of the Under Secretary of Defense for Acquisition and Sustainment, April 27, 2017, as amended.

DoD Instruction 5000.66, "Defense Acquisition Workforce Education, Training, Experience, and Career Development Program", Office of the Under Secretary of Defense for Acquisition and Sustainment, September 13, 2019.

DoD Instruction 5000.67, "Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure," Office of the Under Secretary of Defense for Acquisition and Sustainment, August 31, 2018, as amended.

DoD Instruction 5000.82, "Acquisition of Information Technology (IT)," Office of the Chief Information Officer of the Department of Defense, April 21, 2020.

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage", Office of the Under Secretary of Defense for Research and Engineering, July 20, 2020.

DoD Instruction 5000.85, "Major Capability Acquisition", Office of the Under Secretary of Defense for Acquisition and Sustainment, August 6, 2020.

DoD Instruction 5000.88, "Engineering of Defense Systems," Office of the Under Secretary of Defense for Research and Engineering, November 18, 2020.

DoD Instruction 5000.89, "Test and Evaluation", Office of the Under Secretary of Defense for Research and Engineering, November 19, 2020.

DoD Instruction 5025.13, "DoD Plain Language Program", Office of the Chief Management Officer of the Department of Defense, January 23, 2020.

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, October 1, 2020.

DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," Office of the Under Secretary of Defense for Intelligence and Security/Office of the Under Secretary of Defense for Research and Engineering, Incorporating Change 3, Effective October 1, 2020.

DoD Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),” Office of the Under Secretary of Defense for Intelligence and Security/Office of the Under Secretary of Defense for Research and Engineering, Incorporating Change 3, Effective October 15, 2018.

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 Technical Documents,” Office of the Under Secretary of Defense for Research and Engineering, Incorporating Change 3, October 15, 2018.

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance,” Office of the Chief Information Officer of the Department of Defense, July 14, 2015.

DoD Instruction 8320.03, “Unique Identification (UID) Standards for Supporting the DoD Information Enterprise,”, Office of the Under Secretary of Defense for Acquisition and Sustainment, Incorporating Change 2, August 31, 2018.

DoD Instruction 8320.04, “Item Unique Identification (IUID) Standards for Tangible Personal Property,” Office of the Under Secretary of Defense for Acquisition and Sustainment, Incorporating Change 3, August 271, 2019.

DoD Instruction 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” Office of the Chief Information Officer of the Department of Defense, May 21, 2014, as amended.

DoD Instruction 8500.01, “Cybersecurity,” Office of the Chief Information Officer of the Department of Defense, Incorporating Change 1, Effective October 7, 2019.

DoD Instruction 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information,” Office of the Chief Information Officer of the Department of Defense, Dec 9, 2019.

DoD Manual 4120.24, “Defense Standardization Program Procedures,” Office of the Under Secretary of Defense for Research and Engineering, September 24, 2014, Incorporating Change 2, Effective October 15, 2018.

DoD Manual 4140.01, Volume 11, “DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling,” Office of the Under Secretary of Defense for Acquisition and Sustainment, March 8, 2017, as amended.

DoD Manual 4140.01, “DoD Supply Chain Materiel Management Procedures: Delivery of Materiel.” Office of the Under Secretary of Defense for Acquisition and Sustainment, Feb 10, 2014.

DoD Manual 4140.27, Volume 1, "DoD Shelf-Life Management Program: Program Administration." Office of the Under Secretary of Defense for Acquisition and Sustainment, July 6, 2016, as amended.

DoD Manual 4151.22-M, "Reliability Centered Maintenance (RCM)", Office of the Under Secretary of Defense for Acquisition and Sustainment, Incorporating Change 1, August 31, 2018.

DoD Manual 4160.21-M, Volume 1, "Defense Materiel Disposition: Disposal Guidance and Procedures." Office of the Under Secretary of Defense for Acquisition and Sustainment, Oct. 22, 2015, as amended.

DoD Manual 4160.28, Vol. 1, "Defense Demilitarization: Program Administration." Office of the Under Secretary of Defense for Acquisition and Sustainment, Aug. 9, 2017, as amended.

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-M, "Accessibility of Information and Communications Technology (ICT). Office of the Chief Information Officer of the Department of Defense, November 14, 2017.

DoD 5010.12-M, Procedures for the Acquisition and Management of Technical Data, Office of the Under Secretary of Defense for Acquisition and Sustainment, May 14, 1993, Incorporating Change 1, August 31, 2018.

DoD Modeling and Simulation Catalog. April 21, 2015. Available at: 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. Available at: https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf

DoD Open Systems Architecture Contract Guidebook for Program Managers v 1.1, June 2013.

DoD Operational Energy Strategy: Implementation Plan, March 2012. Available at: https://www.globalsecurity.org/military/library/policy/dod/operational-energy-strategy_implementation-plan201203.pdf

DoD R&M Engineering Management Body of Knowledge, Office of the Deputy Director for Engineering.

DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, January 2017.

DoD Systems Engineering Plan (SEP) Outline v4.0, September, 2021.

DoD Systems Engineering Guide for Systems of Systems v1.1, August 2008.

DoD Technology Readiness Assessment (TRA) Guidance, April 2011.

DTR 4500.9-R, Defense Transportation Regulation.

EIA-649-1, Configuration Management Requirements for Defense Contracts, November 20, 2014.

Engineering of Defense Systems Guidebook and in the R&M Engineering Management Body of Knowledge (DDRE(AC)/Engineering website).

Executive Order 12114, National Environmental Protection Act (NEPA), Environmental Effects Abroad of Major Federal Actions, January 4, 1979

Federal Acquisition Regulation, Subpart 23.2, “Energy and Water Efficiency and Renewable Energy.”

Federal Acquisition Regulation, Subpart 23.4, “Use of Recovered Materials and Biobased Products.”

Federal Acquisition Regulation, Subpart 23.7, “Contracting for Environmentally Preferable Products and Services.”

Federal Acquisition Regulation, Subpart 23.8, “Ozone-Depleting Substances and Greenhouse Gases.”

Federal Acquisition Regulation, Subpart 39.204, “Exceptions.”

"Federal Enterprise Architecture Framework (FEAF) version 2," January 29, 2013. Available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf.

49 CFR Parts 171-180, Transportation.

GAO Report to Congressional Committees 17-77, “Detailed Systems Engineering Prior to Product Development Positions Programs for Success,” November 2016. Available at: https://www.gao.gov/assets/gao-17-77.pdf.

GAO-Report to Congressional Committees 12-400SP, “Assessment of Selected Weapon Programs,” March 2012. Available at: https://www.gao.gov/assets/gao-12-400sp.pdf.

Gill, Karen and Rusyt Mirick, “18848- An approach to ensure Design Considerations are part of the materiel solution: ESOH-related Capabilities in JCIDS Examples.” Defense Acquisition University. (n.d.) Retrieved August 11, 2021, from: https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2016/systems/18848_RobertMirick.pdf.

"Guidance for Tailoring R&M Engineering Data" by Andrew Monje, ODASD, Systems Engineering, April 2016. Available at: https://ac.cto.mil/wp-content/uploads/2020/04/2016-Tailoring-RM-Data-Monje-1.pdf.

A Guide to DoD Program Management Business Processes, forthcoming.

A Guide to Program Management Knowledge, Skills and Practices, forthcoming.

Human Systems Integration Guidebook, forthcoming.

IEEE 15288.1, Standard for Application of Systems Engineering on Defense Programs, July 7, 2015.

IEEE 15288.2 Standard for Technical Reviews and Audits on Defense Programs, July 7, 2015.

Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide, October 21, 2005.

"Intellectual Property: Navigating through Commercial Waters." Under Secretary for Defense Acquisition Technology and Logistics. October 15, 2001.

Intelligence Guidebook, forthcoming

Intelligence Support to the Adaptive Acquisition Framework (ISTAAF) Guidebook, forthcoming

ISO/IEC/IEEE 15288, Systems and Software Engineering-System Life Cycle Processes, July 7, 2015.

JACG Aviation CSI Management Handbook

The Joint Software System Safety Engineering Workgroup, "Joint Software Systems Safety Engineering Handbook. August 27, 2010. Available at: https://www.acqnotes.com/Attachments/Joint-SW-Systems-Safety-Engineering-Handbook.pdf

Life Cycle Sustainment Plan (LCSP) Outline, Version 2.0, January 2017.

Manual for the Operations of the Joint Capabilities Integration and Development System (JCIDS), Dec 18, 2015.

Manufacturing Readiness Level Deskbook, OSD Manufacturing Technology Program in collaboration with The Joint Service/Industry MRL Working Group, September 2020. Available at: https://www.dodmrl.com/MRL%20Deskbook%20V2020.pdf

Manufacturing Readiness Levels Guide. Available at: https://myclass.dau.edu/bbcswebdav/institution/Courses/Deployed/TST/TST204%20and%20

TST204V/Archives/Jan%202017%20Student%20Files/Student%20CD/1%20References/01%20DAU%20Reference/MRL%20Guide.pdf

MIL-HDBK-61, "Configuration Management Guidance," April 7, 2020.

MIL-HDBK-235-1, "Military Operational Electromagnetic Environment Profiles Part 1D General Guidance," [DATE].

MIL-HDBK-237 D, "Electromagnetic Environmental Effects and Spectrum Supportability Guidance for the Acquisition Process," [DATE].

MIL-HDBK-240, "Hazards of Electromagnetic Radiation to Ordnance Test Guide," Nov 1, 2002.

MIL-HDBK-245D, "Preparation of Statement of Work (SOW)," April 3, 1996.

MIL-HDBK-502, "Acquisition Logistics," May 30, 1997.

MIL-HDBK-896A, "Manufacturing Management Program Guide," August 25, 2016.

MIL-STD-129, "Military Marking for Shipment and Storage," [DATE].

MIL-STD-130, "Identification Marking of U.S. Military Property," [DATE].

MIL-STD-461, "Electromagnetic Interference Characteristics Requirements for Equipment," July 31, 1967.

MIL-STD-464, "Electromagnetic Environmental Effects Requirements for Systems," March 18, 1997.

MIL-STD-810, "Environmental Engineering Considerations and Laboratory Tests," [DATE].

MIL-STD-881, Work Breakdown Structures for Defense Materiel Items, October 6, 2020.

MIL-STD-882, System Safety, May 11, 2012.

MIL-STD-963, "Data Item Descriptions," August 31, 1997.

MIL-STD-1472, "Human Engineering," September 15, 2020.

MIL-STD-1546, "Parts, Materials, and Processes Standardization, Control and Management Program for Space and Launch Vehicles," Feb. 12, 1981.

MIL-STD-1547, "Electronic Parts, Materials, and Processes for Space and Launch Vehicles," Dec. 1, 1992.

MIL-STD-11991, “General Standard for Parts, Materials, and Processes,” Aug. 26, 2015.

MIL-STD-2073-1, “Standard Practice for Military Packaging.” May 23, 2008.

MIL-STD-2105, “Hazard Assessment Tests for Non-Nuclear Munitions,” July 14, 2003.

MIL-STD-31000, “Technical Data Packages,” Nov 5, 2009.

MIL-STD-3018, “Parts Management,” Oct. 15, 2007.

MIL-STD-3056, “Design Criteria for Chemical, Biological, and Radiological System Contamination Survivability,” Nov 23, 2016.

MIL-STD-46855, “Human Engineering Requirements for Military Systems, Equipment and Facilities,” May 24, 2011.

Mission Engineering Guide, OUSD(R&E). November 30, 2020. Available at: https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

Navy Technical Manual SL150-AA-PRO-010/DMP - Data Management Program.

NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)

Office of Management and Budget Memorandum, ““Myth-busting 3” Further Improving Industry Communication with Effective Debriefings”, January 5, 2017.

OPNAVINST 2400.20G, “Electromagnetic Environmental Effects and Spectrum Supportability Policy and Management,” Jan 7, 2021.

Public Law 82-436, July 1, 1952.

Public Law 114-328, “National Defense Authorization Act for Fiscal Year 2017,” December 23, 2016.

Public Law 102-538, “The National Telecommunications and Information Administration Organization Act,” October 27, 1992.

RAM-C Rationale Report Outline Guidance

RAM-C Rationale Report Outline Guidance Training

SECNAVINST 4140.2, “Management of Aviation Critical Safety Items.” AFI 20-106. DLAI 3200.4. Jan 25, 2006.

Section 104 of Public Law 102-538, Oct 27 1992.

Section 8104, Public Law 103-355, October 13, 1994.

Section 357 of Public Law 104-106, “National Defense Authorization Act for Fiscal Year 1996,” February 10, 1996.

Section 1054, Public Law 108-375, Oct 28, 2004.

Section 130, Public Law 109-364, Oct 17 2006.

Section 812, Public Law 111-383, Jan 7 2011.

Section 818 of Public Law 112-81, “National Defense Authorization Act for Fiscal Year 2012,” December 31, 2011.

Section 802, Public Law 108-136, enacted to address aviation CSIs, and Section 130 Public Law 109-364, enacted to address ship CSIs, embedded in 10 USC 2319.

Program Protection Plan Outline and Guidance, Version 1.0, July 2011.

SAE-GEIA-HB-649, Configuration Management Standard Implementation Guide, October 1, 2005.SD-2

SD-19 Parts Management Guide, December 1, 2013.

SD-22, Diminishing Manufacturing Sources and Material Shortages, September 2009.

SD-22 Diminishing Manufacturing Sources and Material Shortages, July 2016. (See: https://www.dau.edu/guidebooks/Shared%20Documents/DMSMS%20Guidebook%20(SD-22).pdf)

SD-26 DMSMS Contract Language Guidebook, October 2019.

SECNAVINST 2400.1, “Electromagnetic Spectrum Policy and Management,” May 20, 2019.

SECNAVINST 2400.2, “Electromagnetic Environment Policy and Management,” Aug. 2011.

SECNAVINST 4140.2, “[NAME],” Jan. 25, 2006.

Secretary of Defense Memorandum, "DoD Policy on Submunition Reliability," January 10, 2001

“Software System Safety Implementation Process and Tasks Supporting MIL-STD-882.”

SoS Systems Engineering and Test & Evaluation: Final Rep, ort of the NDIA SE Division SoS SE and T&E Committees.

Sustainment Guidebook, forthcoming.

Systems Engineering Digital Engineering Fundamentals, Department of Defense Digital Engineering Working Group, March 2016. Available at: https://ac.cto.mil/wp-content/uploads/2019/06/DE-Fundamentals.pdf

Technology and Program Protection Guidebook, forthcoming.

Test and Evaluation Enterprise Guidebook, forthcoming.

Unmanned Systems Safety Precepts Guide, Office of the Under Secretary of Defense for Research and Engineering, 2021.

See generally, United States Code, Title 10.

See generally, United States Code, Title 42.

See generally, United States Code, Title 47.

10 USC § 2228, Authorization of appropriations

10 USC § 2319, Encouragement of new competitors

10 USC § 2389, Ensuring safety regarding insensitive munitions

10 USC § 2430, Major defense acquisition system defined

10 USC § 138c, Assistant Secretaries of Defense

10 USC § 2358, Research and development projects

10 USC § 2443, Sustainment factors in weapon system design

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), Nov. 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

29 U.S.C. § 794d, Electronic and information technology (Section 508 of the Rehabilitation Act)

41 USC § 104, Commercially available off-the-shelf item

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 U.S.C. § 902, Establishment; assigned functions

47 USC § 903, Spectrum management activities

47 USC § 904, General administrative provisions

USD(AT&L) Memorandum, "Joint Insensitive Munitions Test Standards and Compliance Assessment," February 10, 2010

USD(R&E), “Manufacturing & Quality,” (n.d.). Retrieved August 11, 2021, from: https://ac.cto.mil/maq/

U.S. Defense Information Systems Agency and the Defense Spectrum Organization. “Joint Services Guide for Development of a Spectrum Supportability Risk Assessment (SSRA).” Available at: https://acc.dau.mil/, September 2011.Joint Services Software Safety Authorities’

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/

Systems Engineering Guidebook

Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd.r-e.comm@mail.mil
https://ac.cto.mil/engineering