CH 3–1. Purpose
The Defense Acquisition Guidebook (DAG), Chapter 3 provides overarching guidance on the systems engineering discipline, its activities and processes and its practice in defense acquisition programs. The Program Manager (PM) and the Systems Engineer should use this chapter to effectively plan and execute program activities across the system life cycle.

CH 3–2. Background
Systems engineering (SE) establishes the technical framework for delivering materiel capabilities to the warfighter. SE provides the foundation upon which everything else is built and supports program success. SE ensures 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 also enables the development of resilient systems that are trusted, assured and easily modified. The value of systems engineering is supported by the GAO Report 17-77, which indicates that, “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 detailed systems engineering is done 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 effective and 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.

"Positive acquisition outcomes require the use of a knowledge-based approach to product development that demonstrates high levels of knowledge before significant commitments are made. In essence, knowledge supplants risk over time." (Source: GAO Report 12-400SP)

Additional SE benefits are that it:

- 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 chapter uses the following terms:

- The "Systems Engineer" refers to the Program Lead Systems Engineer, the Chief Engineer or Lead Engineer with SE responsibility and the SE staff responsible for SE processes and who plan, conduct and/or manage SE activities 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.

Definition of Systems Engineering
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, 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: The System**

- **System**: An aggregation of system elements and enabling system elements to achieve a given purpose or to provide a capability.

  - **System Elements**: Also referred to as configuration items, subsystems, segments, components, assemblies, or parts.
  - **Enabling System Elements**: Provide the means for putting a capability into service, keeping it in service, or ending its service, e.g., processes or products used to enable system development, test, production, training, deployment, support, and disposal.

Each system element or enabling system element may include, but is not limited to, hardware, software, people, data, processes, facilities, and tools.

SE applies critical thinking to the acquisition of a capability. It is a holistic, integrative discipline, whereby the contributions across engineering disciplines, such as structural engineers, electrical engineers, mechanical designers, software engineers, human factors engineers and 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 multi-disciplined 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 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. Prior to program initiation, the Program Manager (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 effectively addresses the capability gap(s), desired operational attributes and associated dependencies of the desired capability. In addition, development planning ensures that there exists a range of technically feasible solutions generated from across the entire solution space and that consideration has been given to near-term opportunities to provide a more rapid interim response to the capability need. Development planning is initiated prior to the Materiel Development Decision review,
continues throughout the Materiel Solution Analysis phase, and transitions the knowledge (documents, tools and related data) to the designated program.

**Affordability**

The Systems Engineer contributes to defining, establishing and achieving affordability goals and caps throughout the life cycle of the system. Affordability goals are set early in the program to inform capability requirements and major design trade-offs to define the product being acquired. Likewise, affordability caps are fixed cost requirements set prior to Milestone B that are equivalent to Key Performance Parameters (KPP). Affordability goals and caps are based on future estimates of what the Department can afford to spend for the capability, including program procurement and sustainment costs. Affordability goals and caps are used as design constraints in the development, procurement and sustainment of an affordable system. See CH 3-4.3.2. Affordability - Systems Engineering Trade-Off Analyses, for more information on how affordability drives design decisions.

The PM controls requirements growth and should use affordability goals early to guide design trades and program decisions. The Systems Engineer assists in managing affordability by working closely with the program cost estimator/analyst team when developing common cost and technical models and aligning baselines. See CH 1-4.2.1.1. for more information on affordability.

Throughout the acquisition life cycle, the PM and Systems Engineer should monitor the system affordability, seek out cost saving opportunities and identify any associated cost, schedule and performance risks. The PM’s emphasis prior to Milestone B should be on defining and achieving affordability goals and caps and desired capabilities. During the Technology Maturation and Risk Reduction (TMRR) phase, the PM and Systems Engineer work to reduce technical risk and develop a sufficient understanding of the materiel solution development to validate design approaches and cost estimates, to refine requirements, and to ensure affordability is designed in to the desired capability. After Milestone B, the affordability emphasis shifts to defining and achieving should-cost estimates.

Should-cost management is a deliberate strategy to drive cost efficiencies and productivity growth into programs. The will-cost estimate is the likely life-cycle cost of the system based on historical data and represents the program’s independent cost estimate, e.g., as generated by the Cost Assessment and Program Evaluation (CAPE) office or Service equivalent. As the program identifies inefficiencies, the should-cost estimate is developed based on specific actions and opportunities to mitigate, eliminate or reduce those inefficiencies that allow the program to come in below the expected will-cost estimates. The PM, with support from the Systems Engineer, develops program office cost estimates reflecting should-cost opportunities and plans. The PM and Systems Engineer use the should-cost estimate as a tool to:

- Influence design trades and choices when analyzing and setting contract/production execution targets
- Manage all costs throughout the product’s life cycle
- Manage the product’s final unit and sustainment cost
- Provide incentives for both of the parties (Government and industry) to execute efficiently: Government managers, who seek more value for the warfighter and taxpayer; and industry managers, who develop, build and sustain the systems and provide needed services

Should-cost management focuses on controlling the cost of both current and planned work. To have an impact, these activities should inform contract negotiations leading up to Engineering and Manufacturing Development (EMD) and Production and Deployment (P&D) phases. Should-cost management does not mean trading away the long-term value of sound design practices and disciplined SE activities for short-term gain; it does mean eliminating low-value-added activities and reports that are not required and that are deemed unessential. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Memorandum, “Should Cost Management in Defense Acquisition” describes that should-cost management is a core initiative of Better Buying Power and is an important tool to control costs in the short term and throughout the product life cycle. For guidance on implementing should-cost management, see the Better Buying Power website.
PMs address affordability requirements and begin to apply should-cost management early in the acquisition life cycle. This includes applying SE to define an affordable system design while also working to eliminate inefficiencies and duplication where applicable and to drive productivity improvements into their programs. Throughout the life cycle, PMs and Systems Engineers should consider Value Engineering as a key tool for meeting or beating affordability constraints and should-cost targets (See CH 3–2.4.4, Value Engineering).

**Systems Engineering Processes**

The practice of SE is composed of 16 processes: eight technical processes and eight technical management processes as listed in Figure 2 and described in CH 3–4. Additional Planning Considerations. 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 management processes are implemented across the acquisition life cycle and provide insight and control to assist the PM and Systems Engineer to meet performance, schedule and cost goals. The eight technical processes closely align with the acquisition life-cycle phases and include the top-down design processes and bottom-up realization processes that support transformation of operational needs into operational capabilities.

The purpose of the SE processes is to 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. Implementation of the SE processes begins with the identification of a validated operational need as shown in the top left corner of the V-diagram (see Figure 2). The technical processes enable the SE team to ensure that the delivered capability accurately reflects the operational needs of the stakeholders. The key activities accomplished by the execution of the technical processes are described below:

- During the Stakeholder Requirements Definition process, the operational requirements and inputs from relevant stakeholders are translated into a set of top-level technical requirements. These requirements are decomposed and elaborated during the Requirements Analysis process to produce a complete set of system functional and performance requirements.
- During the Architecture Design process, the Systems Engineer, 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 together 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 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 focused on providing operational capability to the warfighter while reducing technical and programmatic risk.

**Figure 2: Systems Engineering Processes**
All organizations performing SE should scale their application and use of the processes in CH 3–4. Additional Planning Considerations on 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, life-cycle phase and other relevant considerations. For example, lower-risk, less-complex programs may scale the processes to ensure key 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). In CH 3–4, Figure 30 provides a representation of how much effort is typically focused on each of the SE processes throughout the acquisition life cycle.

**CH 3–2.1 Systems Engineering Policy and Guidance**

Policy and guidance related to systems engineering (SE) 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. Program Managers (PMs) and Systems Engineers should know and understand the statutory and regulatory SE mandates. Table 1 identifies top-level SE-related policy.

**Table 1: Systems Engineering-Related Policy**

<table>
<thead>
<tr>
<th>SE Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoDD 5000.01, The Defense Acquisition System</td>
</tr>
<tr>
<td>DoDI 5000.02, Operation of the Defense Acquisition System</td>
</tr>
</tbody>
</table>
Additional SE-related policy and guidance is provided on the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) website.

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 Acquisition Streamlining and Standardization Information System (ASSIST) database is the official source for current Department of Defense (DoD) specifications and standards.

Compliance with DoD SE policy is required for program approval and completion of successful milestone decisions. 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.

Within this policy and guidance framework, tailoring the acquisition effort to meet program cost, schedule and performance goals is not only desired but mandated in accordance with DoD Directive (DoDD) 5000.01, para 4.3.1 and DoD Instruction (DoDI) 5000.02, para 5. In July 2012, USD(AT&L) emphasized there is no one-size-fits-all optimal program structure. 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, program tailoring should be based on the specifics of the product being acquired, including complexity, acquisition category, risk factors and required timelines to satisfy validated capability requirements. Areas that should be considered for tailoring include:

- Documentation of program information
- Execution of the acquisition phases
- Type of acquisition strategy
- Timing and scope of decision reviews
- Decision approval levels

The requirements of DoD SE policy that are identified for tailoring by the PM are submitted to the Milestone Decision Authority (MDA) 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. Critical thinking during early program formulation is important to clearly 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, para 5.c.3 describes several acquisition models that serve as examples of defense program structures tailored to the type of product being acquired or to the need for accelerated acquisition. (See CH 3–3.1.1, Systems Engineering in
Defense Acquisition Program Models for more information on these models and the expected application for each model, highlighting the relevant SE 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 or is a key enabler 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 CH 3–2.4.5, Lessons Learned, Best Practices, Case Studies).

### CH 3–2.2 Systems Engineering Plan

The purpose of the Systems Engineering Plan (SEP) is to help Program Managers (PMs) develop, communicate and manage the overall systems engineering (SE) approach that guides all technical activities of the program. The SEP documents key technical risks, 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 and/or plans and current status. DoDI 5000.02, Enc 3, sec. 2 requires PMs to prepare a SEP to guide the systems engineering 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 Acquisition Program Baseline (APB), Acquisition Strategy (AS), Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP), Life-Cycle Sustainment Plan (LCSP) and other program plans as appropriate. The SEP should be written in plain language to clearly communicate plans for each phase of the acquisition 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, Major Defense Acquisition Programs (MDAPs) should review, tailor and implement applicable mission assurance concepts and principles when developing their SEP. MDAPs should use resources provided by their service (for example, the Aerospace/Air Force Mission Assurance Guide TOR-2007(8546)-6018).

For MDAPs and Major Automated Information Systems (MAIS), the PM should formally charter a 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 5000.02, Enc 3, sec. 2 requires the Deputy Assistant Secretary of Defense (Systems Engineering) (DASD(SE)) be the approval authority for all programs under AT&L oversight; for all other programs, the MDA will be the approval authority. The formal SEP will be submitted for approval before Milestone A, B, and C and program restructures. DoDi 5000.02, Enc 3, sec. 2 also requires the DASD(SE) to review all MDAPs and MAIS program SEPs. DoD Components are required to submit the SEP to the DASD(SE) 45 calendar days prior to the scheduled Defense Acquisition Board Milestone review for all MDAPs and MAIS programs. Additionally, a draft SEP (as defined in DoDi 5000.02, Enc 1, sec. 3) is due to the MDA at the Development RFP Release Decision Point. For MDAP and MAIS, this draft SEP will be provided to DASD(SE) 45 calendar days prior to the Development RFP Release Decision Point. As a best practice, SEP updates should be approved by the Program Executive Office (PEO) prior to 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 (RMP), 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 5000.02, Enc 3, sec. 2, 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 and Systems 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. 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 key activities, resources, tools and events that support execution of the SE technical processes and technical management processes (see CH 3–4. Additional Planning Considerations) to deliver a balanced solution to meet the warfighter’s needs. It should identify unique processes, tools and/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 CH 3–4.1.5. Risk Management Process).
- The event-driven technical review approach based on successful completion of key activities as opposed to calendar-based deadlines. Document the plans for conducting each technical review with particular emphasis on the entry/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 key 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 and updates. SEPs submitted to the approval authority should include a current schedule, with all appropriate technical reviews, no more than three months old.
- 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.
- The description of the architecture products that will be developed to better describe and understand the system, to include 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/interface specifications.
- The approach for how requirements and technical performance trade-offs are balanced within the larger program scope to deliver operationally effective, suitable and affordable systems. Key design considerations and criteria (see CH 3–4.3.) should be listed in the mandatory table as applicable, with all the associated documentation submitted with each SEP submission.
- The program’s strategy for identifying, prioritizing and selecting the set of technical performance measures 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. The following TPMMs should be considered for inclusion: Risk Management, Schedule Risk, Net Ready KPP, Number of Class 1 Engineering Change Proposals (ECPs) and Number of Class 2 ECPs. Additionally, the program should ensure that each Critical Technical Parameter (CTP) has a corresponding TPM (see CH 3-4.1.3.1. Technical Performance Measures).

- The plan and description should be documented for how the system design enables technology insertion and refresh.
- The SE tools and other enablers integrated and used to support SE processes, technical design initiatives and activities.

**CH 3–2.3 Systems Level Considerations**

A system should not be acquired in isolation from other systems with which it associates in the operational environment. The Program Manager (PM) and Systems Engineer should understand how their system fills the needs for which it was designed and the enterprise context within which it operates. When the system functions as part of a Family of Systems/ System of Systems (FoS/SoS), systems engineers should examine the Concept of Operations (CONOPS)/Operational Mode Summary/Mission Profile (OMS/MP) and Initial Capability Document (ICD) 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 and Systems Engineer should define intersystem interfaces using a systems engineering (SE) document, i.e., the interface control document(s). In addition to interface control documents, the PM and Systems Engineer should also actively pursue Memoranda of Agreement or Memoranda of Understanding (MOA/MOU) with companion programs regarding interfaces, data exchanges, and advance notices 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 are 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 systems of systems. 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. 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, 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 described as 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 and/or among the individual systems being integrated are significantly important and 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, 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: Comparing Systems and Systems of Systems

<table>
<thead>
<tr>
<th></th>
<th>System</th>
<th>System of Systems (SoS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management &amp; Oversight</td>
<td>Clearer set of stakeholders</td>
<td>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</td>
</tr>
<tr>
<td>Stakeholder Involvement</td>
<td></td>
<td>Added levels of complexity due to management and funding for both SoS and systems; No single manager controls all constituent systems in the SoS</td>
</tr>
<tr>
<td>Governance</td>
<td>Aligned PM and funding. Higher levels of governance such as PEO and AT&amp;L (internal and external governance)</td>
<td></td>
</tr>
<tr>
<td>Operational Environment</td>
<td>Designed and developed to meet operational objectives</td>
<td>Called upon to provide integrated capabilities using systems whose objectives have not been directly derived from current SoS system’s objectives</td>
</tr>
</tbody>
</table>

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 & Evaluation              | Test and evaluation (T&E) of the system is possible | Testing more challenging due to 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 |
System | System of Systems (SoS)
--- | ---
evaluate evidence from SoS level activities or roll-ups of system-level activities

### Engineering & Design Considerations

<table>
<thead>
<tr>
<th>Boundaries &amp; Interfaces</th>
<th>Focuses on boundaries and interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance &amp; Behavior</strong></td>
<td>Ability of the system to meet performance objectives</td>
</tr>
<tr>
<td><strong>System of Systems (SoS)</strong></td>
<td>Performance across the SoS that satisfies SoS user capability needs while balancing needs of the systems</td>
</tr>
</tbody>
</table>

### Application of Systems Engineering to Systems of Systems

Systems of systems (SoS) systems engineering (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. Consistent with the DoD transformation vision and enabling net-centric operations, SoS may deliver capabilities by combining multiple collaborative and independent-yet-interacting systems. 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, Appendix G addresses the application of SE to SoS. The DoD guide defines four types of SoS (see Table 3). 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. Due to 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, Department of Defense Net-Centric Services Strategy, provide SE guidance regarding SoS contexts where there is an absence of explicit shared objectives or central management.

#### Table 3: Four Types of Systems of Systems

<table>
<thead>
<tr>
<th>Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed</td>
<td>Directed 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</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>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</td>
</tr>
<tr>
<td>Collaborative</td>
<td>In collaborative SoS, the component systems interact more or less voluntarily to fulfill agreed-upon central purposes</td>
</tr>
</tbody>
</table>
Virtual SoS lacks a central management authority and a centrally agreed-upon purpose for the system of systems. Large-scale behavior emerges and may be desirable but this type of SoS relies upon relatively invisible, self-organizing mechanisms to maintain it.

CH 3–2.3.1 Software

Software (SW) is critical to advanced warfighting capability and virtually all DoD systems: weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR); logistics; enterprise networks; defense business systems; and National Security Systems. SW is a key driver of system complexity and performance and is critical to battlefield dominance and maintaining operational advantage in an environment of change. Accordingly, SW development and sustainment frequently contributes a major portion of total system life-cycle cost, schedule and risk and should be considered throughout the acquisition and Systems Engineering (SE) life cycle.

Key SW Engineering Enablers. Given the challenge and importance of SW acquisition, the Program Manager (PM) should understand and emphasize the following key Software Engineering (SWE) principles that enable efficient capability delivery to the warfighter:

- Integrate SWE into the SE Process:
  - Plan for and integrate SWE activities within SE processes and acquisition documents, particularly for system-level technical reviews and technical baselines.
  - Integrate SWE design analysis, test and demonstrations within SE processes.
- Commit to Measurement: use predictive SW metrics and quantitative analysis techniques to support data-driven decisions at every level (e.g. IPT Lead, Chief SE, PM, PEO, SAE).
- Continuously Evaluate and Update SW Schedule Estimates:
  - Substantiate SW schedule realism with a rigorous basis of estimate.
  - Continuously evaluate the viability and degree of optimism in SW schedules.
- Measure and Project SW Maturity & Readiness for T&E / User: (e.g., defects, stability).
- Rigorously Manage SW Requirements:
  - Integrate SW considerations into system requirements and design.
  - Ensure SW requirements are stable, traceable, allocated to iterations and assessed for dependencies to meet iteration goals for capability and test.
  - Manage cascading/deferred requirements and mitigate development concurrency.
- Adopt Continuous Integration/Delivery and Automated Testing:
  - Measure and incrementally deliver end-to-end performance and capabilities.
  - Verify and validate capabilities (to include prototypes) through early, incremental user demonstrations and tests in high-fidelity environments.
  - Use SW development environments that enable continuous builds and automated test.
- Continuously Assess Sufficiency of SW Staffing: quantity/experience within The Program Management Office/Contractor Program Office (PMO/KTR).

Software Engineering Competencies. In addition to the key enablers above, successful SWE requires unique expertise to address a wide range of SW knowledge areas (e.g., acquisition, development and maintenance) and SW activities and competencies (e.g., contracting, planning, requirements engineering, architecture, design, integration, build planning, measurement, technical data rights, quality assurance, verification and validation (V&V), interoperability, security, development environments, etc.). Critical competencies for SW acquisition professionals include:

- SW Development Methodology Selection: Plan for software acquisition by selecting appropriate software life-cycle models (e.g., incremental, spiral, iterative, evolutionary).
• **SW Build Planning and Management**: Manage an iterative SW development approach using testable and/or deployable builds (integrated subsets of overall capability); establish a build plan that addresses: (1) dependencies, synchronization and integration; (2) prototype- or target-hardware (HW) availability to enable developmental and operational testing of builds; and, (3) detailed SW staffing plans (derived from SW effort and schedule estimates).

• **SW Trade Studies**: Conduct trade-offs of SW technologies (e.g., government off-the-shelf (GOTS); commercial off-the-shelf (COTS) / non-developmental items (NDI); reuse; open source software (OSS); modular open systems approach (MOSA); service-oriented architecture (SOA); cloud, high performance and mobile computing).

• **SW Risk Management**: Evaluate/track SW risks as part of related component/system risks.

• **SW Measurement**: Identify, track and report metrics for SW technical performance (with respect to product performance, process, development progress and quality).

SWE knowledge should cut across the acquirer and developer/supplier teams. PMs should understand SW development principles and best practices (see CH 3–2.4.5, Lessons Learned, Best Practices and Case Studies), terms, tools, development methods (e.g., Agile software), challenges and risks. Developers should have knowledge and demonstrated experience with SW development of similar scale and complexity. Chief System Engineers and SW Engineers should be well versed in the technical and management activities of SW acquisition and SWE. SW Engineers should engage early in the life cycle to ensure that all requirements, cost/schedule estimates and risk identification/mitigation efforts (including uncertainties in estimates) address SW considerations. SW engineers are also needed to evaluate the developer’s artifacts, SW architecture; functional-, allocated-, and product-baselines; monthly SW metrics reports, SW documentation, plans, estimates, modeling and simulation capabilities and facilities/environments. Program-independent SW engineers should support validation activities.

**Software Considerations in the Acquisition Strategy.** As part of the program’s Acquisition Strategy, the PM and Systems Engineer should establish a SW acquisition strategy aligned with the program’s Acquisition Strategy, as early as possible. The strategy should address function and component allocation to determine the SW to be (1) newly developed; (2) provided as GOTS, COTS, or OSS; and (3) acquired from a combination of sources. The strategy should incorporate plans for associated data and intellectual property rights for all acquired SW. In general, DoDI 5000.02, para 5.c.3 emphasizes tailoring and offers several example acquisition models intended to serve as a starting point in structuring a program, including guidance for software-dominant programs (see CH 3–3.1.1, SE in Defense Acquisition Program Models for a summary of the tailored models).

**Software Risk Management.** SW acquisition is a critical high-risk area for most programs. As such, the PM should maintain consistent awareness of its contribution to overall program and system risk, and should manage those aspects of the program. Effective SE and SWE principles and practices should help anticipate, plan for and mitigate SW development and system integration challenges and risks. Risk and opportunity management processes should address SW considerations, particularly with respect to schedule, maturity, integration, interfaces and interoperability.

**Quantitative SWE and SW Measurement.** Quantitative insight is crucial for program success. Commitment to a quantitative (i.e. data-driven) SWE and SE approach is vital to shape program plans; monitor execution; and inform leadership of technical risks throughout the life cycle, particularly in support of major decisions. The lack of effective SW measurement plans and practice—addressing acquirer, supplier and developer needs – exposes the program to high risk.

The PM and SE/SWE should plan and use predictive metrics on a frequent, periodic basis to rigorously: (1) measure and control SW product performance; and, (2) assess SW schedule realism and maturity/readiness of SW for test and delivery to user. Leading indicators provide “early warning” to enable timely risk mitigation. The program’s measurement process and its associated goals, metrics and reports should be planned/contracted for early in the life cycle to ensure maximum insight across the prime and subcontractor suppliers/developers. The plan should consider both knowledge points (and
associated decision makers) and inflection points (changes in metric values/trends that alert decision makers to emerging problems).

Planning Artifacts. A SEP with insufficient SW Technical Performance Measures (TPMs) is inadequate to track, assess and mitigate risks related to complex SW development and maturity. Beyond the TPMs documented in the SEP, a SW Measurement Plan is recommended (for acquirer and developer) to further elaborate the quantitative management approach and to capture finer-grain SW metrics. An example of a template for a SW Measurement Plan is available from Naval Air Systems Command (NAVAIR), as Standard Work Package SWP4140-024, Software Measurement Plan Template, AIR-4.1.4, Version 3.0, dated 25 June, 2015.

Best Practices for SW Acquisition. Table 4 identifies several vital practices, and briefly describes essential elements and approaches for their implementation. Less-than-rigorous implementation of these practices has often contributed to program failure.

Table 4: SWE Best Practices: Essential Elements & Implementation Approaches

<table>
<thead>
<tr>
<th>Practice</th>
<th>Essential Elements and Implementation Approaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish high-confidence cost, effort and schedule estimates.</td>
<td>• Estimate the cost, effort and schedule (planning) as a yardstick for measuring progress and performance (executing)</td>
</tr>
<tr>
<td>For additional guidance on software cost estimation for different system types and operating environments, see the <a href="#">Software Cost Estimation Metrics Manual for Defense Systems</a>.</td>
<td>• Use at least two methods: the methods include, e.g. Wideband Delphi, Analogy, Parametric, Bottoms-Up; SW parametric statistical analysis is a best practice</td>
</tr>
<tr>
<td></td>
<td>• Reconcile multiple estimate methods and derive the estimate confidence level</td>
</tr>
<tr>
<td></td>
<td>• Frequently monitor, reassess and update initial SW estimates and schedules given the uncertainty with initial assumptions (e.g., sizing and staffing estimates)</td>
</tr>
<tr>
<td></td>
<td>• Benchmark estimates against similar DoD projects, industry norms, and most importantly with the developer’s historical performance (e.g., productivity)</td>
</tr>
<tr>
<td></td>
<td>• Update estimates and confidence based on SW metrics collected during execution</td>
</tr>
<tr>
<td></td>
<td>• Present updated estimates-to-complete at every major program review to identify deviations from the original effort/schedule baselines and risk likelihood</td>
</tr>
</tbody>
</table>

Establish and manage to a core set of predictive quantitative metrics. | • Establish predictive metrics within the SEP, SDP and SW Measurement Plan |
| Key areas to monitor include: Requirements development progress and volatility, Design progress, Code development progress (e.g., effective software lines of code (eSLOC), Story Points) eSLOC growth; SW staffing, Build delivery progress; Capability delivery; SW test progress; Defects discovered/ fixed/ deferred /backlog, Defect aging/density, SW maturity/quality (e.g. stability) | • Ensure that the RFP requires the collecting and reporting of SW metrics |
| The PM and developer should select metrics relevant to the development methodology in use. (e.g., Agile metrics – such as Team & Aggregate Velocity) | • Establish time-based plans (monthly, key knowledge points) with thresholds and control bounds to mitigate metrics that are off track from the goal |
| | • Regularly (e.g., monthly) review metrics; understand how they serve as “leading indicators,” provide early warning, and use this information to make informed decisions |
| | • Establish benchmarks based on actual performance to inform future planning |

Ensure the developer establishes and utilizes effective SW development processes, according to a Software Development Plan. | • The SDP provides details below the level of the SEP and the contractor’s SE Management Plan (SEMP) for managing SW development and integration |
| | • The SDP Data Item Description (DID) DI-IPSC-81427 is a tailorable template and a useful starting point in defining the format for an SDP |
| | • The SDP provides the SE with insight into, and a tool for monitoring, the processes being followed by the developer for each activity, the project schedules, the developer’s SW organization and resource allocations |
### Practice
- Compare software development processes and tools to assumptions used in the effort and schedule estimates
- Refer to IEEE 12207 and/or ISO/IEC 15288 for SW processes and activities

### Essential Elements and Implementation Approaches

1. **Establish and manage to quality targets and conduct SW maturity and defect analyses**
   - The PMO should assess SW maturity/readiness and conduct defect analysis that:
     - Establishes realistic defect discovery and burn-down plans by severity and life cycle phase which enable delivery of mature SW to test and the user
     - Evaluates adequacy of resources and capacity for defect resolution
     - Assesses maturity for each increment/release
     - Establishes triggers for reviewing breaches in SW maturity predictions
   - Clearly and unambiguously define quality goals for delivered products at project inception; quality targets and projections should consider the expected number of defects by priority and estimated fix rate, as well as the expected defect density (goals will vary with application types and domains).
   - Projected maturity at delivery should consider capabilities met (e.g., Use Cases delivered, features accepted); trend toward meeting end-to-end and critical mission thread-related TPMs; and key quality attributes (e.g. stability)
   - Defects should be measured during all phases of the life cycle, from requirements through post-deployment, and analyzed in a defect phase containment matrix.

2. **Post-Delivery Software Support (PDSS)**
   - Address SW supportability, the SW test environment, and other equipment, material and documentation, including data rights that are required to provide PDSS for those end users identified in the SDP or documents similar to the Computer Resources Life Cycle Management Plan and LCSP
   - DoDI 5000.02, para 5.d.9, requires SW sustainment processes in place by end of EMD Phase
   - Estimate costs of development and run-time licenses over the system’s life cycle
   - Consider product line practices for leveraging resources across related programs


Development of several software builds using an incremental, spiral, iterative, evolutionary software development approach enables the developers to deliver capability in a series of manageable releases or builds, to gain user acceptance and feedback for the next build or increment and reduce the overall level of risk. Frequent requirements and design validation activities involving the end users can help the program define viable increments of capabilities that have operational value for limited deployment before complete system/capability delivery.

Some programs implementing incremental software development approaches (and specifically those using an Agile software development methodology or an Information Technology (IT) Box approach to requirements) may have multiple build-level reviews and evolving lower-level requirements and design maturity that in turn can impact delivery of fully established technical baselines. In these cases, incremental approaches (particularly Agile) by acquirer and developer can confuse stakeholder expectations at system-level reviews. It is therefore critical to use the SEP to communicate tailoring/expectations for SE technical reviews, exit success criteria and when technical baselines will be fully established -- all without compromising SE rigor. (For additional considerations, see Agile & Incremental SW Development in the Defense Acquisition System.)

For example, the requirements at an initial Preliminary Design Review (PDR) may be fully defined for an initial set of capabilities, with future builds or increments fully defining low-level requirements for additional capabilities and the complete system allocated baseline. Figure 3 shows a single system-level PDR and multiple build-level PDRs for multiple, successive builds. System and software architectures should support both the current build and future builds in accordance with the approved program/system requirements and constraints. PMs and SEs should consider the following practices for incremental development approaches:
- Develop the minimum viable requirements: high-level system (e.g., system requirements specification, functional requirements document) and architecturally significant requirements (non-functional requirements) covering the full scope of effort.
- Define configuration item level requirements for the build(s) or increment under review and those requirements to meet critical functions and key quality attributes.
- Develop a minimum viable architecture that consists of an initial software architecture and design with artifacts to show evidence of SW architectural evaluation and system-level architectural trade-offs (e.g., COTS software candidates to meet requirements).
- Document expectations for lower-level component artifacts and a minimum set of characteristics that defines the level of tailoring and acceptance criteria for these artifacts.
- Conduct a risk assessment that covers the full scope of the system; for design decisions not defined at PDR; track technical debt and architectural dependencies as system-level risks.
- Define progress and product metrics for iterations/builds and total system development.

Figure 3: Example Implementation of PDR for Incremental SW Development

Other reviews (e.g., System Requirements Review (SRR), Software Specification Review (SSR) and Critical Design Review (CDR)) should follow similar practices. See CH 3–3.3, and DoDI 5000.02, Enc 3, sec. 7 for additional information about Technical Reviews.

This type of incremental approach – with expectations for limited deployments – should identify interdependencies and associated technical risks as part of determining the content for each increment or build. It should include a clear understanding of the final end state of supporting physical hardware elements when functionality or capability is added over time, the synchronization of SW and HW requirements and schedules, continuous integration and end-to-end demonstration of the total system, and the ability to release working software on an agreed-to integrated plan and schedule. Memory, processor overhead, and input/output capacity designs should support growth in capability; this includes emerging technologies such as Cloud and Infrastructure-as-a-Service (IaaS).

While DoDI 5000.02, para 5.c.3 supports tailoring for incremental development, limited deployments may not be viable when the end system is not usable until the entire set of essential capabilities is integrated and tested. For example, most weapon systems depend on SW for real-time controls that can affect life and safety; these systems require security, safety and interoperability qualification/certification before release for operational use. (Life-cycle approaches that incrementally deploy SW products or releases
that include intermediate builds (e.g., DoDI 5000.02 Models 3 or 6) should also consider such qualification and certification.) In addition, safety/security assurance certifications and approvals require a predetermined objective level of rigor in verification, validation, and accreditation (VV&A) of these SW releases. This VV&A is based on risk, not on the complexity or size of each release. The Joint Software Systems Safety Handbook provides guidance for implementing safety-critical software designs with the reasonable assurance that the software executes at an acceptable level of safety risk. The Handbook includes discussion of MIL-STD-882 (DoD Standard Practice for System Safety), which is required for implementation of software safety.

SEP Considerations. In addition to identifying SW considerations as an essential element of all SE activities in the SEP, the PM and SE/SWE should ensure that the SEP addresses:

- Software-unique risks, issues and opportunities
- Inclusion of software in technical reviews, with the addition of the SSR as a precursor to the PDR for software-intensive systems
- SW technical performance, process, progress and quality metrics (importantly, those associated with End-to-End performance and capability delivery (see CH 3–4.1.3.1, Technical Performance Measures)
- SW safety, security and protection, including associated SW processes, architecture and interfacing systems
- Configuration Management (CM) for SW integration facilities/laboratories, verification/validation and development tools
- SW technology/infrastructure such as Cloud, common operating environments (COE) and MOSA; associated data rights; and sustainment considerations
- Independent verification and validation (IV&V), especially for contractor-proprietary SW
- Verification of documentation, configuration management, test relevancy and other considerations for reuse of legacy SW as well as new SW

The Services provide additional guidance to assist PMs, Systems Engineers and Software Engineers on software aspects of acquisition programs for all types of systems:

- Navy: Guidebook for Acquisition of Naval Software-Intensive Systems

Software Architecture. Architecture is the bridge between mission drivers and system design, focused on planning, analyzing, organizing and integrating current and emerging operational and system capabilities to achieve desired warfighting mission effects. These outcomes are documented in quality attributes (ranging from “ilities” to system performance), which are then evolved to system requirements and lower-level design. Architecture should consider external interface definition, support growing scale and functionality and accommodate technology insertion opportunities. SW architecture balances trade-offs (e.g., system modularity with very high performance), by frequently using techniques such as system modeling and mission simulation to evaluate solution alternatives. Implementing MOSA as part of the SW design and development can increase design flexibility, support incremental deliveries, allow for opportunities to use COTS SW and OSS, facilitate future upgrades and modifications and support technology insertion (see CH 3–4.3.4, Commercial-Off-the-Shelf and CH 3–2.4.1, Modular Open Systems Approach).

COTS/GOTS SW. Weapon system acquisitions often contain a mix of GOTS SW with complete technical data and software rights, other SW items (e.g., COTS) with restricted Government purpose rights and SW with virtually no rights other than the commercial license to use or access the SW (see FAR (Subpart 27.4)). The PM should be aware of the implications of these differences regarding acquisition and sustainment costs, performance and the consequences on change control and sustainment of deployed systems; this is also particularly relevant in the areas of security and SW assurance. The Systems
Engineer should understand the system concept of operations / operational mode summary / mission profile, any maintenance plans and the expected users of COTS/GOTS SW applications including their level of training. This understanding is necessary to effectively balance cost, scheduling and potential risks in maintenance, training and documentation.

Software Services. In programs for which software capability is procured as a service, the service-level agreement(s) (SLA) should reflect operational or fielded performance requirements, including all path constraints, such as satellite time delays, low data rate access, and intermittent service, as part of the operational environmental constraints and potential security requirements. SLA provisions are important because service providers may not be willing to disclose details of their operations and staffing (such as overseas data centers or help desks).

Software Data Management and Technical Data Rights: Rights associated with commercial products are defined in licenses that may impose limits on product use, such as restricting the buyer’s ability to alter the product or the number of copies the buyer can make. In many cases, commercial vendors offer their products on a completely “as-is” basis, making no assurance of suitability for intended purposes and offering the buyer no recourse in the event of problems. Open-source software, sometimes referred to as “freeware,” may not actually be free; it may also have restrictions or carry embedded modules that are more restrictive than the overall package. The PM, Systems Engineer, software engineer, and contracting officer should be familiar with the restrictions placed on each software item used in the contract or deliverable to the Government. The Program Office should ensure that necessary intellectual property rights to software are determined in advance of the RFP and contract award, and that they are acquired as needed; these rights can include such things as:

- All requirements tools and data sets
- All test software and supporting information necessary to build and execute the tests
- All other software test tools such as interface simulators and test data analyzers whether custom-developed or not
- All information for defects remaining in the software upon delivery to the Government

Software Reuse: Any reuse of any system, hardware, firmware or software throughout the acquisition life cycle should be addressed in multiple plans and processes, including the SEP, Software Development Plan (SDP), firmware development plan, configuration management plan, Test and Evaluation Master Plan (TEMP), Software Test Plan (STP), Independent Verification and Validation (IV&V) Plan and quality assurance plans (system and software). (Note: Software reuse has traditionally been overestimated in the beginning of programs. PMs and Systems Engineers should monitor software reuse as a potential risk.) For more discussion of software reuse, see CH 3–2.4.1, Modular Open Systems Approach.

Software System Safety: Software system safety is applicable to most DoD systems; this reflects the ubiquitous nature of software-driven functions, network connectivity and systems of systems (SoS). Specific mandatory certifications such as safety, security, cybersecurity and airworthiness require attention early in the development cycle to ensure documentation and testing are planned and executed to meet certification criteria. Systems Engineers are encouraged to check with certification authorities frequently, as rules can change during development.

Software Integrated within Acquisition Life Cycles Table 5 through Table 9 identify software considerations and specific activities associated with each phase of the acquisition life cycle. Table entries identify whether the considerations are unique to a particular DoDI 5000.02, para 5.c.3 acquisition life cycle model (hardware dominant Models 1, 2 and 5; software dominant Models 3 and 6; and accelerated acquisition Model 4) or common to all models. Common to all acquisition models, the PMO should consider the integration of hardware/software and plan/resource appropriate software acquisition and risk management. In “SW dominant” acquisition models, hardware may be a commodity (e.g., server racks in MAIS programs) or may have been established in an earlier increment (e.g., SW upgrades to established platform hardware), and software development and integration may then comprise the bulk of
the effort, requiring even greater focus on software issues. In an ‘Accelerated Acquisition’ model, the programs can be integration-intensive, and may require rapidly developing and assembling many software components to deliver capability or services. This may involve limited deployments leading up to full capability/deployment (e.g., IT Box), and may also involve consideration of adopting mature architectures that enable rapid insertion of technology and services (e.g., UAS with evolving CPU and sensor requirements; SOA with orchestrated services in a MAIS). Concerns here can include ‘glue’ code required for integration, and integration and interface concerns that can complicate integration and testing.

**Table 5: Software Considerations During the MSA Phase**

<table>
<thead>
<tr>
<th>LIFE-CYCLE PHASE</th>
<th>ACQUISITION MODEL</th>
<th>SOFTWARE ENGINEERING CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materiel Solution Analysis (MSA)</td>
<td>Common</td>
<td>Identify system requirements that map directly to software requirements to facilitate trade-offs and studies to optimize design and reduce vulnerabilities, risks and life-cycle cost</td>
</tr>
<tr>
<td></td>
<td>SW dominant</td>
<td>Mission-driven capability analysis is key to informing sequencing of software capabilities. An incremental approach will focus on specific content in a first build or increment, followed by additional builds that add or refine capability. The PM, Systems Engineer, and Software Engineer should emphasize mission understanding to set the stage for good systems/software architecture and capability-based releases/increments</td>
</tr>
<tr>
<td></td>
<td>Accelerated Acquisition</td>
<td>For an integration-intensive system that relies substantially if not completely on NDI/COTS/GOTS software, trade-space analysis can provide important information to understand the feasibility of capability and mission requirements. Consider software and system alternatives to refine the system concept and prevent vendor “lock-in.” To discover and mitigate risks, consider materiel solutions opportunities for early software development prototyping, integration, and reuse of NDI/COTS/GOTS software. To the extent possible at this early stage, ensure MSA contracts reduce technical and programmatic risk related to software, particularly for high-risk components. MSA phase should factor software sustainment considerations to inform cost and acquisition strategy, to include government technical data rights</td>
</tr>
</tbody>
</table>

**Table 6: Software Considerations During the TMRR Phase**

<table>
<thead>
<tr>
<th>LIFE CYCLE PHASE</th>
<th>ACQUISITION MODEL</th>
<th>SOFTWARE ENGINEERING CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Maturation and Risk Reduction (TMRR)</td>
<td>Common</td>
<td>Competitive prototyping helps identify and mitigate technical risks. System prototypes may be physical or math models and simulations that emulate expected performance. High-risk concepts may require scaled models to reduce uncertainty too difficult to resolve purely by mathematical emulation. SW prototypes that reflect the results of key trade-off analyses should be demonstrated during the TMRR phase. These demonstrations will provide SW performance data (e.g., latency, security architecture, integration of legacy services and scalability) to inform decisions as to maturity; further, EMD estimates (schedule and life-cycle cost) often depend on reuse of SW components developed in TMRR.</td>
</tr>
<tr>
<td>LIFE CYCLE PHASE</td>
<td>ACQUISITION MODEL</td>
<td>SOFTWARE ENGINEERING CONSIDERATIONS</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>HW dominant</td>
<td></td>
<td>Hardware-dominant programs may conduct a separate SSR to assess requirements and interface specifications for computer software configuration items (CSCI) in support of the system PDR.</td>
</tr>
<tr>
<td>SW dominant</td>
<td></td>
<td>Software programs typically conduct an SSR to assess the software requirements and interface specifications for CSCIs in support of the PDR. The program focused on a given build/release/increment may only produce artifacts for that limited scope, but the chief engineer may need a more comprehensive system-level architecture or design in order to handle capabilities across multiple releases. A PDR or its equivalent needs to maintain this system-level and longer-term, end-state perspective, as one of its functions is to provide data for the Milestone Decision Authority to assess prior to Milestone B.</td>
</tr>
<tr>
<td>Accelerated Acquisition</td>
<td></td>
<td>In an integration-intensive environment, software and system models may be difficult to develop and fully explore if many software or system components come from proprietary sources or commercial vendors with restrictions on data rights. Validating end-to-end system and internal software performance assumptions may be difficult or even impossible. Proactive work with commercial vendors to support model development is important. To the extent possible at this early stage, ensure TMRR contracts reduce technical and programmatic risk related to software, particularly for high-risk components. As is feasible, TMRR phase should factor software sustainment considerations to inform cost and acquisition strategy, to include government technical data rights. The PM, Systems Engineer, and Software Engineer should carefully establish and manage criteria for such reviews in order to properly focus the scope and purpose of the reviews. Increasing knowledge/definition of elements of the integrated system design should include details of support and data rights. Initial SLAs with the user community and vendor community are an important tool for understanding and managing the details of support requirements in a diverse system environment.</td>
</tr>
</tbody>
</table>

Table 7: Software Considerations During the Engineering and Manufacturing Development Phase

<table>
<thead>
<tr>
<th>LIFE CYCLE PHASE</th>
<th>ACQUISITION MODEL</th>
<th>SOFTWARE ENGINEERING CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering and Manufacturing Development (EMD)</td>
<td>Common</td>
<td>CDR software documentation should represent the design, performance, and test requirements, along with development and software/systems integration facilities for coding and integrating the deliverable software. Software and systems used for CSCI development (e.g., simulations and emulations) should be validated, verified, and ready to begin coding upon completion of the CDR. Problem report metadata should be selected so that the reports are relevant in development, test, and in operation to tracking and assessments. Legacy problem report tracking information can be used to generally profile and predict which types of software functions may accrue what levels of problem reports. Assessments of patterns of problem reports among software components of the system can provide valuable information to support program progress decisions.</td>
</tr>
<tr>
<td>SW dominant</td>
<td></td>
<td>For a program using an incremental SW development approach, technical debt may accrue within a given build/increment, or across multiple builds/increments. Technical reviews, both at the system and</td>
</tr>
</tbody>
</table>
### Table 8: Software Considerations During the P&D Phase

<table>
<thead>
<tr>
<th>LIFE CYCLE PHASE</th>
<th>ACQUISITION MODEL</th>
<th>SOFTWARE ENGINEERING CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Production and Deployment (P&amp;D)</strong></td>
<td>Common</td>
<td>Software may be refined as needed in response to Operational Test and Evaluation (OT&amp;E) activities, and in support of the Full-Rate Production and/or Full Deployment Decision and Initial Operational Capability (IOC).</td>
</tr>
<tr>
<td></td>
<td>SW dominant</td>
<td>For a program using an incremental SW development approach, these activities may occur in phases or steps associated with a given build or increment. In an Agile-based software process, collaboration between the test community and the development community increases understanding of system performance and verification requirements. Development and Operational Test may occur in phases or continuously as the system is updated.</td>
</tr>
<tr>
<td></td>
<td>Accelerated Acquisition</td>
<td>Progressive deployment of an integration-intensive system provides infrastructure and services and higher-level capabilities as each release is validated and verified. A rigorous release process includes configuration management and the use of regression test suites. The PM, Systems Engineer, and Software Engineer should ensure user involvement in gaining understanding and approval of changes to form, fit, and/or functions. As much as possible, builds should berationally time-blocked and synchronized to avoid forced upgrades or other problems at end-user sites, and should be tested and supported as a unit. End-user sites that perform their own customization or tailoring of the system installation should ensure</td>
</tr>
</tbody>
</table>
that knowledge of their actions is sent back to the integrator/developer so that problem reporting and resolution activities fully understand operational and performance implications of site-specific changes. Such customizations may also serve as leading indicators of user community preferences or needs when considering future system upgrades and enhancements.

Table 9: Software Considerations During the Operations and Support Phase

<table>
<thead>
<tr>
<th>LIFE CYCLE PHASE</th>
<th>ACQUISITION MODEL</th>
<th>SOFTWARE ENGINEERING CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations and Support (O&amp;S)</td>
<td>Common</td>
<td>A defined block change or follow-on incremental development delivers new or evolved capability, maintenance, safety, or urgent builds and upgrades to the field in a controlled manner. Procedures for updating and maintaining software on fielded systems often require individual user action, and may require specific training. Procedures should be in place to facilitate/ensure effective configuration management and control. There are inherent risks involved in modifying software on fielded weapon systems in use in frontline activities; software updates to business and IT systems can also pose risks to operational availability. PMs and systems and software engineers should maintain vigilance as part of supply chain risk management (see CH 4–3.5, and CH 9–3.2.6), since maliciously altered devices or inserted software can infect the supply chain, creating unexpected changes to systems.</td>
</tr>
<tr>
<td>Accelerated Acquisition</td>
<td></td>
<td>In an integration-intensive environment, security upgrades, technical refreshes and maintenance releases can proliferate, causing confusion and problems at end-user sites. System upgrades/updates should be timed to limit the proliferation of releases and therefore conserve maintenance and support resources. Problem reporting and associated severity should track impacts on other system elements to help establish the true priority of upgrades and updates. Configuration management and regression testing should be used to ensure system coherence.</td>
</tr>
</tbody>
</table>

**CH 3–2.4 Tools, Techniques and Lessons Learned**

Systems engineering (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 Program Manager (PM) and Systems Engineer in performing and managing the SE activities and processes to improve productivity and system cost, schedule, capabilities and adaptability. The PM and Systems 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 weapon 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 a 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 CH 3–4.1.7.)
• 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

Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs 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. This information is documented in the program’s Systems Engineering Plan (SEP) Table 4.7-1 Engineering Tools.

Table 10 lists general capabilities and features of SE tools and the SE processes they might support.

<table>
<thead>
<tr>
<th>SE Process</th>
<th>Tool Capabilities / Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Planning</strong></td>
<td>• Assists in planning and scheduling activities</td>
</tr>
<tr>
<td></td>
<td>• Assists in resource planning, tracking and allocation</td>
</tr>
<tr>
<td></td>
<td>• Facilitates cost estimation</td>
</tr>
<tr>
<td><strong>Decision Analysis</strong></td>
<td>• Assists in trade-off analysis</td>
</tr>
<tr>
<td></td>
<td>• Provides optimization and sensitivity analysis capability</td>
</tr>
<tr>
<td></td>
<td>• Assists in recording, tracking, evaluating and reporting decision outcomes</td>
</tr>
<tr>
<td><strong>Technical Assessment</strong></td>
<td>• Assists in tracking, measuring and assessing metrics</td>
</tr>
<tr>
<td></td>
<td>• Assists in metric collection</td>
</tr>
<tr>
<td><strong>Requirements Management</strong></td>
<td>• Provides requirements bi-directional traceability capability</td>
</tr>
<tr>
<td></td>
<td>• Provides requirements flow-down capability</td>
</tr>
<tr>
<td></td>
<td>• Tracks requirements changes</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>• Assists in risk, issue, opportunity planning, identification, analysis, mitigation/management and monitoring</td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
<td>• Assists in the identification of configuration items</td>
</tr>
<tr>
<td></td>
<td>• Assists in baseline/version control of all configuration items</td>
</tr>
<tr>
<td></td>
<td>• Assists in ensuring configuration baselines and changes are identified, recorded, evaluated, approved, incorporated and verified</td>
</tr>
<tr>
<td><strong>Technical Data Management</strong></td>
<td>• Assists in identification of data requirements</td>
</tr>
<tr>
<td></td>
<td>• Assists in recording and managing data rights</td>
</tr>
<tr>
<td></td>
<td>• Assists in storage, maintenance, control, use and exchange of data</td>
</tr>
<tr>
<td></td>
<td>• Assists in document preparation, update, and analysis</td>
</tr>
<tr>
<td><strong>Interface Management</strong></td>
<td>• Assists in capturing system internal and external interfaces and their requirement specifications</td>
</tr>
<tr>
<td>SE Process</td>
<td>Tool Capabilities / Features</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SE Process</td>
<td></td>
</tr>
</tbody>
</table>
| Stakeholder Requirements  | • Assists in assessing compliance of interfaces among system elements of the system or systems of systems  
                               • Produces a view of interface connectivity                                                                                                                                                                           |
| Definition                |                                                                                                                                                                                                                            |
| Requirements Analysis     | • Assists in capturing and identifying stakeholder requirements  
                               • Assists in analyzing and maintaining stakeholder requirements                                                                                                                                                  |
| 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 operational environment                                                                                               |

**CH 3–2.4.1 Modular Open Systems Approach**

A modular open systems approach (MOSA) is defined as an acquisition and design strategy consisting of a technical architecture that adopts open standards and supports a modular, loosely coupled and highly cohesive system structure. This modular open architecture includes publishing of key interfaces within the system and relevant design disclosure. The key enabler for MOSA is the adoption of an open business model that requires doing business in a transparent way that leverages the collaborative innovation of numerous participants across the enterprise, permitting shared risk, maximized reuse of assets and reduced total ownership costs. 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 and/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
- Enhanced competition
- Facilitation of technology refresh
- Increased innovation
- Potential cost savings or cost avoidance
MOSA benefits Program Managers (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 due 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 chosen should consider both 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 5000.02, Enc 2, sec. 6a and DoDI 5000.02, Enc 3, sec. 14 direct PMs to evaluate and implement MOSA where feasible and cost-effective. The USD(AT&L) memorandum, "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending." November 13, 2012, raises the relevance of MOSA along with the acquisition of data rights for appropriate system elements. 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 DASD(SE) website.

The PM should:

- Establish supportive requirements; business practices; and technology development, acquisition, test and evaluation and product support strategies for effective development of open systems
- Ensure data deliverables support the Intellectual Property (IP) 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 (DID) 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 open 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(AT&L) business case analyses.
- Ensure the system functional architecture is structured to accommodate Open Systems Architecture (OSA) where feasible, due to 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 open 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 Program Executive Office (PEO) level. Re-use 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 re-used by a sister platform that may have its ADS-B and Tactical air navigation software combined in a single module.

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 engineering trade analyses conducted prior to 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 open standards-based interfaces. 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. 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 4: Sample MOSA and Data Rights Analysis**
Figure 4 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. The levels of data rights that need to be required for each MOSA-enabled system element are determined in order to assert the requisite contract requirements to obtain them. The data rights strategy ensures that enterprise-level data rights flow to system elements and that they support the system architecture. Levels of data rights are described in Chapter (CH) 1 and in Appendix 9 of the OSA 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. The Systems Engineering Plan (SEP) is also updated to reflect the MOSA-related updates and modifications employed throughout the system and its system elements.

Specific MOSA-related data deliverables that should be considered include:

- Software Development Plans (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

In addition, 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 system 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
• Acquisition Strategy (AS)
• Program Protection Plan (PPP)
• Analysis of Alternatives (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 DoD Acquisition Streamlining and Standardization Information System (ASSIST) homepage for more data item deliverables that may be appropriate for each specific program and DoD 5010.12-M for data deliverables.

**CH 3–2.4.2 Modeling and Simulation**

Models and simulations are SE tools used by multiple functional area disciplines during all system life-cycle phases. Models, simulations, data and artifacts should be developed in a well-defined and controlled engineering environment to support the program's reuse of the information across the acquisition life cycle or for reuse and repurposing in support of other acquisition efforts. DoDI 5000.02, Enc 3, sec. 9 requires all models, simulations, data and artifacts to be integrated, managed and controlled to ensure that the products maintain consistency with the system and external program dependencies, provide a comprehensive view of the program and increase efficiency and confidence throughout the program's life cycle. Models are essential to aid in understanding complex systems and system interdependencies, and to communicate among team members and stakeholders. Simulation provides a means to explore concepts, system characteristics and alternatives; open up the trade space; facilitate informed decisions and assess overall system performance.

Models and simulations provide:

• Understanding of capabilities and the requirements set
• Data to inform program and technical decisions
• Efficient communication and shared understanding among stakeholders about relationships between system requirements and the system being developed, through precise engineering artifacts and traceability of designs to requirements
• Exploration of system alternatives to support the early identification of viable system solutions and any necessary doctrine change requests
• An alternative solution for building prototypes and enabling cost savings
• Better analysis and understanding of system designs, including system elements and enabling system elements
• Improved capability to address defects and failures at all levels through a greater understanding of the system.
• Support to engineering and design trade-off analysis studies
• Support for early interface and interoperability testing
• Greater efficiencies in design and manufacturing by reducing the time and cost of iterative build/test/fix cycles
• Timely understanding of program impacts of proposed changes
• Insight into program cost, schedule, performance and supportability risk

The **Systems Engineering Digital Engineering Fundamentals** recommends that all programs identify and maintain a system model, representing all necessary viewpoints on the design and capturing all relevant system interactions. The system model should include, but not be limited to, parametric descriptions, structure, definitions of behaviors, design assumptions, internal and external interfaces, cost inputs and traces from operational capabilities to requirements and design constructs.

The system model should be captured digitally to create an integrated set of authoritative technical data, information and knowledge, generated and used by all stakeholders throughout the system life cycle. Use of a digital system model can help drive consistency and integration among SE and analytical tools, and provide the program with a capability to assess potential design changes, as well as system upgrades, throughout the life cycle. The Program Manager (PM) and Systems Engineer should consider establishing and using a digital system model when planning for the development, incorporation and application of models, simulations and analyses on their program. Figure 5 shows some benefits of using models and simulation throughout the acquisition life cycle. This figure is adapted from a 2010 National Defense Industrial Association (NDIA) Systems Engineering Division "Model-Based Engineering (MBE)" study and is used with permission.

**Figure 5: Benefits of Using Models and Simulation throughout the Acquisition Life Cycle**
Models and simulations should take advantage of opportunities for reuse (see DoD Modeling and Simulation Catalog [requires Common Access Card (CAC) to access website]). Models and simulations developed in early acquisition phases may be repurposed for other activities during later phases (e.g., engineering models can be used in training simulations). SE should use models and simulations from many disciplines and across a hierarchy of perspectives that range from an engineering/technical level up to the campaign/strategic level in order to effectively analyze requirements, design, cost, schedule, performance and risk. These models and simulations often exist, but sometimes need to be newly developed, which can be costly. An option for new development is to consider federating existing models and simulations, using any of various interoperability standards in order to create needed capability. PMs and Systems Engineers should consider how to leverage models, simulations, and their interoperability as they plan for their use throughout a program's life cycle. Modeling and simulation is also used to support developmental test and evaluation (DT&E) and operational test and evaluation (OT&E).

Roles, Responsibilities, and Activities

To make effective and appropriate use of models and simulations, the PM and Systems Engineer should ensure that planned modeling and simulation activities are:

- Complete, comprehensive and trusted, including all efforts anticipated throughout the life cycle, to include planning, development and acceptance as well as verification, validation, and accreditation (VV&A) (see CH 8–3.7.7.)
- Integrated into the program’s technical planning (Work Breakdown Structure (WBS), schedules, budgets, Systems Engineering Plan (SEP) and other program documentation; see CH 3–4.1.1. Technical Planning Process)
- Appropriately resourced, including a properly skilled workforce

The PM and Systems Engineer should establish, manage, control, and maintain integrated sources of all relevant models, simulations, data and other artifacts that describe what the system is and does. These data sources also should contain descriptive system information that could be used to feed other models, simulations and acquisition efforts.

Figure 6 provides examples of models, simulations and analyses throughout the life cycle.
The PM and Systems Engineer should ensure that the program’s modeling and simulation activities are coordinated, managed and controlled such that products are consistent with the system and architecture design at all levels. Plans to use models and simulations should be integrated with the overall program plan. The program may choose to integrate the modeling and simulation planning details into the program plan or create a separate modeling and simulation planning document. If the documents are separate, the program ensures the modeling and simulation planning is kept up to date as the program plan adjusts. PMs should follow their organization’s standards for planning, managing and controlling such activities.

Models and simulations should be:

- Developed and matured through the life of the program
- Developed and documented, to include metadata and open standards, to maximize opportunity for reuse and repurposing (both within the program and in support of other acquisition efforts)
- Properly managed and controlled as part of the program’s technical baseline.
- Included as part of the technical data package 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 the required program technical reviews and in the baselined technical data needed to support major program reviews and program decisions.

**CH 3–2.4.3 Sustainability Analysis**

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 total ownership cost (TOC). The Program Manager (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.

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 unintentionally inserted during development or procurement and later exposed by the logistics and operational communities.

"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 total life-cycle costs 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:

- Analysis of Alternatives 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 to include sustainability as one of the elements in the analysis
- Preliminary design to select the most sustainable system that meets performance requirements and end-user needs
- Supportability analysis to help ensure the use of resources throughout the life cycle is considered
- Detailed design to select the most sustainable components

The Streamlined Life Cycle Assessment Process for Sustainability in DoD Acquisitions is specifically for use in the DoD acquisition process. It 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 considerations, such as operational energy, supportability and environment, safety and occupational health (ESOH).

CH 3–2.4.4 Value Engineering

Program Managers (PMs) use Value Engineering (VE) across the life cycle for supplies and services, including those for major systems, and construction. 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, ensuring that a "program, project, system," etc., consistently performs the required basic function at the lowest life-cycle cost while maintaining acceptable levels of performance and quality. VE maximizes the buying power of the DoD and should be considered throughout the life cycle as a way to meet or beat affordability constraints and should-cost targets. 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 the key VE activities, the two parts of VE and the application, including examples, 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: VE proposals (VEP) and VE change proposals (VECP). 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 to include 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 and Systems 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 and Systems Engineer to learn more about VE include the Defense Acquisition University (DAU) Continuous Learning Module, CLE001, “Value Engineering” and the VE initiatives webpage on the DASD(SE) website. For examples of potential areas in which the application of VEPs and VECPs may provide a benefit, see SD-24 Chapter 2, “Opportunities of VE Application,” and Chapter 3, “VE over a System’s Lifecycle.”

**CH 3–2.4.5 Lessons Learned, Best Practices and Case Studies**

Most programs represent a new combination of existing capabilities or the insertion of incremental advances in technology. By reviewing the successes, failures, problems and solutions of similar programs, Program Managers (PMs) and Systems Engineers can gain insights into risks, uncertainties and opportunities that 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 and Systems 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. PMs and Systems Engineers should be aware that Standards are not ad hoc requirements developed by a single engineer or program office. Standards result from years of execution knowledge gained across management, engineering, manufacturing or sustainment.
The Acquisition Streamlining and Standardization Information System (ASSIST) database is the official source for current DoD specifications and standards and identifies 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 Department of Defense by Public Laws or Government Regulations), and U.S.-ratified materiel international standardization agreements (ISAs).

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 and Systems 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 reports
- DoD Systems Engineering community of practice websites
- Defense Standardization Program Office (DSPO)
- Other Departments and Agencies such as National Aeronautics and Space Administration (NASA), Department of Energy (DoE) or National Institute of Standards and Technology (NIST)
- Professional organizations such as the International Council on Systems Engineering (INCOSE) or the Institute of Electrical and Electronics Engineers (IEEE)
- Industry organizations such as National Defense Industrial Association (NDIA) or Aerospace Industries Association (AIA)
- Non-government standards development organizations such as Society of Automotive Engineers (SAE) International and International Organization for Standards (ISO)

PMS and Systems 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 in external collaborative information sharing, the PM and Systems Engineer should ensure that the program establishes and utilizes 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 that is developed throughout the program execution should include enough contextual information about the program and surrounding circumstances so that future practitioners can discern the relevancy and usefulness of the best practice. PMs and Systems Engineers should consider using these data as a form of process improvement feedback, or as evidence for proposing policy and guidance changes.

CH 3–2.5 Engineering Resources

Organizing and staffing the systems engineering (SE) organization and providing supporting resources and tools are critical tasks that merit attention from both the Program Manager (PM) and Systems 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 is an integrated part of the program planning and execution activities. In accordance with DoDI 5000.66, this includes ensuring that program offices for MDAPs or MAIS programs will have a qualified Chief Engineer/Chief Systems Engineer with key leadership position criteria defined in the USD(AT&L) policy memorandum, “Key Leadership Positions and Qualification Criteria,” November 8, 2013.
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 (see CH 3–2.4, Tools, Techniques, and Lessons Learned). 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 Systems Engineering Plan (SEP) describes the SE organizations of both the Government program office and, when available, the developer organization.

### 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., Acquisition Strategy (AS)), program plans (e.g., SEP, Program Protection Plan (PPP), Test and Evaluation Master Plan (TEMP), Life Cycle Sustainment Plan (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 professionals
- Integrating all aspects of the program office, including business processes relating to program management, SE, test and program control
- Ensuring all necessary memoranda of understanding and agreement (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 Engineering Change Proposal (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 systems engineering management plan (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 concept of operations
- 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 system of systems (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 acquisition phase as detailed in the SEP
• 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
  o Integration risks
  o Engineering risks
  o Critical technology risks assessed in the Technology Readiness Assessment (TRA) (MDAPs only)
• Measuring and tracking program maturity using technical performance measures, requirements stability, and integrated schedules
• Updating the PPP
• Staffing the engineering team with qualified and appropriate engineers.
• Supporting updates to the TEMP and LCSP
• Supporting test and evaluation activities as documented in the TEMP (see Chief Developmental Tester responsibilities in CH 8–2.4.1.)
• Reviewing requirements traceability matrix and cross reference matrix (verification)
• Managing root cause and corrective action (RCCA) efforts along with supporting the risk and opportunity boards
• Supporting the selection of qualified 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 key responsibilities of the Systems Engineer is to provide insight/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, 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 and Systems 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 on DASD(DT&E) oversight, Systems Engineers will be included on the Test and Evaluation (T&E) Working-Level Integrated Product Team (WIPT), as a test data stakeholder. 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 test and evaluation 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.
Stakeholders

The PM has the critical role of approving a systems engineering (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 have the ability to actively participate throughout the life cycle in support of SE-related activities.

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

- Warfighters and other end users
- Milestone Decision Authority (MDA)
- Resource sponsors
- Budget authority
- Developers
- Enabled or enabling systems in the system of systems (SoS)
- Security Manager 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 build, test, deploy and/or support the capability under development
- Companion programs

Integrated Product Teams

An effective SE organization is typically structured as one or more integrated product teams (IPTs). An IPT is a multidisciplinary group of representatives from all appropriate functional disciplines 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 and Systems 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 and Systems Engineer may organize multiple IPTs to align with the major products in the program’s Work Breakdown Structure. 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 continuous engagement is necessary to ensure a common understanding of program goals, objectives, and activities. These Government/developer IPTs should further maintain effective communication as they manage and execute those 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.

For Major Defense Acquisition Programs, the PM ensures that the program office is structured to interface 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. The SE WIPT includes representatives from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) and the component acquisition executive’s organization, both Government and developer IPT leads from the program, the Program Executive Office Systems Engineer, and the developer Systems Engineer. A generic SE WIPT charter is available on the ODASD(SE) Policy and Guidance website under "Guidance and Tools." Additional information about IPTs can be found in CH 1–3.3.5.

CH 3–2.6 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 systems engineering (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 can begin flight testing. Often programs insufficiently plan for the number of required certifications. Insufficient planning for certifications can have a negative impact on program costs and schedule.

Obtaining the various certifications can be a lengthy process. As a result, the Program Manager (PM) should ensure that the time necessary to obtain any required certification is factored into technical planning. By planning for the activities required to achieve the necessary certifications, the PM and Systems 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 Systems Engineering Plan (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 Integrated Master Schedule (IMS) and the Integrated Master Plan (IMP).

A non-exhaustive list of certifications is available on the DASD(SE) website. Furthermore, PMs and Systems Engineers should consult both Joint and Service-specific domain experts to determine other certifications that may be required.

CH 3–2.7 Systems Engineering Role in Contracting
The Systems Engineer should actively 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 Statement of Work (SOW), Statement of Objectives (SOO), or Performance Work Statement (PWS) is necessary to ensure that the final system meets 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 Contract Data Requirements List (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.

The Systems Engineer should contribute to the development of contract incentives and/or incentive approaches that promote an understanding of the technical risks and opportunities inherent in the selected development approach. Incentives such as award fee may be tied to program performance and progress that may be evaluated during technical reviews, or more frequently the incentive is tied to the completion of a technical review. 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 Program Manager (PM) exercise best judgment in an objective and informed manner to ensure the reviews are not prematurely declared 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:

- Technical performance measurement (TPM)
- Progress against requirements
- Development maturity
- Exit criteria of life-cycle phases
- Significant work packages and work products

Additional information about EVMS can be found in CH 1–4.2.16. 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. It is equally important for the contracting officers as they develop acquisition strategies, seek opportunities for small businesses, and negotiate contract terms. The best source of this information is usually found within industry partners. 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 that the Government clearly 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 communications plans, consistent with existing law and regulation, which promote responsible exchanges.

The program office uses a Request for Information (RFI) 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 Integrated Master Plan (IMP), Work Breakdown Structure (WBS), Integrated Master Schedule (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 clearly 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 Program Manager, the Systems Engineer should ensure that technical documents accurately and clearly communicate the Government’s requirements including mandatory design, build, test, certification, approval, and acceptance criteria. This ensures the developer is made aware of all required processes and objective quality evidence (OQE) to be produced, to include processes leading to certification, approval, and acceptance using predetermined OQE. In addition, the PM should consider providing all offerors with the Program Protection Plan (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 5000.02, Enc 3, sec. 2, 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 and Systems 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, Major Defense Acquisition Programs should review, tailor and implement applicable mission assurance concepts and principles when developing their contract requirements. Major Defense Acquisition Programs should use resources provided by their service (for example, the Aerospace/Air Force Mission Assurance Guide TOR-2007(8546)-6018).

Although there are many opportunities for contract-related interactions between the Government and potential offerors prior to 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 and risk management; see CH 3–4, Additional Planning Considerations).
- Providing available and appropriate architecture(s) characterizing the system’s interoperability requirements.
- Identifying any design considerations including production; reliability and maintainability (R&M); environment, safety and occupational health (ESOH); human systems integration (HSI); and security.
- Identifying for delivery Government-required technical data rights produced by the developer.
- 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 test and evaluation requirements.
- Providing a requirements verification traceability database (requirements and test method).
- Specifying meetings and technical documentation between the program office and the developer.
- Conducting a review of the deliverables (what data, 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, to include providing inputs to the development of source selection criteria.
- Performing schedule risk assessments 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 (see CH 9–3.1.)
- Providing a clear description of the minimum technical requirements used to determine the technical acceptability of a proposal.

Table 11 contains the typical technical contents of the RFP and the associated Systems Engineer’s responsibilities, and should not be considered an exhaustive or mandatory list.

Table 11: Typical Technical Contents of a RFP

<table>
<thead>
<tr>
<th>Typical Technical Contents</th>
<th>SE Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section C</strong></td>
<td></td>
</tr>
<tr>
<td>• Statement of Work (SOW)</td>
<td>• Provide program technical requirements and technical aspects in the SOW</td>
</tr>
<tr>
<td>• System Performance Specification</td>
<td>• Generate the system performance specification</td>
</tr>
<tr>
<td>Section</td>
<td>Typical Technical Contents</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Description of Work to Be Performed</td>
<td>• Operational Documents (CONOPS/OMS/MP, SoS, Requirements, etc.) • Available and applicable architecture(s) • Engineering processes</td>
</tr>
<tr>
<td><strong>Section H</strong> Special Contract Requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Key personnel • Government-furnished equipment or information (GFE or GFI) • Obsolescence management • Warranties • Options for delivery of software • Award fees</td>
</tr>
<tr>
<td><strong>Section J</strong> Attachments</td>
<td>• 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</td>
</tr>
<tr>
<td><strong>Section K</strong> Representations, Certifications, and Other Statements</td>
<td>• Data rights</td>
</tr>
<tr>
<td><strong>Section L</strong> Instructions on Content and Structure of RFP Response</td>
<td>• Systems engineering solution • Systems engineering management processes • Technical baseline management • Technical reviews and audits</td>
</tr>
<tr>
<td>Typical Technical Contents</td>
<td>SE Responsibilities</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Risk management processes and known key risk areas</td>
<td>• Demonstrate alignment with Government processes</td>
</tr>
<tr>
<td>• Mandatory (i.e., statute- and regulation-driven) and advised design considerations</td>
<td></td>
</tr>
<tr>
<td>• Technical organization</td>
<td></td>
</tr>
<tr>
<td>• Technical data required for a Streamlined Life Cycle Assessment (LCA)</td>
<td></td>
</tr>
<tr>
<td>• Demonstrate alignment with Government processes</td>
<td></td>
</tr>
<tr>
<td>• Define technical evaluation factors and provide SE specific evaluation criteria used to assess proposals</td>
<td></td>
</tr>
<tr>
<td>• Participate on or lead the technical evaluation team</td>
<td></td>
</tr>
<tr>
<td>• Provide technical personnel to participate on each evaluation factor team (e.g.,</td>
<td></td>
</tr>
<tr>
<td>management, past performance, cost)</td>
<td></td>
</tr>
<tr>
<td>• Provide consistency across the SOW and system performance specifications</td>
<td></td>
</tr>
<tr>
<td>• Evaluate RFP responses against technical requirements, threshold requirements,</td>
<td></td>
</tr>
<tr>
<td>management (e.g., SEMP, WBS, and program schedule), and consistency across the proposal (e.g., link between WBS, program schedule, risks, and cost)</td>
<td></td>
</tr>
<tr>
<td>• Identify and assess the technical risks and opportunities for each proposal, including schedule risks and related risk and opportunity handling plans</td>
<td></td>
</tr>
<tr>
<td>• 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)).</td>
<td></td>
</tr>
</tbody>
</table>


This section is split into three subsections:

- **CH 3–3.1:** Life-Cycle Expectations provides introductory material and life-cycle context
- **CH 3–3.2:** Systems Engineering Activities in Life-Cycle Phases describes the Systems Engineer’s role in each phase of the weapon system acquisition life cycle. The notional technical reviews and audits in each phase are identified
- **CH 3–3.3:** Technical Reviews and Audits provides an in-depth description of technical reviews and audits. This arrangement accommodates the planning and conducting of the technical reviews and audits in accordance with a program’s specific needs. Some large and complex
programs may require each technical review and audit; others may combine technical reviews and audits or get permission to not conduct certain reviews.

CH 3–3.1 Life-Cycle Expectations
Systems engineering (SE) provides the technical foundation for all acquisition activities regardless of acquisition category (ACAT or acquisition model (e.g., weapon system or information system). The SE framework described in this chapter spans the entire acquisition life cycle and is based on Department of Defense Directive (DoDD) 5000.01, Enc. 1 and Department of Defense Instruction (DoDI) 5000.02, para 5.d. Framework content should be tailored and structured to fit the technology maturity, risks, interdependencies, related characteristics and context for the program or the system of interest. The succeeding sections identify the SE activities, processes, inputs, outputs, and expectations during each acquisition phase and for each technical review and audit.

Acquisition milestones and SE technical reviews and audits serve as key points throughout the life cycle to evaluate significant achievements and assess technical maturity and risk. Table 12: Technical Maturity Points identifies the objectives of each SE assessment and the technical maturity point marked by each review. The Materiel Development Decision (MDD) review is the entry point into the acquisition process and is mandatory for all programs in accordance with DoDI 5000.02, para 5.d.1. Depending on the maturity of the preferred materiel solution, the Milestone Decision Authority (MDA) designates the initial review milestone. This would normally be the MDD, but it can be A, B, or C. In any case, the decision is documented in the Acquisition Decision Memorandum (ADM) published immediately after an MDD event. Since the review milestone is chosen consistent with the maturity of the preferred materiel solution, entry at any milestone requires evidence of the associated solution maturity, as summarized in Table 12: Technical Maturity Points.

Department experience (e.g., Government Accountability Office (GAO) Report 12-400SP) has found that successful programs use knowledge-based product development practices that include steps to gather knowledge to confirm the program’s technologies are mature, their designs are stable and their production processes are in control. Successful materiel developers ensure a high level of knowledge is achieved at key junctures in development. Table 12 summarizes the concept of technical maturity points.

Table 12: Technical Maturity Points

<table>
<thead>
<tr>
<th>DoD Acquisition Milestone/Decision Point &amp; Technical Review/Audit</th>
<th>Objective</th>
<th>Technical Maturity Point</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materiel Development Decision (MDD)</td>
<td>Decision to assess potential materiel solutions and appropriate phase for entry into acquisition life cycle.</td>
<td>Capability gap met by acquiring a materiel solution.</td>
<td>Technically feasible solutions have the potential to effectively address a validated capability need. Technical risks understood.</td>
</tr>
<tr>
<td>Alternative Systems Review (ASR)</td>
<td>Recommendation that the preferred materiel solution can affordably meet user needs with acceptable risk.</td>
<td>System parameters defined; balanced with cost, schedule and risk.</td>
<td>Initial system performance established and plan for further analyses (e.g., assessing technical maturity and associated risks) supports Milestone A criteria.</td>
</tr>
<tr>
<td><strong>DoD Acquisition Milestone/Decision Point &amp; Technical Review/Audit</strong></td>
<td><strong>Objective</strong></td>
<td><strong>Technical Maturity Point</strong></td>
<td><strong>Additional Information</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Milestone A</strong></td>
<td>Decision to invest in technology maturation and preliminary design.</td>
<td>Affordable solution found for identified need with acceptable technology risk, scope, and complexity.</td>
<td>Affordability goals identified and technology development plans, time, funding, and other resources match customer needs. Prototyping and end-item development strategy for Technology Maturation and Risk Reduction (TMRR) phase focused on key technical risk areas.</td>
</tr>
<tr>
<td><strong>System Requirements Review (SRR)</strong></td>
<td>Recommendation to proceed into development with acceptable risk.</td>
<td>Level of understanding of top-level system/performance requirements is adequate to support further requirements analysis and design activities.</td>
<td>Government and contractor mutually understand system/performance requirements including: (1) the preferred materiel solution (including its support concept) from the Materiel Solution Analysis (MSA) phase; (2) plan for technology maturation; and (3) maturity of interdependent systems.</td>
</tr>
<tr>
<td><strong>System Functional Review (SFR)</strong></td>
<td>Recommendation that functional baseline satisfies performance requirements and to begin preliminary design with acceptable risk.</td>
<td>Functional baseline established and under formal configuration control. System functions in the system performance specification decomposed and defined in specifications for lower level elements, that is, system segments and major subsystems.</td>
<td>Functional requirements and verification methods support achievement of performance requirements. Acceptable technical risk of achieving allocated baseline. See CH 3–4.1.6, Configuration Management Process for a description of baselines.</td>
</tr>
<tr>
<td>DoD Acquisition Milestone/Decision Point &amp; Technical Review/ Audit</td>
<td>Objective</td>
<td>Technical Maturity Point</td>
<td>Additional Information</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Capability Development Document (CDD) Validation</strong></td>
<td>Requirements validation authority action. Provides a basis for preliminary design activities and the PDR.</td>
<td>Major cost and performance trades have been completed and enough risk reduction has been completed to support a decision to commit to the set of requirements (i.e., CDD or equivalent)</td>
<td>Support preparation for CDD validation by performing systems engineering trade-off analysis addressing relationships of cost, requirements, design, and schedule. Once validated, a Configuration Steering Board assumes responsibility to review all requirements changes and any significant technical configuration changes for ACAT I and IA programs in development, production, and sustainment that have the potential to result in cost and schedule impacts to the program.</td>
</tr>
<tr>
<td><strong>Preliminary Design Review (PDR)</strong></td>
<td>Recommendation that allocated baseline satisfies user requirements and developer ready to begin detailed design with acceptable risk.</td>
<td>Allocated baseline established such that design provides sufficient confidence to proceed with detailed design. Baseline also supports 10 USC 2366b certification, if applicable.</td>
<td>Preliminary design and basic system architecture support capability need and affordability goals and/or caps achievement. See CH 3–4.1.6. Configuration Management Process for a description of baselines.</td>
</tr>
<tr>
<td><strong>Development Request for Proposal (RFP) Release Decision Point</strong></td>
<td>Determination that program plans are affordable and executable and that the program is ready to release RFPs for EMD and/or for LRIP (or Limited Deployment options for MAIS programs).</td>
<td>Systems engineering trades completed and have informed program requirements. Competitive and risk reduction prototyping and the development of the preliminary design have influenced risk management plans and should-cost initiatives.</td>
<td>The Request for Proposal (RFP) reflects the program’s plans articulated in the draft (as defined in DoDI 5000.02, para 5.d.6) Acquisition Strategy and other draft, key planning documents such as the Systems Engineering Plan (SEP), Program Protection Plan (PPP), Test and Evaluation Master Plan (TEMP), and Life-Cycle Sustainment Plan (LCSP).</td>
</tr>
<tr>
<td>DoD Acquisition Milestone/Decision Point &amp; Technical Review/Audit</td>
<td>Objective</td>
<td>Technical Maturity Point</td>
<td>Additional Information</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Milestone B</td>
<td>Decision to invest in product development, integration, and verification as well as manufacturing process development; decision on LRIP quantity (or scope of Limited Deployments for MAIS programs).</td>
<td>Critical technologies assessed able to meet required performance and are ready for further development. Resources and requirements match.</td>
<td>Maturity, integration, and producibility of the preliminary design (including critical technologies) and availability of key resources (time, funding, other) match customer needs. Should-cost goals defined.</td>
</tr>
<tr>
<td>Critical Design Review (CDR)</td>
<td>Recommendation to start fabricating, integrating, and testing test articles with acceptable risk.</td>
<td>Product design is stable. Initial product baseline established.</td>
<td>Initial product baseline established by the system detailed design documentation; affordability/should-cost goals confirmed. Government assumes control of initial product baseline as appropriate. See CH 3–4.1.6. Configuration Management Process for a description of baselines.</td>
</tr>
<tr>
<td>System Verification Review (SVR)/Functional Configuration Audit (FCA)</td>
<td>Recommendation that the system as tested has been verified (i.e., product baseline is compliant with the functional baseline) and is ready for validation (operational assessment) with acceptable risk.</td>
<td>System design verified to conform to functional baseline.</td>
<td>Actual system (which represents the production configuration) has been verified through required analysis, demonstration, examination, and/or testing. Synonymous with system-level Functional Configuration Audit (FCA). See CH 3–4.1.6. Configuration Management Process for a description of baselines.</td>
</tr>
<tr>
<td>Production Readiness Review (PRR)</td>
<td>Recommendation that production processes are mature enough to begin limited production with acceptable risk.</td>
<td>Design and manufacturing are ready to begin production.</td>
<td>Production engineering problems resolved and ready to enter production phase.</td>
</tr>
<tr>
<td>DoD Acquisition Milestone/Decision Point &amp; Technical Review/ Audit</td>
<td>Objective</td>
<td>Technical Maturity Point</td>
<td>Additional Information</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Milestone C and Limited Deployment Decision</strong></td>
<td>Decision to produce production-representative units for operational test and evaluation (OT&amp;E) and/or decision that increment of capability is ready for Limited Deployment.</td>
<td>Manufacturing processes are mature enough to support Low-Rate Initial Production (LRIP) (and/or Limited Deployment) and generate production-representative articles for OT&amp;E. Increment of capability has stable design.</td>
<td>Production readiness meets cost, schedule, and quality targets. Begin initial deployment and/or deploy increment of capability.</td>
</tr>
<tr>
<td><strong>Physical Configuration Audit (PCA)</strong></td>
<td>Recommendation to start full-rate production and/or full deployment with acceptable risk.</td>
<td>Product baseline established. Verifies the design and manufacturing documentation, following update of the product baseline to account for resolved OT&amp;E issues, matches the physical configuration.</td>
<td>Confirmation that the system to be deployed matches the product baseline. Product configuration finalized and system meets user’s needs. Conducted after OT&amp;E issues are resolved. See CH 3-4.1.6, Configuration Management Process for a description of baselines.</td>
</tr>
<tr>
<td><strong>Full-Rate Production Decision Review (FRP DR) or Full Deployment Decision Review (FDDR)</strong></td>
<td>Decision to begin full-rate production and/or decision to begin full deployment.</td>
<td>Manufacturing processes are mature and support full-rate production and/or capability demonstrated in operational environment supporting full deployment (i.e., system validated through OT&amp;E).</td>
<td>Delivers fully funded quantity of systems and supporting materiel and services for the program or increment to the users.</td>
</tr>
</tbody>
</table>

Figure 7: Weapon System Development Life Cycle provides the end-to-end perspective and the integration of SE technical reviews and audits across the system life cycle.

The Systems Engineer supports the Program Manager in the development and implementation of a technical program strategy. SE processes help deliver capabilities that meet warfighter needs within cost and schedule by balancing end-user needs, design considerations, resource constraints and risk. The Systems Engineer uses technical reviews and audits to assess whether preplanned technical maturity points are reached during the acquisition life cycle as the system and system elements mature. The identification and mitigation of technical risks leading up to reviews and audits facilitates achieving entrance criteria at each of these points (see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.) Special attention should be made to ensure the consistency of analysis that supports key decision and transition points throughout the program's life cycle. For instance,
models, simulations, tools and data should be integrated into the SE activities and reused to the greatest extent possible (see CH 3–2.4.2, Modeling and Simulation). This knowledge forms the basis for the Systems Engineer’s recommendations to the Program Manager (PM) on how to technically proceed with the program.

Figure 7: Weapon System Development Life Cycle

CH 3–3.1.1 Systems Engineering in Defense Acquisition Program Models

DoDI 5000.02, para 5.c identifies several acquisition models for Program Managers (PMs) to use as a starting point in structuring a program to acquire a specific product. The PM selects and tailors the acquisition model based on the dominant characteristics of the product being acquired or the need for accelerated acquisition. This chapter contains information nominally based upon the Hybrid Model A (Hardware Dominant), since most weapon system programs include software development, hardware development and integration.

The PM and the Systems Engineer can use the descriptions of technical reviews and audits, phases, decision points and processes in this chapter to help select and tailor an acquisition strategy for a program. The resulting program structure is documented in the Acquisition Strategy and other plans, including the Systems Engineering Plan.

Table 13: Acquisition Models contains a summary of the set of acquisition models described in DoDI 5000.02, para 5.c. The second column contains the expected application for each model and highlights the relevant systems engineering activities identified in this chapter. This information can be used to guide the application of processes described in CH 3–4., as necessary.

Table 13: Acquisition Models
<table>
<thead>
<tr>
<th>Acquisition Program Model</th>
<th>Key Characteristics and Systems Engineering Considerations</th>
</tr>
</thead>
</table>
| **Model 1:** Hardware Intensive Program | **Key Characteristics**  
- Products requiring development of DoD unique hardware  
**Systems Engineering Considerations**  
- Activities: See CH 3–3.2.  
- Reviews: See CH 3–3.3.; assumes minimal software development so Software Specification Review (SSR) may not be necessary  
- Products: See CH 3–3.2. |
| **Model 2:** Defense Unique Software Intensive Program | **Key Characteristics**  
- Products requiring complex, defense unique software where several software builds are developed, integrated and tested before a mature software product can be deployed.  
- Generally hosted on commercial off-the-shelf computing platforms or existing military computing platforms  
**Systems Engineering Considerations**  
- Activities: See CH 3–2.3.1. and CH 3–3.2.; assumes minimal hardware development so manufacturing aspects may not apply; some Commercial Off the Shelf (COTS) production planning may be necessary  
- Reviews: See CH 3–3.3.; SSR as precursor to Preliminary Design Review (PDR), System Verification Review/Functional Configuration Audit (SVR/FCA), minimal Physical Configuration Audit (PCA), no Low-Rate Initial Production (LRIP) and no Full Rate Production (FRP) decisions; include Full Deployment (FD) decision; multiple reviews may be necessary for each build, Post Implementation Review (PIR) may be appropriate. Development RFP Release decision point determines scope of limited deployment for MAIS programs. At Milestone B finalize scope of limited deployment. At Milestone C and/or Limited Deployment decision, the increment of capability is reviewed for limited deployment.  
- Products: See CH 3–3.2. and CH 6–3.3. |
### Model 3: Incrementally Deployed Software Intensive Program

(See also DoDI 5000.02, Enc 11, DoDI 5000.75, and DAG Chapter 6, "Acquiring IT & Business Systems")

**Key Characteristics**
- Products requiring the integration of existing software adapted for DoD
- Distinguished from Model 2 by the fact of incremental deployment of a capability in relatively short intervals
- Model sometimes adopted for Defense Business Systems (DBS) (See DoDI 5000.75)
- Uses limited deployment decisions in lieu of MS C
- Each incremental capability starts with a separate pre-Milestone B decision
- Several increments necessary to achieve overall required capability; for DBS there are schedule constraints

**Systems Engineering Considerations**
- Activities: See CH 3—2.3.1. and CH 3—3.2.; assumes no hardware development so manufacturing aspects do not apply; may be some COTS production planning necessary
- Reviews: See CH 3—3.3.; SSR as precursor to PDR, minimal PCA, no LRIP, and no FRP decisions; multiple reviews may be necessary for each build and/or increment including PIR; multiple pre-Milestone B decisions; include Limited Deployment Decisions (LDD) and Full Deployment Decisions (FDD); IOC occurs before FDD. Development RFP Release decision point determines scope of limited deployment for MAIS programs. At Milestone B finalize scope of limited deployment. At Milestone C and/or Limited Deployment decision, the increment of capability is reviewed for limited deployment
- Products: See CH 3—3.2.

### Model 4: Accelerated Acquisition Program

**Key Characteristics**
- Products requiring development and deployment as quickly as possible, usually motivated by a potential adversary achieving technological surprise, and featuring a greater acceptance of program risk
- For accelerated acquisition programs regardless of ACAT level. For programs to be deployed in less than 2 years and below the cost thresholds for ACAT I and IA programs see DoDI 5000.02, Enc 13
- Schedule considerations take precedence over cost and technical risk considerations
- Compresses or eliminates phases of the process
- May combine objectives of the nominal milestones and decision points into fewer decision events

**Systems Engineering Considerations**
- Activities: Close and frequent interaction with the operational sponsor to ensure operational objective and measurable desired operational effect is clearly understood. System trade studies weigh achieving operational objectives and effect more highly than long term sustainability or cost. Conduct safety assessment and address risks. Minimum development and test with some concurrency
- Reviews: Tailored to program objectives; balance technical risks, operational needs, and timelines
- Products: Only as necessary to support PM decisions, DAB decisions, statutory requirements, planned deployment and sustainment needs

### Model 5: Hybrid Program A (Hardware Dominant)

**Key Characteristics**
- Products requiring hardware development and/or integration as well as software development
- Program structure combines the characteristics of Models 1 and 2
### Acquisition Program Model

<table>
<thead>
<tr>
<th>Key Characteristics and Systems Engineering Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Milestone B and C decisions should include criteria for software maturity</td>
</tr>
<tr>
<td>- Many modern weapon systems contain substantial hardware and software development resulting in some form of this Model 5</td>
</tr>
</tbody>
</table>

**Systems Engineering Considerations**

- Activities: See CH 3–2.3.1, and CH 3–3.2.; Hardware development may determine overall schedule, decision points and milestones, but software development requires tight integration and may dictate pace of program execution.
- Reviews: See CH 3–3.3.; SSR may be appropriate
- Products: See CH 3–3.2.

---

<table>
<thead>
<tr>
<th>Model 6: Hybrid Program B (Software Dominant)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Characteristics</strong></td>
</tr>
<tr>
<td>- Products requiring software development and/or integration as well as limited hardware development</td>
</tr>
<tr>
<td>- Each increment includes intermediate builds</td>
</tr>
<tr>
<td>- Each incremental capability starts with a separate Milestone B decision</td>
</tr>
<tr>
<td>- Several increments necessary to achieve overall required capability.</td>
</tr>
</tbody>
</table>

**Systems Engineering Considerations**

- Activities: See CH 3–2.3.1, and CH 3–3.2.; software development is tightly integrated and coordinated with limited hardware development; software development organized into series of builds
- Reviews: See CH 3–3.3.; SSR as precursor to PDR, minimal PCA, multiple reviews may be necessary for each build and/or increment including PIR; multiple pre-Milestone B decisions; include LF and FD decisions; IOC occurs before FDD. Development RFP Release decision point determines scope of limited deployment for MAIS programs. At Milestone B finalize scope of limited deployment. At Milestone C and/or Limited Deployment decision, the increment of capability is reviewed for limited deployment.
- Products: See CH 3–3.2, and CH 6–3.3.

---

As a subset of Model 4, products with less than ACAT I or IA cost thresholds, to be deployed in less than two years, and responding to Urgent Operational Needs (UONs) may fall within the procedures described in DoDI 5000.02, Enc 13 for Urgent Capability Acquisition (UONs are defined in CJCSI 3170.01.) The rapid acquisition life cycle has no Materiel Development Decision (MDD) and usually combines objectives of the generic milestones and decision points into fewer decision events. Since these products are usually non-developmental items (NDI) or near-NDI products, the primary systems engineering (SE) considerations are to ensure the capability is safe and secure, and meets warfighter needs and national security needs.

Life-cycle phase names may vary by acquisition model. For instance, some models are appropriate for incremental deliveries and have a subset of phases that are repeated, as identified in Table 14. The table provides a visual sense of the variation in phases between the DoDI 5000.02, para 5.c. acquisition models. This can help the PM and Systems Engineer select and tailor the acquisition model for the program. The transition from one phase to another is program-unique, documented in the Acquisition Strategy and approved by the Milestone Decision Authority (MDA).

**Table 14: Variation in Phase Terminology for Each Acquisition Model**
<table>
<thead>
<tr>
<th>Acquisition Model</th>
<th>Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generic</strong></td>
<td></td>
</tr>
<tr>
<td>Model 1: Hardware Intensive Program</td>
<td>MSA</td>
</tr>
<tr>
<td>Model 2: Defense Unique Software Intensive Program</td>
<td>MSA</td>
</tr>
<tr>
<td>Model 3: Incrementally Deployed Software Intensive Program</td>
<td>MSA</td>
</tr>
<tr>
<td>Model 4: Accelerated Acquisition Program</td>
<td>MSA</td>
</tr>
<tr>
<td>Model 5: Hybrid Program A (Hardware Dominant)</td>
<td>MSA</td>
</tr>
<tr>
<td>Model 6: Hybrid Program B (Software Dominant)</td>
<td>MSA</td>
</tr>
<tr>
<td>Urgent Capability Acquisition</td>
<td>Pre-Development</td>
</tr>
</tbody>
</table>

**Legend**
- EMD - Engineering and Manufacturing Development
- MSA - Materiel Solution Analysis
- O&S - Operations and Support
- P&D - Production and Deployment
- TMRR - Technology Maturation and Risk Reduction

Note: * = repeated for each increment

The meaning of Limited Deployment, as used in Models 2, 3 and 6, is contextually dependent. The scope of deployments can be driven by deployment of the full capability to a limited number of sites (i.e., Model 2), or driven by deployment of software increments and therefore increments of capability (i.e., Model 3), or a combination of both (i.e., Model 6).
CH 3–3.1.2 Systems of Systems

Whether or not a system is formally acknowledged as a system of systems (SoS), nearly all DoD systems function as part of an SoS to deliver a necessary capability to the warfighter (see Systems Engineering Guide for Systems of Systems on the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE) website). SoS systems engineering (SE) is an ongoing iterative process as shown in the SoS SE Implementers’ View in Figure 8: SoS SE Implementers’ View. The backbone of SoS SE implementation is a continuous analysis that considers changes from the broader operational mission environment as well as feedback from the ongoing engineering process.

Capability solutions to support a mission or set of missions are a challenge that may require a level of iterative analysis performed at the nexus between SoS SE and mission analysis. This iterative analysis is a multi-disciplinary activity called mission engineering. Mission Engineering (ME) is the deliberate planning, analyzing, organizing and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.

The ME results provide the basis for developing and evolving the SoS architecture, identifying or negotiating changes to the constituent systems that impact the SoS and working with the constituent systems to implement and integrate those changes. This view of SoS SE implementation provides structure to the evolution of the SoS through changes in constituent systems, which are typically on different life-cycle timelines, adapting as systems come in and move out and as Concept of Operations / Operational Mode Summary / Mission Profile (CONOPS/OMS/MP) adapt and change. Hence the need for continually updating the SoS analysis and adapting the architecture and updating systems on an ongoing basis.

Therefore, SoS SE planning and implementation should consider and leverage the development plans of the individual systems in order to balance SoS needs with individual system needs. Finally, SoS SE should address the end-to-end behavior of the ensemble of systems, addressing the key issues that affect this end-to-end behavior with particular emphasis on integration and interoperability. Effective application of SoS SE addresses organizational as well as technical issues in making SE trades and decisions. The Systems Engineer has different roles and authorities at the system versus the SoS level.

The SoS-level Systems Engineer can provide the technical foundation for effective user capabilities by conducting balanced technical management of the SoS, using an SoS architecture based on open systems and loose coupling and focusing on the design strategy and trades (both at establishment and through evolution). They should collaborate with multiple Systems Engineers across multiple systems. Each Systems Engineer has the authority for his or her system implementation. These waves of implementations and upgrades taken as a whole provide the SoS capability. For a more detailed discussion of Figure 8, see the paper, “An Implementers’ View of Systems Engineering for Systems of Systems”.

Consideration of SoS in SE for Individual Systems
Most acquisition programs address the development or major upgrade of individual systems (in contrast to SoS). Understanding the SoS context(s) of the system (including use in multiple operational environments) is critical to developing requirements for the system, so when delivered, it operates effectively in user operational environments. From the Joint Capabilities Integration and Development System (JCIDS) Capabilities-Based Assessment (CBA) through sustainment activities, it is important to recognize how the system context influences system requirements. An up-to-date CONOPS/OMS/MP for the system is basic to understanding the system context, notably, mission and task threads and data exchanges that have an impact on the system. Systems engineers of individual systems should ensure SoS considerations and risks are addressed throughout the acquisition life cycle by:

- Identifying system dependencies and interoperability needs (See CH 3–4.3.13, Interoperability and Dependencies)
- Factoring these into the development of system concepts, requirements and risks
- Addressing these through trade analysis, system architecture and design, interface development and management and verification and validation

Both from an individual system perspective and the SoS perspective, PMs and Systems Engineers have found it difficult to coordinate and balance the acquisition objectives and strategies for a given system with those of the SoS and other constituent systems. A senior governance body is useful to provide a forum for discussion and decision. This forum should address functional capabilities, technical plans, configuration management and strategies with respect to interfaces, interdependences, risks and risk mitigation. It is critical to address all equities and make collective decisions that can be implemented in changes to a system’s configuration.

One SoS best practice is to monitor closely interdependent programs, with checkpoints at scheduled design reviews to assess program progress, assess related risks and determine actions to mitigate potentially negative impacts. Another best practice is to have the technical representatives from each system participate in each others’ SFR, PDR, and CDR.

Table 15 lists SoS considerations for systems at each stage of acquisition. At each phase, the SE approach to addressing SoS-related dependencies should be addressed in the Systems Engineering Plan (SEP).

**Table 15: Key SoS Considerations for Systems by Acquisition Phase**

<table>
<thead>
<tr>
<th>Acquisition Phase</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Materiel Development Decision (Pre-MDD)</strong></td>
<td><strong>Focus</strong>&lt;br&gt;- Define role of the system in supporting a mission capability, including relationship to other systems in the SoS which support that capability&lt;br&gt;<strong>Evidence/Products</strong>&lt;br&gt;- End-to-end depiction (e.g., mission thread) of capability gap in context of systems currently supporting capability&lt;br&gt;<strong>Measure/Metrics</strong>&lt;br&gt;- Activities supported by the system in relationship to other systems and the context&lt;br&gt;- Physical environment information needs Joint Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities and Policy (DOTmLPF-P) for the system and the SoS&lt;br&gt;- Identification of stakeholders&lt;br&gt;<strong>Responsibilities/ Interdependencies</strong>&lt;br&gt;- Provided by the JCIDS analysis and the evidence provided at MDD</td>
</tr>
<tr>
<td>Acquisition Phase</td>
<td>Considerations</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Materiel Solution Analysis (MSA)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>In the Analysis of Alternatives (AoA), consider the alternatives in the context of the larger SoS supporting the capability</td>
</tr>
<tr>
<td></td>
<td>In the operational analysis and concept engineering for the preferred materiel solution, consider the new system in the SoS context; identify dependencies and relationships with other systems, including key interfaces and technical risks based on SoS considerations to be addressed in Technology Maturation and Risk Reduction (TMRR)</td>
</tr>
<tr>
<td></td>
<td>Identify the nature of the dependencies and interfaces, including the parties involved, and an initial plan for addressing these including initial memorandum of agreement (MOAs)</td>
</tr>
<tr>
<td></td>
<td>Identify non-materiel changes needed to implement a specific materiel solution, e.g. changes to tools, techniques and procedures to enable the SoS capability.</td>
</tr>
<tr>
<td><strong>Evidence/Products</strong></td>
<td>AoA criteria or results relevant to SoS dependencies or interfaces</td>
</tr>
<tr>
<td></td>
<td>Definition of key system dependencies or interfaces that influence system requirements</td>
</tr>
<tr>
<td></td>
<td>Initial management plans with supporting MOAs, including draft Interface Control Agreements (ICAs) for collaborations with other systems in a SoS</td>
</tr>
<tr>
<td></td>
<td>Risks associated with SoS dependencies (both programmatic and technical) and interoperability requirements, including environment, safety and occupational health (ESOH), and security risks to be accepted by Joint Authorities</td>
</tr>
<tr>
<td><strong>Measure/Metrics</strong></td>
<td>SoS-related requirements in draft system performance specification and/or Pre-MS A Request for Proposal (RFP)</td>
</tr>
<tr>
<td></td>
<td>MOAs with key parties in SoS dependencies or relationships</td>
</tr>
<tr>
<td><strong>Responsibilities/Interdependencies</strong></td>
<td>Systems engineers of the systems involved in the SoS or SoS SE if one exists</td>
</tr>
<tr>
<td></td>
<td>End users</td>
</tr>
<tr>
<td></td>
<td>Requirements Manager (s) for requirements per JCIDS Manual</td>
</tr>
<tr>
<td></td>
<td>PM(s) responsible for Memorandum of Agreements (MOA)</td>
</tr>
<tr>
<td></td>
<td>Contracting Officer(s) responsible for RFPs</td>
</tr>
<tr>
<td>Acquistion Phase</td>
<td>Considerations</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **Technology Maturation and Risk Reduction (TMRR)** | **Focus**  
  - Assess the technical approaches and risks for addressing system requirements including considerations for the system as a component operating in a SoS context (including dependencies, interoperability and interfaces)  
  - Address considerations of changes needed in other systems for the systems in acquisition to meet capability objectives  
| **Evidence/Products**  
  - An interface management plan that is a part of a configuration management plan, including ICAs  
  - Risks associated with SoS dependencies (both programmatic and technical) and interoperability requirements, including environment, safety and occupational health (ESOH), and security risks to be accepted by Joint Authorities.  
  - Output of studies which validate the technical fit and operational suitability of the system under development within the SoS  
| **Measure/Metrics**  
  - Final interface specifications  
  - MOAs and schedule for interface management plan  
  - Progress with respect to schedule and plan milestones  
  - Progress with respect to expected performance  
| **Responsibilities/Interdependencies**  
  - Developers of this system and the other systems involved with the dependencies of interface; shared configuration management (CM)  
  - Interface Management Working Group (IMWG)  
  - End users  |
| **Engineering Manufacturing Development (EMD)** | **Focus**  
  - Develop, verify and validate the detailed design that addresses system requirements, considering the SoS context including recognized dependencies and interfaces  
| **Evidence/Products**  
  - Interface documentation, test plans and test reports  
  - Progress on MOAs with system’s dependencies  
  - Risks associated with SoS dependencies (both programmatic and technical) and interoperability requirements, including environment, safety and occupational health (ESOH), and security risks to be accepted by Joint Authorities.  
| **Measure/Metrics**  
  - Successful development and test of interfaces  
  - Progress with respect to SoS schedule and plan milestones  
  - Progress with respect to expected performance  
| **Responsibilities/Interdependencies**  
  - Materiel developers  
  - IMWG  
  - Testers  
  - End users |
### Acquisition Phase Considerations

<table>
<thead>
<tr>
<th>Production &amp; Deployment (P&amp;D) and Operations and Support (O&amp;S)</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Verify the as-built interfaces meet specs and support operational needs.</td>
</tr>
<tr>
<td></td>
<td>• Support effective system operation in a SoS context</td>
</tr>
<tr>
<td>Evidence/Products</td>
<td>• Test reports</td>
</tr>
<tr>
<td>Measure/Metrics</td>
<td>• Successful test results</td>
</tr>
<tr>
<td>Responsibilities/Interdependencies</td>
<td>• Materiel developers</td>
</tr>
<tr>
<td></td>
<td>• Testers</td>
</tr>
<tr>
<td></td>
<td>• End users</td>
</tr>
</tbody>
</table>


### CH 3–3.2 Systems Engineering Activities in Life-Cycle Phases

This section describes, from several perspectives, the technical activities typically performed in each phase of the acquisition life cycle. First, the objectives and an overview of the phase are described to provide context. Then, a sequence of subsections address the roles and responsibilities of a System Engineer in a program office, along with the inputs normally required to constrain the technical activities. Each phase description ends with a table summarizing the expected technical outputs from the phase. While technical reviews and audits are mentioned in this section, the details are covered in CH 3–3.3, Technical Reviews and Audits.

#### CH 3–3.2.1 Pre-Materiel Development Decision

The objectives of the pre-Materiel Development Decision (MDD) efforts are to obtain a clear understanding of user needs, identify a range of technically feasible candidate materiel solution approaches, consider near-term opportunities to provide a more rapid interim response and develop a plan for the next acquisition phase, including the required resources. This knowledge supports the Milestone Decision Authority’s (MDA) decision to authorize entry into the acquisition life cycle and pursue a materiel solution. An additional objective is to characterize trade space, risks and mission interdependencies to support the start of the Analysis of Alternatives (AoA).

Policy in this area comes from two perspectives: the Joint Capabilities Integration and Development System (JCIDS) defined in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 and the Defense Acquisition System (DAS) defined in DoDD 5000.01.

Development planning (DP) encompasses the engineering analysis and technical planning activities that provide the foundation for informed investment decisions on the path a materiel development follows to meet operational needs effectively, affordably and sustainably. DP activities are initiated prior to the Materiel Development Decision, continue throughout the Materiel Solution Analysis phase, and eventually transition to the program environment.

Attention to critical systems engineering (SE) processes and functions, particularly during early phases in acquisition, is essential to ensuring that programs deliver capabilities on time and on budget. The effective execution of pre-MDD SE efforts provides the foundation for user-driven requirements and technically feasible solution options that ensure an executable program. At MDD, the MDA not only decides whether an investment is made to fill the capability gap but also determines the fundamental path the materiel development will follow. This decision should be based on effective development planning.

An important aspect of the pre-MDD effort is to narrow the field of possible solutions to a reasonable set that is analyzed in the AoA. Early recognition of constraints, combined with analysis of technical
feasibility, can eliminate many initial ideas because they lack the potential to meet the need in a timely, sustainable and cost-effective manner. Conversely, the range of alternatives analyzed in the AoA are chosen from a sufficiently broad solution space. Whenever possible, the Systems Engineer should try to engage with the end user (e.g., Requirements Manager) before the Initial Capabilities Document (ICD) and associated operational architecture is validated by the Joint Requirements Oversight Council (JROC) (see CH 3–4.2.1, Stakeholder Requirements Definition Process).

Studies have found that "programs that considered a broad range of alternatives tended to have better cost and schedule outcomes than the programs that looked at a narrow scope of alternatives." (See GAO-09-665 Analysis of Alternatives, Page 6.)

The work performed in this time frame should be well documented and transitioned to be used in future phases of the Acquisition Life Cycle. This is so the Program Manager (PM) and Systems Engineer, when assigned, can benefit from the mutual understanding of the basis of need (requirements) and the art of the possible (concepts/materiel solutions). To achieve these benefits, the Systems Engineer should proactively collaborate with the Science and Technology (S&T) and user communities.

Roles and Responsibilities

Often there is no assigned PM or Systems Engineer at this point in the weapon system's life cycle. Instead, a designated Service representative (e.g., Requirements Manager) is orchestrating and leading the preparations for MDD. This leader is responsible for synthesizing the necessary information to support a favorable decision. See DoDI 5000.02, Enc 3, sec. 3 and MDD Development Planning Templates. As a best practice, consideration should be given to designating a Service engineering representative to support concept and requirements definition and associated decisions in preparation for the MDD.

The designated Service representative should make use of appropriate models and simulations (CH 3–2.4.2, Modeling and Simulation) to develop required MDD evidence. The designated Service representative also should consider issuing a Request for Information (RFI) to industry to help identify and characterize alternative solutions.

Inputs

Table 16 summarizes the primary inputs and technical outputs associated with this part of the life cycle. Unlike the sections that follow, this pre-MDD period is the bridge between JCIDS and the DAS.

<table>
<thead>
<tr>
<th>Inputs for Pre-MDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Initial Capabilities Document (ICD) (See CJCSI 3170.01)</td>
</tr>
<tr>
<td>• Product of Capability-Based Assessment (CBA) or equivalent</td>
</tr>
<tr>
<td>Other analyses</td>
</tr>
<tr>
<td>• Other prior analytic, experimental, prototyping and/or technology demonstration efforts may be provided by the S&amp;T community</td>
</tr>
<tr>
<td>• Results of Market Research: 1) to identify existing technologies and products; and, 2) to understand potential solutions, technologies and sources</td>
</tr>
</tbody>
</table>

The MDD review requires an ICD that represents an operational capability need validated in accordance with CJCSI 3170.01. The Joint Staff provides this document, which is generally the output of a Capability-Based Assessment (CBA) or other studies. The designated Service representative should have access to both the ICD and supporting studies. Other technical information (such as models and simulations) may be useful for understanding both the need and its context. The S&T community can contribute pertinent data and information on relevant technologies, prototypes, experiments and/or analysis. The DASD(SE)
web site provides an example of how a program may provide evidence at the MDD review to support the MDA decision.

**Activities**

Figure 9 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 9: Weapon System Development Life Cycle**

During pre-MDD, SE activities focus on:

- Achieving an in-depth understanding of the operational capability gaps defined in the ICD and identifying the sources of the gap(s), which, if addressed by a materiel solution, could achieve the needed capability
- Identifying an appropriate range of candidate materiel solutions from across the trade space to meet the need
- Identifying near-term opportunities to provide a more rapid interim response to the capability need
- Working with the S&T community (across Government, industry and academia) as well as other collaborators to build the technical knowledge base for each candidate materiel solution in the AoA Guidance to include experimentation and prototyping
- Analyzing trade space to determine performance versus cost benefits of potential solutions
- Planning for the technical efforts required during the next phase
- Performing an early evaluation of risks associated with the alternatives to be analyzed in the next phase
- Working with requirements developers to ensure the quality of all operational requirements from an SE perspective

**Outputs and Products**

This effort ends after a successful MDD review in which the MDA approves entry into the Defense Acquisition System. This decision is documented in a signed Acquisition Decision Memorandum (ADM), which specifies the approved entry point, typically the Materiel Solution Analysis (MSA) phase. Outputs of
pre-MDD efforts provided in Table 17 also include approved AoA Guidance and an AoA Study Plan, which should be informed by SE.

**Table 17: Technical Outputs Associated with Pre-MDD**

<table>
<thead>
<tr>
<th>Technical Outputs from Pre-MDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to the ICD</td>
</tr>
<tr>
<td>Informed advice to the AoA Guidance and Study Plan (See CH 2–2.3.)</td>
</tr>
<tr>
<td>Informed advice to the plan and budget for the next phase, including support to the AoA and</td>
</tr>
<tr>
<td>non-AoA technical efforts required to prepare for the initial milestone review</td>
</tr>
<tr>
<td>Informed advice to the ADM</td>
</tr>
</tbody>
</table>

All potential materiel solutions pass through an MDD before entering the DAS. However, the MDA may authorize entry at any point in the acquisition life cycle based on the solution’s technical maturity and risk. Technical risk has several elements: technology risk, engineering risk and integration risk. If the Service-recommended entry point is beyond the MSA phase, for example, part way through the Technology Maturation and Risk Reduction (TMRR) phase, the program provides evidence that all MSA and TMRR phase-specific entrance criteria and statutory requirements are met and that the solution’s technical maturity supports entry at the point in the phase being proposed. Emphasis should be placed on the soundness of supporting technical information and plans in order to inform the MDA’s decision, as opposed to which documents may or may not be complete.

As the next section explains, the MSA phase is made up of more than an AoA; it includes technical tasks to determine the preferred materiel solution based on the AoA results and technical tasks to prepare for the initial milestone review. Therefore, the technical plan and budget presented at the MDD should reflect the full range of activities required in the next phase.

**CH 3–3.2.2 Materiel Solution Analysis Phase**

The objective of the Materiel Solution Analysis (MSA) phase is to select and adequately describe a preferred materiel solution to satisfy the phase-specific entrance criteria for the next program milestone designated by the Milestone Decision Authority (MDA). Prior to completion of the MSA Phase, the Component Acquisition Executive (CAE) selects a Program Manager (PM) and establishes a Program Office to complete the necessary actions associated with planning the acquisition program. Usually, but not always, the next milestone is a decision to invest in technology maturation, risk reduction activities and preliminary design in the Technology Maturation and Risk Reduction (TMRR) phase. The systems engineering (SE) activities in the MSA phase result in several key products. First, a system model and/or architecture is developed that captures operational context and envisioned concepts, describes the system boundaries and interfaces, and addresses operational and functional requirements. Second, a preliminary system performance specification is developed that defines the performance of the preferred materiel solution. Third, the Systems Engineer advises the PM on what is to be prototyped, why and how.

During the MSA phase, the program team identifies a materiel solution to address user capability gaps partially based on an Analysis of Alternatives (AoA) (i.e., analysis of the set of candidate materiel solutions) led by the Director, Cost Analysis and Program Evaluation (CAPE) and conducted by a designated DoD Component. Once the Service sponsor selects a preferred materiel solution, the program team focuses engineering and technical analysis on this solution to ensure development plans, schedule, funding and other resources match customer needs and match the complexity of the preferred materiel solution. SE activities should be integrated with MSA phase-specific test, evaluation, logistics and sustainment activities identified in CH 8–4.1. and CH 4–3.1.

This phase has two major blocks of activity: (1) the AoA; and (2) the post-AoA operational analysis and concept engineering to prepare for a next program milestone designated by the MDA (see Figure 10: Activities in Materiel Solution Analysis Phase).
The AoA team considers a range of alternatives and evaluates them from multiple perspectives as directed by the AoA Guidance and AoA Study Plan. Engineering considerations including technical risk should be a component of the AoA Guidance and be addressed in the AoA Study Plan.

**Figure 10: Activities in Material Solution Analysis Phase**

The objective of the AoA is to analyze and characterize each alternative (or alternative approach) relative to the others. The AoA does not result in a recommendation for a preferred alternative; it provides information that the Service sponsor uses to select which materiel solution to pursue. The Systems Engineer should participate in the AoA to help analyze performance and feasibility and to optimize alternatives. Using the AoA results, the Service sponsor may conduct additional engineering analysis to support the selection of a preferred materiel solution from the remaining trade space of candidate materiel solutions. After choosing the preferred materiel solution, the Service sponsor matures the solution in preparation for the next program milestone designated by the MDA.

After the AoA, program systems engineers establish the technical performance requirements consistent with the draft Capability Development Document (CDD), required at the next program milestone designated by the MDA, assuming it is Milestone A. These requirements form the basis for the system performance specification placed on contract for the TMRR phase; they also inform plans to mitigate risk in the TMRR phase.

In the MSA phase, the DoD Component combat developer (e.g., Requirements Manager) prepares a Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP), consistent with the validated/approved capability requirements document, typically an Initial Capabilities Document. The CONOPS/OMS/MP includes the operational tasks, events, durations, frequency, operating conditions and environment in which the recommended materiel solution is to perform each mission and each phase of a mission. The CONOPS/OMS/MP informs the MSA phase activities and the development of plans for the next phase.
During MSA, several planning elements are addressed to frame the way forward for the MDA’s decision at the next program milestone. SE is a primary source for addressing several of these planning elements. The planning elements include:

- Capability need, architecture
- System concept, architecture
- Key interfaces (including external interfaces and dependencies)
- Acquisition approach
- Engineering/technical approach
- Test and evaluation approach
- Program management approach
- External dependencies/agreements
- Schedule
- Resources
- Risks

See CH 3–4.1.1, Technical Planning Process. These planning elements are documented in various program plans such as the Acquisition Strategy (AS), Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP), next-phase Request for Proposal (RFP) and the Systems Engineering Plan (SEP). The SEP describes the SE efforts necessary to provide informed advice to these other planning artifacts (see the SEP Outline).

SE provides, for example, the technical basis for TMRR phase planning and execution, including identification of critical technologies, development of a competitive and risk reduction prototyping strategy and establishment of other plans that drive risk-reduction efforts. This early SE effort lays the foundation for the TMRR phase contract award(s) and preliminary designs, which confirm the system’s basic architecture.

Roles and Responsibilities

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the PM focuses on the following MSA activities, which rely on and support SE efforts:

- Preparing for and supporting source selection activities for the upcoming phase solicitation and contract award
- Supporting the requirement community with the development of the draft CDD, assuming the next phase is TMRR
- Developing the AS, which incorporates necessary risk-reduction activities
- Staffing the program office with qualified (trained and experienced) systems engineers

In addition to the general roles and responsibilities described in CH 3–2.5, Engineering Resources, during this phase it is the Systems Engineer’s responsibility to:

- Lead and manage the execution of the technical activities in this phase
- Measure and track the system’s technical maturity
- Identify technologies that should be included in an assessment of technical risk.
- Perform trade studies
- Support preparations for the RFP package and assist in structuring the evaluation teams for technical aspects of the review
- Develop the system performance specification. See CH 3–4.1.6, Configuration Management Process. A particular program’s naming convention for specifications should be captured in the SEP and other plans and processes tailored for the program
- Ensure integration of key design considerations into the system performance specification
- Develop technical approaches and plans, and document them in the SEP.
- Ensure the phase technical artifacts are consistent and support objectives of the next phase
**Inputs**

Table 18 summarizes the primary inputs associated with this part of the life cycle (see DoDI 5000.02, para 5.d.2). The table assumes the next phase is TMRR, but most of the technical outputs would be applicable going into any follow-on phase.

**Table 18: Inputs Associated with MSA Phase**

<table>
<thead>
<tr>
<th>Inputs for MSA Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Capabilities Document (ICD) (See CJCSI 3170.01)</td>
</tr>
<tr>
<td>• Product of Capability Based Assessment (CBA) or equivalent</td>
</tr>
<tr>
<td>Validated On-Line Life-cycle Threat (VOLT) Report (See DoDI 5000.02 (Enc 1, Table 2) and CH 7–4.1.2.)</td>
</tr>
<tr>
<td>AoA Guidance and AoA Study Plan (See CH 2–2.3.)</td>
</tr>
<tr>
<td>Acquisition Decision Memorandum (ADM) (may contain additional direction)</td>
</tr>
<tr>
<td>Other analyses generated pre-MDD</td>
</tr>
<tr>
<td>• Other prior analytic, prototyping and/or technology demonstration efforts conducted by the S&amp;T community; technology insertion/transition can occur at any point in the life cycle</td>
</tr>
<tr>
<td>• Results of Market Research: 1) to identify existing technologies and products; and 2) to understand potential solutions, technologies, and sources</td>
</tr>
</tbody>
</table>

The ICD, AoA Guidance, and AoA Study Plan should be available prior to the start of the MSA phase. Results of other related analyses may be available, for example, from the Capability Based Assessment (see CH 3–4.2.1, Stakeholder Requirements Definition Process) or other prior analytic and/or prototyping efforts conducted by the S&T community.

**Activities**

The MSA phase activities begin after a favorable MDD review has been held (see CH 3–3.2.1, Pre-Materiel Development Decision) and end when the phase-specific entrance criteria for the next program milestone, designated by the MDA, have been met. Figure 11 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 11: Weapon System Development Life Cycle**
Referring back to Figure 10, which shows the major blocks of technical activities in the MSA phase:

- **Conduct AoA.** Includes all activities and analyses conducted by the AoA Study team under the direction of the Senior Advisory Group/Executive Steering Committee (SAG/ESC) and CAPE, or Service equivalent. Concludes with a final SAG/ESC and AoA Report. Systems Engineers should support this activity.

- **Perform Analysis to Support Selection of a Preferred Materiel Solution.** Includes all engineering activities and technical analysis performed to support Service selection of the preferred materiel solution by balancing cost, performance, schedule and risk.

- **Perform Operational Analysis on Preferred Materiel Solution.** Supports the definition of the performance requirements in the operational context, Functional Capabilities Board (FCB) review and the development of the draft CDD (see CJCSI 3170.01 Joint Capabilities Integration and Development System (JCIDS) and CH 3–4.2.1. Stakeholders Requirements Definition Process). The Systems Engineer should support the operational requirement/user/operational test community to ensure the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP) is detailed enough to verify and validate system performance and operational capability. This activity could include the development of design reference missions/use cases that assist in the verification and validation process. Through analysis, the Systems Engineer also helps to identify key technology elements, determine external interfaces and establish interoperability requirements.

- **Perform Engineering and Technical Analysis on Preferred Materiel Solution.** This includes all engineering activities and technical analysis performed on the Service-selected preferred materiel solution in support of the development and maturation of a materiel solution concept, associated system performance specification and technical plans for the next phase.

- **Establish Program Framework and Strategies.** All activities to converge on the overarching strategies and plans for the acquisition of the system. Attention should be given to identifying and documenting agreements with external organizations. This documentation should include, for example, the contributions of S&T organizations and plans for transitioning technology into a program.
• **Prepare for Initial Review Milestone and Next Phase.** Includes all activities to compile technical and programmatic analysis and plans to meet the entrance criteria for the next program milestone designated by the MDA. See DoDI 5000.02, para 5.d.2 for phase objectives and exit criteria.

The technical review typically conducted in the MSA phase is the Alternative Systems Review (ASR) (see CH 3–3.3.1, Alternative Systems Review).

**Outputs and Products**

The knowledge gained during this phase, based on both the AoA and other analyses, should provide confidence that a technically feasible solution approach matches user needs and is affordable with reasonable risk (See Table 19. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.)

**Table 19: Technical Outputs Associated with MSA Phase**

<table>
<thead>
<tr>
<th>Technical Outputs from MSA Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to the draft Capability Development Document (CDD)</td>
</tr>
<tr>
<td>Informed advice to Acquisition Decision Memorandum (ADM) and, when applicable, 10 USC 2366a certification</td>
</tr>
<tr>
<td>Informed advice to the AoA Report (See CH 2–2.3.)</td>
</tr>
<tr>
<td>Informed advice to the selection of the preferred materiel solution</td>
</tr>
<tr>
<td>• Selection of the preferred materiel solution is documented in the ADM</td>
</tr>
<tr>
<td>SEP (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2, Systems Engineering Plan)</td>
</tr>
<tr>
<td>Reliability, Availability, Maintainability, and Cost Rationale Report (RAM-C Report) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>• Attachment to SEP</td>
</tr>
<tr>
<td>Reliability Growth Curves (RGC) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>• Included in SEP</td>
</tr>
<tr>
<td>PPP (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.2.)</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>• Results could include knees-in-the-curves sensitivity analyses, product selections, etc.</td>
</tr>
<tr>
<td>Assumptions and constraints</td>
</tr>
<tr>
<td>• Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td>Environment, Safety and Occupational Health (ESOH) planning (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)</td>
</tr>
<tr>
<td>Assessment of technical risk and development of mitigation plans (See CH 3-4.1.5, and the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)</td>
</tr>
<tr>
<td>Consideration of technology issues</td>
</tr>
<tr>
<td>Initial identification of critical technologies</td>
</tr>
<tr>
<td>Interdependencies/interfaces/memoranda of agreement (MOAs)</td>
</tr>
<tr>
<td>• Understanding of the unique program interdependencies, interfaces, and associated MOAs</td>
</tr>
<tr>
<td>Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)</td>
</tr>
<tr>
<td>• Initial LMDP</td>
</tr>
<tr>
<td>Draft system performance specification</td>
</tr>
</tbody>
</table>
Technical Outputs from MSA Phase

Other technical information generated during the MSA phase:
- Architectures, system models and simulations
- Results of Market Research: 1) to identify existing technologies and products; and 2) to understand potential solutions, technologies, and sources appropriate for maturing the product in the next phase

Prototyping strategy (See DoDI 5000.02, para 5.d.4 and DoDI 5000.02, Enc 1, Table 2, Acquisition Strategy))
- Relationship between draft system performance specification and prototyping objectives is established and plans for next phase are consistent with it, both from a prototyping and preliminary system design perspective
- Includes identification of key system elements to be prototyped prior to Milestone B
- Documented in the AS

Informed advice to Affordability and Resource Estimates (See CH 3–2.4.4, Value Engineering, CH 3–4.3.2, Affordability – Systems Engineering Trade-Off Analyses, CH 1–4.2.15., and CH 2–2.1.)
- Affordability goals are established and treated as Key Performance Parameters (KPPs) at the next program milestone designated by the MDA
- Identify the likely design performance points where trade-off analyses occur during the next phase
- Value engineering results, as appropriate

Informed advice to the Life-Cycle Sustainment Plan (LCSP) (See CH 4–3.1.)
Informed advice to the Test and Evaluation Master Plan (TEMP) (See CH 8–4.1.)
Informed advice to the developmental test and evaluation (DT&E) planning including Early Operational Assessments (EOAs) (See CH 8–4.1.)
Informed advice to the Request for Proposal (RFP)
- Informed advice including system performance specification, SOW, CDRLs and source-selection criteria

Informed advice to the Acquisition Strategy (AS) (See CH 1–4.1.)
- Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule and risks

Informed advice for the Spectrum Supportability Risk Assessment (See DoDI 4650.01 and CH 3–4.3.20.)

CH 3–3.2.3 Technology Maturation and Risk Reduction Phase

The primary objective of the Technology Maturation and Risk Reduction (TMRR) phase is to reduce technical risk and develop a sufficient understanding of the materiel solution to support sound investment decisions at the pre-Engineering and Manufacturing Development (EMD) Review and at Milestone B regarding whether to initiate a formal acquisition program. The Systems Engineer supports the production of a preliminary system design that achieves a suitable level of system maturity for low-risk entry into EMD (See Figure 12.) Usually the Systems Engineer implements a strategy of prototyping on a system element or subsystem level, balancing capability needs and design considerations to synthesize system requirements for a preliminary end-item design for the system. The prototyping objectives should focus on risk reduction and/or competition.

The major efforts associated with the TMRR phase are:
- Determining the appropriate set of technologies to integrate into a full system.
- Maturing the technologies, including demonstrating and assessing them in a relevant environment.
- Conducting prototyping of the system and/or system elements.
- Performing trade studies, refine requirements and revise designs.
- Developing the preliminary design, including functional and allocated baselines, specifications, interface control drawings/documents, architectures and system models.
- Performing developmental test activities as appropriate.

**Figure 12: Systems Engineering Activities in the Technology Maturation and Risk Reduction Phase**

SE activities should be integrated with TMRR phase-specific test and evaluation and logistics and sustainment activities identified in CH 8–4.2 and CH 4–3.2, respectively.

During the TMRR phase, the program develops and demonstrates prototype designs to reduce technical risk, validate design approaches, validate cost estimates and refine requirements. In addition, the TMRR phase efforts ensure the level of expertise required to operate and maintain the product is consistent with the force structure. Technology development is an iterative process of maturing technologies and refining user performance parameters to accommodate those technologies that do not sufficiently mature (requirements trades). The Initial Capabilities Document, the Acquisition Strategy (AS), Systems Engineering Plan (SEP) and Capability Development Document (CDD) guide the efforts of this phase. The CDD enters the TMRR phase as a draft (as described in DoDI 5000.02, Enc 1, Table 2 and CJCSI 3170.01) and is validated during this phase to support preliminary design activities and the PDR.

There are two key technical objectives in the TMRR phase: technical risk reduction and initial system development activity, culminating in preliminary design. The Systems Engineer in the TMRR phase manages activities to evaluate prototyped solutions (competitive and risk reduction prototypes) against performance, cost and schedule constraints to balance the total system solution space. This information can then be used to inform the finalization of the system performance specification as a basis for functional analysis and preliminary design.

Effective systems engineering (SE), applied in accordance with the SEP and gated by technical reviews, reduces program risk, identifies potential management issues in a timely manner and supports key program decisions. The TMRR phase provides the Program Manager (PM) with a preliminary design and allocated baseline that are realistic and credible.
**Roles and Responsibilities**

The program office team provides technical management and may employ industry, Government laboratories, the Service science and technology (S&T) community or Federally Funded Research and Development Centers (FFRDCs)/universities to accomplish specific risk-reduction or prototype tasks as described in the SEP.

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the PM focuses on the following TMRR activities, which rely on and support SE efforts:

- Awarding TMRR phase contract(s).
- Providing resources for technical reviews.
- Planning and executing the Technology Readiness Assessment (TRA) (MDAPS only).
- Influencing development of the CDD.
- Developing the Acquisition Strategy (AS).
- Developing the strategy and objectives for use of prototypes; considering both contracted efforts and government sources.
- Supporting the Development RFP Release Decision Point.
- Ensuring the Government preserves the rights needed to be consistent with the life-cycle acquisition and support strategy. During TMRR, proprietary development and design can often lead to issues with intellectual property and associated data rights (see CH 3–4.1.7, Technical Data Management Process).
- Supporting the Configuration Steering Board in accordance with DoDI 5000.02, para 5.d.5b once the CDD has been validated. This board assumes responsibility to review all requirements changes and any significant technical configuration changes for ACAT I and IA programs in development, production and sustainment that have the potential to result in cost and schedule impacts to the program.

In addition to the general roles and responsibilities described in CH 3–2.5, Engineering Resources, during this phase it is the Systems Engineer’s responsibility to:

- Lead and manage the execution of the technical activities as documented in the SEP.
- Plan and execute technical reviews, including the System Requirements Review (SRR), System Functional Review (SFR), and Preliminary Design Review (PDR).
- Measure and track program maturity using technical performance measures, requirements stability and integrated schedules.
- Support award of TMRR phase contract(s), as necessary.
- Balance and integrate key design considerations.
- Maintain the Systems Engineering Plan (SEP), including generating the update in support of Milestone B.
- Lead the initial development of the system to include functional analysis, definition of the functional and allocated baselines and preliminary design (see CH 3–4.2.2, Requirements Analysis Process and CH 3–4.2.3, Architecture Design Process).
- Support configuration management of the baselines, since they are required in later technical reviews, audits and test activities (e.g., functional baseline at the Functional Configuration Audits (FCAs)).
- Conduct technical activities in support of the Development RFP Release Decision Point.
- Conduct a rigorous and persistent assessment of technical risk, determine risk mitigation plans and work with the PM to resource the mitigation plans.
- Support the Technology Readiness Assessment (TRA) including creation of the plan, the pre-EMD preliminary TRA and the TRA final report (MDAPs only).
- Support requirements management, and monitor for unnecessary requirements growth (e.g., derived versus implied requirements).
- Manage interfaces and dependencies.
- Maintain oversight of the system (software and hardware) development processes, system testing, documentation updates and tracking of the system development efforts.
- Support the PM in his interactions with the Configuration Steering Board.

**Inputs**

Table 20 summarizes the primary inputs associated with this part of the life cycle.

**Table 20: Inputs Associated with TMRR Phase**

<table>
<thead>
<tr>
<th>Inputs for TMRR Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Component combat developer (e.g., Requirements Manager) provides:</td>
</tr>
<tr>
<td>- Draft Capability Development Document (CDD)</td>
</tr>
<tr>
<td>- Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP)</td>
</tr>
<tr>
<td>Analysis of Alternatives (AoA) Report and AoA Sufficiency Report (See CH 2–2.3.)</td>
</tr>
<tr>
<td>Preferred materiel solution</td>
</tr>
<tr>
<td>- Selection of preferred materiel solution is documented in the ADM</td>
</tr>
<tr>
<td>Acquisition Decision Memorandum (ADM) (may contain additional direction)</td>
</tr>
<tr>
<td>SEP (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2, Systems Engineering Plan)</td>
</tr>
<tr>
<td>Reliability, Availability, Maintainability and Cost Rationale (RAM-C) Report (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>- Attachment to SEP</td>
</tr>
<tr>
<td>Reliability Growth Curves (RGC) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>- Included in SEP</td>
</tr>
<tr>
<td>Program Protection Plan (PPP) (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.2.)</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>- Results could include knees-in-the-curves sensitivity analyses, product selections, results of automation trades, etc.</td>
</tr>
<tr>
<td>Assumptions and constraints</td>
</tr>
<tr>
<td>- Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td>Environment, safety and occupational health (ESOH) planning (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)</td>
</tr>
<tr>
<td>Risk assessment (See CH 3–4.1.5.)</td>
</tr>
<tr>
<td>- Key risks identified at Milestone A guide TMRR phase activities</td>
</tr>
<tr>
<td>Consideration of technology issues</td>
</tr>
<tr>
<td>Initial identification of critical technologies</td>
</tr>
<tr>
<td>- MSA phase may have identified an initial list of critical technologies</td>
</tr>
<tr>
<td>Interdependencies/interfaces/memoranda of agreements (MOAs)</td>
</tr>
<tr>
<td>Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)</td>
</tr>
<tr>
<td>Draft system performance specification</td>
</tr>
<tr>
<td>Other technical information generated during the MSA phase</td>
</tr>
<tr>
<td>- Architectures, system models and simulations</td>
</tr>
<tr>
<td>- Results of Market Research: 1) to identify existing technologies and products; and 2) to understand potential solutions, technologies, and sources appropriate for maturing the product in this phase</td>
</tr>
<tr>
<td>Prototyping strategy (See DoDI 5000.02, para 5.d.4 and DoDI 5000.02, Enc 1, Table 2, Acquisition Strategy))</td>
</tr>
<tr>
<td>- Includes identification of key system elements to be prototyped prior to Milestone B</td>
</tr>
</tbody>
</table>
### Inputs for TMRR Phase

<table>
<thead>
<tr>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validated On-Line Life-cycle Threat (VOLT) Report</td>
<td>DoDI 5000.02 (Enc 1, Table 2) and CH 7–4.1.2.</td>
</tr>
<tr>
<td>Affordability Assessment</td>
<td>CH 1–4.2.15. and CH 3–4.3.2.</td>
</tr>
<tr>
<td>• Affordability goals are established and treated as a Key Performance</td>
<td></td>
</tr>
<tr>
<td>Parameters (KPPs) at Milestone A</td>
<td></td>
</tr>
<tr>
<td>• Affordability goals drive engineering trade-offs and sensitivity analyses</td>
<td></td>
</tr>
<tr>
<td>about capability priorities in the TMRR phase</td>
<td></td>
</tr>
<tr>
<td>AS</td>
<td>CH 1–4.1.</td>
</tr>
<tr>
<td>Life-Cycle Sustainment Plan (LCSP)</td>
<td>CH 4–3.1.</td>
</tr>
<tr>
<td>Test and Evaluation Master Plan (TEMP)</td>
<td>CH 8–4.1.</td>
</tr>
<tr>
<td>Informed advice to the developmental test and evaluation (DT&amp;E) assessments</td>
<td>CH 8–4.1.</td>
</tr>
<tr>
<td>• Includes Early Operational Assessments (EOAs)</td>
<td></td>
</tr>
<tr>
<td>Draft and final Request for Proposal (RFP)</td>
<td></td>
</tr>
<tr>
<td>Security Classification Guide (SCG)</td>
<td></td>
</tr>
<tr>
<td>Other analyses</td>
<td></td>
</tr>
<tr>
<td>• Other prior analytic, prototyping and/or technology demonstration efforts</td>
<td></td>
</tr>
<tr>
<td>done by the S&amp;T community. Technology insertion/transition can occur at</td>
<td></td>
</tr>
<tr>
<td>any point in the life cycle</td>
<td></td>
</tr>
<tr>
<td>Spectrum Supportability Risk Assessment</td>
<td>DoDI 4650.01 and CH 3–4.3.20.</td>
</tr>
</tbody>
</table>

### Activities

The TMRR phase activities begin when a favorable Milestone A decision has been made (see CH 3–3.2.2, Materiel Solution Analysis Phase) and end with a successful Milestone B decision. Figure 13 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 13: Weapon System Development Life Cycle**
The TMRR phase addresses a set of critical activities leading to the decision to establish a program of record. The SE activities are aimed at reducing technical risk and providing the technical foundation for this decision. Depending on the nature of the technology development strategy, the order and characteristics of these activities may change. During the TMRR phase, systems engineers follow comprehensive, iterative processes to accomplish the following:

- **Perform Technology Maturation.** The AS identifies technologies requiring further maturation before they can be implemented within a solution. Technology maturation involves design, development, integration and testing. There could be one or more risk areas related to hardware, software or information technology, and there may be multiple industry contracts/Government efforts for maturing the technology. The TEMP should stipulate the test and evaluation approach for assessing the results of the technology maturation activities (see CH 8-4.2). The Systems Engineer participates in the technology readiness assessment (TRA). The TRA focuses only on technology maturity as opposed to engineering and integration risk. DoDI 5000.02, para 5.d.4 and OSD TRA Guidance provide policy and guidance for TRAs.

- **Perform Prototyping.** Prototyping is an engineering technique employed for several reasons: to reduce risk, inform requirements and encourage competition. For example, the primary objective for competitive prototyping (CP) is acquiring more innovative solutions at better value by ensuring competition. CP are addressed in statute for MDAPs (see P.L. 114-92 (SEC. 822 para (c))). Other prototypes should be considered if they materially reduce engineering and manufacturing development risk at an acceptable cost. At this point in the life cycle, the CP strategy should focus on mitigating key technical risk areas. The program office should have a clear understanding of technical, engineering and integration risks at Milestone A. Current policy does not require full-up system prototypes; therefore, competitive prototyping may include prototyping critical technologies, system elements, integration of system elements or full-up prototypes. Because a primary objective of this type of prototyping is to support a follow-on award choice between developers, contract incentives should be aligned to CP strategy goals. These goals most often emphasize cost, schedule and performance realism and quantification. Contract goals should require the solutions demonstrated during CP be used in the subsequent PDR/CDR designs. The CP strategy should be identified in the SEP and AS, tasks specified in RFPs/Task Orders, technically managed by the program office and included in the TEMP with specific test
objectives. Risk reduction prototypes can be at the system level or can focus on technologies, sub-components or components, and may or may not include objectives associated with competitive contracts. And in nearly all cases, prototypes can be extremely useful in assessing technical performance, supporting trade studies and updating requirements.

- **Perform System Trade Analysis.** The Systems Engineer assesses alternatives with respect to performance, cost, schedule and risk, and makes a recommendation to the PM. The SE assessment should consider the full range of relevant factors, for example, affordability goals and caps, technology maturity, development and deployment constraints, modular open system approaches and user-identified needs and shortfalls. System trades should be used to inform and shape the CDD and cost and schedule objectives to be documented in the Acquisition Program Baseline (APB).

- **Develop System Architecture.** See CH 3–4.2.3, Architecture Design Process for additional information.

- **Develop Functional Baseline.** See CH 3–4.1.6, Configuration Management Process for additional information.

- **Develop Allocated Baseline.** See CH 3–4.1.6, Configuration Management Process for additional information.

- **Develop Preliminary Design(s).** May involve competitive, preliminary design activities up to and including PDRs. See CH 3–3.3.4, Preliminary Design Review for additional information.

- **Develop Allocated Technical Performance Measures (TPMs).** The allocated baseline establishes the first physical representation of the system as system elements with system-level capabilities allocated to system element-level technical performance measures.

- **Support CDD Validation.** The purpose of this support is to inform the MDA and requirements validation authority about the technical feasibility, affordability and testability of the proposed requirements. CDD (or an equivalent requirements document) forms a basis for the set of requirements used for design activities, development and production. Specific SE attention is given to trade-off analysis, showing how cost varies as a function of system requirements (including Key Performance Parameters), major design parameters and schedule. The results should identify major affordability drivers.

- **Support Development RFP Release Decision Point.** The purpose of the MDA-level review is to assess the AS, RFP and key related planning documents and determine whether program plans are affordable and executable and reflect sound business arrangements. Specific SE attention is given to engineering trades and their relationship to program requirements and risk management. Typically, this event occurs after PDR to allow for feedback from the PDR into the technical aspects of the RFP. The Development RFP Release event can come before the PDR if there is confidence the RFP will not need to be substantially changed.

- **Finalize Documents.** The Systems Engineer updates the SEP and PPP and provides inputs for updating the LCSP, TEMP and other program documents.

The Systems Engineer uses technical reviews and audits to assess whether preplanned technical maturity points are reached during the acquisition life cycle as the system and system elements mature. A key method for doing this 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.) Technical reviews typically conducted in the TMR phase are:

- **System Requirements Review (SRR)** (see CH 3–3.3.2, System Requirements Review)
- **System Functional Review (SFR)** (see CH 3–3.3.3, System Functional Review)
- **Software Specification Review (SSR)** for programs with significant software development; a SSR is typically performed before, and in support of, a PDR. The SSR technical assessment establishes the software requirements baseline for the system elements under review (e.g., computer software configuration items (CSCI)) to ensure their preliminary design and, ultimately, the software solution has a reasonable expectation of being operationally effective and suitable.
- **Preliminary Design Review (PDR)** mandated (unless formally waived) to confirm the development of the allocated baseline (see CH 3–3.3.4, Preliminary Design Review)
Test activities during the TMRR phase that depend on SE support and involvement include developmental test and evaluation of system and/or system element prototypes and Early Operational Assessments (EOAs). Developmental Test and Evaluation (DT&E) activities, for example, should be closely coordinated between the engineering and test communities, since DT&E activities support:

- Technical risk identification, risk assessment and risk mitigation
- Providing empirical data to validate models and simulations and
- Assessing technical performance and system maturity (see CH 8–4.2.)

**Outputs and Products**

The technical outputs identified in Table 21 are some of the inputs necessary to support SE activities in the EMD phase. The outputs should support the technical recommendation at Milestone B that an affordable solution has been found for the identified need with acceptable risk, scope and complexity.

Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

<table>
<thead>
<tr>
<th>Technical Outputs from TMRR Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to Acquisition Decision Memorandum (ADM) and, when applicable, 10 USC 2366b certification</td>
</tr>
<tr>
<td>Preliminary system design</td>
</tr>
<tr>
<td>- Updated functional and allocated baselines</td>
</tr>
<tr>
<td>- Associated technical products including associated design and management decisions</td>
</tr>
<tr>
<td>SEP (updated) (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2, Systems Engineering Plan)</td>
</tr>
<tr>
<td>- If programs enter the acquisition life cycle at Milestone B, this is their initial SEP</td>
</tr>
<tr>
<td>Updated Integrated Master Plan (IMP), Integrated Master Schedule (IMS) and memoranda of agreement (MOAs)/memoranda of understanding (MOUs)</td>
</tr>
<tr>
<td>RAM-C Report (updated) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>- Attachment to SEP</td>
</tr>
<tr>
<td>- If programs enter the acquisition life cycle at Milestone B, this is their initial RAM-C Report</td>
</tr>
<tr>
<td>RGC (updated) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>- Included in SEP and TEMP</td>
</tr>
<tr>
<td>PPP (updated) (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–4.3.2.3.)</td>
</tr>
<tr>
<td>- If programs enter the acquisition life cycle at Milestone B, this is their initial PPP</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>- Updated results could include knees-in-the-curves sensitivity analyses, product selections, etc.</td>
</tr>
<tr>
<td>- Updated results of automation trades: Informed advice for automation levels as related to system architecture or software and personnel cost trades</td>
</tr>
<tr>
<td>- Informed advice for CDD validation; showing how cost varies as a function of system requirements (including Key Performance Parameters), major design parameters and schedule; identify major affordability drivers</td>
</tr>
<tr>
<td>Assumptions and constraints</td>
</tr>
<tr>
<td>- Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td>- Interdependencies defined</td>
</tr>
<tr>
<td>Environment, safety and occupational health (ESOH) analyses (See DoDI 5000.02, Enc 3, sec. 16)</td>
</tr>
<tr>
<td>- Programmatic Environment, Safety and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule</td>
</tr>
<tr>
<td>Assessment of technical risk (See CH 3–4.1.5, and the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)</td>
</tr>
</tbody>
</table>
### Technical Outputs from TMRR Phase

- Ensure key risks are adequately mitigated before exiting the TMRR phase
- Include SoS risks associated with governance, interdependencies and complexity

#### Consideration of technology issues

<table>
<thead>
<tr>
<th>Technology Readiness Assessment (TRA) (MDAPs only)</th>
<th>DoDI 5000.02, Enc 1, Table 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRA Plan</td>
<td></td>
</tr>
<tr>
<td>Confirmation at the end of TMRR phase that critical technologies have been demonstrated in a relevant environment</td>
<td></td>
</tr>
<tr>
<td>Preliminary TRA required at Development RFP Release Decision Point</td>
<td></td>
</tr>
<tr>
<td>TRA final report</td>
<td></td>
</tr>
</tbody>
</table>

#### Interdependencies/interfaces/memoranda of agreement (MOAs)

- Understanding of the unique program interdependencies, interfaces and associated MOAs

#### Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (updated)

- See CH 7–4.1.3. and CH 3–4.3.12. Intelligence (Life-Cycle Mission Data Plan)

#### Updated system performance specification

- System preliminary design including functional baseline and allocated baseline

#### Other technical information generated during the TMRR phase

- Architectures, system models and simulations
- Results of Market Research: 1) to identify existing technologies and products; and 2) to understand potential solutions, technologies and sources appropriate for maturing the product in the next phase

#### Prototyping strategy and results of TMRR prototyping activities

- Including identification of key system elements to be prototyped in EMD Phase and documented in the Acquisition Strategy (AS)

#### PDR assessment (See DoDI 5000.02, Enc 3, sec. 7, DoDI 5134.16, and CH 3–3.3.4.)

- For ACAT ID and ACAT IAM programs, DASD(SE) performs the assessment to inform the MDA
- For ACAT IC and ACAT IAC programs, the Component Acquisition Executive conducts the PDR assessment

#### Informed advice to Acquisition Program Baseline (APB)

- APB inputs include the SE affordability assessments, schedule inputs and performance inputs

#### Establishes technical information that is the basis of the cost analysis requirements description (CARD) and manpower documentation (See CH 2–3.5. and CH 5–3.1.)

#### Informed advice to Affordability and Resource Estimates (See CH 3–2.4.4. Value Engineering, CH 3–4.3.2. Affordability – Systems Engineering Trade-Off Analyses, CH 1–4.2.15. and CH 2–2.1.)

- Affordability caps continue to be treated as KPPs at Milestone B; results of engineering trade-off analyses showing how the program established a cost-effective design point for cost/affordability drivers
- Should-cost goals defined at Milestone B to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability
- Value engineering results, as appropriate

#### Informed advice to Acquisition Strategy (AS) (See CH 1–4.1.)

- Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule, and risks

#### Informed advice to LCSP (updated) (See CH 4–3.2.)

- System support and maintenance objectives and requirements established; updated will-cost values and affordability goals and caps as documented in the Life-Cycle Sustainment Plan (LCSP), including Informed advice to manpower documentation

#### Initial Information Support Plan (ISP) (See CH 6–3.8.)
<table>
<thead>
<tr>
<th>Technical Outputs from TMRR Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to Test and Evaluation Master Plan (TEMP) (See CH 8–4.2.)</td>
</tr>
<tr>
<td>Early developmental test and evaluation (DT&amp;E) assessments, including Early Operational Assessments (EOAs) (See CH 8–4.2.)</td>
</tr>
<tr>
<td>Informed advice to draft and final Development Request for Proposal (RFP)</td>
</tr>
<tr>
<td>- Informed advice including system performance specification, SOW, CDRLs and source selection criteria</td>
</tr>
<tr>
<td>- Support preparation for Development RFP Release Decision Point</td>
</tr>
<tr>
<td>Informed advice for the Spectrum Supportability Risk Assessment (See DoDI 4650.01 and CH 3–4.3.20.)</td>
</tr>
<tr>
<td>Informed advice for Waveform Assessment Application (See DoDI 4630.09)</td>
</tr>
</tbody>
</table>
CH 3–3.2.4 Engineering and Manufacturing Development Phase
The primary objective of the Engineering and Manufacturing Development (EMD) phase is to develop the initial product baseline, verify it meets the functional and allocated baselines and transform the preliminary design into a producible design, all within the schedule and cost constraints of the program.

Figure 14: Systems Engineering Activities in the Engineering and Manufacturing Development Phase

Systems engineering (SE) activities support development of the detailed design, verification that requirements are met, reduction in system-level risk and assessment of readiness to begin production and/or deployment (see Figure 14).

Primary SE focus areas in EMD include:

- Completing the detailed build-to design of the system.
- Establishing the initial product baseline.
- Conducting the integration and tests of system elements and the system (where feasible).
- Demonstrating system maturity and readiness to begin production for operational test and/or deployment and sustainment activities.

The EMD phase includes technical assessment and control efforts to effectively manage risks and increase confidence in meeting system performance, schedule and cost goals. SE activities should be integrated with EMD phase-specific test and evaluation, and logistics and sustainment activities identified in CH 8–4.3, and CH 4–3.3, respectively. The planning, scheduling and conduct of event-driven technical reviews (Critical Design Review (CDR), Functional Configuration Audit (FCA), System Verification Review (SVR), and Production Readiness Review (PRR)) are vital to provide key points for assessing system maturity and the effectiveness of risk-reduction strategies.

A well-planned EMD phase Systems Engineering Plan (SEP) builds on the results of previous activities and significantly increases the likelihood of a successful program compliant with the approved Acquisition Program Baseline (APB).

The Limited Deployment Decisions in program Model 3 (see CH 3–3.1.1, Systems Engineering in Defense Acquisition Program Models) are the points at which an increment of capability is reviewed for Limited Deployment. Approval depends in part on specific criteria defined at Milestone B and included in the Milestone B ADM. Implementing the technical planning as defined in the approved SEP guides the execution of the complex and myriad tasks associated with completing the detailed design and integration, and supports developmental test and evaluation activities. The SEP also highlights the linkage between Technical Performance Measures (TPM), risk management and earned-value
management activities to support tracking of cost growth trends. Achieving predefined EMD technical review criteria provides confidence that the system meets stated performance requirements (including interoperability and supportability requirements) and that design and development have matured to support the initiation of the Production and Deployment (P&D) phase.

Roles and Responsibilities

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the Program Manager (PM) focuses on the following EMD activities, which rely on and support SE efforts:

- Conducting activities in support of the EMD contract award.
- Resourcing and conducting event-driven CDR, FCA, SVR and PRR, and assess whether review criteria are met.
- Ensuring the Government preserves the rights they need, consistent with the life-cycle acquisition and support strategy.
- Establishing and manage the initial product baseline established at the CDR.
- Determining path forward on configuration changes to the initial product baseline after CDR, to the extent the competitive environment permits (see CH 3–4.1.6, Configuration Management Process).
- Accepting system deliveries (i.e., DD-250), as appropriate.
- Supporting the Configuration Steering Board in accordance with DoDI 5000.02, para 5.d.5.b.

In addition to the general roles and responsibilities described in CH 3–2.5, Engineering Resources, during this phase it is the Systems Engineer's responsibility for:

- Managing the system design to satisfy the operational requirements, within the constraints of cost and schedule, and to evaluate the system design, identify deficiencies and make recommendations for corrective action.
- Conducting or supporting the technical evaluation in support of source selection for the EMD contract award.
- Maintaining requirements traceability and linkage to the initial product baseline.
- Conducting event-driven technical reviews, advising the PM on review criteria readiness.
- Leading preparation and conduct of technical reviews.
- Tracking and reporting initial product baseline changes after CDR and recommend the path forward in accordance with the Configuration Management (CM) process, to the extent the competitive environment allows (see CH 3–4.1.6, Configuration Management Process).
- Supporting determination of production rates and delivery schedules.
- Supporting test and evaluation activities: identify system evaluation targets driving system development and support operational assessments as documented in the Test and Evaluation Master Plan (TEMP) (see CH 8–4.3).
- Aligning the SEP with the TEMP on SE processes, methods and tools identified for use during test and evaluation.
- Analyzing deficiencies discovered from operational assessments and verification methods (developmental test and evaluation); develop and implement solutions to include, but not limited to, rebalancing of system requirements.
- Supporting logistics and sustainment activities as documented in the Life-Cycle Sustainment Plan (LCSP) (see CH 4–3.3).
- Maintaining the SEP, including generating the update in support of Milestone C.
- Ensure manufacturing process development and maturation efforts.
- Developing approaches and plans to verify mature fabrication and manufacturing processes and determine manufacturing readiness (see the Manufacturing Readiness Level (MRL) Deskbook as one source for assessing manufacturing readiness).
- Conducting a rigorous production risk assessment and determine risk mitigation plans.
• Identifying system design features that enhance producibility (efforts usually focus on design simplification, fabrication tolerances and avoidance of hazardous materials).
• Applying value engineering techniques to system design features to ensure they achieve their essential functions at the lowest life-cycle cost consistent with required performance, reliability, quality and safety.
• Conducting producibility trade studies to determine the most cost-effective fabrication and manufacturing process.
• Assessing Low-Rate Initial Production (LRIP) feasibility within program constraints (may include assessing contractor and principal subcontractor production experience and capability, new fabrication technology, special tooling and production personnel training requirements).
• Identifying long-lead items and critical materials.
• Supporting update to production costs as a part of life-cycle cost management.
• Continuing to support the configuration management process to control changes to the product baseline during test and deployment.
• Maintaining oversight of the system (software and hardware) development processes, system testing, documentation updates and tracking of the system development efforts.
• Supporting the PM in his or her interactions with the Configuration Steering Board.

Inputs

Table 22 summarizes the primary inputs associated with this part of the life cycle.

<table>
<thead>
<tr>
<th>Inputs for EMD Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Development Document (CDD) and Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP)</td>
</tr>
<tr>
<td>Acquisition Decision Memorandum (ADM) (may contain additional direction)</td>
</tr>
<tr>
<td>Preliminary system design including functional and allocated baselines (see CH 3–4.1.6. Configuration Management Process)</td>
</tr>
<tr>
<td>SEP (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2. Systems Engineering Plan)</td>
</tr>
<tr>
<td>• If programs enter the acquisition life cycle at Milestone B, this is their initial SEP</td>
</tr>
<tr>
<td>Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19)</td>
</tr>
<tr>
<td>• Attachment to SEP</td>
</tr>
<tr>
<td>• If programs enter the acquisition life cycle at Milestone B, this is their initial RAM-C Report</td>
</tr>
<tr>
<td>Reliability Growth Curves (RGCs) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>• Included in SEP and TEMP</td>
</tr>
<tr>
<td>Program Protection Plan (PPP) (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.3.)</td>
</tr>
<tr>
<td>• If programs enter the acquisition life cycle at Milestone B, this is the initial PPP</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>• Results could include knees-in-the-curves sensitivity analyses, product selections, etc.</td>
</tr>
<tr>
<td>Assumptions and constraints</td>
</tr>
<tr>
<td>• Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td>• Interdependencies defined</td>
</tr>
<tr>
<td>Environment, safety and occupational health (ESOH) analyses (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)</td>
</tr>
<tr>
<td>• Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule</td>
</tr>
<tr>
<td>Assessment of technical risk (See CH 3–4.1.5.)</td>
</tr>
<tr>
<td>Consideration of technology issues</td>
</tr>
</tbody>
</table>
## Inputs for EMD Phase

<table>
<thead>
<tr>
<th>Technology Readiness Assessment (TRA) (MDAPs only) (See DoDI 5000.02, Enc 1, Table 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Confirmation that critical technologies have been demonstrated in a relevant environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interdependencies/interfaces/memoranda of agreement (MOAs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System performance specification, including verification matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other technical information, such as architectures, system models and simulations generated during the TMRR phase</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prototyping strategy (See DoDI 5000.02, para 5.d.4 and DoDI 5000.02, Enc 1, Table 2, Acquisition Strategy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validated On-Line Life-cycle Threat (VOLT) Report (See DoDI 5000.02 (Enc 1, Table 2) and CH 7-4.1.2.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acquisition Program Baseline (APB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affordability Assessment (See CH 1–4.2.15, and CH 3–4.3.2.)</td>
</tr>
<tr>
<td>- Affordability caps treated as KPPs; results of engineering trade-off analyses show cost/schedule/performance trade space around affordability drivers</td>
</tr>
<tr>
<td>- Should-cost goals designed to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acquisition Strategy (AS) (See CH 1–4.1.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life-Cycle Sustainment Plan (LCSP) (updated) (See CH 4–3.2.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test and Evaluation Master Plan (TEMP) (See CH 8–4.2.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to the developmental test and evaluation (DT&amp;E) planning, including Operational Assessments (OAs) (See CH 8–4.2.)</td>
</tr>
<tr>
<td>- System test objectives</td>
</tr>
</tbody>
</table>

| Draft and final Request for Proposal (RFP) |
| Security Classification Guide (SCG) (updated) |

<table>
<thead>
<tr>
<th>Other analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Other prior analytic, prototyping and/or technology demonstration efforts performed by the S&amp;T community. Technology insertion/transition can occur at any point in the life cycle</td>
</tr>
</tbody>
</table>

| Spectrum Supportability Risk Assessment (See DoDI 4650.01 and CH 3–4.3.20.) |

## Activities

The EMD phase activities begin when a favorable Milestone B decision has been made (see CH 3–3.2.3, Technology Maturation and Risk Reduction Phase) and end with a successful Milestone C decision. Figure 15 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

*Figure 15: Weapon System Development Life Cycle*
SE activities to support the EMD effort include:

- Realization of the system architecture.
- Performance of system element trade-offs.
- Use of prototypes to mature system designs and drawings. If the program strategy includes competitive development, this may include competitive prototyping during the EMD phase.
- Conduct Human Systems Integration analysis such as task and functional analysis, develop mission use and operational use scenarios and establish initial human performance thresholds.
- Development of the initial product baseline and a stable design that conforms to program cost, schedule and performance requirements (see CH 3–4.1.6. Configuration Management Process).
- Support for the establishment of the developmental test and evaluation environment and associated resources (e.g., people, equipment, test cases and test ranges).
- Support of materiel readiness and logistical support efforts.
- Preparation for production by identifying critical manufacturing processes, key product characteristics and any manufacturing risks.
- Build, integrate and test system elements.
- Fabricate and assemble the system elements and system to the initial product baseline.
- Manage changes of software requirements, projected changes to software size and integration of software components.
- Identify the process to proactively manage and mitigate Diminishing Manufacturing Sources and Material Shortages (DMSMS) issues in future life-cycle phases.
- Integrate the system and verify compliance with the functional and allocated baselines through developmental test and evaluation (DT&E) efforts (see CH 8–4.3, for more on DT&E).
- Update risk, issue and opportunity plans. Identify, analyze, mitigate and monitor risks and issues; and identify, analyze, manage and monitor opportunities. (See the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)
- Address problem/failure reports through the use of a comprehensive data-collection approach, such as Failure Reporting, Analysis, and Corrective Action System (FRACAS).
- Refine the initial product baseline and support the development of the Capability Production Document (CPD).
• Complete producibility activities supporting manufacturing readiness or implementation and initial deployment activities for information systems.
• Support initiation of materiel readiness and logistical support activities including deployment options and training development.
• Perform Environment, Safety and Occupational Health (ESOH) risk management analyses and ESOH risk acceptance.
• Produce NEPA/OE 12114 documentation.
• Perform corrosion risk assessment.
• Complete certifications as appropriate (see CH 3–2.6, Certifications).
• Evolve the system architecture to reflect EMD trade-off decisions and incorporate stakeholder feedback.

The Systems Engineer uses technical reviews and audits to assess whether preplanned technical maturity points are reached during the acquisition life cycle as the system and system elements mature. A key method for doing this 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 available on the DASD(SE) web site.) Technical reviews and audits typically conducted in EMD:

• Critical Design Review (CDR) (mandated, establishes initial product baseline, see CH 3–3.3.5, Critical Design Review)
• System Verification Review/Functional Configuration Audit (SVR/FCA) (See CH 3–3.3.6, System Verification Review/Functional Configuration Audit)
• Production Readiness Review (PRR) (CH 3–3.3.7, Production Readiness Review)

Test activities during the EMD phase that depend on SE support and involvement include Test Readiness Reviews (TRRs), Developmental Test and Evaluation (DT&E) and Operational Assessments (OAs). The Systems Engineer, in collaboration with the Chief Developmental Tester, should identify system evaluation targets driving system development and support operational assessments as documented in the Test and Evaluation Master Plan (TEMP). Associated SE activities and plans should be in the SEP (see CH 3–2.2, Systems Engineering Plan, 3.3. Technical Reviews and Audits, and CH 8–3.5).

Outputs and Products

The technical outputs and products identified in Table 23 are some of the inputs necessary to support SE processes in the P&D phase. They should support the technical recommendation at Milestone C that manufacturing processes are mature enough to support Low-Rate Initial Production (LRIP) and generate production-representative articles for operational test and evaluation (OT&E). Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 23: Technical Outputs Associated with EMD Phase

<table>
<thead>
<tr>
<th>Technical Outputs from EMD Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to CPD</td>
</tr>
<tr>
<td>Informed advice to Acquisition Decision Memorandum (ADM) and 10 USC 2366b certification (if Milestone C is program initiation)</td>
</tr>
<tr>
<td>Verified system</td>
</tr>
<tr>
<td>• Updated functional, allocated, and initial product baselines; verified production processes and verification results/decisions</td>
</tr>
<tr>
<td>• Associated technical products including associated design and management decisions</td>
</tr>
<tr>
<td>SEP (updated) (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2, Systems Engineering Plan)</td>
</tr>
<tr>
<td>Updated IMP, IMS, and MOAs/MOUs</td>
</tr>
</tbody>
</table>
## Technical Outputs from EMD Phase

<table>
<thead>
<tr>
<th>RAM-C Report (updated) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Attachment to SEP</td>
</tr>
<tr>
<td>RGC (updated) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.)</td>
</tr>
<tr>
<td>• Included in SEP and TEMP</td>
</tr>
<tr>
<td>PPP (updated) (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.4.)</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>• Results could include knees-in-the-curves sensitivity analyses, product selections, etc.</td>
</tr>
<tr>
<td>Assumptions and constraints</td>
</tr>
<tr>
<td>• Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td>• Interdependencies updated</td>
</tr>
<tr>
<td>ESOH analyses (See DoDI 5000.02, Enc 3, sec. 16)</td>
</tr>
<tr>
<td>• Updated Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/E.O. 12114 Compliance Schedule</td>
</tr>
<tr>
<td>Human Systems Integration Analysis results (See CH 5–3.2.)</td>
</tr>
<tr>
<td>• Mapping of all tasks/functions to human and/or system,</td>
</tr>
<tr>
<td>• Mission and Operational Use scenarios that support downstream testing and</td>
</tr>
<tr>
<td>• Informed advice relative to crew/maintainer skill level and numbers of personnel required to support operations</td>
</tr>
<tr>
<td>Assessment of technical risk (See CH 3–4.1.5. and the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)</td>
</tr>
<tr>
<td>• Risk assessment identifying mitigation plans for acceptable risks to allow the program to initiate production, deployment and operational test and evaluation activities</td>
</tr>
<tr>
<td>• Update system of systems (SoS) risks associated with governance, interdependencies and complexity</td>
</tr>
<tr>
<td>Manufacturing readiness (See DoDI 5000.02, Enc 3, sec. 10 and CH 3–4.3.18.)</td>
</tr>
<tr>
<td>• Assessment of manufacturing readiness supports Milestone C and initiation of production</td>
</tr>
<tr>
<td>• Manufacturing processes have been effectively demonstrated and are under control</td>
</tr>
<tr>
<td>Interdependencies/interfaces/memoranda of agreement (MOAs)</td>
</tr>
<tr>
<td>• Understanding of the unique program interdependencies, interfaces and associated MOAs</td>
</tr>
<tr>
<td>Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (updated) (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)</td>
</tr>
<tr>
<td>System performance specification (updated if necessary), including verification matrix</td>
</tr>
<tr>
<td>• System element specifications, including verification matrix</td>
</tr>
<tr>
<td>Initial product baseline</td>
</tr>
<tr>
<td>Other technical information, such as architectures, system models and simulations generated during the EMD phase</td>
</tr>
<tr>
<td>Results of EMD prototyping activities</td>
</tr>
<tr>
<td>Manufacturing prototyping activities support P&amp;D phase</td>
</tr>
<tr>
<td>Critical Design Review (CDR) Assessment (See DoDI 5000.02, Enc 3, sec. 7, DoDI 5134.16, and CH 3–3.3.5.)</td>
</tr>
<tr>
<td>• For ACAT ID and ACAT IAM programs, DASD(SE) performs the assessment to inform the Milestone Decision Authority (MDA)</td>
</tr>
<tr>
<td>• For ACAT IC and ACAT IAC programs, the Component Acquisition Executive conducts the CDR assessment</td>
</tr>
<tr>
<td>Informed advice to APB</td>
</tr>
<tr>
<td>• Updated will-cost values and affordability caps as documented in the Acquisition Program Baseline and Acquisition Strategy</td>
</tr>
</tbody>
</table>
## Technical Outputs from EMD Phase

<table>
<thead>
<tr>
<th>Establishes technical information that is the basis of the updates to the Cost Analysis Requirements Description (CARD) and manpower documentation (See <a href="#">CH 2–3.5</a> and <a href="#">CH 5–3.1</a>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informed advice to Affordability and Resource Estimates (See <a href="#">CH 3–2.4.4</a>, Value Engineering, <a href="#">CH 3–4.3.2</a>, Affordability – Systems Engineering Trade-Off Analyses, <a href="#">CH 1–4.2.15</a>, and <a href="#">CH 2–2.1</a>).</td>
</tr>
<tr>
<td>• Should-cost goals updated to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability</td>
</tr>
<tr>
<td>• Value engineering results, as appropriate</td>
</tr>
<tr>
<td>Manufacturing, performance and quality metrics critical to program success are identified and tracked</td>
</tr>
<tr>
<td>• Manufacturing drawings are sufficiently complete</td>
</tr>
<tr>
<td>Production budget/cost model validated and resources considered sufficient to support LRIP and FRP</td>
</tr>
<tr>
<td>• Inputs to Milestone C, LRIP, and FRP DR</td>
</tr>
<tr>
<td>Informed advice to Acquisition Strategy (AS) (See <a href="#">CH 1–4.1</a>).</td>
</tr>
<tr>
<td>• Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule and risks</td>
</tr>
<tr>
<td>Informed advice to LCSP (updated) (See <a href="#">CH 4–3.3</a>).</td>
</tr>
<tr>
<td>• System Support and Maintenance Objectives and Requirements established</td>
</tr>
<tr>
<td>• Updated will-cost values and affordability caps as documented in the LCSP, including Informed advice to manpower documentation</td>
</tr>
<tr>
<td>• Confirmation of logistics and sustainment needs (i.e., facilities, training, support equipment) and implementation supporting initial deployment efforts</td>
</tr>
<tr>
<td>ISP of Record (See <a href="#">CH 6–3.8</a>).</td>
</tr>
<tr>
<td>Informed advice to TEMP (updated) (See <a href="#">CH 8–4.3</a>).</td>
</tr>
<tr>
<td>• System test objectives</td>
</tr>
<tr>
<td>Informed advice to the DT&amp;E assessments (See <a href="#">CH 8–4.3</a>).</td>
</tr>
<tr>
<td>• System test objectives</td>
</tr>
<tr>
<td>Informed advice to draft &amp; final RFP for LRIP</td>
</tr>
<tr>
<td>• Informed advice, including system performance specification, Statement of Work (SOW), Contract Data Requirements List (CDRLs), and source selection criteria</td>
</tr>
<tr>
<td>Informed advice for the Spectrum Supportability Risk Assessment (See <a href="#">DoDI 4650.01</a> and <a href="#">CH 3–4.3.20</a>).</td>
</tr>
<tr>
<td>Informed advice for Waveform Assessment Application (See <a href="#">DoDI 4630.09</a>).</td>
</tr>
</tbody>
</table>

### CH 3–3.2.5 Production and Deployment Phase

The objective of the Production and Deployment (P&D) phase is to validate the product design and to deliver the quantity of systems required for full operating capability, including all enabling system elements and supporting material and services. Systems engineering (SE) in P&D delivers the product baseline as validated during operational testing, and supports deployment and transition of capability to all end users, the warfighters and supporting organizations. SE activities, for example, maintenance approach, training and technical manuals, should be integrated with P&D phase-specific test and evaluation and logistics and sustainment activities identified in [CH 8–4.4](#) and [CH 4–3.4](#), respectively. This phase typically has several major efforts as shown in Figure 16: Low-Rate Initial Production (LRIP), Operational Test and Evaluation (OT&E), Full-Rate Production (FRP) and Full Deployment (FD), and deployment of capability in support of the Initial and Full Operational Capabilities. The Full-Rate Production Decision Review (FRP DR) and/or Full Deployment Decision Review (FD DR) serves as a key decision point between LRIP (and OT&E) and FRP/FD.

**Figure 16: Systems Engineering Activities in the Production and Deployment Phase**
Manufacturing development should be complete at Milestone C, but improvements or redesigns may require unanticipated, additional manufacturing process development and additional testing (e.g., delta qualification or delta first article test). For example, it may be discovered that changing the product design may provide enhancements in manufacturing or other supporting processes. At the conclusion of LRIP, all manufacturing development should be completed, with no significant manufacturing risks carried into FRP. The dynamic nature of the varied production elements requires a proactive approach to mitigate emerging risks.

Readiness for OT&E is a significant assessment of a system’s maturity (see CH 8–3.9.2). The Systems Engineer plays a key role in ensuring systems are ready to enter OT&E. Scarce resources are wasted when an operational test is halted or terminated early because of technical problems, which should have been resolved before the start of OT&E.

During deployment, units attain Initial Operational Capability (IOC), then Full Operational Capability (FOC).

Besides ensuring a successful FOC, SE activities include:

- Maturing manufacturing, production and deployment procedures.
- Responding to deficiencies and develop corrective actions.
- Supporting validation of system performance associated with OT&E.
- Validating the production configuration prior to FRP / FD.

**Roles and Responsibilities**

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the Program Manager (PM) focuses on the following P&D activities, which rely on and support SE efforts:

- Conducting activities in support of the production contract award(s).
- Ensuring Government intellectual property and data rights information are captured in the technical baseline.
- Resourcing and conducting event-driven technical reviews (including the Physical Configuration Audit (PCA), Post Implementation Review (PIR), and FRP and/or FD DR) and ensure that criteria are met.
- Managing and controlling the product baseline.
- Managing risks, in particular the manufacturing, production and deployment risks.
- Accepting system deliveries (i.e., DD-250).
• Supporting the Configuration Steering Board in accordance with DoDI 5000.02, para 5.d.5.b.

In addition to the general responsibilities identified in CH 3–2.5. Engineering Resources, the Systems Engineer is responsible for:

• Analyzing deficiencies discovered from OT&E, acceptance tests, production reports and maintenance reports and provide correction actions.
• Conducting rigorous production risk assessments; plan and resource effective risk mitigation actions.
• Continuing conducting producibility trade studies to determine the most cost-effective fabrication/manufacturing process.
• Developing approaches and plans to validate fabrication/manufacturing processes.
• Assessing full-rate production feasibility within program constraints. This may include assessing contractor and principal subcontractor production experience and capability, new fabrication technology, special tooling and production personnel training requirements.
• Identifying long-lead items and critical materials; plan for obsolescence and implement DMSMS measures to mitigate impacts to production and sustainment.
• Updating production costs as a part of life-cycle cost management.
• Supporting updates to the production schedules.
• Supporting technical reviews and production decisions.
• Supporting materiel readiness and logistical activities, including deployment and training.
• Continuing to support the configuration management process to control changes to the product baseline during test and deployment.
• Updating and maintain system certifications and interfaces with external systems, as necessary.
• Maintaining oversight of the system (software and hardware) development processes, system testing, documentation updates and tracking of the system development efforts.
• Supporting the PM in his or her interactions with the Configuration Steering Board.

Inputs

Table 24 summarizes the primary inputs associated with this part of the life cycle.

Table 24: Inputs Associated with P&D Phase

<table>
<thead>
<tr>
<th>Inputs for P&amp;D Phase</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Production Document (CPD) and Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP)</td>
<td></td>
</tr>
</tbody>
</table>
| Acquisition Decision Memorandums (ADM) associated with Milestone C, LRIP and FRP DR and FD DR | • ADMs may contain additional direction  
• Milestone C may not coincide with LRIP  
• FRP DR and FD DR ADMs are issued during P&D phase |
| SEP (See DoDI 5000.02, Enc 3, sec. 2 and CH 3–2.2, Systems Engineering Plan) | • Updated functional, allocated and product baselines; verified and validated production processes and validation results/decisions  
• Updated technical products including associated design and management decisions |
| Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.) | • Attachment to SEP |
| Reliability growth curves (RGCs) (See DoDI 5000.02, Enc 3, sec. 12 and CH 3–4.3.19.) | • Included in SEP and TEMP |
| PPP (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.4.) | |
## Inputs for P&D Phase

- Updated at FRP DR and/or FD DR

### Trade-off analysis results (see DoDI 5000.02, Enc 3, sec. 4)
- Results could include knees-in-the-curves sensitivity analyses, product selections, etc.
- P&D phase trade studies may support manufacturing or other system mods (technology insertion, technology refresh, etc.)

### Assumptions and constraints
- Rationale for all assumptions, constraints, and basis for trades

### Environment, Safety and Occupational Health (ESOH) analyses (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)
- Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule

### Risk assessment (See CH 3–4.1.5.)
- Risk mitigation plans
- Acceptable risks for achieving Initial Operational Capability (IOC) and Full Operational Capability (FOC)

### Manufacturing readiness (See DoDI 5000.02, Enc 3, sec. 10 and CH 3–4.3.18.)
- Assessment of manufacturing readiness supports Milestone C and initiation of production

### Interdependencies/interfaces/memoranda of agreement (MOAs)
- Understanding of the unique program interdependencies, interfaces and associated MOA

### Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)

### System performance specification (updated if necessary) including verification matrix
- System element specifications (updated if necessary) including verification matrix

### Manufacturing, performance and quality metrics critical to program success are identified and tracked
- Manufacturing drawings are sufficiently complete

### Product baseline

### Product acceptance test

### Other technical information such as architectures, system models and simulations generated during the EMD phase

### Results of EMD prototyping activities

### Manufacturing prototyping activities supporting P&D phase

### Validated On-Line Life-cycle Threat (VOLT) Report (See DoDI 5000.02 (Enc 1, Table 2) and CH 7-4.1.2.)

### Acquisition Program Baseline (APB)

### Affordability and Resource Estimates (See CH 3–2.4.4, Value Engineering, CH 3–4.3.2, Affordability – Systems Engineering Trade-Off Analyses, CH 1–4.2.15, and CH 2–2.1.)
- Affordability goals treated as KPPs
- Should-cost goals to achieve efficiencies and control unproductive expenses
- Updated will-cost values and affordability caps as documented in the Life-Cycle Sustainment Plan (LCSP), including informed advice to manpower documentation
- Value engineering results, as appropriate

### Supply chain sources

### Updated Manufacturing processes

### Production budget/cost model validated and resources considered sufficient to support LRIP and FRP
Inputs for P&D Phase

<table>
<thead>
<tr>
<th>Acquisition Strategy (AS) (See CH 1–4.1.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCSP (See CH 4–3.3.)</td>
</tr>
<tr>
<td>Human Systems Integration (HSI) analyses (See CH 5–3.2.)</td>
</tr>
<tr>
<td>• Manpower, personnel and training (MPT) requirement updates</td>
</tr>
<tr>
<td>• Refinement of HSI inputs to specifications, human system interfaces design, multi-domain verification, testing and usability evaluations</td>
</tr>
<tr>
<td>TEMP (See CH 8–4.3.)</td>
</tr>
<tr>
<td>• System test objectives</td>
</tr>
<tr>
<td>Developmental test and evaluation (DT&amp;E) assessments (See CH 8–4.3.)</td>
</tr>
<tr>
<td>• System test objectives</td>
</tr>
<tr>
<td>Draft and final RFP</td>
</tr>
<tr>
<td>Security Classification Guide (SCG)</td>
</tr>
<tr>
<td>Information Support Plan (ISP) of Record (See CH 6–3.8.)</td>
</tr>
<tr>
<td>Other analyses</td>
</tr>
<tr>
<td>• Other prior analytic, prototyping and/or technology demonstration efforts completed by the science and technology (S&amp;T) community; technology insertion/transition can occur at any point in the life cycle</td>
</tr>
</tbody>
</table>

Spectrum Supportability Risk Assessment (See DoDI 4650.01 and CH 3–4.3.20.)

Activities

The P&D phase SE activities begin when a favorable Milestone C decision has been made (see CH 3–3.2.4. Engineering and Manufacturing Development Phase) and end when FOC is achieved. Figure 17 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 17: Weapon System Development Life Cycle

Notes:
- Derived from DoD 5000.02, Model 5: Hybrid Program A (Hardware Dominant)
- The actual number and type of builds during the program will depend on system type and program strategy.
SE activities that occur throughout the P&D phase include:

- Providing technical support to prepare for the Operations and Support (O&S) phase, reviewing and providing inputs on the maintenance approach, acquisition strategy, training and technical manuals.
- Updating risk, issue and opportunity 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.)
- Assessing the impact of system requirements changes resulting from evolving threats, changes to operational environment or in response to changes within the SoS or interfacing systems.
- Analyzing system deficiencies generated during OT&E, acceptance testing, production and deployment.
- Addressing problem/failure reports through the use of a comprehensive data collection approach like a Failure Reporting, Analysis and Corrective Action System (FRACAS).
- Managing and controlling configuration updates (hardware, software and specifications) to the product baseline.
- Re-verifying and validating production configuration.

SE provides inputs to OT&E readiness assessments including:

- Assessment of DT&E, coordinated with the Chief Developmental Tester, to support approval to enter OT&E.
- Analysis of the system’s progress in achieving performance metrics (see CH 3–4.1.3, Technical Assessment Process).
- Assessment of technical risk.
- Assessment of software maturity and status of software trouble reports.
- Identification of any potential design constraints affecting the system’s expected performance during OT&E.

In both the P&D and O&S phases the Systems Engineer should identify and plan for potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS)).

DMSMS problems are an increasing concern as the service lives of DoD weapon systems are extended and the product life cycle for high-technology system elements decreases.

The PCA is a SE audit typically conducted in the P&D phase (see CH 3–3.3.8, Physical Configuration Audit for additional information regarding the PCA). The Systems Engineer should identify technical risks associated with achieving entrance criteria for this audit (see the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)

Test activities during the P&D phase that depend on SE support and involvement include the DT&E Assessment, Operational Test Readiness Reviews (OTRRs), initial and follow-on OT&E (IOT&E and FOT&E) and live-fire test and evaluations (LFT&E), as appropriate (see CH 8–4.4.). In addition, any corrective actions or design changes implemented in response to test identified deficiencies require additional regression testing.

The Systems Engineer, in collaboration with the Chief Developmental Tester, should identify the technical support needed for operational assessments and document in the Test and Evaluation Master Plan (TEMP). Associated SE activities and plans should be in the SEP (see CH 3–2.2, Systems Engineering Plan, CH 3–3.3, Technical Reviews and Audits Overview, and CH 8–3.5).

Outputs and Products

The technical outputs and products from the P&D phase identified in Table 25 are some of the inputs necessary to support SE processes in the O&S phase. They should support the program’s transition into full operations and sustainment. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.
<table>
<thead>
<tr>
<th>Technical Outputs from P&amp;D Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Informed advice to CPD Update</strong></td>
</tr>
<tr>
<td>- CPD may be updated to justify system enhancements and modifications from the P&amp;D phase</td>
</tr>
<tr>
<td><strong>Informed advice to ADM</strong></td>
</tr>
<tr>
<td><strong>Updated IMP, IMS, and MOAs/MOUs</strong></td>
</tr>
<tr>
<td><strong>Validated system</strong></td>
</tr>
<tr>
<td>- Updated functional, allocated and product baselines; verified and validated production processes and validation results/decisions</td>
</tr>
<tr>
<td>- Associated technical products including associated design and management decisions</td>
</tr>
<tr>
<td><strong>PPP (updated)</strong> (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.5.)</td>
</tr>
<tr>
<td>- Updated at FRP DR and/or FD DR</td>
</tr>
<tr>
<td><strong>Trade-off analysis results</strong> (See DoD 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>- P&amp;D Phase trade studies may support manufacturing or other system mods (technology insertion, technology refresh, etc.)</td>
</tr>
<tr>
<td><strong>Assumptions and constraints</strong></td>
</tr>
<tr>
<td>- Rationale for all assumptions, constraints and basis for trades</td>
</tr>
<tr>
<td><strong>ESOH analyses</strong> (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)</td>
</tr>
<tr>
<td>- Updated Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule</td>
</tr>
<tr>
<td><strong>Assessment of technical risk</strong> (updated) (See CH 3–4.4.1.5. and DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)</td>
</tr>
<tr>
<td>- Risk assessment identifying mitigation plans, acceptable risks for achieving FOC</td>
</tr>
<tr>
<td><strong>Interdependencies/interfaces/memoranda of agreement (MOAs)</strong></td>
</tr>
<tr>
<td>- Understanding of the unique program interdependencies, interfaces and associated MOA</td>
</tr>
<tr>
<td><strong>Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs</strong> (updated) (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)</td>
</tr>
<tr>
<td><strong>System performance specification</strong> (updated if necessary) including verification matrix; system element specifications (updated if necessary) including verification matrix</td>
</tr>
<tr>
<td><strong>Manufacturing and production metrics</strong></td>
</tr>
<tr>
<td><strong>PCA results and an updated product baseline</strong> (See CH 3–3.3.8.)</td>
</tr>
<tr>
<td><strong>Acceptance test data to assess product conformance and to support DD250 of end items</strong></td>
</tr>
<tr>
<td><strong>Other technical information such as architectures, system models and simulations generated during the P&amp;D phase</strong></td>
</tr>
<tr>
<td><strong>Technical information that is the basis of the updates to the Cost Analysis Requirements Description (CARD) and manpower documentation</strong> (See CH 2–3.5. and CH 5–3.1.)</td>
</tr>
<tr>
<td><strong>Industrial base capabilities; updated manufacturing processes and supply chain sources</strong></td>
</tr>
<tr>
<td><strong>Informed advice to Life-Cycle Sustainment Plan (LCSP)</strong> (See CH 4–3.4.)</td>
</tr>
<tr>
<td>- Updated at FRP DR and/or FDDR</td>
</tr>
<tr>
<td>- Updated will-cost values and affordability caps as documented in the LCSP, including informed advice to manpower documentation</td>
</tr>
<tr>
<td>- Value engineering results, as appropriate (see CH 3–2.4.4.)</td>
</tr>
<tr>
<td>- Updated list of production tooling and facilities that need to be retained post-production to support continued operational and maintenance of the system.</td>
</tr>
<tr>
<td><strong>Human Systems Integration (HSI) analyses</strong> (See CH 5–3.2.)</td>
</tr>
<tr>
<td>- Final manpower and personnel requirements</td>
</tr>
<tr>
<td>- Training program implementation</td>
</tr>
<tr>
<td>- HSI participation in Engineering Change Proposal (ECP) process</td>
</tr>
</tbody>
</table>
### Technical Outputs from P&D Phase

<table>
<thead>
<tr>
<th>Outputs</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human performance results (includes workload, situation awareness,</td>
<td>includes task, errors)</td>
</tr>
<tr>
<td>time to perform tasks, errors)</td>
<td></td>
</tr>
<tr>
<td>Informed advice to TEMP (updated) (See CH 8–4.4.)</td>
<td></td>
</tr>
<tr>
<td>System Test Objectives</td>
<td></td>
</tr>
<tr>
<td>Operational Test and Evaluation (OT&amp;E) Assessments/Reports (See CH</td>
<td></td>
</tr>
<tr>
<td>8–4.4.)</td>
<td></td>
</tr>
<tr>
<td>System Test Objectives</td>
<td></td>
</tr>
<tr>
<td>Draft and final RFP(s) for production and SE support to O&amp;S activities</td>
<td></td>
</tr>
<tr>
<td>Informed advice for the Spectrum Supportability Risk Assessment (See</td>
<td>DoDI 4650.01 and CH 3–4.3.20.)</td>
</tr>
</tbody>
</table>

### CH 3–3.2.6 Operations and Support Phase

The objective of the Operations and Support (O&S) phase is to execute a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. Planning for this phase begins in the Materiel Solution Analysis (MSA) phase, matures through the Technology Maturation and Risk Reduction (TMRR) and Engineering and Manufacturing Development (EMD) phases, and is documented in the Life-Cycle Sustainment Plan (LCSP). Systems engineering (SE) in the O&S phase assesses whether the deployed system and enabling system elements continue to provide the needed capability in a safe, sustainable and cost-effective manner. SE efforts consist of data collection, assessment and corrective action cycles to maintain a system’s operational suitability and operational effectiveness.

Sustainment activities supporting system operations begin in this phase and should address two major efforts: life-cycle sustainment and disposal. SE efforts during life-cycle sustainment include Environment, Safety and Occupational Health (ESOH) assessments, technology refresh, functionality modification and life-extension modifications. (See CH 3–4.3, Design Considerations for other technical factors needing continued attention during this phase.)

When the system no longer provides an effective or efficient capability to the warfighter, the Department should make an informed decision to either modify or dispose of it. However, a related proactive aspect in the Production and Deployment and O&S phases is engineering analysis to identify potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS)). DMSMS problems are an increasing concern as the service lives of DoD weapon systems are extended and the product life cycle for high-technology system elements decreases (see CH 3–4.3.8, Diminishing Manufacturing Sources and Material Shortages).

### Roles and Responsibilities

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the Program Manager (PM) focuses on the following O&S activities, which rely on and support SE efforts include:

- Working with the user to document performance and sustainment requirements in performance agreements, specifying objective outcomes, measures, resource commitments and stakeholder responsibilities.
- Employing effective Performance-Based Life-Cycle Product Support implementation and management.
- Maintaining operational readiness.
- Following acquisition program practices for major modifications or Service Life Extension Program (SLEP).
- Supporting the Configuration Steering Board in accordance with DoDI 5000.02, para 5.6.5.b.

In addition to the general responsibilities identified in CH 3–2.5, Engineering Resources, the Systems Engineer is responsible for the following tasks:
• Refining the maintenance program to minimize total life-cycle cost while achieving readiness and sustainability objectives.
• Assessing end-user feedback and conducting engineering investigations as required.
• Leading teams to translate end-user feedback into corrective action plans and recommending technical changes.
• Developing and implementing approved system proposed changes to ensure end-user needs continue to be met.
• Conducting ESOH risk assessments and maintaining oversight of critical safety item supply chain management.
• Conducting analysis to identify and mitigate potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS)).
• Supporting implementation of follow-on development efforts in response to formal decisions to extend the weapon system’s service life (e.g., through a Service Life Extension Program (SLEP)) or to initiate a major modification (may be treated as a stand-alone acquisition program).
• Updating and maintaining system certifications and external SoS interfaces.
• Supporting the PM in his interactions with the Configuration Steering Board.

Inputs

Table 26 summarizes the primary inputs associated with this part of the life cycle.

<table>
<thead>
<tr>
<th>Inputs for O&amp;S Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition Decision Memoranda (ADMs) associated with Milestone C and Full Deployment (FD) decision review (DR)</td>
</tr>
<tr>
<td>- ADMs may contain additional direction</td>
</tr>
<tr>
<td>- O&amp;S may start as early as Milestone C (e.g., software) and overlap P&amp;D phase</td>
</tr>
<tr>
<td>- FD DR would involve O&amp;S</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>- P&amp;D phase trade studies may support manufacturing or other system modifications (technology insertion, technology refresh, etc.)</td>
</tr>
<tr>
<td>ESOH analyses (updated) (See DoDI 5000.02, Enc 3, sec. 16 and CH 3–4.3.9.)</td>
</tr>
<tr>
<td>- ESOH analyses continue during O&amp;S to include hazard analysis and supporting NEPA/EO 12114 compliance for modifications and disposal</td>
</tr>
<tr>
<td>Risk assessment (See CH 3–4.1.5.)</td>
</tr>
<tr>
<td>Interdependencies/interfaces/memoranda of agreement (MOAs)</td>
</tr>
<tr>
<td>System performance specification</td>
</tr>
<tr>
<td>Field failures</td>
</tr>
<tr>
<td>Other technical information, such as architectures, system models and simulations generated during the P&amp;D phase</td>
</tr>
<tr>
<td>LCSP (See CH 4–3.4.)</td>
</tr>
<tr>
<td>Information Support Plan (ISP) of Record (See CH 6–3.8.)</td>
</tr>
<tr>
<td>Test and Evaluation Master Plan (TEMP) (See CH 8–4.4.)</td>
</tr>
<tr>
<td>Request for Proposal (RFP) for SE support to O&amp;S activities</td>
</tr>
<tr>
<td>Program Protection Plan (PPP) (See DoDI 5000.02, Enc 3, sec. 13 and CH 9–3.4.2.5.)</td>
</tr>
<tr>
<td>Other analyses</td>
</tr>
<tr>
<td>- End-user feedback and trouble reports</td>
</tr>
<tr>
<td>- Other prior analytic, prototyping, and/or technology demonstration efforts conducted by the science and technology (S&amp;T) community</td>
</tr>
</tbody>
</table>
**Inputs for O&S Phase**

- Technology insertion/transition studies can occur at any point in the life cycle

Spectrum Supportability Risk Assessment (See DoDI 4650.01 and CH 3–4.3.20.)
Life-Cycle Mission Data Plan for Intelligence Mission Data (IMD)-dependent programs (See CH 3–4.3.12, Intelligence (Life-Cycle Mission Data Plan) and CH 7–4.1.3.)

**Activities**

The O&S phase overlaps with the Production and Deployment (P&D) phase, since O&S activities begin when the first system is deployed. O&S ends when a system is demilitarized and disposed of. Figure 18 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 18: Weapon System Development Life Cycle**

SE activities should be integrated with O&S phase-specific test and evaluation and logistics and sustainment activities identified in CH 8–4.5, and CH 4–3.5, respectively. The O&S activities in which the Systems Engineer should participate include:

- Updating risk, issue and opportunity 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).
- Addressing problem/failure reports through the use of a comprehensive data collection approach such as a Failure Reporting, Analysis and Corrective Action System (FRACAS).
- Processing and analyzing mission data.
- Managing preplanned product improvements (P3I) and assessing the impact of system requirements changes resulting from evolving threats, changes to operational environment or in response to changes within the SoS or interfacing systems.
• Making changes to the system technical baseline to maintain it as the authoritative source; changes may be due to PCAs, ECPs or changes to interfaces to external systems.
• Developing and implementing technology refresh schedules.
• Conducting technology insertion efforts as needed to maintain or improve system performance.
• Updating system safety assessments.
• Performing engineering analysis to investigate the impact of DMSMS issues.
• Working with vendors and the general technical community to determine opportunities for technology insertion to improve reliability and affordability.

The disposal activities in which the Systems Engineer should participate include:

• Supporting demilitarizing and disposing of the system; in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security and the environment.
• Documenting lessons learned.
• Archiving data.

Outputs and Products

The technical outputs and products identified in Table 27 are necessary to support SE processes to sustain the system, including modifications.

Table 27: Technical Outputs Associated with O&S Phase

<table>
<thead>
<tr>
<th>Technical Outputs from O&amp;S Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe, sustainable and reliable system that meets operational needs</td>
</tr>
<tr>
<td>Trade-off analysis results (See DoDI 5000.02, Enc 3, sec. 4)</td>
</tr>
<tr>
<td>• O&amp;S phase trade studies support system modifications and/or disposal efforts</td>
</tr>
<tr>
<td>Assessment of technical risk (See CH 3–4.1.5, and the DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs.)</td>
</tr>
<tr>
<td>Interdependencies/interfaces/memoranda of agreement (MOAs)</td>
</tr>
<tr>
<td>Information Support Plan (ISP) of Record (See CH 6–3.8.)</td>
</tr>
<tr>
<td>In-service performance and failure data</td>
</tr>
<tr>
<td>Value engineering results, as appropriate (See CH 3–2.4.4, Value Engineering)</td>
</tr>
<tr>
<td>Engineering Change Proposal (ECP) packages</td>
</tr>
</tbody>
</table>

CH 3–3.3 Technical Reviews and Audits

For DoD weapon systems development, a properly tailored series of technical reviews and audits provide key points throughout the life cycle to evaluate significant achievements and assess technical maturity and risk. DoDI 5000.02, Enc 1 presents the statutory, regulatory and milestone requirements for acquisition programs. The Program Manager (PM) and Systems Engineer work to properly align the 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 and Systems 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 (see Technical Maturity Point table in CH 3–3.1, Life Cycle Expectations).

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. A key 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). Systems
engineering (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 Integrated Master Schedule 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 19 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle. Any program that is not initiated at Milestone C is required by DoDI 5000.02, Enc 3, sec. 7 to include a PDR and CDR.

**Figure 19: Weapon System Development 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 Joint Capabilities Integration and Development System (JCID) and Planning, Programming, Budgeting and Execution (PPBE) processes
- Providing a technical assessment and assurance that the end product fulfills the design and process requirements

Successful development of a complex weapon 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 Government Accountability Office’s (GAO) study on Assessments of Selected Weapons Programs (GAO-12-400SP) provides quantitative evidence to affirm this best practice.

Figure 19 illustrates the notional sequence of technical reviews and audits. It also provides typical timing associated with the acquisition phases. 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 acquisition phase in the outline for the Systems Engineering Plan (SEP). These policy and guidance documents provide a starting point for the PM and Systems Engineer to develop the program's unique set of technical reviews and audits. Tailoring is expected to best suit the program objectives (see CH 3–2. Background). 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 important issues and assumptions. They define options necessary to balance risk in support of continued development.

The technical baseline (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 Acquisition Program Baseline (APB).
- Program technical plans and schedules, which also inform the APB.
- Contracting activity.
- Test and Evaluation 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 Request for Proposal (RFP) and requiring the contractor deliver a SE Management Plan (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.

While the Test Readiness Reviews (TRR) is a technical review, it is addressed in CH 8–3.9. The TRR is used to assess a contractor’s readiness for testing configuration items, including hardware and software. They typically involve a review of earlier or lower-level test products and test results from completed tests and a look forward to verify the test resources, test cases, test scenarios, test scripts, environment and test data have been prepared for the next test activity. TRRs typically occur in the EMD and P&D phase of a program.

To design for security, the program protection planning and execution activities should be integrated into the systems engineering technical reviews and audits. See CH 9–3.4.3, for system security engineering (SSE) criteria for each systems engineering 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 that actions 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 and Systems Engineer should be considered in the absence of specific Service or lower level (e.g., System Command or Program Executive Officer (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 5000.02, Enc 1.
- 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 19 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 for each event, informed by the knowledge point objectives in Table 12: Technical Maturity Points
- Identifying the resources required to support the plan; ensuring the activities leading up to the official review and audit are integrated. See Figure 20.
- Ensuring technical reviews and audits are incorporated into the IMP and IMS
- Coordinating with Chief Development Tester to provide at each technical review: 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., Statement of Work (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 recommend to the chairperson and PM when a system technical review should be considered complete, see Figure 20

Figure 20: Technical Review Process
The PM and Systems Engineer should identify key stakeholders who have an interest or role in the review, which may include:

- Technical review chairperson
- Program Executive Office
- Contracting Officer
- Defense Contract Management Agency (DCMA) and Defense Contract Audit Agency (DCAA)
- Product Support Manager
- Product Improvement Manager/Requirements Officer
- End-user Community
- Chief Developmental Tester
- Interdependent Acquisition Programs
- Business Financial Manager
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))
- Service Technical Leadership such as chief engineers
- Subject Matter Experts

**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 DASD(SE) website. If a Program Management Office (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 is focused 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 CH 8–3.9.1.
- 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.

**CH 3–3.3.1 Alternative Systems Review**
The Alternative Systems Review (ASR) is held to support a dialogue between the end user and acquisition community and leads to a draft performance specification for the preferred materiel solution. The ASR typically occurs during the Materiel Solution Analysis (MSA) phase, after completion of the Analysis of Alternatives (AoA) and before Milestone A. It focuses 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 Initial Capabilities Document (ICD) and meeting affordability, technology and operational effectiveness and suitability goals.

The ASR helps the Program Manager (PM) and Systems Engineer ensure that further engineering and technical analysis needed to draft the system performance specification is consistent with customer needs.

**CJCSI 3170.01** calls for a Functional Capabilities Board (FCB) review prior to Milestone A. This FCB review should ensure compatibility between the operational capability needs in the ICD and the maturity, feasibility and risks of the preferred materiel solution.

**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. Figure 21 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.
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.

**Figure 21: Weapon System Development Life Cycle**

- 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 Concept of Operations/Operational Mode Summary/Mission Profile (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 28 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 28: ASR Products and Criteria**

<table>
<thead>
<tr>
<th>Product</th>
<th>ASR Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refined Joint Requirements</td>
<td>- Joint context and initial CONOPS/OMS/MP updated to reflect current user position about capability gap(s), supported missions,</td>
</tr>
</tbody>
</table>
interfacing/enabling systems in the operational architecture; overall system of systems (SoS) context

- Required related solutions and supporting references (ICD and CDDs) identified
- Joint refined thresholds and objectives initially stated as broad measures of effectiveness and suitability (e.g., KPPs, KSAs, need date)

**Initial Architecture for the Preferred Materiel Solution(s)**

- High-level description of the preferred materiel solution(s) is available and sufficiently detailed and understood to enable further technical analysis in preparation for Milestone A
- SoS interfaces and external dependencies are adequately defined

**System Performance Specification**

- Clear understanding of the system requirements consistent with the ICD and draft CDD (if available)
- 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 AoA
- 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 ICD (or draft CDD if available) 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

### 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
- Informed advice to the user-developed draft Capability Development Document (CDD) required at Milestone A

### CH 3–3.3.2 System Requirements Review

The System Requirements Review (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. 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) from the Materiel Solution Analysis (MSA) phase.
- Are consistent with technology maturation plans.
- Adequately consider the maturity of interdependent systems.
All system requirements and performance requirements derived from the Initial Capabilities Document (ICD) or draft Capability Development Document (CDD) 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.

For Major Defense Acquisition Programs (MDAPs), DoDI 5000.02, para 5.d.3 requires a Milestone A before approving release of the final Request for Proposal (RFP) for the Technology Maturation and Risk Reduction (TMRR) phase; therefore, it is suggested that the program office perform a review similar to an SRR to assess readiness and risks of the technical content of the draft RFP(s) prior to Milestone A and ensure performance requirements are traceable to capability requirements. This program office review should occur after the selection of the preferred solution and after sufficient analysis has occurred to develop a draft system performance specification.

If the program’s Acquisition Strategy (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 also ensures that system of systems (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 ICD and/or draft CDD. These requirements are documented in the system performance specification and managed through external communication and technical interfaces in accordance with the Systems Engineering Plan (SEP).

Roles and Responsibilities

The unique Program Manager (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 System Functional Review (SFR) in applicable contract documents, including the SE Master Plan, Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the plan includes subject matter experts 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 in the draft CDD including Key Performance Parameters (KPPs), Key System Attributes (KSAs), other system attributes and the system performance specification (see JCIDS Manual (Enclosure D)) (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 22 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 at Milestone A.

**Figure 22: Weapon System Development Life Cycle**
Table 29 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., Program Protection Plan (PPP), Test and Evaluation Master Plan (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 29: SRR Products and Criteria

<table>
<thead>
<tr>
<th>Product</th>
<th>SRR Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost Estimate</strong></td>
<td>• Preliminary Cost Analysis Requirements Description (CARD) is consistent with the approved system performance specification</td>
</tr>
<tr>
<td></td>
<td>• Preliminary software development estimates established with effort, schedule, and cost analysis</td>
</tr>
<tr>
<td></td>
<td>• Updated cost estimate fits within the existing budget</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>• Technical risks are identified, and mitigation plans are in place</td>
</tr>
<tr>
<td><strong>System Performance Specification</strong></td>
<td>• Contractor clearly demonstrates an understanding of the system requirements consistent with the ICD and draft CDD</td>
</tr>
<tr>
<td></td>
<td>• System requirements are sufficiently detailed and understood to enable functional definition and functional decomposition</td>
</tr>
<tr>
<td></td>
<td>• System requirements are assessed to be verifiable (see Chief Developmental Tester in CH 8-4.2.)</td>
</tr>
<tr>
<td></td>
<td>• Requirements can be met given the plans for technology maturation</td>
</tr>
<tr>
<td>Product</td>
<td>SRR Criteria</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>• External interfaces to the system have been documented in interface control documents</td>
</tr>
<tr>
<td></td>
<td>• SoS technical interfaces are adequately defined, including interdependences associated with schedule, test, and configuration changes</td>
</tr>
<tr>
<td></td>
<td>• Preliminary identification of all software components (tactical, support, deliverable, non-deliverable, etc.) are completed</td>
</tr>
<tr>
<td></td>
<td>• Human Systems Integration (HSI) and sustainment requirements have been reviewed and included in the overall system design (See CH 3–4.3.10, and CH 5–4.)</td>
</tr>
<tr>
<td></td>
<td>• Contractor has adequately expanded the system performance specification to reflect tailored, derived and correlated design requirements</td>
</tr>
<tr>
<td></td>
<td>• Bidirectional requirements traceability between the draft CDD, the Statement of Work (SOW) and the system performance specification has been documented</td>
</tr>
<tr>
<td></td>
<td>• System performance specification is approved, including stakeholder concurrence, with sufficiently conservative requirements to allow for design trade space</td>
</tr>
<tr>
<td>Technical Plans</td>
<td>• Contractors Systems Engineering Management Plan (SEMP) is complete and adequate</td>
</tr>
<tr>
<td></td>
<td>• Cost and critical path drivers have been identified</td>
</tr>
<tr>
<td></td>
<td>• The program schedule is executable with an acceptable level of technical and cost risk</td>
</tr>
<tr>
<td></td>
<td>• Adequate processes and metrics are in place for the program to succeed</td>
</tr>
<tr>
<td></td>
<td>• SE is properly staffed</td>
</tr>
<tr>
<td></td>
<td>• Program is executable within the existing budget</td>
</tr>
<tr>
<td></td>
<td>• Software functionality in the system performance specification is consistent with the software-sizing estimates and the resource-loaded schedule</td>
</tr>
<tr>
<td></td>
<td>• Programming languages and architectures, security requirements and operational and support concepts have been identified</td>
</tr>
<tr>
<td></td>
<td>• Hazards have been reviewed and mitigating courses of action have been allocated within the overall system design</td>
</tr>
<tr>
<td></td>
<td>• Key technology elements have been identified, readiness assessed and maturation plans developed</td>
</tr>
<tr>
<td></td>
<td>• Software development strategy is complete and adequate</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Draft verification methodologies have been adequately defined for each specification requirement</td>
</tr>
<tr>
<td></td>
<td>• Certifying agencies have been identified and certification requirements are understood</td>
</tr>
<tr>
<td></td>
<td>• Draft test plans have been developed in support of the TMRR phase (See Chief Developmental Tester in CH 8–4.2.)</td>
</tr>
<tr>
<td></td>
<td>• Government and contractor configuration management (CM) strategies are complete and adequate</td>
</tr>
<tr>
<td></td>
<td>• Planning for creation and/or use of models and simulations has begun and is captured in appropriate program plans.</td>
</tr>
<tr>
<td></td>
<td>• The manufacturing and production strategy is complete and adequate</td>
</tr>
<tr>
<td>Product</td>
<td>SRR Criteria</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
|         | • Integrated Master Schedule (IMS) adequately identifies the critical path and is resourced at reasonable levels, based on realistic performance/efficiency expectations  
|         | • Unique work requirements for risk reduction prototyping and competitive prototyping have been identified  
|         | • Product support plan and sustainment concepts have been defined with the corresponding metrics |

### Output 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.

#### CH 3–3.3.3 System Functional Review

The System Functional Review (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 Initial Capabilities Document (ICD) and draft Capability Development Document (CDD). The Program Manager (PM) establishes Government control of the functional baseline at the SFR and verifies it through Functional Configuration Audits (FCA) leading up to the system level FCA or the System Verification Review (SVR). For additional information, see CH 3–4.1.6, Configuration Management Process.

A successful SFR, which typically occurs during the Technology Maturation and Risk Reduction (TMRR) phase, reduces the risk of continuing the technical effort toward the Preliminary Design Review (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
- 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 Systems Engineering Plan (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 SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the plan includes subject matter experts 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 to include Key Performance Parameters (KPPs), Key System Attributes (KSAs) other system attributes, and the system performance specification (see CJCSI 3170.01 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 at Milestone A. Figure 23 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 23: Weapon System Development Life Cycle**

Table 30 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 Acquisition Strategy (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 30: SFR Products and Criteria

<table>
<thead>
<tr>
<th>Product</th>
<th>SFR Criteria</th>
</tr>
</thead>
</table>
| **Functional Baseline Documentation** | • 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  
• Documented performance requirements traced to (draft) 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 verification requirements, including testing, for FCA/SVR |
| **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 ESOH mitigation measure requirements, at levels that warrant continued engineering development                                                                 |
| **Technical Plans**             | • Established detailed plan/schedule, sufficiently resourced to continue design and development                                                                                                               |

### 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.

**CH 3–3.3.4 Preliminary Design Review**

The Preliminary Design Review (PDR) should provide sufficient confidence to proceed with detailed design. The PDR ensures 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 the validated Capability Development Document (CDD). 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 Program Manager (PM) establishing the complete allocated baseline at the system-level PDR. The PM then verifies the allocated baseline at the Functional Configuration Audit (FCA) and/or System Verification Review (SVR) (see **CH 3–4.1.6. Configuration Management Process**).
The PDR is mandatory per DoDI 5000.02, Enc 3, sec. 7. The timing of the review should consider the following:

- PDR is conducted prior to Milestone B and prior to the contract award for Engineering and Manufacturing Development for all programs unless waived. (See DoDI 5000.02, para 5.d.4 and DoDI 5000.02, para 5.d.7.) Additionally, 10 U.S.C. 2366b requires the Milestone Decision Authority (MDA) certify all Major Defense Acquisition Programs (MDAPs) at Milestone B. This certification requires the conduct and assessment of a PDR, unless waived for national security reasons.
- The timing of PDR relative to the Development Request for Proposal (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. Regardless of this relationship, the PDR assessment is done after PDR and prior to Milestone B to support the MDA decision to enter detailed design. (See DoDI 5000.02, para 5.d.7.)

For MDAPs and MAIS programs, a PDR assessment is conducted and provided to the MDA. For ACAT ID and ACAT IAM programs, DASD(SE) conducts a PDR assessment to inform the MDA of technical risks and the program’s readiness to proceed into detailed design. For ACAT IC and ACAT IAC programs, the Component Acquisition Executive conducts the PDR assessment.

Any tailoring with respect to establishing an allocated baseline at PDR prior to Milestone B should be consistent with the approved Acquisition Strategy (AS) and documented in the Systems Engineering Plan (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 Engineering and Manufacturing Development (EMD) bidders with a complete technical package, best practices dictate that the PDR be completed prior to the Development RFP Release Decision Point. The tailoring strategy may also include conduct of a delta-PDR after Milestone B 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, 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 the Milestone B investment decision and Acquisition Program Baseline (APB).
- Is fully captured and properly allocated in the specifications for each system element and all interface documentation (including system of systems (SoS) interdependencies).

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

- All 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).
- All external interfaces to the system, as addressed at the System Requirements Review, have been documented in interface control documents.
- All internal interfaces of the system (system element to system element) have been documented in interface control documents.
- Verification requirements to demonstrate achievement of all specified allocated performance characteristics have been documented.
- Design 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 Cost Analysis Requirements Description (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, EMD contract specifications and Statement of Work (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. 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 and Systems Engineer should update relevant program plans.

Roles and Responsibilities

The PM and Systems 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 and Systems 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 and Systems 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 SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the SEP includes subject matter experts to participate in each review.
- 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 assessments and risks associated with all design constraints and considerations are conducted, documented and provided (e.g., reliability and maintainability, corrosion and Environment, Safety and Occupational Health (ESOH) considerations).
- Updating risk, issue and opportunity 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
Figure 24 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 24: Weapon System Development Life Cycle**

The PDR review criteria are developed to best support the program’s technical scope and risk; they are documented in the program’s SEP no later than Milestone A. Table 31 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 31: PDR Products and Criteria**

<table>
<thead>
<tr>
<th>Product</th>
<th>PDR Criteria</th>
</tr>
</thead>
</table>
| Cost Estimate | • System cost model has been updated, allocated to lower system element levels and tracked against targets; production cost model constructed  
• Updated 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 defined in the Test and Evaluation Master Plan (TEMP) accounts for risks with a mitigation plan; necessary integration and test resources are documented within the TEMP and current availability align with the program IMS (SE coordinates with the Chief Developmental Tester in this area; refer to CH 8–4.2.) |
<table>
<thead>
<tr>
<th>Product</th>
<th>PDR Criteria</th>
</tr>
</thead>
</table>
| **Technical Baseline Documentation (Allocated)** | • Capability Development Document (CDD) is validated per CJCSI 3170.01  
• Analysis of system performance is complete and assessed to meet requirements  
• Preliminary design satisfies design considerations (see CH 3–4.2.2, 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 success (operationally effective and operationally suitable)  
• All Critical Safety Items (CSIs) and Critical Application Items (CAIs) are identified  
• Functional failure mode, effects and criticality analysis (FMECA) is completed  
• 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 (SRSs) 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 CSUs  
• 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, is complete and satisfies all requirements in the functional baseline  
• Requirements trace between functional and allocated baselines is complete and consistent |
| **Technical Plans** | • All entry criteria stated in the contract (e.g., Statement of Work (SOW), SEP, approved SEMP and system performance specification) have been satisfied  
• Integrating activities of any lower-level PDRs have occurred; identified issues are documented in action plans  
• Plan to CDR is accurately documented in the SEP as well as the IMP and IMS |
<table>
<thead>
<tr>
<th>Product</th>
<th>PDR Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Program is properly staffed</td>
</tr>
<tr>
<td></td>
<td>• Adequate processes and metrics are in place for the program to succeed</td>
</tr>
<tr>
<td></td>
<td>• Program schedule, as depicted in the updated IMS (See CH 3–4.1.1.2, Integrated Master Plan and CH 3–4.1.1.3, Integrated Master Schedule) is executable within acceptable technical and cost risks</td>
</tr>
<tr>
<td></td>
<td>• Program is executable with the existing budget and the approved product baseline</td>
</tr>
<tr>
<td></td>
<td>• Trade studies and system producibility assessments are under way</td>
</tr>
<tr>
<td></td>
<td>• Majority of manufacturing processes have been defined, characterized, and documented</td>
</tr>
<tr>
<td></td>
<td>• Logistics (sustainment) and training systems planning and documentation are sufficiently complete to support the review</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Information Support Plan (ISP) is drafted and scheduled for formal review prior to Milestone B</td>
</tr>
<tr>
<td></td>
<td>• LCSP includes software support requirements</td>
</tr>
<tr>
<td></td>
<td>• Long-lead and key supply chain elements are identified</td>
</tr>
<tr>
<td></td>
<td>• Computer system and software design/development approach have been confirmed through analyses, demonstrations, and prototyping in a relevant environment</td>
</tr>
<tr>
<td></td>
<td>• Software increments have been defined and capabilities allocated to specific increments</td>
</tr>
<tr>
<td></td>
<td>• Software trade studies addressing commercial-off-the-shelf, reuse, and other software-related issues are completed</td>
</tr>
<tr>
<td></td>
<td>• Software development process is defined in a baselined Software Development Plan and reflected in the IMP and IMS</td>
</tr>
<tr>
<td></td>
<td>• Software development schedules reflect contractor software processes and IMP/IMS software events for current and future development phases</td>
</tr>
<tr>
<td></td>
<td>• Software development environment and test/integration labs have been established with sufficient fidelity and capacity</td>
</tr>
<tr>
<td></td>
<td>• Software metrics have been defined and a reporting process has been implemented; metrics are being actively tracked and assessed</td>
</tr>
<tr>
<td></td>
<td>• The TEMP documents the overall structure and objectives of the Test and Evaluation program and articulates the necessary resources to accomplish each phase of test. It provides a framework within which to generate detailed T&amp;E plans and documents schedule and resource implications associated with the T&amp;E program</td>
</tr>
<tr>
<td></td>
<td>• Software development estimates (i.e., size, effort (cost), and schedule) are updated</td>
</tr>
</tbody>
</table>

**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.

CARD is updated and reflects the design in the allocated baseline.

LCSP is updated to reflect development efforts and schedules.

**Preliminary Design Review (PDR) Assessment**

A system-level PDR assessment is required for MDAPs and MAIS programs per DoDI 5000.02, Enc 3, sec. 7. 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, for MDAPS only, 10 USC 2366b Milestone B certification. In compliance with DoDI 5000.02, Enc 3, sec. 7, the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) conducts PDR assessments on ACAT ID and ACAT IAM programs, and the Component Acquisition Executive (CAE) conducts the PDR assessments on ACAT IC and ACAT IAC programs. In support of this, MDAP and MAIS PMs are required to invite the DASD(SE) and the CAE to their PDRs and make the PDR artifacts available.

DASD(SE) reviews the conduct of the program’s PDR, to include system element-level reviews as appropriate, and provides the MDA with an assessment of the following:

- The conduct and adequacy of the PDR to include the participation of stakeholders, technical authorities and subject matter experts; 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 schedule risk assessments.
- 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.

**CH 3–3.3.5 Critical Design Review**

The Critical Design Review (CDR), which occurs during the EMD phase, 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 the acquisition community 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 Capability Development Document (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 fabricating, integrating, and testing pre-production 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 5000.02, Enc 3, sec. 8, the Program Manager (PM) assumes control of the initial product baseline at the completion of the system level CDR to the extent that the competitive environment permits. This does not necessarily mean that the PM takes delivery and acceptance of the Technical Data Package (TDP) (for more information, see CH 3–4.1.6, Configuration Management Process).

Roles and Responsibilities

The Systems Engineer documents the approach for the CDR in the Systems Engineering Plan (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 and Systems 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; it further ensures that documentation for the detailed design correctly and completely captures each such specification. The PM and Systems 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 System Verification Review (SVR) in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the plan includes subject matter experts to participate in each review.
- Controlling the configuration of the Government-controlled subset of the functional, allocated and product baselines; convene 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., reliability and maintainability, corrosion, and Environment, Safety and Occupational Health (ESOH) considerations).
- Updating risk, issue and opportunity 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 CDR closure plans.
- Documenting the plan to SVR in the SEP and elsewhere as appropriate.

The CDR is mandatory for MDAP and MAIS programs per DoDI 5000.02, Enc 3, sec. 7. A CDR assessment will be conducted -- assessing the conduct of the review and the program technical risk -- and will be provided to the MDA. For ACAT ID and IAM programs, DASD(SE) conducts the CDR.
assessment. For ACAT IC and IAC programs, the Component Acquisition Executive conducts the CDR assessment.

**Inputs and Review Criteria**

Figure 25 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

![Figure 25: Weapon System Development Life Cycle](image)

The March 2012 Government Accountability Office (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 Critical Safety Items (CSIs) and Critical Application Items (CAIs) should be complete in order to provide tangible evidence of a stable product design. 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 no later than Milestone B.

Table 32 identifies the products and associated review criteria normally seen as part of the CDR. 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.

<p>| Table 32: CDR Products and Criteria |</p>
<table>
<thead>
<tr>
<th>Product</th>
<th>CDR Criteria</th>
</tr>
</thead>
</table>
| Cost Estimate                 | • Updated Cost Analysis Requirements Description (CARD) is 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 (Initial Product) | • Detailed design (hardware and software), including interface descriptions, are complete and satisfy all requirements in the functional baseline  
• Requirements trace among functional, allocated and initial product baselines is complete and consistent  
• Key product characteristics having the most impact on system performance, assembly, cost, reliability and sustainment or ESOH have been identified to support production decisions  
• Initial product baseline documentation is 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 success (operationally effective and operationally suitable) (See CH 8–4.3.)  
• 100% of Critical Safety Items and Critical Application Items have completed drawings, specifications and instructions  
• Failure mode, effects and criticality analysis (FMECA) is complete  
• Estimate of system reliability and maintainability based on engineering analyses, initial test results or other sources of demonstrated reliability and maintainability  
• Detailed design satisfies sustainment and Human Systems Integration (HSI) requirements (See CH 5–4.)  
• Software functionality in the approved initial product baseline is consistent with the updated software metrics and resource-loaded schedule  
• Software and interface documents 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 key product characteristics have been identified, and the capability to meet design tolerances has been determined  
• Verification (developmental test and evaluation (DT&E)) assessment to date is consistent with the initial product baseline and indicates the potential for test and evaluation success (See Test and Evaluation Master Plan (TEMP) and Chief Developmental Tester in CH 8–4.3.) |
| Risk Assessment                | • All risk assessments and risk mitigation plans have been updated, documented, formally addressed and implemented  
• Approach/Strategy for test and evaluation defined in the TEMP accounts for risks with a mitigation plan; necessary integration and test resources are documented in the TEMP and current availabilities align with the Program’s IMS (Systems Engineer coordinates with Chief Developmental Tester in this area; see CH 8–4.3.)  
• ESOH risks are known and being mitigated  
• Risks associated with intelligence mission data (IMD) dependencies have been identified and addressed; refer to CH 3–4.3.12. Intelligence (Life-Cycle Mission Data Plan) |
<p>| Technical Plans                | • PDR is successfully completed; all PDR actions are closed |</p>
<table>
<thead>
<tr>
<th>Product</th>
<th>CDR Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Integrating activities of any lower-level CDRs have occurred; identified issues are documented in action plans</td>
</tr>
<tr>
<td></td>
<td>• All entry criteria stated in the contract (e.g., SOW, SEP, approved SEMP and system performance specification) have been satisfied</td>
</tr>
<tr>
<td></td>
<td>• Adequate processes and metrics are in place for the program to succeed</td>
</tr>
<tr>
<td></td>
<td>• Program schedule as depicted in the updated IMS (see CH 3-4.1.1.2, Integrated Master Plan and CH 3-4.1.1.3, Integrated Master Schedule) is executable (within acceptable technical/cost risks)</td>
</tr>
<tr>
<td></td>
<td>• Program is properly staffed</td>
</tr>
<tr>
<td></td>
<td>• Program is executable with the existing budget and the approved initial product baseline</td>
</tr>
<tr>
<td></td>
<td>• Detailed trade studies and system producibility assessments are under way</td>
</tr>
<tr>
<td></td>
<td>• Issues cited in the ISP are being satisfactorily addressed</td>
</tr>
<tr>
<td></td>
<td>• Materials and tooling are available to meet the pilot line schedule</td>
</tr>
<tr>
<td></td>
<td>• Logistics (sustainment) and training systems planning and documentation are sufficiently complete to support the review</td>
</tr>
<tr>
<td></td>
<td>• Life-Cycle Sustainment Plan (LCSP), including updates on program sustainment development efforts and schedules based on current budgets, test and evaluation results and firm supportability design features, is approved</td>
</tr>
<tr>
<td></td>
<td>• Long-lead procurement plans are in place; supply chain assessments are complete</td>
</tr>
</tbody>
</table>

**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, test and evaluation, 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 at the detailed level 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 weapon system development.

**Critical Design Review (CDR) Assessment**

A system-level CDR assessment is required for MDAPs and MAIS programs. This assessment informs the MDA of the technical risks and the program’s readiness to proceed. In compliance with DoDI 5000.02, Enc 3, sec. 7, the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) is directed to conduct CDR assessments on ACAT ID and ACAT IAM programs; and the Component Acquisition Executive (CAE) is to conduct CDR assessments on ACAT IC and ACAT IAC programs. In support of this policy direction, MDAP and MAIS PMs are required to invite DASD(SE) and CAE to their CDRs and make the CDR artifacts available.
DASD(SE) reviews the conduct of the program’s CDR, to include 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 subject matter experts; status of the CDR entrance and exit criteria; open Requests for Action/Information; and closure of the system elements and system-level reviews.
- The program technical schedule and schedule risk assessments.
- 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, 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.

### CH 3–3.3.6 System Verification Review/Functional Configuration Audit

The System Verification Review (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 Functional Configuration Audit (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. The SVR/FCA typically occurs during the Engineering and Manufacturing Development (EMD) phase.

When a full-up 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.

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

- Assess whether system development is satisfactorily completed.
- Review the completed documentation of the Verification Process for completeness and adequacy.
- Determine that the system is ready to proceed to the next phase and OT&E with acceptable risk (see CH 8–4.3.)
- 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 Capability Development Document (CDD) and/or Capability Production Document (CPD).

### Roles and Responsibilities

The unique Program Manager (PM) responsibilities associated with an SVR/FCA include:

- Approving, funding and staffing the SVR/FCA as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer.
- Establishing the plan to the Production Readiness Review (PRR) in applicable contract documents, including the SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the SEP includes subject matter experts to participate in each technical review/audit.
- Continuing to control appropriate changes to the product baseline (see CH 3–4.1.6, 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.
- 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

Figure 26 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 26: Weapon System Development Life Cycle**

The SVR/FCA 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 B. Table 33 identifies the products and associated review criteria normally seen as part of the SVR/FCA. The Chief 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 Chief 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 33: SVR/FCA Products and Criteria**
<table>
<thead>
<tr>
<th>Product</th>
<th>SVR/FCA Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Baseline Documentation (Functional and/or Allocated) Verification</td>
<td>• 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 (EOAs), Operational Assessments (OAs)) and/or live fire testing) • Assessment that the documented product baseline for the initial production system has an acceptable risk of operational test failure during OT&amp;E</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>• Identified and documented risks (including ESOH) have been accepted at the appropriate management level prior to initial production for the system to be used in OT&amp;E</td>
</tr>
<tr>
<td>Technical Plans</td>
<td>• Detailed plan/schedule has been established and sufficiently resourced to continue development</td>
</tr>
</tbody>
</table>

**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.

**CH 3-3.3.7 Production Readiness Review**

The Production Readiness Review (PRR) for the system 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 accomplished at various points in the life cycle of a program.

In the early stages, production readiness assessments should focus on high-level manufacturing concerns such as the need for identifying 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, held prior to Milestone C, 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. See the EMD Phase production activities described in DoDI 5000.02, para 5.d.9.

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. See CH 3–3.3, Technical Reviews and Audits for more on this incremental approach.

**Roles and Responsibilities**

The unique Program Manager (PM) responsibilities associated with a system PRR include:

- Approving, funding and staffing the PRR as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer.
• Establishing the plan to Physical Configuration Audit (PCA) in applicable contract documents, including the SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
• Ensuring the plan includes subject matter experts 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 CH 3–4.1.6, 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 met to make sure 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

Figure 27 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 27: Weapon System Development Life Cycle**

**Notes:**
- Derived from DoD 5000.02, Model 5: Hybrid Program A (Hardware Dominant).
- The actual number and type of builds during the program will depend on system type and program strategy.
The PRR 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 B. Table 34 identifies the products and associated review criteria normally seen as part of the PRR. The Chief 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 Chief 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 34: PRR Products and Criteria

<table>
<thead>
<tr>
<th>Product</th>
<th>PRR Criteria</th>
</tr>
</thead>
</table>
| **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** | • 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)  
• Environment, Safety and Occupational Health (ESOH) risks are known and mitigated |
| **Technical Baseline Documentation (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  
• Manufacturing processes are stable and have been demonstrated in a pilot line environment  
• Adequate production line processes and metrics are in place for the delivery of on-time, quality products |
| **Technical Plans** | • Prior readiness reviews are completed and action items closed  
• Supply chain is stable and adequate to support planned LRIP and FRP  
• Program is properly staffed with qualified production, quality (engineering and assurance) and manufacturing personnel  
• Product acceptance system, including acceptance test procedures and associated equipment, has been validated and put under configuration control  
• Production facilities are ready and required personnel are trained  
• Delivery schedule is executable (technical/cost risks, long lead items)  
• Diminishing Manufacturing Sources and Material Shortages (DMSMS) plan is in place and mitigates the risk of obsolescence during LRIP and FRP |

A follow-on PRR may be appropriate in the Production and Deployment (PD) phase for the prime contractor and major subcontractors if:

- Changes (from the Engineering and Manufacturing Development (EMD) phase system design) in materials and/or manufacturing processes are required when entering or during the Production and Deployment (P&D) phase.
- 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 CH 3–4.3.18, 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 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.

CH 3–3.3.8 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 Operational Test and Evaluation (OT&E) and the associated documentation currently under configuration control. A successful PCA provides the Milestone Decision Authority (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 prior to the Full-Rate Production Decision Review (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 Functional Configuration Audit (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 Program Manager (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 Systems Engineering Plan (SEP) developed by the Systems Engineer.
- Establishing the plan to FRP DR in applicable contract documents, including the SE Management Plan (SEMP), Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).
- Ensuring the plan includes subject matter experts 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 CH 3–4.1.6, 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.
- Ensuring the pre-established review criteria have been met to make sure 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 is 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 Technical Data Packages (TDP) 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**

Figure 28 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

**Figure 28: Weapon System Development Life Cycle**
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 35 identifies the products and associated review criteria normally seen as part of the PCA. The Chief 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 Chief 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" can be used as a resource for audit preparation. This is a best practice audit.

Table 35: PCA Products and Criteria

<table>
<thead>
<tr>
<th>Product</th>
<th>PCA Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Baseline Documentation</strong></td>
<td>• Assessment that the product baseline is complete and accurately reflects the configuration of the representative production item that was inspected and validated through OT&amp;E</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>• Risks are identified and documented at levels low enough to continue with full-rate production and deployment</td>
</tr>
<tr>
<td><strong>Technical Plans</strong></td>
<td>• A detailed plan and schedule are established and sufficiently resourced to proceed with full-rate production and deployment</td>
</tr>
</tbody>
</table>

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.

CH 3–4. Additional Planning Considerations

The systems engineering (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 provide a consistent framework for managing technical activities and identifying the technical information and events critical to the success of the program. The eight technical processes ensure the system design, and the delivered capability reflect the requirements that the stakeholders have expressed. All 16 SE processes are applicable to each of the six Defense Acquisition Program Models. As a whole, the SE processes provide a systematic approach focused on providing needed capability to the operational end user. Successful implementation of the SE processes results in an integrated capability solution that is:

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

All organizations performing SE should scale their application 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 36, discuss the SE processes in more detail.

Table 36: Systems Engineering Processes

<table>
<thead>
<tr>
<th>Technical Management Processes</th>
<th>Technical Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Planning (CH 3–4.1.1.)</td>
<td>Stakeholder Requirements Definition (CH 3–4.2.1.)</td>
</tr>
<tr>
<td>Decision Analysis (CH 3–4.1.2.)</td>
<td>Requirements Analysis (CH 3–4.2.2.)</td>
</tr>
<tr>
<td>Technical Assessment (CH 3–4.1.3.)</td>
<td>Architecture Design (CH 3–4.2.3.)</td>
</tr>
<tr>
<td>Requirements Management (CH 3–4.1.4.)</td>
<td>Implementation (CH 3–4.2.4.)</td>
</tr>
<tr>
<td>Risk Management (CH 3–4.1.5.)</td>
<td>Integration (CH 3–4.2.5.)</td>
</tr>
<tr>
<td>Configuration Management (CH 3–4.1.6.)</td>
<td>Verification (CH 3–4.2.6.)</td>
</tr>
<tr>
<td>Technical Data Management (CH 3–4.1.7.)</td>
<td>Validation (CH 3–4.2.7.)</td>
</tr>
<tr>
<td>Interface Management (CH 3–4.1.8.)</td>
<td>Transition (CH 3–4.2.8.)</td>
</tr>
</tbody>
</table>

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

- IEEE 15288.1, Standard for Application of Systems Engineering on Defense Programs

ISO/IEC/IEEE 15288 is a non-Government standard (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. It 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.

Both ISO/IEC/IEEE 15288 and IEEE 15288.1 have been adopted for use by DoD. 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 Program Management Office (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 DASD(SE) website.

There is not a one-to-one mapping between the SE processes in the ISO/IEC/IEEE 15288 and the DAG, but the same information is conveyed in both documents. Figure 29 depicts how the DAG 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 is outside the scope of DoD acquisition.

Roles, Responsibilities, and Activities

The Program Manager (PM) and Systems Engineer use 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 and Systems 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 30 is a representation of how much effort is typically focused on each of the SE processes throughout the acquisition life cycle. The PM and Systems Engineer should apply appropriate resources with the requisite skill sets to ensure successful execution of each process.

**Figure 30: Notional Emphasis of Systems Engineering Processes throughout the Defense Weapon System Acquisition Life Cycle**

<table>
<thead>
<tr>
<th>Technical Management Processes</th>
<th>Pre-MDD</th>
<th>MSA</th>
<th>TMRR</th>
<th>EMD</th>
<th>P&amp;D</th>
<th>O&amp;S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision Analysis</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Technical Planning</td>
<td>•</td>
<td></td>
<td>•</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Assessment</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Requirements Management</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Risk &amp; Opportunity Management</td>
<td></td>
<td>•</td>
<td></td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Data Management</td>
<td></td>
<td></td>
<td>•</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Management</td>
<td></td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stakeholder Requirements Definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements Analysis</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Architecture Design</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Integration</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Transition</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

**CH 3–4.1 Technical Management Processes**

In DoD systems engineering, there are 8 technical management processes. The technical management processes are the foundational, enabling processes and are used consistently throughout the system life cycle to help manage the system development. The technical management processes are described in Sections 4.1.1 through 4.1.8.

**CH 3–4.1.1 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 Program Manager (PM) and Systems Engineer with a framework to accomplish the technical activities that collectively increase product maturity and knowledge and reduce technical risks. Defining the scope of the technical effort provides:

- An accurate basis for program cost and schedule estimates, documented in the Independent Cost Estimate (ICE), Cost Analysis Requirements Description (CARD) and Acquisition Program Baseline (APB).
• A foundation for risk identification and management (see CH 3–4.1.5, Risk Management Process).
• Quantitative measures supporting the Technical Assessment process (see CH 3–4.1.3) 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, establish the plan for accomplishing work against which contract performance is measured and enable mandatory program certifications (e.g., 10 USC 2366a or 10 USC 2366b).

Technical planning includes the program’s plan for technical reviews and audits (see CH 3–3.3). 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, key 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 and Systems 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 (see CH 3–3.2.1, Pre-Materiel Development Decision) and during the Materiel Solution Analysis (MSA) phase (see CH 3–3.2.2, Materiel Solution Analysis Phase). Beginning in MSA, programs begin to capture their technical planning in the Systems Engineering Plan (SEP) (see CH 3–2.2, Systems Engineering Plan), which is required at each milestone review from Milestone A to Milestone C. Technical planning leverages the Concept of Operations/Operational Mode Summary/Profile (CONOPS/OMS/MP), which is available in the MSA phase. The CONOPS/OMS/MP is a document consistent with the validated/approved capability requirements document to include 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.

As the system matures and issues arise throughout the life cycle, the PM and Systems 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 (See CH 1–3.4). The Systems Engineer is responsible for:

• Developing, maintaining and executing the program’s SEP.
• Tracking alignment of the developer’s Systems Engineering Management Plan (SEMP).
• Providing key technical inputs and ensuring SEP alignment to other program plans (Acquisition Strategy (AS), Test and Evaluation Master Plan (TEMP), Life-Cycle Sustainment Plan (LCSP) 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 and Systems 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.
• 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, Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP))
• 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 engineering approach and development strategy
• The strategy and approach for test and evaluation, for both developmental and operational testing (See CH 8–3.1, and CH 8–3.2, for additional information regarding interactions with the Chief Developmental Tester)
• 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:

• Work Breakdown Structure (see CH 3–4.1.1.1) -- a framework for specifying program objectives
• Integrated Master Plan (see CH 3–4.1.1.2) -- an event-based plan consisting of a hierarchy of program events that need to be accomplished
• Integrated Master Schedule (see CH 3–4.1.1.3) -- an integrated, networked schedule that contains all lower-level tasks required to support program events

Other useful resources available to assist the PM and Systems Engineer in the Technical Planning process can be found in the “Guidance & Tools” section of the ODASD(SE) Policy and Guidance website.

CH 3–4.1.1.1 Work Breakdown Structure

The Work Breakdown Structure (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. 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 systems engineering (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 Report (IPMR)).

The WBS integrates technical, cost and schedule parameters, giving the Program Manager (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.

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 Statement of Work (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 Earned Value Management System (EVMS), the Integrated Master Plan (IMP) and the Integrated Master Schedule (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 CH 1–4.2.16.

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.

**CH 3–4.1.1.2 Integrated Master Plan**

The Integrated Master Plan (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 Integrated Product Team (IPT) and Work Breakdown Structure (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.
CH 3–4.1.1.3 Integrated Master Schedule

The Integrated Master Schedule (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, to include start date, event duration and finish date for all activities, to organize the overall hierarchical flow of work. This assists the Program Manager (PM) in comprehending the links and relationships between various activities, including the resources supporting them.

Together, the PM and Systems 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 Earned Value Management System (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 key acquisition milestones

Figure 31: IMP/IMS Hierarchy and Content
Figure 31 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 and Systems Engineer should ensure that the System Engineering Plan (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.

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 Report (IPMR)), 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 and Systems 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 Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide provides additional guidance on developing and implementing these technical planning tools.

**CH 3–4.1.1.4 Schedule Risk Assessments**

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

Monte Carlo is one technique used to generate multiple runs simulating project progress. It performs a schedule risk assessment against a baseline program plan for all non-summary, non-milestone tasks (see Figure 32). 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 CH 3–4.1.5, Risk Management Process).

When part of the contract, the DI-MGMT-81861 (Integrated Program Management Report (IPMR)) specifies when SRAs should be performed. Contractors and subcontractors should perform an SRA on their schedule prior to 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 32: Schedule Risk Assessment Histogram**
**CH 3–4.1.2 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 CH 3–4.1.1.)
- Technical Assessment (see CH 3–4.1.3.)
- Stakeholder Requirements Definition (see CH 3–4.2.1.)
- Requirements Analysis (see CH 3–4.2.2.)
- Architecture Design (see CH 3–4.2.3.)

A well-executed decision analysis or trade-off analysis helps the Program Manager (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, subject matter experts 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 CH 3–2.4. 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.
CH 3–4.1.3 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 Program Manager (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 in the Materiel Solution Analysis (MSA) phase. During the Technology Maturation and Risk Reduction (TMRR) and Engineering and Manufacturing Development (EMD) phases, 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 also include manufacturing and production activities during the Production and Deployment (P&D) phase and continue through the Operations and Support (O&S) phase to support reliability growth and sustainment engineering efforts.

The PM and Systems Engineer evaluate technical maturity in support of program decisions at the key event-driven technical reviews and audits (see CH 3–3.3, Technical Reviews and Audits) that occur throughout the acquisition life cycle. The PM and Systems Engineer use various measures and metrics, including Technical Performance Measures (TPM) and leading indicators, to gauge technical progress against planned goals, objectives and requirements. (See CH 3–4.1.3.1, Technical Performance Measures 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 CH 3–3.3, 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 (see CH 3–4, Additional Planning Considerations); 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) (see CH 1–4.2.16.2.1.) to capture time-phased measures against the Work Breakdown Structure (WBS) (see CH 3–4.1.3.1, Technical Performance
Measures); (2) a resource-allocated Integrated Master Schedule (IMS) (see CH 3–4.1.1.3.); and (3) the Systems Engineering Plan (see CH 3–2.2.) 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 technical performance measures and metrics. 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 key 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 subject matter experts as appropriate for reviews and audits.

Inputs to the Technical Assessment process should include approved program plans (e.g., Systems Engineering Plan, Acquisition Strategy (AS), Acquisition Program Baseline (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, Program Support Assessment (PSA) findings or test reports).

**CH 3–4.1.3.1 Technical Performance Measures**

Technical performance measures and metrics (TPMs) are the method of collecting and providing information to Program Managers (PM) and Systems Engineers at routine intervals for decision making. Metrics 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. Additionally, 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 acquisition phase of 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 (e.g., Pre-Milestone A), 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 DASD(SE) 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 37: Core TPM Category Definitions, the PM and System 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 Key Performance Parameter (KPP) and each Key System Attribute (KSA). The traceability of the TPMs to the core categories should be documented in the SEP. The following two figures address the organization of the core TPM categories as well as their definitions.

Table 37: Core TPM Category Definitions

<table>
<thead>
<tr>
<th>Core TPM Category</th>
<th>Description of TPM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission Integration Management (SoS Integration /Interoperability)</strong></td>
<td>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 DAG CH 3–4.2.5, Integration and CH 3–4.3.13, Interoperability and Dependencies)</td>
</tr>
<tr>
<td><strong>Mission (End-to-End) Performance</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Reliability, Availability and Maintainability (RAM)</strong></td>
<td>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 CH 3–4.3.19, Reliability and Maintainability Engineering)</td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td>Metrics should evaluate the performance of the system or subsystem elements in achieving critical technical attributes (e.g., weight) that contribute to meeting system requirements. There should be multiple TPMs to monitor forecasted performance of KPPs and KSAs.</td>
</tr>
<tr>
<td><strong>System (Information) Security</strong></td>
<td>System assurance evaluates the safeguarding of the system and the technical data anywhere in the acquisition process, to include the technologies being developed, the support systems (e.g., test and simulation equipment) and research data with military applications. (See CH 9–3.2.)</td>
</tr>
<tr>
<td><strong>Manufacturing Management</strong></td>
<td>Metrics should evaluate the extent to which the product can be manufactured with relative ease at minimum cost and maximum reliability. (See CH 3–4.3.18, Producibility, Quality, and Manufacturing Readiness)</td>
</tr>
<tr>
<td><strong>Manufacturing Quality</strong></td>
<td>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 CH 3–4.3.18, Producibility, Quality, and Manufacturing Readiness)</td>
</tr>
<tr>
<td><strong>Schedule Management</strong></td>
<td>Include metrics to assess both schedule health (e.g., the DCMA 14-point health check), associated completeness of the WBS and the risk register. A</td>
</tr>
</tbody>
</table>
Core TPM Category | Description of TPM
---|---

healthy, complete and risk-enabled schedule forms the technical basis for EVMS. Strong schedule metrics are paramount for accurate EVMS data.  (See CH 1–4.2.16.)

**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. Also see Table 49: 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 CH 3–2.3.1, Software)

**Software Quality** | Metrics should address software technical performance and quality (e.g., defects, rework) evaluating the software's ability to meet user needs. (See CH 3–2.3.1, Software)

**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 CH 3–4.1.4, 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 CH 3–4.1.5, 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). (See CH 8–3.5.5.)

**TPM Hierarchy**

As shown in Figure 33, 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 33: TPM Hierarchy**
TPM Characteristics

Figure 34 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, schedule health, requirements stability and mission integration/interoperability.

Figure 34: 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 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. Important to note is that 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 35 depicts the relationship between Contingency, CBE, WCE, Threshold and Margin, as well as example criteria of how contingency changes as the system/testing matures.

**Figure 35: TPM Contingency Definitions**
Program Support Assessments

The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) conducts Program Support Assessments (PSAs) of Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) programs and other programs as directed by the DAE to help shape the program's technical planning and management approaches. Like any independent review, the PSA prevents problems by early recognition of risks and identification of proposed mitigation activities. PSA requirements appear in DoDI 5000.02, Enc 3, sec. 20. The assessments are designed to help Program Managers (PMs) shape technical planning and improve execution by providing actionable recommendations and by identifying engineering and integration risks as well as mitigation activities.

DoD Components will provide access to all Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) program records and data, including technical review artifacts, classified, unclassified, competition sensitive, and proprietary information that the DASD(SE) considers necessary to carry out these assessments within the scope of DoD Instruction 5134.16. ODASD(SE) personnel conducting PSAs will possess proper identification, personnel security clearance (as required), Non-Disclosure Agreement (NDA) (as required), and need to know. Early conduct of PSAs should help the PM identify and resolve any program planning or execution issues well before major program decisions. Table 38 lists important PSA attributes.

| Cross-functional | No "stovepipes"  
|                  | All reviewers look at multiple areas  
|                  | All observations and comments are adjudicated with the entire team and program office  
| Multidisciplinary | Wide range of functional representation (internal ODASD(SE), AT&L, consultants)  
|                  | Wide range of reviewer expertise  
|                  | Multiple reviewers look at each area  
| Independent      | Minimize "program expert" bias  
|                  | No Government or contractor competitors  
|                  | No program advocates or antagonists  
| Consistent       | Application of common criteria derived from policy and guidance ensure all potential risks, issues, and opportunities are considered  
|                  | Treat all programs equally and fairly  
| Tailorable       | Adapt to type of review  
|                  | Adapt focus on identified challenges  

The Service (SAE, PEO, PMO) can request similar non-advocate reviews, which may serve as independent technical risk peer reviews. These assessments can be tailored for a specific request, and results are provided only to the requester.

Activities and Products

When practical, the initial PSA occurs nine to twelve months before a milestone decision review; follow-up engagements in concert with scheduled program activities and a final engagement (two to three months before the milestone), which assesses the implementation of key recommendations and the mitigation of risks in order to improve program planning and execution. The PSA typically consists of two- to three-day visits to the program office (and developer(s) as applicable).

PSAs focus on all SE processes appropriate to the life cycle phase but are broader in scope to consider all aspects of acquisition management, including resource planning, management methods and tools, earned value management, logistics and other areas. The Defense Acquisition Program Support (DAPS)
Methodology is a source for tailorable criteria and review questions and helps ensure consistency in reviews. The DAPS Methodology includes:

- Mission capabilities/requirements generation
- Resources
- Management
- Technical planning and process
- Program performance

Insights from PSAs aid the development of the Systems Engineering Plan (SEP) (see CH 3–2.2, Systems Engineering Plan) as well as the Request for Proposals (RFPs), and they ensure that the program has adequately addressed SE equities in these documents. After its engagement with the program in preparation for the pre-Milestone A PSA, the ODASD(SE) staff maintains continuous engagement with the program to monitor its execution of the planning reflected in the SEP. PSAs before Milestones B, C, and the Full-Rate Production decision can make use of information already vetted during SE WIPT meetings, various technical reviews (see CH 3–3.3, Technical Reviews and Audits), and program management reviews in order to help reduce the PSA burden on the program office and developer staff. PSA action items may be documented in the milestone review's Acquisition Decision Memorandum (ADM).

CH 3–4.1.4 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 CH 3–4.2.1, 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 CH 3–4.1.6, Configuration Management Process), can help the program to 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 Program Manager (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 5000.02, para 5.d.5.b, Component Acquisition Executives (CAE) establish Configuration Steering Boards (CSB), following Capability Development Document (CDD) validation, for Acquisition Category (ACAT) I and IA 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 Total Ownership Cost (TOC), the PM, in consultation with the Program Executive Officer (PEO) and requirements sponsor, will identify and propose to the CSB recommended requirements changes, to include 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.

CH 3–2.4. 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 Work Breakdown Structure.

CH 3–4.1.5 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 key 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 acquisition phase to enter, based on the type and level of key 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, quality, manufacturing, logistics, requirements, software, test and reliability. DoDI 5000.02, Enc 2, sec. 6.d requires the Program Manager (PM) to present top program risks and associated risk mitigation plans at all relevant decision points and milestones. DoDI 5000.02, Enc 2, sec. 6.d also specifies risk management techniques the PM is required to consider when developing the acquisition strategy. Technical risk management is addressed in DoDI 5000.02, Enc 3, sec. 5.

Technical, programmatic and business events can develop into risks, issues or opportunities, each with cost, schedule or performance consequences as shown in Figure 36.

Figure 36: 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 Acquisition Strategy (AS) for major defense acquisition programs and major systems. Per statute, the approach for major defense acquisition programs 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 (P.L. 114-92 (SEC. 822 paras (a) and (b))).

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 Systems Engineering Plan. 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 Integrated Master Schedule and Integrated Master Plan.

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, systems engineering, 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 risk reduction for individual risks (i.e., the output of the processes), are significantly 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 utilize 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 CH 3–4.3. Design Considerations. Two specific examples of risk context are Environment, Safety and Occupational Health (ESOH) and cybersecurity. CH 3–4.3.9. addresses ESOH and contains information regarding ESOH-related risk management. CH 3–4.3.24. addresses System Security Engineering and contains information on the Risk Management Framework for DoD Information Technology. The associated DoDI 8510.01 establishes processes for ensuring confidentiality, integrity and availability for DoD Information Technology 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 DASD(SE) web site.

**CH 3–4.1.5.1 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. The PM could recommend the program enter the life cycle at Milestone A, B, or C, depending on the maturity of the material solution and associated risks. 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 or requirements stability risks exist, the PM should structure a program to enter the life cycle at Milestone A to conduct Technology Maturation and Risk Reduction (TMRR). Examples of TMRR phase 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 systems engineering 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 Milestone B to begin Engineering and Manufacturing Development (EMD) with acceptable risk. Examples of EMD phase risk reduction activities include:

- Performing technical reviews to finalize the design and verification testing to confirm it meets requirements.
- Performing manufacturing readiness assessments (MRA) 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 (SWAP-C) 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 fund 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 39 describes an overview of the focus of each activity and the products that are generally produced from the activity.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Answers the Question</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Planning</td>
<td>What is the program's risk management process?</td>
<td>• Program Risk Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Likelihood and consequence criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Risk tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tailored program risk training material</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>What can go wrong? Are there emerging risks based on TPM performance trends or updates?</td>
<td>• List of potential risk statements in an “If…, then…” construct</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>What is the likelihood of the undesirable event occurring and the severity of the consequences?</td>
<td>• Quantified likelihood and consequence ratings, should the risk be realized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Approved risks entered and tracked in a risk register</td>
</tr>
</tbody>
</table>
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 DASD(SE) 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 below in Figure 37.

**Figure 37: 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 their ability to mitigate risks exceeds their authority or resources. As an example, see the concept of risk acceptance authority in the Military Handbook (MIL-HDBK) 882, para 4.3. Control seeks to actively 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 utilize mature technology in case technology is not developed successfully to meet critical program performance or schedule) for selected technologies in the IMS.
- Conducting systems engineering 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 burndown 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 Technical Performance Measures (TPM) and metrics 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 (SWAP-C) 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 Program Executive Officer’s (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 Memorandums of Agreements (MOA) between PMs and PEOs to identify and manage critical interfaces.
- Set up an Interface Control Working Group 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.

CH 3–4.1.5.2 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 40.

Table 40: Issue Management Process Activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Answers the Question</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue Planning</td>
<td>What is the program’s issue management process?</td>
<td>• Issue management process&lt;br&gt;• Issue management plan</td>
</tr>
<tr>
<td>Issue Identification</td>
<td>What has or will go wrong?</td>
<td>• Statements of the problems</td>
</tr>
<tr>
<td>Issue Analysis</td>
<td>What is the consequence of the issue?</td>
<td>• Cost, schedule and performance impacts on the program quantified&lt;br&gt;• Issues entered and tracked in an issue register</td>
</tr>
<tr>
<td>Issue Mitigation</td>
<td>Should the issue be ignored or controlled?</td>
<td>• Approved courses of action (COA) to address the issue&lt;br&gt;• Activities entered into IMS&lt;br&gt;• Metrics identified to track progress</td>
</tr>
<tr>
<td>Issue Monitoring</td>
<td>Has the issue changed?</td>
<td>• Status updates of COA activities&lt;br&gt;• Issue tracking sheet updated&lt;br&gt;• Closure of issue</td>
</tr>
</tbody>
</table>
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 38.

**Figure 38: Issue Reporting Matrix**

![Issue Reporting Matrix](image)

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 and Systems Engineers should develop a course of action, similar to that described in CH 3–4.1.5.1, 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.

**CH 3–4.1.5.3 Opportunity Management**

An opportunity is a potential future benefit to the program's cost, schedule, and/or performance baseline. Program Managers (PMs) and Systems 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 41.

**Table 41: Opportunity Management Process Activities**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Answers the Question</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity Planning</td>
<td>What is the program’s opportunity management process?</td>
<td>• Opportunity management process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Opportunity management plan</td>
</tr>
<tr>
<td>Opportunity Identification</td>
<td>What can be improved?</td>
<td>• Statements of the opportunity</td>
</tr>
<tr>
<td>Opportunity Analysis</td>
<td>What is the business case analysis of the opportunity?</td>
<td>• Benefits quantified in terms of cost, schedule and performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cost and likelihood to achieve benefit understood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cost-benefit analysis report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Opportunity entered into register</td>
</tr>
<tr>
<td>Opportunity Management</td>
<td>Should the opportunity be pursued, reevaluated or rejected?</td>
<td>• Allocated resources to pursue opportunity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activities entered into IMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Metrics identified to track progress</td>
</tr>
</tbody>
</table>
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 Integrated Master Schedule 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 39 and management plans adjusted as required.

<table>
<thead>
<tr>
<th>Opportunity Monitoring</th>
<th>How has the opportunity changed?</th>
<th>Products</th>
</tr>
</thead>
</table>
|                        |                                  | • Status updates of management activities  
|                        |                                  | • Opportunity tracking sheet updated  
|                        |                                  | • Closure of opportunity  |

**Figure 39: Opportunity Tracking Matrix Example**

<table>
<thead>
<tr>
<th>Opportunity</th>
<th>Likelihood</th>
<th>Cost to Implement</th>
<th>Return on Investment</th>
<th>Program Priority</th>
<th>Management Strategy</th>
<th>Owner</th>
<th>Expected Closure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity 1: Procure Smith rotor blades instead of James rotor blades.</td>
<td>Mod</td>
<td>$3.2M</td>
<td>$4.1 M 3 month margin 49% greater lift</td>
<td>#2</td>
<td>Reevaluate - Summarize the mitigation plan</td>
<td>Mr. Bill Smith</td>
<td>March 2017</td>
</tr>
<tr>
<td>Opportunity 2: Open Architecture Cockpit</td>
<td>Mod</td>
<td>$2.2M</td>
<td>$8.2M 56 M</td>
<td>#3</td>
<td>Defer</td>
<td>Ms. Dana Jones</td>
<td>May 2017</td>
</tr>
<tr>
<td>Opportunity 3: Cheaper composite mounting plates</td>
<td>High</td>
<td>$211K</td>
<td>$9.4M 3.6 M 4 months less lead time needed 15 lbs less weight</td>
<td>#1</td>
<td>Summarize the mitigation plan to realize the opportunity</td>
<td>Ms. Kim Johnson</td>
<td>January 2017</td>
</tr>
</tbody>
</table>

**CH 3–4.1.6 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 Engineering Change Proposal (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 Initial Capabilities Document (ICD). The Program Manager (PM) establishes Government control of the functional baseline at the System Functional Review (SFR) and verifies it through Functional Configuration Audits (FCA) leading up to the system-level FCA or the System Verification Review (SVR). Attributes of the functional baseline include:
  o Assessed to be achievable within cost and schedule constraints
  o Documentation of established interfaces between functional segments
  o Documented performance requirements traced to (draft) Capability Development Document (CDD) requirements
  o Reflects design considerations and clear linkage in the systems of systems (SoS) context
  o 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 Preliminary Design Review (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:
  o All system-level functional performance requirements decomposed (or directly allocated) to lower-level specifications (configuration items (CI) for system elements)
  o Uniquely identified CIs for all system elements at the lowest level of the specification tree
  o All interfaces, both internal (between element CIs) and external (between the system under development and other systems), documented in interface control documents
  o Verification requirements to demonstrate achievement of all specified functional performance characteristics (element CI to element CI level and at the system level) documented
  o 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. 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
Critical Design Review (CDR) and verified later at the Physical Configuration Audit. In accordance with DoDI 5000.02, Enc 3, sec. 8, the PM assumes control of the initial product baseline at the completion of the system-level CDR to the extent that the competitive environment permits. This does not necessarily mean that the PM takes delivery and acceptance of the Technical Data Package. Attributes of the product baseline include:

- Requirements Traceability Matrix (RTM) is complete.
- The detailed design (hardware and software), including interface descriptions, satisfies the CDD or any available draft Capability Production Document (CPD) and pertinent design considerations.
- Hardware, software and interface documentation are complete.
- Key product characteristics having the most impact on system performance, assembly, cost, reliability, 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 Configuration Control Board (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 Systems Engineering Plan (SEP) and the supporting Configuration Management Plan (CMP) (as appropriate). In accordance with DoDI 5000.02, Enc 3, sec. 8, the PM, with the support of the Systems Engineer, ensures that the configuration management approach is consistent with the Intellectual Property Strategy (See CH 3–4.1.7, 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.

**CH 3–4.1.7 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 CH 3–4.3.24, System Security Engineering for information
regarding protection of critical program information). Key Technical Data Management considerations include understanding and protecting Government intellectual property and data rights, achieving competition goals, maximizing options for product support and enabling performance of downstream life-cycle functions. DoDI 5000.02, Enc 2, sec. 6.a contains Technical Data Management requirements for Acquisition Category (ACAT) I and II programs.

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 weapon 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 total ownership costs (TOC).

Activities and Products

The Program Manager (PM) and Systems Engineer, in conjunction with the Product Support Manager, should ensure that life-cycle requirements for weapon 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 40 shows the activities associated with Technical Data Management, including:

- Identify Data Requirements
  - Formulate the program’s Intellectual Property (IP) Strategy and technical data management approach, with an emphasis on technical and product data needed to provide support throughout the acquisition life cycle. (See CH 1–4.2.18, for more information about Data Rights).
  - Ensure that data requirements are documented in the IP Strategy; summarized in the Acquisition Strategy (AS) and presented with the Life-Cycle Sustainment Plan (LCSP) during the Operations and Support Phase; and submitted at each milestone before award of the contract for the next life-cycle phase.
  - 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 Statement of Work (SOW) tasks to require the developer to perform the work that generates the required data. The content, format and quality requirements should be specified in the contract.
  - Use current, approved Data Item Descriptions (DID) and Contract Data Requirements Lists (CDRL) in each contract to order the delivery of the required technical data 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 CH 3–2.4.1. 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 40: Data Management Activities**
In support of the Government’s requirement for a Technical Data Package (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 (CAD) models, technical manuals, etc.). Figure 41 provides a notional representation of different types of product-related data.

**Caution:** PMs and Systems 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)
- MIL-HDBK-245 (Preparation of Statement of Work (SOW))
- MIL-STD-963 (Data Item Descriptions)
- MIL-STD-31000 (Technical Data Packages)

**Figure 41: Data Taxonomy**
Data Protection

The Program Manager 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.

**CH 3–4.1.8 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 systems of systems (SoS). The design, definition and management of the physical and logical interfaces, both internal (communications between system elements) and external (communications between the 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 (see CH 3–3.1.2, Systems of Systems). 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 standard interface specifications enables a modular and open systems approach (see CH 3–2.4.1, Modular 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.

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 systems engineering (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 Program Manager (PM) and Systems 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 and Systems Engineer should ensure that the developer documents all system interface requirements (see CH 3–4.1.4, 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 key tasks throughout the life cycle, including:

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

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

### CH 3–4.2 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.

#### CH 3–4.2.1 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 due to 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 Joint Capabilities Integration and Development System (JCIDS) CJCSI 3170.01, and the acquisition of a materiel solution, governed by the Defense Acquisition System, i.e., DoDD 5000.01 and DoDI 5000.02. Defense Business Systems (DBS) do not employ JCIDS procedures for the development and validation of capability requirements documents (See DoDI 5000.75).

The Stakeholder Requirements Definition process complements Requirements Analysis and Architecture Design (see CH 3–4.2.2, Requirements Analysis Process and CH 3–4.2.3, 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 DoD Architecture Framework (DoDAF) provides an approach for DoD architecture development, presentation and integration for both warfighting operations and business operations and processes. For the Net Ready Key Performance Parameter (NR-KPP), the JCIDS manual specifies the data needed to
elaborate, communicate, verify and validate a system’s interoperability requirements and design. System architectural descriptions contain three primary viewpoints: Capability, Operational, and Systems. In the case of the NR-KPP, these viewpoints contain essential architecture data that describe a system’s interoperability requirements and design from multiple perspectives. DoDAF provides a standardized approach for capturing and presenting this architectural data. This standardization facilitates improved communication and sharing of technical information among various stakeholders and across organizational boundaries.

The Program Manager (PM) and Systems Engineer are responsible for supporting the Stakeholder Requirements Definition process and should work with the end user to establish and refine operational needs, attributes, 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 perceived constraints on a system solution.
  - Define the relevant environment (including threat target and critical intelligence parameters per JCIDS Manual Page B-28) and support scenarios that can be used to analyze the operation of the system.
  - 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 Initial Capabilities Document (ICD), Capability Development Document (CDD), and the Capability Production Document (CPD). 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. In preparation for, and presentation at the CDD Validation or Requirements Decision Point, DoDI 5000.02, para 5.d.4 requires the PM to conduct a systems engineering trade-off analysis showing how cost varies as a function of the major design parameters. (Also, see CH 3–4.3.2, Affordability – Systems Engineering Trade-Off Analyses.)

**CH 3–4.2.2 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 CH 3–4.2.1, 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 systems engineering (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, verifiable and feasible system performance specification requirements.
- Incorporation of design considerations, including statutory and regulatory constraints (see CH 3–4.3, 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 set of performance requirements by defining the functional boundaries of the system in terms of the 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 CH 3–4.2.6, Verification Process and CH 3–4.2.7, 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
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 CH 3–4.1.4, Requirements Management Process and CH 3–4.1.6, Configuration Management Process, respectively).

**CH 3–4.2.3 Architecture Design Process**

The Architecture Design process is a trade and synthesis method to allow the Program Manager (PM) and Systems 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 key 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 key system aspects and attributes such as reliability, maintainability, survivability, sustainability, performance and total ownership cost.

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) 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 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 (see the DoD CIO DoDAF page for additional information).

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, Work Breakdown Structures (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 key 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. 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.

**CH 3–4.2.4 Implementation Process**

The Implementation process is comprised 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 Analysis of Alternatives 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 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 technical data package.
- 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 ESOH, security, and privacy.
- Determining system elements functionality against specified product quality characteristics.
- Document fabrication and production 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.

CH 3–4.2.5 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 Program Manager (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 of integration 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 Systems Engineering Plan (SEP). The SEP Outline requires that all programs with external dependencies and/or interfaces establish Memoranda of Agreement (MOA) in order to formally establish
commitments and management procedures. A current table showing the status of all MOAs is mandated as part of the program SEP, which is updated in each phase.

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

CH 3–4.2.6 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 a key 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 Program Manager (PM) and Systems 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 CH 8–3.3. and in DoDI 5000.02, Enc 5, sec. 11.a.

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.

Verification may be accomplished by 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.

Designs are verified 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.

Verification activities and results are documented among the artifacts for Functional Configuration Audits (FCA) and the System Verification Review (SVR) (see CH 3–3.3.6, System Verification Review/Functional Configuration Audit). When possible, verification should stress the system, or system elements, under realistic conditions representative of its intended use.

The individual system elements provided by the Implementation process are verified through developmental test and evaluation (DT&E), acceptance testing or qualification testing. During the Integration process, the successively higher-level system elements may be verified 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, each change should be assessed 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 (IOT&E). The SVR provides a determination of the extent to which the system meets the system performance specification.

**CH 3–4.2.7 Validation Process**
The Validation process provides the objective evidence that the capability provided by the system 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 Program Manager (PM) and Systems Engineer support the Validation process. The Chief Developmental Tester is responsible for the execution of the Validation process, which is typically conducted by independent testers as documented in the Test and Evaluation Master Plan (TEMP) (See CH 8–3.6). System end users and other stakeholders are typically involved in validation activities. Guidance for managing and coordinating integrated testing activities can be found in CH 8–3.3. and DoDI 5000.02, Enc 5, sec. 11.a. 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 Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP), system performance specifications, use cases, functional and physical system architectures and test cases. Validation is applied 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 CH 3–4.2.6. 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 ultimately improves system performance during the final validation activity (e.g., operational test and evaluation (OT&E)) (See CH 8–3.2.)

Final validation involves operational testing on a production-representative system in an operationally realistic environment (See CH 8–3.2.1.) The product of the Validation process is a validated system and enabling system elements, leading to approval for Full-Rate Production (FRP) and/or a Full Deployment (FD) Decision Review (DR).

**CH 3–4.2.8 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 end-item system may need to be integrated with other systems in the operational environment, honoring the defined external interfaces. In this case, the Transition process needs to be performed 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, 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 and/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. The DoDI 5000.02, Enc 6, sec. 3 requires that 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 Full-Rate Production Decision Review (FRP DR).

The Program Manager (PM), Systems Engineer, and Product Support Manager 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.

**CH 3–4.3 Design Considerations**

The Program Manager (PM) and Systems Engineer should consider and document all statutory and regulatory requirements, as well as other design considerations, 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 and Systems 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 a discrete item to investigate during the design process, 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 and Systems Engineer should consider them in conjunction with one another, as early as the Analysis of Alternatives, to achieve better mission performance and to preclude a stovepipe view during design.

The design considerations listed in Table 42 should be assessed for applicability to the system, as they may not all be appropriate. Table 42 lists the statutory requirements for the design considerations covered in this chapter, as well as applicable policy and guidance related to those design considerations. See the DAG Chapter 3 Design Considerations Standards supplemental guidance for a partial list of government and Department of Defense (DoD) adopted non-government standards relevant to the design considerations listed in Table 42. Program Managers and Systems Engineers can incorporate the standards into acquisition contracts to support delivery of required operational capability. It is important to note the supplemental guidance contains several mandatory standards.

Table 42 is not all inclusive; it does not include any 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 42: Design Considerations**

<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Section Number</th>
<th>Statutory Requirement</th>
<th>Policy &amp; Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility (Section 508 Compliance)</td>
<td>4.3.1</td>
<td>• Section 508 of the Rehabilitation Act (i.e., 29 U.S.C. 794d)</td>
<td>• DoDD 8000.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DoDI 5000.02, Enclosure 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DoD 8400.01-M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• FAR 39.204</td>
</tr>
<tr>
<td>Affordability - SE Trade-Off Analysis</td>
<td>4.3.2</td>
<td></td>
<td>• DoDI 5000.02, Enclosures 1, 2, 3, and 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Capabilities through Technical Excellence and Innovation,” April 9, 2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• USD(AT&amp;L) memorandum, “Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Productivity in Defense Spending,” November 13, 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• USD(AT&amp;L) memorandum, “Better Buying Power: Guidance for Obtaining Greater Efficiency and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Productivity in Defense Spending,” September 14, 2010</td>
</tr>
<tr>
<td>Anti-Counterfeiting</td>
<td>4.3.3</td>
<td>• P.L. 112-81 (SEC 818)</td>
<td>• DoDI 4140.67</td>
</tr>
<tr>
<td>Commercial-Off-the-Shelf (COTS)</td>
<td>4.3.4</td>
<td>• 41 USC 104 and 1907</td>
<td>• SD-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• P.L. 103-355 (SEC 8104)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• P.L. 104-106 (SEC 357)</td>
<td></td>
</tr>
<tr>
<td>Corrosion Prevention and Control (CPC)</td>
<td>4.3.5</td>
<td></td>
<td>• DoDD 5000.01, Enclosure 1, paragraph E1.1.17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DoDI 5000.02, Enclosures 1 and 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DoDI 5000.67</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DoD Corrosion Prevention and Control Planning Guidebook</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DFARS 223.73</td>
</tr>
<tr>
<td>Design Consideration</td>
<td>Section Number</td>
<td>Statutory Requirement</td>
<td>Policy &amp; Guidance</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Critical Safety Item (CSI) | 4.3.6 | - P.L. 108-136 (SEC 802)  
- P.L. 109-364 (SEC 130)  
- 10 USC 2319 | - DoDM 4140.01, Encl. 11  
- JACG Aviation CSI Management Handbook  
- SECNAVINST 4140.2  
- AFI 20-106  
- DA Pam 95-9  
- DALI 3200.4  
- DCMA INST CSI (AV) Management of Aviation Critical Safety Items  
- DFARS 209.270, 246.407, 246.504, 246.371 and 252.246-7003 |
| Demilitarization and Disposal | 4.3.7 | | - DoDI 4160.28, Volume 1  
- DoDI 5000.02 Procedures and Encl. 6 and 13  
- DoDM 4140.01, Encl. 6  
- DoDM 4160.21, Volume 1 |
| Diminishing Manufacturing Sources and Material Shortages (DMSMS) | 4.3.8 | | - SD-22 |
| Environment, Safety and Occupational Health (ESOH) | 4.3.9 | - 42 USC 4321  
- EO 12114 | - DoDI 5000.02, Encl. 1, 3, 6, 7, and 13  
- DoDD 4715.21  
- DFARS 223.73  
- FAR 23.2, 23.4, 23.7 and 23.8 |
| Human Systems Integration (HSI) | 4.3.10 | | - DoDD 5000.01, Encl. 1, para E1.1.29  
- DoDI 5000.02, Encl. 7 |
| Insensitive Munitions | 4.3.11 | - 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 forInsensitive Munitions, Revision 02, November 2008 |
| Intelligence (Life-cycle Mission Data Plan (LMDP)) | 4.3.12 | | - DoDD 5250.01  
- DoDI 5000.02, Encl. 1 |
<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Section Number</th>
<th>Statutory Requirement</th>
<th>Policy &amp; Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interoperability and Dependency (I&amp;D)</td>
<td>4.3.13</td>
<td>44 USC 3506</td>
<td>• DoDD 4630.05&lt;br&gt;• DoDD 5000.01&lt;br&gt;• DoDI 2010.06&lt;br&gt;• DoDI 4630.8&lt;br&gt;• DoDI 5000.02&lt;br&gt;• CJCSI 3170.01&lt;br&gt;• JCIDS Manual</td>
</tr>
<tr>
<td>Item Unique Identification (IUID)</td>
<td>4.3.14</td>
<td></td>
<td>• DoDD 8320.03&lt;br&gt;• DoDI 4151.19&lt;br&gt;• DoDI 5000.02, Encl. 1 and 3&lt;br&gt;• DoDI 5000.64&lt;br&gt;• DoDI 8320.04&lt;br&gt;• DoD Guide to Uniquely Identifying Items, Version 2.5, September 15, 2012&lt;br&gt;• DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements, April 20, 2007&lt;br&gt;• DFARS 211.274-2, 252.211-7003, 252.211-7007</td>
</tr>
<tr>
<td>Operational Energy</td>
<td>4.3.16</td>
<td>10 USC 138c</td>
<td>• CJCSI 3170.01&lt;br&gt;• JCIDS Manual</td>
</tr>
<tr>
<td>Packaging, Handling, Storage and Transportation (PHS&amp;T)</td>
<td>4.3.17</td>
<td>49 CFR Parts 171-180</td>
<td>• DoDI 4540.07&lt;br&gt;• DoD 4145.19-R&lt;br&gt;• DoD 4140.27-M&lt;br&gt;• DTR 4500.9-R</td>
</tr>
<tr>
<td>Producibility, Quality &amp; Manufacturing (PQM)</td>
<td>4.3.18</td>
<td>P.L. 111-383 (SEC 812)</td>
<td>• DoDD 5000.02, Encl. 3&lt;br&gt;• DFARS 207.105, 215.304</td>
</tr>
<tr>
<td>Design Consideration</td>
<td>Section Number</td>
<td>Statutory Requirement</td>
<td>Policy &amp; Guidance</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Engineering</td>
<td></td>
<td>47 USC 305, 47 USC 901 - 904, P.L. 102-538 (SEC 104)</td>
<td>DoDi 3222.03, DoDi 4650.01, DoDi 5000.02, Encl. 1 and 3, AR 5-12, AFI 33-118, SECNAVINST 2400.1 and 2400.2, OPNAVINST 2400.20</td>
</tr>
<tr>
<td>Spectrum Management</td>
<td>4.3.20</td>
<td>10 USC 2451-2457, P.L. 82-436</td>
<td>DoDi 4120.24, DoDM 4120.24, SD-19</td>
</tr>
<tr>
<td>Standardization</td>
<td>4.3.21</td>
<td>P.L. 108-375 (SEC 1053)</td>
<td>DoDi 3150.09, DoDi 5000.02, Encl. 4, and 5</td>
</tr>
<tr>
<td>Supportability</td>
<td>4.3.22</td>
<td>10 USC 2358</td>
<td>DoDi 5000.02, Encl. 1, 3, and 11, DoDi 5200.39, DoDi 5200.44, DoDi O-5240.24, DoDi 8500 Series, DoDi 8582.01, Program Protection Plan Outline and Guidance, Version 1.0, July 2011</td>
</tr>
<tr>
<td>Survivability (including CBRN) &amp; Susceptibility</td>
<td>4.3.23</td>
<td>P.L. 108-375 (SEC 1053)</td>
<td>DoDi 5000.02, Encl. 1, 3, and 11, DoDi 5200.39, DoDi 5200.44, DoDi O-5240.24, DoDi 8500 Series, DoDi 8582.01, Program Protection Plan Outline and Guidance, Version 1.0, July 2011</td>
</tr>
<tr>
<td>System Security Engineering (SSE)</td>
<td>4.3.24</td>
<td>10 USC 2358</td>
<td>DoDi 5000.02, Encl. 1, 3, and 11, DoDi 5200.39, DoDi 5200.44, DoDi O-5240.24, DoDi 8500 Series, DoDi 8582.01, Program Protection Plan Outline and Guidance, Version 1.0, July 2011</td>
</tr>
</tbody>
</table>

**CH 3–4.3.1 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 clearly stated in the Acquisition Strategy and Systems Engineering Plan.

Program Managers (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 43. Additional information on accessibility is found in DoDI 5000.02, Enc 11, sec. 14; DAG Chapter 5 Manpower Planning & Human Systems Integration; and Chapter 6 Acquiring Information Technology and Business Systems.

Table 43: Links to Section 508 Government Resources

<table>
<thead>
<tr>
<th>Description of Link</th>
<th>Active Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 508 technical standards</td>
<td><a href="http://www.access-board.gov/508.htm">http://www.access-board.gov/508.htm</a></td>
</tr>
<tr>
<td>Federal rules for Section 508 implementation hosted by GSA has:</td>
<td><a href="https://www.section508.gov/">https://www.section508.gov/</a></td>
</tr>
<tr>
<td>- Roles and responsibilities of procurement officials and engineers</td>
<td></td>
</tr>
<tr>
<td>- 508 best practices</td>
<td></td>
</tr>
<tr>
<td>- Products and techniques</td>
<td></td>
</tr>
<tr>
<td>The &quot;Buy Accessible System&quot; GSA site has free tools and guides for conduct of Section 508-compliant acquisitions as well as on-line training and help desk</td>
<td><a href="https://www.buyaccessible.gov/">https://www.buyaccessible.gov/</a></td>
</tr>
<tr>
<td>Department of Health and Human Services has:</td>
<td><a href="http://www.hhs.gov/">http://www.hhs.gov/</a> found by searching on &quot;section 508“</td>
</tr>
<tr>
<td>- Check lists</td>
<td></td>
</tr>
<tr>
<td>- Code library</td>
<td></td>
</tr>
<tr>
<td>- Test tools</td>
<td></td>
</tr>
<tr>
<td>Department of Justice home page for ADA has federal laws and pending legislation</td>
<td><a href="https://www.ada.gov/">https://www.ada.gov/</a></td>
</tr>
<tr>
<td>Department of Veteran Affairs reports on Section 508 products and tools and tracks user comments</td>
<td><a href="http://www.section508.va.gov/">http://www.section508.va.gov/</a></td>
</tr>
</tbody>
</table>

CH 3–4.3.2 Affordability -- Systems Engineering Trade-Off Analyses

Affordability is the degree to which the capability benefits are worth the system’s total life-cycle cost and support DoD strategic goals. Systems engineering (SE) trade-off analyses for affordability, a special application of the Decision Analysis process (see CH 3–4.1.2) should:

- Support the establishment of realistic affordability caps as documented in the program’s Acquisition Program Baseline (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.

DoDi 5000.02, Enc 8, sec. 3.e requires the Milestone Decision Authority (MDA) to establish tentative cost and inventory goals at Materiel Development Decision (MDD) and affordability goals at Milestone A to inform early requirements and design trade-offs. Affordability caps are set at the Development RFP Release Decision, Milestone B, and beyond for unit procurement and sustainment costs. According to DoDi 5000.02, Enc 8, sec. 3.e, affordability caps are established as fixed-cost requirements equivalent to Key Performance Parameters (KPP).
The affordability goal forms the basis for the SE trade-off and sensitivity analyses conducted to ensure that requirements are affordable and technically feasible, and to inform the validation of the Capability Development Document (or equivalent requirements document) from an affordability standpoint. SE trade-off analyses also support the establishment of affordability caps at the Development RFP Release Decision, Milestone B, and subsequent reviews. The affordability goal is nominally the average unit acquisition cost and average annual operations and support cost per unit. For indefinite quantity of production units, the affordability goal may be the total acquisition cost (see CH 1–4.2.15, and DoDI 5000.02, Enc 8, for more information regarding the affordability goal/cap).

The independently generated will-cost estimate is used to defend the program budget but does not account for potential efficiencies. The should-cost target is based on the efficient use of resources and effective implementation of processes identified as should-cost initiatives, and is the focus of SE activities and program management decisions across the life cycle. Should-cost management is implemented in all acquisition programs (all ACATs) regardless of the life-cycle phase in accordance with DoDI 5000.02, Enc 2, sec. 6.e.

The SE trade-offs are conducted among cost, schedule and performance objectives to ensure the program is affordable. The Program Manager (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 and Systems 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; subject matter experts 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 (should-cost initiatives), and conducts SE trade-off analyses as needed to meet program cost, schedule and performance requirements.

**CH 3–4.3.3 Anti-Counterfeiting**

An increasing threat of counterfeit (and fraudulent) parts in the global marketplace affects every component of the program from commercial-off-the-shelf (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) and/or malicious intent. Counterfeits may appear at all phases of the life cycle, making it necessary for the Program Manager (PM), Systems Engineer, and Product Support Manager 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 44, with many of the other design considerations outlined in CH 3–4.3, Design Considerations, such as:

<p>| Table 44: Anti-Counterfeit Design Considerations Relationships |</p>
<table>
<thead>
<tr>
<th>Design Consideration</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commercial-Off-the-Shelf (COTS)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Corrosion Prevention and Control (CPC)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Critical Safety Items (CSI)</strong></td>
<td>From an anti-counterfeiting risk-based approach, CSIs should be more carefully scrutinized to ensure no counterfeits infiltrate the supply chain.</td>
</tr>
<tr>
<td><strong>Demilitarization and Disposal</strong></td>
<td>An excellent source for counterfeiters to obtain parts that can be turned into “used sold as new” parts (fraudulently certified as new).</td>
</tr>
<tr>
<td><strong>Diminishing Manufacturing Sources and Material Shortages (DMSMS)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Environment, Safety and Occupational Health (ESOH)</strong></td>
<td>Several examples of counterfeit materials that can increase ESOH risks include: false R-134, a refrigerant which 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.</td>
</tr>
<tr>
<td><strong>Item Unique Identification (IUID)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Modular Open Systems Approach (MOSA)</strong></td>
<td>MOSA could provide a means to quickly certify a newer, more available part for use in weapon 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.</td>
</tr>
<tr>
<td><strong>Producibility, Quality and Manufacturing (PQM)</strong></td>
<td>PQM can be severely degraded if supply is contaminated with counterfeits.</td>
</tr>
<tr>
<td><strong>Reliability and Maintainability Engineering</strong></td>
<td>Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the “honest” part.</td>
</tr>
<tr>
<td><strong>Supportability</strong></td>
<td>Increased failure rates due to counterfeits can have a negative impact on supportability and might drive the wrong problem-resolution behaviors and increase sustainment costs.</td>
</tr>
<tr>
<td><strong>System Security Engineering (SSE)</strong></td>
<td>SSE implements anti-counterfeiting protection measures as part of a comprehensive plan to protect CPI and mission-critical functions and components (See DAG Chapter 9).</td>
</tr>
</tbody>
</table>

During development of the Systems Engineering Plan (SEP) and Program Protection Plan (PPP), the PM, Systems Engineer and Product Support Manager should consider these relationships and develop plans to address the threat.
CH 3–4.3.4 Commercial-Off-the-Shelf

The use of commercial-off-the-shelf (COTS) items, including Non-Developmental Items, 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 Program Manager (PM) and Systems 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; Environment, Safety and Occupational Health (ESOH); reliability; and durability.
- If integration requires a "modified COTS product," meaning that 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 very 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.
- Difficulty in finding suitable replacements and/or alternate items if the COTS vendor stops manufacturing the product or changes the configuration drastically, requiring the need to maintain different configurations of a single product.
- The program needs to understand the "pedigree" of the qualified vendors for the COTS product.
- The graphical user interface (GUI) design may not completely support user tasks, which can cause inefficient workarounds and improper use of the system by the user.

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 and/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 ESOH and security risks, survivable technology insertion, or refresh throughout the projected system life cycle.

The PM and Systems 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, Human System Integration, ESOH, hardware/software integrity, reliability risk, program protection and corrosion susceptibility/risk
- Planning for life-cycle activities (including sustainment, supply chain risks, obsolescence, 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
- Test and evaluation of COTS items (including early identification of screening, functionality testing and usability assessments) (See CH 8–2.1.)
- 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 (IP) 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 and/or test aspects of COTS products

CH 3–4.3.5 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 Environment, Safety and Occupational Health (ESOH) factors. Therefore, acquisition officials should fully consider corrosion prevention and mitigation as early as possible in the acquisition life cycle (even prior to Milestone A), and 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 Program Managers (PMs), Systems Engineers, Product Support Managers and other program staff develop and execute a comprehensive CPC approach.

DoDI 5000.02, DoDI 5000.67 and DoDD 4151.18 require CPC planning and execution for all acquisition programs across the life cycle. In accordance with DoDI 5000.02, Enc 3, sec. 15, the PM is responsible for identifying and evaluating corrosion considerations throughout the acquisition and sustainment phases to reduce, control or mitigate corrosion. The PM and Systems Engineer should conduct CPC planning, ensure corrosion control requirements are included in the system design and verified as part of test and acceptance programs and include CPC management and design considerations in the Systems Engineering Plan (SEP) and Life-Cycle Sustainment Plan (LCSP). DoDI 5000.02, Enc 6, sec. 2 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, to include facilities (see DAG Chapter 4).
• Identifying planning, resourcing and acquisition of corrosion-related features for longevity, lowest total ownership cost (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. For Major Automated Information System (MAIS) programs, the extent of CPC planning and the breadth of documentation should consider the type of system and correlate the system’s corrosion risk to mission criticality and the harshness of the operational environment. 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:

• Acquisition Strategy (AS)
• Test and Evaluation Master Plan (TEMP)
• Request for Proposal (RFP) and contract
• Program schedule -- Integrated Master Plan/Integrated Master Schedule (IMP/IMS)
• Funding/budget
• Programmatic ESOH Evaluation (i.e., DFARS (Subpart 223.73, Minimizing the Use of Hexavalent Chromium))
• System finish/process specification (add to the Statement of Work (SOW) and as a Data Item Description (DID) to the Contract Data Requirements List (CDRL))
• Contractor Corrosion Prevention and Control Plan (add to the SOW/Statement of Objectives (SOO)/Performance Work Statement (PWS) 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 CH 3–2.7, Systems Engineering Role in Contracting and the DoD Corrosion Prevention and Control Planning Guidebook for MS&E).

CH 3–4.3.6 Critical Safety Item
A Critical Safety Item (CSI) is a part, assembly or 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 Program Managers (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 specific 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 (CSIs) Management Handbook_. This guidance establishes standard user-level operating practices for aviation CSIs across the Services, the Defense Logistics Agency (DLA), the Defense Contract Management Agency (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 and/or revised to address ship CSIs as defined by public law.

The Defense Federal Acquisition Regulation Supplement (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 that 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 Operations and Support (O&S) phase. The PM should ensure that the allocated baseline established at the Preliminary Design Review (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. Prior to the Critical Design Review (CDR), the program office, with support from the DCA and developer/OEM contractors, should ensure there is a clear understanding of CSI processes, terms and criteria. The initial product baseline, established at CDR, should have 100% of
drawings completed for the CSIs. Throughout Low-Rate Initial Production (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 Full-Rate Production/Full Deployment Decision Review (FRP/FD DR), a final CSI list should be documented and approved by the DCA.

CH 3–4.3.7 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

Program Managers (PMs) and Product Support Managers should ensure, as an essential part of systems engineering, that DEMIL and disposal requirements are incorporated in system design to minimize DoD’s liabilities, reduce costs and protect critical program information and technology. This includes integrating DEMIL and disposal into the allocated baseline approved at the Preliminary Design Review (PDR) and refining DEMIL and disposal requirements in the initial product baseline at the Critical Design Review (CDR). DEMIL and disposal requirements are included in the program’s Systems Engineering Plan (SEP), Life-Cycle Sustainment Plan (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 or disruption. 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 DoDM 4140.01, Volume 6 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 Environment, Safety and Occupational Health (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.

CH 3–4.3.8 Diminishing Manufacturing Sources and Material Shortages
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 weapon 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 Program Manager (PM) should incorporate a technology management strategy into design activities as a best practice to reduce DMSMS cost and readiness impacts throughout the life cycle. The PM and Systems Engineer should develop a technology management strategy for maintaining insight into technology trends and internal product changes by the manufacturer, and testing the effects of those changes on the system when necessary. This insight into technology trends could potentially:

- Result in seamless upgrade paths for technologies and system elements.
- Provide a timetable for replacing system elements even if they are not obsolete.

The Systems Engineer should be aware of and consider DMSMS management during system design. Following are several practices that the program should consider to minimize DMSMS risk throughout the life cycle of the system:

- 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 Modular Open Systems Approach (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 (GIDEP), 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 part obsolescence due to DMSMS.

A useful resource for additional guidance is SD-22 (Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook).

**CH 3–4.3.9 Environment, Safety and Occupational Health**

Environment, Safety and Occupational Health (ESOH) analyses are an integral, ongoing part of the systems engineering (SE) process throughout the life cycle. The benefits of early integration of ESOH considerations include:

- Mitigation of program cost and schedule risks from actions that cause damage to people, equipment or the environment.
- Reduction of Operations and Support and disposal costs to achieve system affordability.
- Provision of a safe, suitable, supportable and sustainable capability able to operate world-wide, including opportunities for Foreign Military Sales.

Throughout each acquisition phase, programs conduct their ESOH analyses to:

- Identify and mitigate potential risks to the system and its associated personnel.
- Manage ESOH design considerations from the beginning of the SE effort.
- Plan for compliance with 42 USC 4321, National Environmental Policy Act (NEPA), and Executive Order (EO) 12114, Environmental Effects Abroad of Major Federal Actions.
- Ensure compliance with statutory ESOH requirements.

**ESOH in Systems Engineering**
**DoDI 5000.02, Enc 3, sec. 16** requires programs to use the system safety 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 Milestone A SEP to cover Technology Maturation and Risk Reduction (TMRR) activities and continues throughout the system’s life cycle.

DoD defines ESOH in **MIL-STD-882 (System Safety)** 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 system safety methodology for the identification, documentation and management of ESOH hazards and their associated risks during the system’s development and sustainment. The Program Manager, with support from the Systems Engineer, eliminates hazards where possible, and manages ESOH risks where hazards cannot be eliminated. MIL-STD-882 provides a matrix and defines probability and severity criteria to categorize ESOH risks.

MIL-STD-882 provides a structured, yet flexible, framework for hazard analysis and risk assessment for a specific system application (including system hardware and software). As an example for software, Subject Matter Experts (SMEs) use the MIL-STD 882 process for assessing the software contribution to system risk, which considers the potential risk severity and degree of control the software exercises over the hardware, and dictates the analysis level of rigor needed to reduce the risk level. The Joint Services Software Safety Authorities’ “Software System Safety Implementation Process and Tasks Supporting MIL-STD-882” is a concise “Implementation Guide” to assist in the implementation of the software system safety requirements and guidance contained in MIL-STD-882 and the Joint Software System Safety Engineering Handbook (JSSSEH) process descriptions complement MIL-STD-882 for these analyses.

The PM and Systems Engineer should also identify and integrate ESOH requirements into the SE process. Examples of this include, but are not limited to, the following:

- Complying with NEPA, EO 12114, and applicable environmental quality requirements, which will require assessing the system’s operation and maintenance pollutant emissions.
- Obtaining required design certifications, such as Airworthiness for air systems.
- Prohibiting or strictly controlling the use of banned or restricted hazardous materials, such as hexavalent chrome and ozone-depleting substances.

The PM and the Systems Engineer ensure ESOH is addressed during the Technology Maturation and Risk Reduction (TMRR) phase by including their ESOH plans in the Milestone A SEP. This is critical because the program conducts most of their developmental testing and finalizes a significant portion of the system design during TMRR. During TMRR, the ESOH SME can provide the most cost-effective ESOH support to the program by identifying and then eliminating or mitigating ESOH hazards and ensuring ESOH compliance during system testing and design development.

At Milestone B, the Systems Engineer and their ESOH SMEs document the results of their TMRR ESOH activities in the Programmatic ESOH Evaluation (PESHE) and their NEPA/EO 12114 Compliance Schedule. The PESHE consists of the ESOH hazard data, hazardous materials management data and any additional ESOH compliance information required to support analyses at test, training, fielding and disposal sites.

Finally, properly integrating ESOH in SE requires addressing the following key areas:

- Programs should integrate ESOH and system safety activities by incorporating various functional disciplines such as system safety engineers, fire protection engineers, occupational health professionals and environmental engineers to identify hazards and mitigate risks through the SE process.
- Programs should document ESOH management planning in the SEP, not the PESHE. The PESHE should document data generated by ESOH analyses conducted in support of program execution.
• 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 ESOH risks) or to add hazards.

ESOH System Design Requirements

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

ESOH in Program Documents

Together the Systems Engineer and their ESOH SMEs use the SEP to document the program's plan to integrate ESOH into the SE process, incorporating ESOH as a mandatory design, test, sustainment and disposal consideration. They use the Programmatic ESOH Evaluation (PESHE) and the NEPA/EO 12114 Compliance Schedule to document the results of the program’s implementation of their ESOH planning. This approach segments required ESOH information across the SEP, PESHE and NEPA/EO 12114 Compliance Schedule to avoid duplication and enhance ESOH integration.

The SEP should include the ESOH management planning information listed in Table 45.

Table 45: ESOH Information in SEP

<table>
<thead>
<tr>
<th>Column Heading in SEP Table 4.6-1</th>
<th>Expected Information (provided or attached)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognizant PMO Organization</td>
<td>Organizational structure for integrating ESOH (or refer to Table 3.4.4-2 if it includes the ESOH team details) and the Program Office ESOH point of contact</td>
</tr>
<tr>
<td>Certification</td>
<td>Required ESOH approvals, endorsements, releases, and the designated high and serious risk acceptance user representative(s)</td>
</tr>
<tr>
<td>Documentation</td>
<td>PESHE and NEPA/EO 12114 Compliance Schedule</td>
</tr>
<tr>
<td>Contractual Requirements (CDRL#)</td>
<td>ESOH contractual language, ESOH Contract Data Requirements List (CDRL) items, and ESOH DFARS clauses</td>
</tr>
<tr>
<td>Description / Comments</td>
<td>Description of how design minimizes ESOH risks by summarizing how the program has integrated ESOH considerations into SE processes including the method for tracking hazards and ESOH risks and mitigation plans throughout the life cycle of system</td>
</tr>
</tbody>
</table>

The Systems Engineer and ESOH SMEs also provide input to other program documentation such as the: Acquisition Strategy (AS), Test and Evaluation Master Plan (TEMP), Life-Cycle Sustainment Plan (LCSP), system performance specifications, solicitations, contracts and capability documents.

As the repository for ESOH data and information, the PESHE includes, but is not limited to:

• ESOH 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 PESHE.)

• The following data for each hazard: Hazard Tracking System (HTS) identification number; identified hazards (to include descriptions); associated mishaps (potential mishaps resulting from the hazard); risk assessments (to include the initial, target, and event(s) Risk Assessment Codes (RACs) and risk levels); identified risk mitigation measures; selected (and funded) mitigation measures; hazard status (current RAC and risk level based on any mitigation 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 to include the names of the risk acceptance authority and user representative(s); and dates of risk acceptance and user concurrence(s). (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, 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. (NOTE: 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.

**NOTE:** Programs should use the results of the sustainability analysis (see CH 3–2.4.3, Sustainability Analysis) to inform the hazard analysis.

**DoDI 5000.02, Enc 3, sec. 16** 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 Office's Integrated Master Schedule (IMS) and Integrated Master Plan (IMP).

Because actions occurring during the TMRR phase may require NEPA/EO 12114 compliance, the program should identify these compliance requirements in the Milestone A SEP. **DoDI 5000.02, Enc 3, sec. 16** also requires programs to support other organizations NEPA/EO 12114 analyses involving their systems.

**ESOH Activities by Phase**

Table 46 aligns typical ESOH activities by phase.

**Table 46: ESOH Activities by Phase**

<table>
<thead>
<tr>
<th>Acquisition Phase</th>
<th>Typical ESOH Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materiel Solution Analysis (MSA)</td>
<td>• Participate in Analysis of Alternatives (AoA)</td>
</tr>
<tr>
<td></td>
<td>• Provide inputs to the SEP, draft Capability Development Document (CDD), Corrosion</td>
</tr>
<tr>
<td></td>
<td>Prevention and Control (CPC) Planning, AS, Life-Cycle Sustainment Plan (LCSP) and draft</td>
</tr>
<tr>
<td></td>
<td>Request for Proposal (RFP)</td>
</tr>
<tr>
<td>Technology Maturation and Risk Reduction</td>
<td>• Participate in prototyping and design development through the Integrated Product</td>
</tr>
<tr>
<td>(TMRR)</td>
<td>Team (IPT) structure to identify and mitigate ESOH risks in the product to be</td>
</tr>
<tr>
<td></td>
<td>developed in the next phase</td>
</tr>
<tr>
<td></td>
<td>• Prepare initial PESHE and NEPA/EO 12114 Compliance Schedule</td>
</tr>
<tr>
<td></td>
<td>• Ensure NEPA/EO 12114 compliance, ESOH risk acceptance, Preliminary Design Review (PDR)</td>
</tr>
<tr>
<td></td>
<td>risk reporting, and safety releases</td>
</tr>
<tr>
<td></td>
<td>• Inputs to SEP, CPC Planning, final CDD, Test and Evaluation Master Plan (TEMP), LCSP,</td>
</tr>
<tr>
<td></td>
<td>and draft RFP</td>
</tr>
<tr>
<td>Acquisition Phase</td>
<td>Typical ESOH Activities</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Engineering and Manufacturing Development (EMD) | • Participate in trades and design development activities through the IPT structure  
• Evaluate Test and Evaluation (T&E) results, to include assessment of ESOH risk mitigations  
• Update NEPA/EO 12114 Compliance Schedule and PESHE; support NEPA/EO 12114 compliance activities, ESOH risk acceptance  
• Obtain required ESOH approvals, endorsements and releases; provide inputs to the SEP, CPC Planning, LCSP, Capability Production Document (CPD) and draft RFP |
| Production and Deployment (P&D)          | • Participate in initial Configuration Control Board (CCB) process  
• Evaluate T&E results, to include assessment of ESOH risk mitigations  
• Analyze deficiency reports  
• Review Physical Configuration Audit (PCA)  
• Update NEPA/EO 12114 Compliance Schedule and PESHE  
• Support NEPA/EO 12114 compliance activities and ESOH risk mitigations  
• Obtain required ESOH approvals, endorsements and releases  
• Support Initial Operational Capability (IOC) and Full Operational Capability (FOC)  
• Provide inputs to the LCSP, CPC Planning, and product support package |
| Operations and Support (O&S)             | • Participate in mishap investigations and the CCB process  
• Analyze system use data such as deficiency reports, hazard reports, regulatory violations, etc.  
• Keep the PESHE data current; support NEPA/EO 12114 compliance activities and ESOH risk acceptance  
• Provide inputs to draft Joint Capabilities Integration and Development System (JCIDS) documents and CPC Planning |

**ESOH Risk Management**

The PM is also responsible for ensuring the appropriate management level accepts ESOH risks prior to exposing people, equipment or the environment to those risks.

- High ESOH risks require Component Acquisition Executive (CAE) acceptance
- Serious ESOH risks require Program Executive Officer (PEO)-level acceptance
- Medium and Low ESOH risks require PM acceptance

Any time a risk level increases the PM should ensure the appropriate management level accepts the new risk level prior to exposing people, equipment or the environment to the new risk level. This means a given ESOH 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 mitigations.
- During testing, the risk level may change due to 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.
The Systems Engineer, in support of the PM, uses the MIL-STD-882 methodology to manage ESOH risks. DoDI 5000.02, Enc 3, sec. 16 identifies the appropriate management level authorized to accept ESOH risks. Before accepting a risk, the appropriate acceptance authority requires user representative concurrence from the DoD Component(s) responsible for the personnel, equipment or environment exposed to the risk.

For joint programs, the ESOH risk acceptance authorities reside within the lead DoD Component (unless the Milestone Decision Authority (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 memorandum of agreement (MOA) to document risk acceptance authority and user representative offices, they should attach the MOA to the PESHE.

The program documents formal risk acceptances as part of the program record (e.g., Hazard Tracking System). If a risk level increases for a hazard, a new risk acceptance is required prior to 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 5000.02, Enc 3, sec. 16 requires programs to report the status of current high and serious ESOH risks at program reviews and fielding decisions and the status of all ESOH risks at technical reviews. The purpose of this reporting is to inform the MDA, PEO, PM and end user about trades being made and ESOH risks that need to be accepted. Each ESOH 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.

Hazardous Materials Management

When Hazardous Materials (HAZMAT) and chemicals/materials of evolving regulatory concern are designed into the system or used for system operation and maintenance, the Program Manager and Systems Engineer assess and document the ESOH 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 Aerospace Industries Association (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 Program Manager and Systems Engineer should document the following data elements for each listed HAZMAT:

- HAZMAT item or substance name (with Chemical Abstract Services (CAS) Number if available)
- HAZMAT Category (Prohibited, Restricted or Tracked)
- Special Material Content Code (SMCC) 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 (PPE) and storage requirements, to include provision of required Safety Data Sheets (SDSs), previously called Material Safety Data Sheets (MSDSs)

The Systems Engineer manages hexavalent chromium usage in systems to balance the requirements for corrosion prevention and control 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.

Safety Release for Testing

The PM, in concert with the user and the T&E community, provides safety releases (to include formal ESOH risk acceptance in accordance with DoDI 5000.02, Enc 3, sec. 16), 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.

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.

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

CH 3–4.3.10 Human Systems Integration

Systems engineering (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.

Throughout the acquisition life cycle, the Systems Engineer should apply Human Systems Integration (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 Program Manager (PM) has overall responsibility for integrating the HSI effort into the program. These responsibilities are described in DAG Chapter 5 Manpower Planning & Human Systems Integration.

The Systems Engineer supports the PM by leading HSI efforts. The Systems Engineer should work with the manpower, personnel, training, safety, health, habitability, personnel survivability and Human Factors Engineering (HFE) stakeholders to develop the HSI effort. The Systems Engineer translates and integrates those human capability considerations, as contained in the capabilities documents, into quantifiable system requirements. Requirements for conducting HSI efforts should be specified for inclusion in the Statement of Work and contract. HSI should also be addressed in the Systems Engineering Plan (SEP), specifications, Test and Evaluation Master Plan (TEMP), Software Development Plan (SDP), Life-Cycle Sustainment Plan (LCSP) and other appropriate program documentation. The SEP Outline requires that HSI be addressed as a design consideration.

Elements of an effective HSI effort, described in DAG Chapter 5 Manpower Planning & Human Systems Integration, should:

- Provide a better 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.
- 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.

CH 3–4.3.11 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 due to 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). In accordance with DoD 5000.01, Enc. 1 and DoDI 5000.02, Enc 3, sec. 17, the Program Manager (PM) and Systems 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 and Systems Engineer for munitions programs, regardless of ACAT level, should have safety as a top consideration when performing trade studies or making program decisions. The PM and cognizant technical staff should coordinate harmonized 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 ServicesInsensitive Munitions Technical Panel (JSIMTP), Joint Service Hazard classifiers and the DoD Explosives Safety Board (DDESB), 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), as required by USD(AT&L) memorandum, "Insensitive Munitions Strategic Plans," July 21, 2004, which establishes DoD policy for the annual submission of IMSPs to the Joint Requirements Oversight Council (JROC) and Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD(AT&L)), by the Program Executive Officer (PEO) for munitions programs. USD(AT&L) memorandum, "Joint Insensitive Munitions Test Standards and Compliance Assessment." February 10, 2010, establishes policy for oversight and compliance assessment. The DoD Standard Operating Procedure (SOP) 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.

CH 3–4.3.12 Intelligence (Life-Cycle Mission Data Plan)
In collaboration with the intelligence community and the operational sponsor(s), the Program Manager (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 support (see Figure 42 and DoD 5250.01.)

Modern weapon systems are inherently dependent on a variety of scientific and technical intelligence products throughout every stage of their life cycle. Hence, planning for intelligence Mission Data (IMD) support, which informs design and development trade-offs, risk assessments and decisions is essential to satisfying system requirements. Similarly, 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. See CH 7–4.1.4 for more information on CIPs.

Intelligence life-cycle mission data planning is necessary to effectively:

- Derive functional baseline requirements and life-cycle IMD requirements necessary to identify, define, and refine sensors, algorithms and intelligence data needs and trade-offs.
- Design, develop, test and evaluate IMD-dependent sensors, algorithms, systems, processes and interfaces.
- Conduct effectiveness analyses and risk assessments.
- Identify and acquire threat and target parameters that support digital modeling and simulation (see CH 3–2.4.2, Modeling and Simulation).
- Develop technical performance measures to inform test and evaluation.
- 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 42: Intelligence Mission Data (IMD) Life Cycle Timeline**

The initial Life-Cycle Mission Data Plan (LMDP) is due at Milestone A, with a draft update due at the Development RFP Release Decision Point and approval at Milestone B by the DoD Component (see DoDI 5000.02, Enc 1, Table 2). Additional updates to the LMDP are due at Milestone C and the Full Rate Production/Full Deployment Decision.

**CH 7–4.1.3** provides key linkages to the system performance specification (sometimes called the System Requirements Document (SRD)), Systems Engineering Plan (SEP) and Test and Evaluation Master Plan (TEMP). These three products are directly affected by IMD requirements.

**CH 3–4.3.13 Interoperability and Dependencies**

Almost all DoD systems operate in a system of systems (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 (see CH 3–3.1.2., Systems of Systems). These include, but are not limited to, physical requirements (e.g., size, power limits, etc.), electronic requirements (e.g., signature, interference, etc.) and information exchange/management (e.g., network, bandwidth, information needs, etc.). These system requirements also include interdependencies with other systems. For efficiency, systems often rely on either 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 CH 3–4.1.8. Interface Management Process) and is essential for the creation of systems of systems (SoS). Every system is required to be certified interoperable before it is fielded. The Joint Interoperability Test Command (JITC) 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/or coordination between separate programs. Two common ways to meet this need are memoranda of agreements (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 Program Manager (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 has the responsibility for ensuring all interoperability and dependency impacts are analyzed and collaborated 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 interoperability and dependencies (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 key 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. These contexts are analyzed 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, are directed at ensuring that systems work effectively with other systems:
Interoperability of information technology and National Security System (NSS) acquisition programs are required to comply with DoDI 8330.01, CJCSI 3170.01, the JCIDS Manual (requires Common Access Card (CAC) to access website), and 44 USC 3506.

DoDD 5000.01, Enc. 1:
- Ability of acquired systems to exchange information and services with other systems and to interoperate with other United States forces and coalition partners, and, as appropriate, with other United States Government departments and agencies.
- Providing systems and systems of systems that are interoperable and able to communicate across a universal infrastructure that includes organizational interactions, other systems, networks and information-exchange capabilities.

DoDI 5000.02: An integrated system design that defines system and system of systems functionality and interfaces, and reduces system-level risk.

DoDI 2010.06: Pursuing opportunities throughout the acquisition life cycle that enhance international cooperation and improve interoperability.

CH 3–4.3.14 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 both better weapon system reliability and readiness at reduced total ownership cost. IUID-enabled SIM provides DoD with a standard methodology to:
  - Consistently capture the value of all individual items it buys/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.

Program Managers (PMs) and Product Support Managers should budget, plan for and implement IUID-enabled SIM as an integral activity within MIL-STD-130 (Identification Marking of U.S. Military Property) requisites 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 DoDI 5000.02, Enc 1, Table 2. IUID-specific design considerations are required in the Systems Engineering Plan (SEP) and SIM planning and implementation required by DoDI 4151.19 are addressed in the Life-Cycle Sustainment Plan (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 Department of Defense (DoD) contractors and their suppliers, who put unique item identifier (UII) marks on new items during production, as directed in the contract.

CH 3–4.3.15 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. Designing for modularity is a key technical principle for implementing a modular open systems approach (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 systems, where modules can be decoupled, separated or even re-arranged. 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. It is important for the program management 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 five individually useful areas, which often overlap: cost savings/cost avoidance; increased competition; enhanced interoperability; application of innovative elements; and ability to realize technology upgrade opportunities easily.

Program Managers (PMs) should understand both the positive and negative outcomes from implementing a modular design and determine if the realization of a particular benefit outweighs the potential negative consequence. When scoping where the system should implement modular design, the PM and Systems Engineer should consider multiple factors, such as anticipated obsolescence, technical innovation, preplanned product improvements to meet performance, etc. These circumstances will vary across systems. System 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. (For additional details see CH 3–2.4.1. Modular Open Systems Approach.)

CH 3–4.3.16 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 systems engineering (SE) category is a significant change in practice and thinking that will help manage emerging operational challenges.

The Program Manager (PM) and Systems 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 Key Performance Parameter (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 Joint Capabilities Integration and Development System (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 and/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/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 Analysis of Alternatives (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 and Systems 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

NOTE: The results of the sustainability analysis (see CH 3–2.4.3, Sustainability Analysis) can be used to inform energy analyses.

**CH 3–4.3.17 Packaging, Handling, Storage and Transportation**

The program team employs Packaging, Handling, Storage and Transportation (PHS&T) principles/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, repairable 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.

Program Managers (PMs) and Systems Engineers should ensure PHS&T is addressed during the requirements analysis process, and validated throughout each phase of the systems engineering (SE) development of the weapon 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 weapon system delivery to the warfighter during low rate initial production. DoDI 4540.07 identifies specifics regarding PHS&T as related to systems engineering of weapon 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
- DTR 4500.9-R, Defense Transportation Regulation
- 49 CFR Parts 171-180, Transportation

**CH 3–4.3.18 Producibility, Quality and Manufacturing Readiness**

Producibility

Producibility is a design accomplishment for the relative ease of manufacturing. Like manufacturing and other key 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 Program Manager (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 measured. 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.

To assess producibility within a manufacturing enterprise level, the organization should evaluate producibility performance on a product-specific basis. This evaluation allows the organization to understand the strengths and weaknesses of its producibility approach better, so enhancements can be identified and measures of processes, products, and the producibility system (integrated processes and resources needed for achieving producibility) can be tailored to strive for continuous improvement.

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. Determine Process Capability:
   - Determine Process Capability (Cpk)
   - Understand and document company and supplier processes
   - Plan for future process capabilities

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 Preliminary Design Review (PDR), Critical Design Review (CDR), Production Readiness Review (PRR) and Full-Rate Production Design Review (FRP DR)
   - Optimize manufacturing plans as the design matures

5. Measure producibility processes, products and systems.

Producibility should be a Technical Performance Measure (TPM) for the program, and the program’s strategy for producibility should be contained in paragraph 3.6 of the program’s Systems Engineering Plan (SEP). Planned producibility engineering activities for previous and subsequent phases also should be summarized in the SEP. As a key design accomplishment, producibility should be included in the SEP, mapping key design considerations into the Request for Proposal (RFP) and subsequently into the contract.

Quality in Design

Design engineering focuses on concurrent development of the total system, using capable 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 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.

To ensure consistency in applying quality planning and process control, the program should establish a Quality Management System (QMS) early, ideally at Milestone A (See CH 1-4.2.19 for more information on Quality Management.) The QMS should be defined and documented in the Acquisition Strategy (AS). The process should be integrated into these documents as a systems engineering (SE) practice that supports the successful transition of capability development to full-rate production and delivery of systems to support warfighter missions.

The primary focus of the QMS should be to ensure efficiency in processes, and should be integrated with Statistical Process Control (SPC) to eliminate defects and control variation in production. The QMS should aid the transition from system development to production by controlling life-cycle cost and 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 PM and Systems 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. Data collection efforts should be continuously refined, using test articles, through production.

In addition to QMS and SPC, understanding and improving processes may require common and/or new tools and techniques to eliminate defects and variation in processes.

Another quality management tool available to the PM is parts management. MIL-STD-3018 (Parts Management) provides requirements for the implementation of an effective Parts Management Program (PMP) on DoD acquisitions.

Quality should be a TPM for the program, and the program’s strategy for managing quality should be included in the SEP. Planned quality engineering and management activities for previous and subsequent phases also should be summarized in the SEP. As a key design accomplishment, quality should be included in the SEP mapping key design considerations into contracts.

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

**Assessing Manufacturing Readiness and Risk**

PMs of programs with a manufacturing component should ensure contractors have a robust manufacturing management system. Planned manufacturing management activities for previous and subsequent phases also should be summarized in the SEP. As a key design accomplishment, efficient and cost-effective manufacturing should be included in the SEP, mapping key design considerations into contracts. The SAE AS6500, Manufacturing Management Program, contains best practices for a manufacturing management system, has been adopted for use by DoD and may be placed on contract with tailoring appropriate to the program's needs.
Manufacturing feasibility, processes and risk should be assessed early in the Materiel Solution Analysis (MSA) phase, and continuously through the Production and Deployment (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 system risk reduction, manufacturing process reliability and producibility.

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 5000.02, Enc 3, sec. 10, 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 manufacturing readiness assessments, 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:

- 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.
- Design: assess the maturity and stability of the evolving system design and evaluate any related impact on manufacturing readiness.
- Cost and Funding: examine the risk associated with reaching manufacturing cost targets.
- Materials: assess the risks associated with materials (including basic/raw materials, components, semi-finished parts and subassemblies).
- Process Capability and Control: assess the risks that the manufacturing processes are able to reflect the design intent (repeatability and affordability) of key characteristics.
- Quality Management: assess the risks and management efforts to control quality and foster continuous improvement.
- Manufacturing Workforce (Engineering and Production): assess the required skills, certification requirements, availability and required number of personnel to support the manufacturing effort.
- Facilities: assess the capabilities and capacity of key manufacturing facilities (prime, subcontractor, supplier, vendor and maintenance/repair)
- 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 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 and Systems Engineer 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 and Systems Engineer should assess manufacturing readiness during the acquisition life cycle, as described in Table 47.

Table 47: Manufacturing Readiness Assessment Points During the Acquisition Life Cycle

<table>
<thead>
<tr>
<th>Manufacturing Readiness Assessment Points</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| **1. Post-AoA assessment during the Materiel Solution Analysis Phase.** As part of the AoA, manufacturing risks should have been assessed for each of the competing alternatives (see the MRL Implementation 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 whether: | • Program critical technologies are ready for the Technology Maturation and Risk Reduction 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 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. Technology Maturation and Risk Reduction, Development RFP Release Decision.** As the program approaches the Development RFP Release Decision and the Milestone B decision, critical technologies should have matured sufficiently for 2366b certification and demonstrated in a relevant environment and should consider: | • The program should be nearing acceptance of a preliminary system design  
• 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 |
<table>
<thead>
<tr>
<th>Manufacturing Readiness Assessment Points</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Preliminary design, producibility assessments, and trade studies of key technologies and components should have been completed</td>
<td></td>
</tr>
<tr>
<td>• 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</td>
<td></td>
</tr>
<tr>
<td>• 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</td>
<td></td>
</tr>
<tr>
<td>• Producibility considerations should have shaped system development plans, and the Industrial Base Capabilities assessment (in the AS for Milestone B) has confirmed the viability of the supplier base</td>
<td></td>
</tr>
<tr>
<td>• The detailed system design is complete and stable to support low-rate initial production (LRIP)</td>
<td></td>
</tr>
<tr>
<td>• Technologies are mature and proven in a production environment, and manufacturing and quality processes are capable, in control and ready for low-rate production</td>
<td></td>
</tr>
<tr>
<td>• 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</td>
<td></td>
</tr>
<tr>
<td>• Cost and yield and rate analyses are updated with pilot line results</td>
<td></td>
</tr>
<tr>
<td>• Known producibility risks pose no significant challenges for low-rate production</td>
<td></td>
</tr>
<tr>
<td>• Supplier qualification testing and first article inspections have been completed</td>
<td></td>
</tr>
<tr>
<td>• Industrial base capabilities assessment for Milestone C has been completed and shows that the supply chain is adequate to support LRIP</td>
<td></td>
</tr>
</tbody>
</table>

3. Production Readiness Review. A production readiness review identifies the risks of transitioning from development to production. Manufacturing is a function of production; in order to transition to production without significant risk it is important that key processes have been considered and evaluated during the PRR, such as ensuring:

<table>
<thead>
<tr>
<th>4. Full Rate Production (FRP) Decision Review</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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):</td>
<td></td>
</tr>
<tr>
<td>• LRIP learning curves that include tested and applied continuous improvements</td>
<td></td>
</tr>
<tr>
<td>• Meeting all systems engineering and design requirements</td>
<td></td>
</tr>
<tr>
<td>• Evidence of a stable system design demonstrated through successful test and evaluation</td>
<td></td>
</tr>
<tr>
<td>• Evidence that materials, parts, manpower, tooling, test equipment and facilities are available to meet planned production rates</td>
<td></td>
</tr>
<tr>
<td>• Evidence that manufacturing processes are capable, in control, and have achieved planned FRP objectives</td>
<td></td>
</tr>
</tbody>
</table>
CH 3–4.3.19 Reliability and Maintainability Engineering

The purpose of Reliability and Maintainability (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 cost 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 as early as the Engineering and Manufacturing Development (EMD) phase.

DoDI 5000.02, Enc 3, sec. 12 requires Program Managers (PMs) to implement a comprehensive R&M engineering program as an integral part of the systems engineering (SE) process. The Systems Engineer should understand that R&M parameters have an impact on the system’s performance, availability, logistics supportability, and total ownership cost. To ensure a successful R&M engineering program, the Systems Engineer should as a minimum integrate the following activities across the program’s engineering organization and processes:

- Providing adequate R&M staffing.
- Ensuring R&M engineering is fully integrated into SE activities, Integrated Product Teams and other stakeholder organizations (i.e., Logistics, Test & Evaluation (T&E), and System Safety).
- Ensuring specifications contain realistic quantitative R&M requirements traceable to the Initial Capabilities Document (ICD), Capability Development Document (CDD) and Capability Production Document (CPD).
- Ensuring that R&M engineering activities and deliverables in the Request for Proposal (RFP) are appropriate for the program phase and product type.
- Ensuring that R&M Data Item Descriptions (DIDs) that will be placed on contract are appropriately tailored (see the Guidance for Tailoring R&M Engineering Data on the DASD(SE) website).
- Integrating R&M engineering activities and reliability growth planning curve(s) in the Systems Engineering Plan (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 Test and Evaluation Master Plan (TEMP), along with a reliability growth planning curve beginning at Milestone B.
- 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 Technical Performance Measures.
- Assessing R&M status during program technical reviews.
- Including consideration of R&M in all configuration changes and trade-off analyses.

As part of the SE process, the R&M engineer should be responsible for the R&M activities by the acquisition phase outlined in Table 48.
### Table 48: R&M Activities by Acquisition Phase

<table>
<thead>
<tr>
<th>Acquisition Phase</th>
<th>R&amp;M Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Materiel Solution Analysis (MSA) Phase.</strong></td>
<td>During the MSA Phase, the R&amp;M engineer, as part of the program SE team, should:</td>
</tr>
<tr>
<td></td>
<td>• Analyze conceptual design approaches and estimate the feasibility with respect to R&amp;M ICD performance capabilities</td>
</tr>
<tr>
<td></td>
<td>• Perform AoA trade-off studies among R&amp;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, using the <a href="#">DoD RAM-C Rationale Report Manual</a></td>
</tr>
<tr>
<td></td>
<td>• Conduct a Reliability, Availability, Maintainability and Cost (RAM-C) analysis. For Major Defense Acquisition Programs (MDAP), prepare a preliminary RAM-C Rationale Report and attach the report to the SEP for Milestone A</td>
</tr>
<tr>
<td></td>
<td>• Translate ICD performance capabilities and draft CDD thresholds to R&amp;M specification requirements based on the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP), failure definitions and utilization rates</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Use data from the RAM-C Rationale Report to provide the following for logistics design support:</td>
</tr>
<tr>
<td></td>
<td>a. The initial failure mode assessment, including effects of failure on system performance and the probable manner in which each failure mode would be detected to provide guidance to planning and the conceptual design of the diagnostics concept and maturation process</td>
</tr>
<tr>
<td></td>
<td>b. 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</td>
</tr>
<tr>
<td></td>
<td>• Define contractor R&amp;M engineering activities in the RFP and contract Statement of Work for the TMRR phase, which should include:</td>
</tr>
<tr>
<td></td>
<td>a. Allocations</td>
</tr>
<tr>
<td></td>
<td>b. Block diagrams and modeling</td>
</tr>
<tr>
<td></td>
<td>c. Predictions</td>
</tr>
<tr>
<td></td>
<td>d. Failure Mode, Effects and Criticality Analysis (FMECA)</td>
</tr>
<tr>
<td></td>
<td>e. Subsystem and system-level reliability growth planning activities</td>
</tr>
<tr>
<td></td>
<td>f. R&amp;M tests and demonstrations</td>
</tr>
<tr>
<td></td>
<td>g. Failure Reporting, Analysis and Corrective Action System (FRACAS)</td>
</tr>
<tr>
<td><strong>Technology Maturation and Risk Reduction (TMRR) Phase.</strong></td>
<td>During the TMRR phase, the R&amp;M engineer, as part of the program SE team, should:</td>
</tr>
<tr>
<td></td>
<td>• Participate in trade studies during requirements analysis and architecture design</td>
</tr>
<tr>
<td></td>
<td>• Review results of R&amp;M engineering analyses, verification tests, design approach, availability assessments and maintenance concept optimization to verify conformance to requirements, and to identify potential R&amp;M problem areas</td>
</tr>
<tr>
<td>Acquisition Phase</td>
<td>R&amp;M Activities</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>• Contribute to integrated test planning to avoid duplication and afford a more complete utilization of all test data for R&amp;M assessment. Comprehensive test planning should include subsystem reliability growth and maintainability and BIT demonstrations as appropriate.</td>
</tr>
<tr>
<td></td>
<td>• Understand schedule and resource constraints, and adjust the reliability growth planning curve based on more mature knowledge points. Include updated reliability growth planning curve in the SEP at the Development RFP Release Decision Point and at Milestone B, and in the TEMP at Milestone B.</td>
</tr>
<tr>
<td></td>
<td>• Integrate R&amp;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.</td>
</tr>
<tr>
<td></td>
<td>• Verify that plans have been established for the selection and application criteria of parts, materials, and processes to limit reliability risks.</td>
</tr>
<tr>
<td></td>
<td>• Define contractor R&amp;M engineering activities in the RFP and contract Statement of Work (SOW) for the EMD phase, during which R&amp;M quantitative requirements and verification methods are incorporated.</td>
</tr>
<tr>
<td></td>
<td>• Update the RAM-C analysis to support the Development RFP Release Decision Point ensuring the JCIDS Sustainment Thresholds in the CDD are valid and feasible. For MDAPs, attach the updated RAM-C Rationale Report to the SEP for Milestone B.</td>
</tr>
<tr>
<td>Engineering and Manufacturing Development (EMD) Phase. During the EMD phase, the R&amp;M engineer, as part of the program SE team, should:</td>
<td>• Perform evaluations to assess R&amp;M status and problems.</td>
</tr>
<tr>
<td></td>
<td>• Update the RAM-C analysis, ensuring the JCIDS Sustainment Thresholds in the CPD are valid. For MDAPs, attach the updated RAM-C Rationale Report to the SEP for Milestone C.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the product baseline design and required testing can meet the R&amp;M requirements.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the detailed R&amp;M prediction to assess system potential to meet design requirements is complete.</td>
</tr>
<tr>
<td></td>
<td>• 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 TEMP.</td>
</tr>
<tr>
<td></td>
<td>• Verify system conformance to specified R&amp;M requirements through appropriate demonstration and test.</td>
</tr>
<tr>
<td></td>
<td>• Implement a FRACAS to ensure feedback of failure data during test and to apply and track corrective actions.</td>
</tr>
</tbody>
</table>
|                   | • Coordinate with the Chief Developmental Tester (T&E Lead) and Operational Test Agencies (OTA) 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.
<table>
<thead>
<tr>
<th>Acquisition Phase</th>
<th>R&amp;M Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Define contractor R&amp;M engineering activities in the RFP and contract SOW for the P&amp;D phase to ensure adequate R&amp;M engineering activities take place during P&amp;D and the RFP and contract SOW provide adequate consideration of R&amp;M in re-procurements, spares and repair parts</td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
</tr>
</tbody>
</table>

**Production and Deployment (P&D) Phase.** During the P&D phase, 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 (ECP), 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 utilized during all design change efforts including change proposals, variations, substitutions, product improvement efforts or any other hardware change effort

**Operations and Support (O&S) Phase.** During the O&S phase, 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

**CH 3–4.3.20 Spectrum Management**
Warfighters use spectrum-dependent systems for communications, sensors (i.e., radar), navigation beacons, jammers, homing devices, anti-Improvised Explosive Devices (IED) and other purposes. Often emitters are in close 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 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 Government-furnished equipment (GFE), the platform Program Manager (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 Pre-Milestone A Analysis of Alternatives (AoA) should address spectrum needs as part of concept formulation. Both the SSRA and DD-1494 are required for each milestone (see DoD 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 (ITU) 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 (HERO), Personnel (HERP) and Fuel (HERF). 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 and Systems 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 DoD 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 1C 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 43 for spectrum activities by acquisition phase. This figure summarizes the requirements of DoD 4650.01.

**Figure 43: Spectrum-Related Activities by Life-Cycle Phase**
CH 3–4.3.21 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 standard interfaces and open systems. Standardization is an enabling tool to provide the warfighter with systems and equipment that are interoperable, reliable, sustainable and affordable. Standardization plays a key role in defining systems engineering (SE) best practices and processes.

The Program Manager (PM) balances the decision to use standardized agreements, practices, products, parts, processes, interfaces and methods with required capabilities, operational environment, technology feasibility and growth and cost-effectiveness.

DoDM 4120.24, Enclosure 4, Standardization in the Acquisition Process, provides policies on standardization considerations, how to document standardization decisions, and a discussion of the tailoring of standardization documents. It also provides references to key resources for the standardization process.

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 part obsolescence due to Diminishing Manufacturing Sources and Material Shortages (DMSMS). MIL-STD-3018 (Parts Management) dictates that program offices should apply standardization processes to:

---

[Diagram of standardization processes and strategies]

---
• Improve parts commonality.
• Reduce total ownership costs.
• 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.

Additional guidance on parts management may be found in SD-19 (Parts Management Guide).

CH 3–4.3.22 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 Program Manager (PM), through the Systems Engineer and Product Support Manager, 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 Product Support Manager to develop and define the system’s support strategy. It includes sustainment-related should-cost management and risk and opportunity management efforts across the life cycle. Supportability analysis begins in stakeholder requirements definition, as part of the Analysis of Alternatives (AoA), and continues through the design, test and evaluation, production and deployment activities/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/decision environment.

Early consideration of supportability needs during Requirements Analysis, Architecture Design and Implementation processes are critical to ensure the delivered capability is operationally suitable, effective, 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 5000.02, Enc 6 and DAG Chapter 4, but typical product support considerations are listed in Table 49.

Table 49: Product Support Considerations

<table>
<thead>
<tr>
<th>Element</th>
<th>Typical Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manpower and Personnel</td>
<td>Specifically support personnel for installation, checkout sustaining support and maintenance</td>
</tr>
<tr>
<td>Training and Training Support</td>
<td>For the system operators and maintenance personnel</td>
</tr>
<tr>
<td>Supply Support</td>
<td>Including repairable and non-repairable spares, consumables and special supplies</td>
</tr>
<tr>
<td>Element</td>
<td>Typical Considerations</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Support Equipment</td>
<td>Including tools, condition and state monitoring, diagnostic and checkout special test and calibration equipment</td>
</tr>
<tr>
<td>Computer Resources</td>
<td>Operating systems and software supporting logistics functions and associated infrastructure</td>
</tr>
<tr>
<td>Packaging, Handling, Storage and Transportation</td>
<td>Special provisions, containers and transportation needs</td>
</tr>
<tr>
<td>Facilities and Infrastructure</td>
<td>Including facilities to support logistics and sustainment actions at all levels</td>
</tr>
<tr>
<td>Technical Data</td>
<td>Including system installation and checkout procedures; operating and maintenance instructions and records; alteration and modification instructions, etc.</td>
</tr>
<tr>
<td>Usage and Maintenance Data</td>
<td>Including data acquisition, movement, storage and analytic capability to support life-cycle support decisions</td>
</tr>
</tbody>
</table>

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 end users early in the Stakeholder Requirements Definition process to develop a performance-based product support strategy (including maintenance, servicing and calibration requirements). Reliability Centered Maintenance (RCM) analysis and Conditioned Based Maintenance Plus (CBM+) (see DoD 4151.22-M and DoDI 4151.22) are important initiatives that 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/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.

Additionally, the Product Support Manager and Systems Engineer should ensure that supportability analysis activities are documented in the Systems Engineering Plan (SEP) and the Life-Cycle Sustainment Plan (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 Product Support Manager 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 Key Performance Parameter/Key System Attributes (KPP/KSA) to establish affordable and achievable goals and caps (see CH 3–2, Background, CH 3–4.3.2, Affordability – Systems Engineering Trade-Off Analyses, and CH 1–4.2.15.). Once the goals are established the focus turns to the specific metrics driving the Operation and Support (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 (Ao) and Materiel Availability (Am) (see DAG Chapter 4). The cost-benefit analysis, jointly conducted by the Systems Engineer and Product Support Manager within the supportability analysis process, provides insight into supportability drivers and includes the impact of resources on readiness. Engineering analyses (i.e., Failure Mode, Effects and Criticality Analysis...
(FMECA); supportability analysis predictions; and diagnostics architecture) provide critical data to impact the design for supportability and to influence the product support package.

CH 3–4.3.23 Survivability and Susceptibility

A system with a balanced survivability and susceptibility approach ensures operational crew and personnel safety while satisfying mission effectiveness and operational readiness requirements.

Survivability is the capability of a system and its crew to avoid or withstand a hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Susceptibility is the degree to which a device, piece of equipment or weapon system is open to effective attack as a result of one or more inherent weaknesses. 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 environment 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), and cyber environment should also be considered in system design.

Susceptibility is a function of operational tactics, countermeasures, probability of an enemy threat, etc. Susceptibility is considered a subset of survivability. Vulnerability is 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. Vulnerability is also considered a subset of survivability.

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 Program Manager (PM), supported by the Systems Engineer, should fully assess system and crew survivability against all anticipated threats, at all levels of conflict, throughout the system life cycle. The goal of survivability and susceptibility 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.

The mandatory System Survivability Key Performance Parameter (KPP) is applicable to all Capability Development Documents (CDD) and Capability Production Documents (CPD). The System Survivability KPP may include:

- Reducing a system’s likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability and countermeasures.
- Reducing the system’s vulnerability if hit by hostile fire, through attributes such as armor and redundancy of critical components.
- Enabling operation in degraded electromagnetic (EM), space or cyber environments.
- Allowing the system to survive and continue to operate in, or after exposure to, a chemical, biological, radiological and nuclear (CBRN) environment, if required.

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 CBRN mission-critical system, the PM should address CBRN survivability, in accordance with DoDI 3150.09, The Chemical, Biological, Radiological and Nuclear (CBRN) Survivability Policy. The PM should ensure that progress toward CBRN survivability requirements is documented in the applicable Service CBRN mission-critical report. More information on CBRN can be found on the CBRN Survivability DoDTechipedia page [CAC-enabled].

Unless waived by the Milestone Decision Authority (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 (VOLT) Report (see DoDI 5000.02 (Enc 1, Table 2) and CH 7-4.1.2.).

The Systems Engineer should describe in the Systems Engineering Plan:

- How the design incorporates susceptibility and vulnerability reduction and CBRN survivability requirements.
- How progress toward these are tracked over the acquisition life cycle.

Additional techniques include rapid reconstruction (reparability) to maximize wartime availability and sortie rates and incorporating damage tolerance in the system design.

**CH 3–4.3.24 System Security Engineering**

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 system engineering (SE) that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. 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, 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 Program Protection Plan (PPP) (see CH 9–2.3.) documents the comprehensive approach to system security engineering analysis and the associated results.

SSE analysis results should be captured in the PPP, provided at each technical review and audit (see CH 9–3.4.) and incorporated into the technical review assessment criteria as well as the functional, allocated and product baselines. The PPP is approved by the Milestone Decision Authority (MDA) at each milestone decision review and at the Full-Rate Production/Full-Deployment (FRP/FD) decision, with a draft PPP (as defined in DoDI 5000.02, Enc 1, Table 2 and DoDI 5000.02, Enc 3, sec. 13.a) due at the Development Request for Proposals (RFP) Release Decision Point. The analysis should be used to update the technical baselines prior to each technical review and key knowledge point throughout the life cycle. It should also inform the development and release of each RFP (see CH 9–4.1.) by incorporating SSE process requirements and the system security requirements into the appropriate solicitation documentation.

The Program Manager (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 the relevant 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. CH 9–2.5 further details the program protection roles and responsibilities.

To address SSE as a design consideration, the Systems Engineering 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, security technical implementation guides 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.

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.)

CH 3—Version and Revision History
The table below tracks chapter changes. It indicates the current version number and date published, and provides a brief description of the content.

<table>
<thead>
<tr>
<th>Version #</th>
<th>Revision Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2/1/17</td>
<td>Chapter 3 initial upload</td>
</tr>
<tr>
<td>1</td>
<td>5/5/17</td>
<td>Minor updates to align with DoDI 5000.02 Change 2 and to address comments received from the user community.</td>
</tr>
<tr>
<td>2</td>
<td>9/25/17</td>
<td>Minor updates to fix broken hyperlinks and update references.</td>
</tr>
</tbody>
</table>