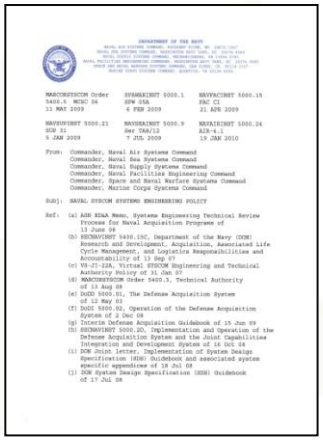
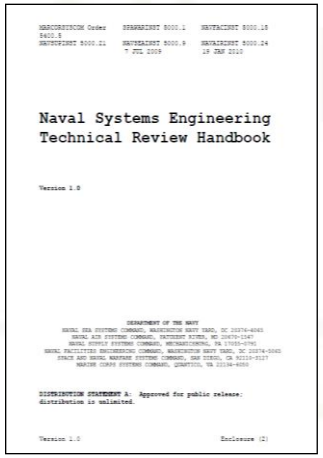
Safety in Naval Systems Engineering Technical Reviews (SETR)

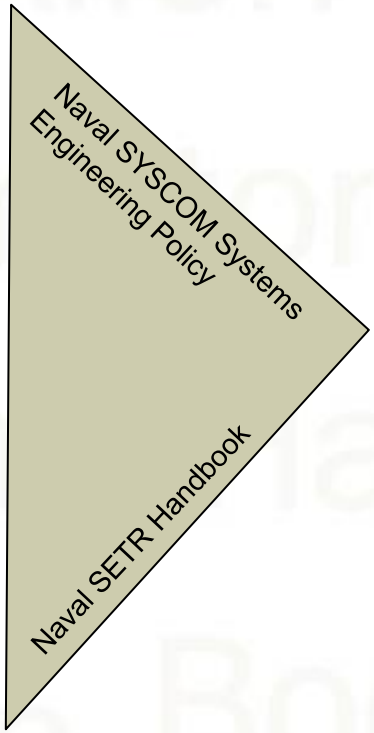
Karen Gill
Kristin Thompson

October 2010

Naval Systems Engineering Policy and Guidance







- Establishes systems engineering policy for all Naval SYSCOMs and affiliated PEOs and Direct Reporting Program Managers
- Establishes a common Systems Engineering Technical Review (SETR) process within DON as promulgated by the Naval SETR Handbook
- Handbook provides guidance to implement Naval SYSCOM Systems Engineering Policy
- Identifies planning, execution, and follow-on activities for the SETR process.

Introduction

- Background
  - ASN (RDA) Chief Systems Engineer (CHSENG) is chartered by Systems Engineering Stakeholders Group (SESG) to update the Naval Systems Engineering Technical Review (SETR) Handbook
    - Appendixes being developed for Common Functional Areas (CFA) – one of which is Safety
    - Safety Appendix will contain Enterprise-level Safety Criteria Checklists (i.e. common to all SYSCOMS)
  - CHSENG Safety Lead established Safety Working Group (SWG) of safety functional area subject matter experts to develop Safety input
    - Membership from NAVSEA, MARCORSYSCOM, SPAWAR, NAVAIR, NAVFAC, OPNAV N45, Navy and Marine Corps Public Health Center
    - CHSENG support facilitates government SMEs

What is SETR?

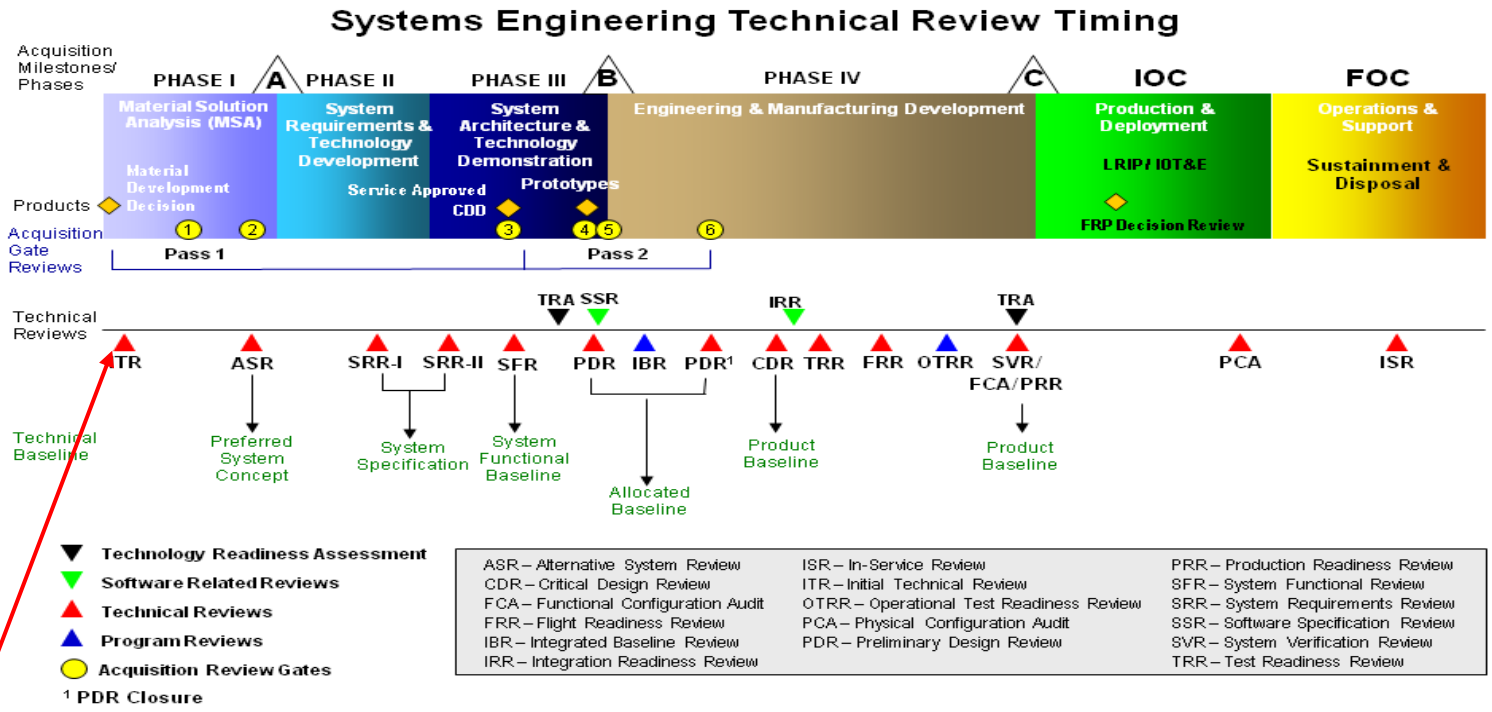
- System Engineering Technical Review (e.g. PDR, CDR, TRR, etc)
  - Technical reviews that are integral to Naval and System Engineering processes
  - Technical assessment of key health and progress of Program
  - Provides PMs with independent assessments of program readiness to enter the next technical phase
  - Assists program office management teams in documenting technical requirements, synthesizing certifiable designs, assessing performance and system safety risk, and producing and deploying systems to achieve required capability
  - When requested by the PM, chaired by a senior government employee appointed by the SYSCOM Chief Engineer (CHENG), conducts the SETR assessments in collaboration with program management
  - SETR Lead is an independent Technical Authority from outside the PMO but usually from inside the SYSCOM

Renewed Emphasis on Early Systems Engineering

- The 2008 revision of DoDI 5000.02 and the Weapon System Acquisition Reform Act of 2009 place emphasis on conducting systems engineering tasks that were traditionally performed after Milestone B (post-acquisition) prior to Milestone B (pre-acquisition) in order to establish a feasible design based on mature technologies.

- This, and other changes to the DoD acquisition process, made it necessary to realign the timing of many of the SETR events to occur earlier in the acquisition process to support the DoD desire for more technical maturity of design and technologies prior to milestone B.

Overlap View of DODI 5000.02 and SECNAV 5000.2D



First SETR

Underpinning Design Maturity to PoPs/Gate Review Process

Recommended SETRs

- Initial Technical Review - Supports technical basis for initial cost estimates and POM budget submissions.
- Alternative Systems Review - Reviews results of Materiel Solution Analysis phase and assesses technology development plan and preferred system concept.
- System Requirements Review - Assesses technical readiness to enter Engineering & Manufacturing Development phase.
- System Functional Review - Assesses System Functional Baseline and readiness to begin functional allocation.
- Preliminary Design Review - Assesses System Allocated Baseline and readiness to begin detailed design.
- Critical Design Review - Assesses System Product Baseline and supports Design Readiness Review.
- Test Readiness Review - Assesses system readiness to begin Developmental Test and Evaluation (DT&E).
- System Verification Review - Assesses system compliance with functional baseline.
- Production Readiness Review - Assesses system readiness to enter production.
- Physical Configuration Review - Assesses the as-delivered system for compliance with the product baseline and supports full-rate production decision.

Building the SETR Criteria

General Systems Engineering

Technical Management (e.g. SEP, IPTs)
Constraints: (1) Statutory (2) Regulatory (3) Standards (4) Modular Open Systems Architecture
Systems Control: (1) Risk Management (2) CM (3) Interface (4) Quality
Total Life Cycle Systems Management: (1) RAM (2) Logistics & Sustainment (4) Manufacturing & Production
Requirements Management: (1) Development (2) Verification/Validation

Functional Areas

Common DoD & DoN	SYSCOM or Program Specific Requirements
SE and PM Tasks	
Human Systems Integration	
Information Protection	
Software-Intensive Architecture	
Safety	Submarine Safety
	Air Worthiness
Reliability, Availability, and Maintainability	
Standardization & Interoperability	
Electromagnetic Environmental Effects, Spectrum Supportability	
Survivability and Susceptibility	
Facilities and Infrastructure	

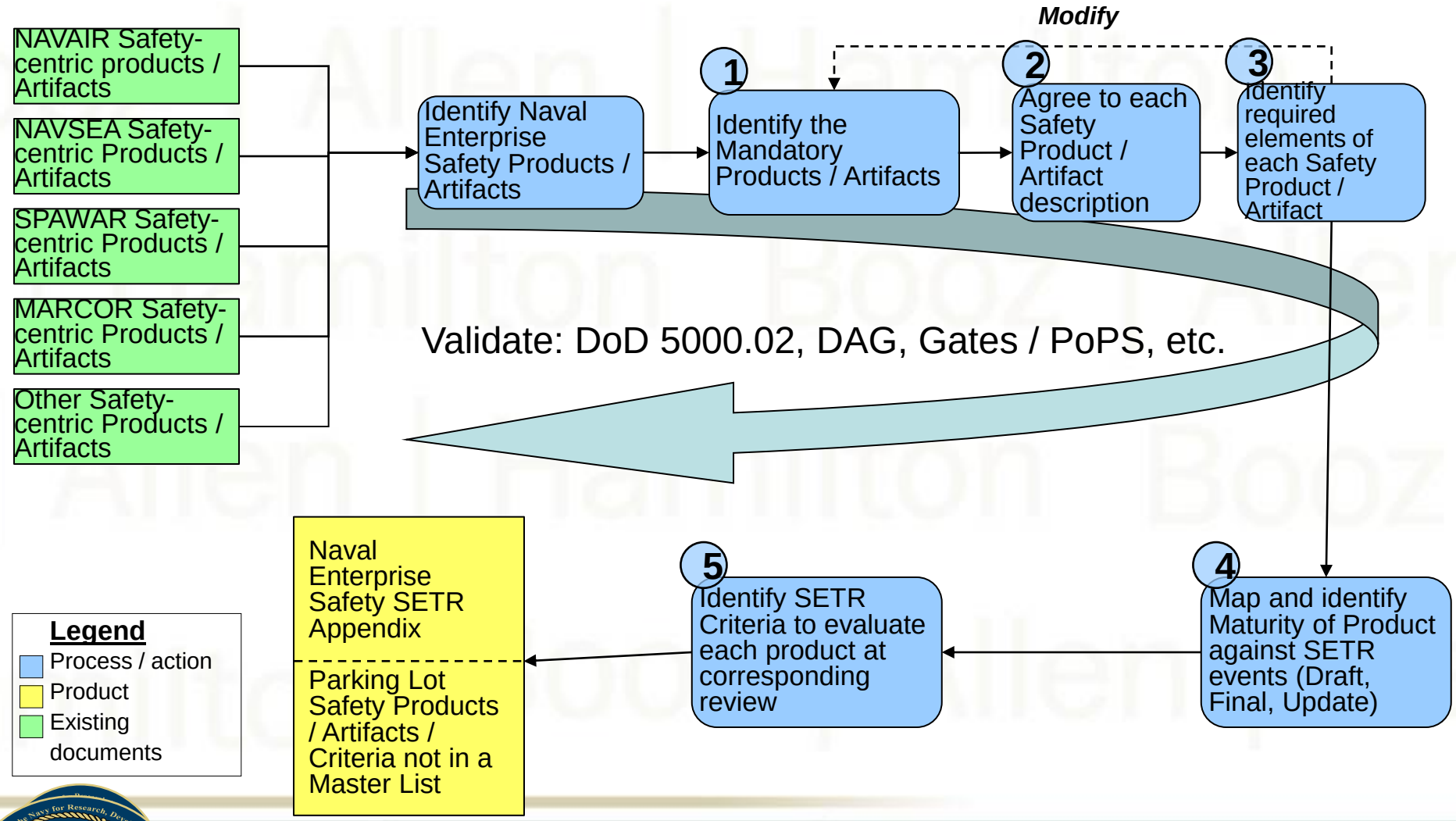
Our Focus – Safety Common Functional Area

- The safety in SETR goal is to develop a set of Naval Enterprise level safety criteria statements for each of the SETR events.
- These criteria statements, or questions, form the basis of safety in SETR for all Navy and Marine Corps acquisition programs.
- Each systems command (SYSCOM) may develop additional SYSCOM-specific criteria for the SETRs.
- The safety in SETR effort also focused on better integrating safety engineering into the overall systems engineering process by developing safety criteria for non-safety focused documents such as the Systems Engineering Plan and Test and Evaluation Master Plan.

Process to Develop Safety Criteria Statements

- The ASN(RDA)/CHSENG lead organized a Safety Horizontal Integration Team (HIT) to coordinate the development of the Safety SETR Appendix to the Naval SETR Handbook.
- The HIT formed a Safety Working Group (SWG) that included subject matter experts from different safety disciplines across the Navy SYSCOMS, Office of the Chief of Naval Operations, and the Navy and Marine Corps Public Health Center.
- The SWG followed a HIT developed process to systematically identify acquisition-related products and elements and link them to safety-related policy requirements.
- The Safety in SETR workflow was a five step process ending with completion on Safety SETR Criteria Statements for the Handbook.

Safety in SETR - Process Workflow



Safety in SETR – Work Products

Mandatory Products/Artifacts

Discipline Author	POPS Parent (Gate)	SE Parent	Products/Process	Description	NAVAIR	MARCOR	SPAWAR	NAVSEA
Safety and Domain Products								
SS-SW			AOP 52 Compliance	Y	Y	Y		N
SS-S			Code Level Hazard Anal	Y	Y	Y	Y	Y
SS			ESOH Risk Acceptance	Y	Y		Y	Y
SS		PESHE	ESOH Risk Assessment Matrix	Y	Y		Y	Y
SS			Functional Hazard Analysis	Y	Y		Y	Y
SS		SEP/PESHE	Hazard Tracking System	Y	Y	Y	Y	Y
Env.			HAZMAT Management Plan	Y	Y	N	Y	Y
Env.		SEP/PESHE	Health Hazard Assessment	Y	Y	Y	Y	Y
SS			Integrated Hazard Analysis	Y	Y	Y	Y	Y
SS		SEP/PESHE	Operating and Support Hazard Analysis	Y	Y	Y	Y	Y
Env.	5, 6		Programmatic Environment, Safety, and Occupational Health Evaluation	Y	Y	Y	Y	Y
SS			PFS/PESOH/Safety Lead/Safety Manager Resource Allocation	Y	Y	Y	Y	Y

1 – Author of Product
2 – PoPs traceability
3 – SE traceability
4– Safety Products/Artifacts
5 – SYSCOM Vote
6 – Reference
7 – SETR Review
8 – Gate Review
9 – Maturity Level

				SETR Reviews		ITR	ASR	SRR1	SRR2	SFR	SSR
				Gate Reviews	1		2			3	4
Policy	Guidance	Standards									
								D	D	D	
	JSSSEH										
DoD 5000.02											
		MIL-STD-882				D	D	D		F	
	JSSSEH						D			D	
		MIL-STD-882						D		F	
								D		U	F

Safety Products/Artifacts/Elements

1 - Safety Products/Artifacts
2 - Safety Elements
3 - Reference (e.g. DID)

Safety Product/Artifact Elements

Product	Safety Element	Reference
Safety and Domain Products		
AOP 52 Compliance	a) Software Safety Engineering b) Generic Software Design Requirements c) Previously Developed Software d) Test and Assessment Guidelines	
Code Level Hazard Analysis (1)	a) Analysis of architecture -flow of the program -calls made by the executive routine - structure of the modules -logic flow of each module, and the implementation in the code b) Interfaces with other software modules c) Interaction with the system	
ESOH Risk Acceptance	a) Residual risk accepted by the appropriate authority b) User representative concurrence (if high or serious) (2)	
ESOH Risk Assessment Matrix	a) Residual risk	
Functional Hazard Analysis	a) System Description b) Data used to determine the safety aspects of design features c) Hazard analysis results -Summary of results -List of identified Hazards to include: -System/Subsystem unit -Component failure modes -Subsystem failure modes -System component/phase -System event phase -System operation description -Hazard description to include: -Brief description of hazard -Complete description of the potential/actual hazards inherent in the item being analyzed -Hazard identification/indication -Effect of hazard -Risk assessment -Recommended action -Effect of recommended action -Remarks -Status -Caution and warning notes	(3) DI-SAFT-80101

Safety Criteria Statements

Safety Criteria Statements (SRR1)

SRR1 - Updated Criteria Statements

	Criteria Statement	Artifact/Product	Mandatory DoD/Navy Requirement	Source
1	Has the Government's system safety engineering approach been clearly and fully documented? (MIL-STD-882)	System Safety Management Plan	4.1 … Document the developer's and program manager's approved system safety engineering approach.	MIL-STD-882 Section 4
2	Has the Developer's system safety engineering approach been clearly and fully documented? (MIL-STD-882)	System Safety Program Plan	4.1 … Document the developer's and program manager's approved system safety engineering approach.	MIL-STD-882 Section 4
3	Has the program developed a plan to manage software safety? (MIL-STD-882)	Software Safety Program Plan	4.1 … Document the developer's and program manager's approved system safety engineering approach.	MIL-STD-882 Section 4
4	Has a hazard tracking system been developed in accordance with MIL-STD-8822 (MIL-STD-882)	Hazard Tracking System	4.8 … Track hazards, their closure actions, and the residual mishap risk. **Maintain a tracking system that includes hazards, their closure actions, and residual mishap risk throughout the system life cycle.** The program manager shall keep the system user advised of the hazards and residual mishap risk	MIL-STD-882 Section 4

1 - Criteria Statement
2 - Corresponding Product/Artifact
3 - Requirement from Policy
4- Source of requirement

Element Maturity Tables

Artifact: Safety Requirements/Criteria Assessment
Created By: Developer

Artifact Elements	SRR1	SFR	PDR	TRR	SVR
Artifact maturity	D	D	F	U	U
a) Review of design specifications, safety standards and guidelines	HI	P	P	HI	HI
b) Initial safety requirements (prescribed or newly derived for the system)	HI	P	HI	P	HI
c) Hazards with corresponding design (safety) requirements to eliminate or mitigate the hazard,	P	P	HI	P	HI
d) Verification and validation of safety requirements	--	P	HI	HI	P
e) safety critical functions list	P	P	HI	P	P
f) safety critical software functions	P	P	HI	P	P
g) Safety critical software requirements	P	P	HI	P	P

Examples – Safety Criteria Statements (ITR)

	Initial Technical Review	Y/N
1	Does the program have an approved draft Programmatic ESOH Evaluation document that identifies ESOH responsibilities, how the program will integrate system safety-ESOH considerations into the systems engineering process, the ESOH risk management process, method for hazard tracking, and preliminary ESOH hazards and their associated risks? (Ships only) (DoDI 5000.02)	
2	Have appropriate potential hazards been derived from historical data lessons learned from -similar legacy systems -fielded versions of the same system -Science and Technology Programs, -Independent Research and Development Programs -Research and Development? (MIL-STD-882)	
3	Has the program identified all Critical Safety Items and safety related Critical Application Items? (SECNAVINST 5000.2D)	
1	Does the Analysis of Alternatives (AoA) Plan include safety/ESOH considerations?	
2	Has the Concept of Operations been reviewed for potential operational safety/ESOH constraints?	
3	Do the cost estimates contain appropriate ESOH/safety-related cost data?	
4	Has safety/ESOH reviewed the Initial Capabilities Document for high level ESOH-related capability statements?	
5	Does the Request for Proposal for alternative solution studies contain ESOH requirements that the government wants the contractor to address?	
6	Does the Test and Evaluation Strategy include safety/ESOH planning?	
7	Does the Technology Development Strategy include safety/ESOH hazard analysis planning as part of technology development?	

Examples – Safety Criteria Statements (PDR)

	Preliminary Design Review	Y/N
1	Is the Safety Lead/Manager or PFS chairing System Safety Working Groups on a regular basis with documented results? (OPNAVINST 5100.24)	
2	Are all ESOH Hazards assessed using the program's approved ESOH Risk Matrix? (MIL-STD-882)	
3	Have identified hazards been assessed in accordance with MIL-STD-882 and have they been documented in the hazard tracking system? (MIL-STD-882)	
4	Have design alternatives for eliminating hazards or reducing their impact been considered for each potential hazard? (MIL-STD-882)	
5	Has the expected effectiveness of each alternative risk mitigation been documented in the hazard tracking system? (MIL-STD-882)	
6	Does the program maintain a National Environmental Policy Act (NEPA)/Executive Order 12114 compliance schedule for all system-related NEPA/EO 12114 analyses? (DoDI 5000.02)	
7	Does the program maintain a Programmatic ESOH Evaluation document that identifies ESOH responsibilities, how the program will integrate system safety-ESOH considerations into the systems engineering process, the ESOH risk management process, the hazard tracking system, and ESOH hazards and their associated risks? (DoDI 5000.02)	
8	Has the program reported the current status of all high and serious ESOH risks and applicable ESOH technology requirements at program reviews? (Include in Risk Management Board (RMB), GATES and Milestone Reviews)	
9	Has the plan for managing Hazardous Materials been approved? (MIL-STD-882)	
10	Have hazards associated with hazardous materials been identified, analyzed and documented in the hazard tracking system? (MIL-STD-882)	
11	Has the program identified safety critical functions and have they been allocated to the sub-system? (MIL-STD-882)	

Next Steps

- Finalize all work products to date
  - Update products based on feedback from CFA IPT
- Coordinate with ASN (RDA) CHSENG CFA to further develop Safety Appendix and exchange input with other CFAs
  - Work with CFA IPT lead to develop strategic process to integrate all CFA data and create useful tool for PM
  - Participate in CFA IPT meetings

Contact Information

- Karen Gill – gill_karen@bah.com, 703-412-7436
- Kristin Thompson – thompson_kristin@bah.com, 540-288-5078

Questions


Assistant Secretary of the Navy for Research, Development, & Acquisition
SECRETARY OF THE NAVY
UNITED STATES OF AMERICA
CHIEF SYSTEMS ENGINEER

BACK-UP


Assistant Secretary of the Navy for Research, Development, & Acquisition
SECRETARY OF THE NAVY
UNITED STATES OF AMERICA
CHIEF SYSTEMS ENGINEER

SETR Events

- **Initial Technical Review (ITR)** – is conducted to support the program's POM (Program Objective Memorandum) submission.
  - The ITR assesses the envisioned requirements and conceptual approach of the program and verifies that the requisite research, development, test, engineering, logistic, and programmatic bases for the project reflect the complete spectrum of technical challenges and risks.
  - This review ensures that a program's technical baseline is sufficiently rigorous to support a valid cost estimate (with acceptable cost risk), and enable an independent assessment of that estimate by cost, technical, and program management subject matter experts.
- **Alternative Systems Review (ASR)** – is conducted to ensure that the resulting set of requirements agrees with the customers' needs and expectations and that the system under review can proceed into Technology Development phase.
  - The ASR assesses the alternative systems that have been evaluated during Materiel Solution Analysis phase, and ensures that the Technology Development plan is consistent with the preferred system solution and is adequately resourced to reduce Engineering & Manufacturing Development entry risk to an acceptable level.
  - The ASR ensures the preferred system alternative is cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk.

SETR Events, cont'd

- **System Requirements Review (SRR)** – is conducted to ensure that the system under review can proceed into the Engineering & Manufacturing Development (EMD) phase.
  - The SRR ensures that all system and performance requirements derived from the Initial Capabilities Document (ICD) or draft Capability Development Document (CDD) are defined and consistent with cost (program budget), schedule (program schedule), and other system constraints.
- **Technology Readiness Assessment (TRA**) – is a regulatory information requirement per DODI 5000.02. The TRA is a systematic metrics-based process that assesses the maturity of Critical Technology Elements (CTEs) and is a requirement for all acquisition programs.
  - The TRA scores the current readiness level of selected system elements, using defined Technology Readiness Levels (TRLs), highlighting critical technologies and other potential technology risk areas requiring Program Manager attention.
  - The TRA may be conducted concurrently with other technical reviews, specifically SRR, CDR, SVR, and/or PRR.
- **Integrated Baseline Review (IBR)** – process is employed by Program Managers throughout the life of projects requiring Earned Value Management (EVM).
  - The IBR establishes a mutual understanding of the Performance Baseline (PMB) and provides for an agreement on a plan of action to evaluate risks inherent in the PMB and the management processes that operate during project execution.

SETR Events, cont'd

- **System Functional Review (SFR)** – is conducted to ensure that the system under review can proceed into preliminary design.
  - The SFR ensures that all system requirements and functional performance requirements derived from the Capabilities Development Document (CDD) are defined and consistent with cost (program budget), risk, and other system constraints.
  - The SFR assesses the system functional requirements as captured in system specifications (functional baseline), and ensures that all required system performance is fully decomposed and defined in the functional baseline.

- **Preliminary Design Review (PDR)** – is conducted to ensure that the system under review can proceed into detailed design, and can meet stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.
  - The PDR assesses the system preliminary design as captured in performance specifications for each configuration item in the system (allocated baseline), and ensures that each functional baseline has been allocated to one or more system configuration items.

- **Critical Design Review (CDR)** – is conducted to ensure the system under review can proceed into system fabrication, demonstration, and test, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints.
  - The CDR assesses the system final design as captured in product specifications for each configuration item in the system (product baseline), and ensures that each product in the product baseline has been captured in the detailed =design documentation.

SETR Events, cont'd

- **Test Readiness Review (TRR)** – is conducted to ensure that the subsystem or system under review is ready to proceed into formal test.
  - The TRR assesses test objectives, test methods and procedures, scope of tests, and determines if required test resources have been properly identified and coordinated to support planned tests.
  - Depending on the program, additional reviews, such as Flight Readiness Review in case of aircraft, should be included in the Systems Engineering Plan.

- **System Verification Review (SVR) (FCA)** – is conducted to ensure that the system under review can proceed into Low Rate Initial Production (LRIP) and Full Rate Production (FRP) within cost (program budget), risk, and other system constraints.
  - SVR is synonymous with Functional Configuration Audit (FCA). The SVR is an audit trail from the CDR and assesses that the system final product, as evidenced in its production configuration, meets the functional requirements as derived from the CDD/draft Capability Production Document (CPD) to the functional, allocated, and product baselines.

- **Production Readiness Review (PRR)** - is an examination of a program to determine if the design is ready for production and the producer has accomplished adequate production planning without incurring unacceptable risks that will breach thresholds of schedule, performance, cost, or other established criteria.
  - The SVA (FCA) and PRR are typically conducted by the same group and at the same location. They are often conducted concurrently, which is why they are grouped together on the table.

SETR Events, cont'd

- **Operational Test Readiness Review (OTRR)** – is conducted to ensure that the "production configuration" system can proceed into Operational Testing (OT) with a high probability of success.

- **Physical Configuration Audit (PCA)** – examines the actual configuration of an item being produced in order to verify that the related design documentation matches the item specified in the contract.
  - The PCA confirms that the manufacturing processes, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled.

- **In-Service Review (ISR)** – is conducted to ensure that the system under review is operationally employed with well-understood and managed risk.
  - The ISR is intended to characterize the in-service technical and operational heath of the deployed system by providing an assessment of risk, readiness, technical status, and trends in a measurable form that will substantiate in-service budget problems.