Ordnance Safety & Security Activity

Lessons Learned with the Application of MIL-STD-882D at the Weapon System Explosives Safety Review Board

Mary Ellen Caro

Naval Ordnance Safety and Security Activity

Systems Safety/Joint Programs

mary.caro@navy.mil

Presented to:

8th Systems Engineering Conference

26 October 2005

Agenda

- WSESRB Background
- MIL-STD-882D Evolution
- MIL-STD-882D Implications for
  - System Acquisition
  - System Safety Program Planning
  - Safety Program Execution
  - Safety Risk Management
- Conclusion

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

WSESRB Background

- The WSESRB was established in 1967 as a result of several mishaps aboard aircraft carriers

- The purpose of the WSESRB is to provide an independent and technical review of the adequacy of the Program's system safety program and artifacts

USS Oriskany (1966)

USS Forrestal (1967)

WSESRB Authority

DODI 5000.2 Para E7.7

- PM shall identify, evaluate and manage safety and health hazards
- Explains the process for accepting risk

SECNAVINST 5000.2C

- CNO may establish system safety advisory boards (7.3.3)
- WSESRB is primary explosives safety review prior to DT/OT and Milestones (5.2.1.4.2)

SECNAVINST 5100.10H

- Directs CNO/CMC to establish safety programs

OPNAVINST 8020.14/MCO P8020.11

- Explosives Safety Policy
- Tasks COMNAVSEASYSCOM to establish WSESRB

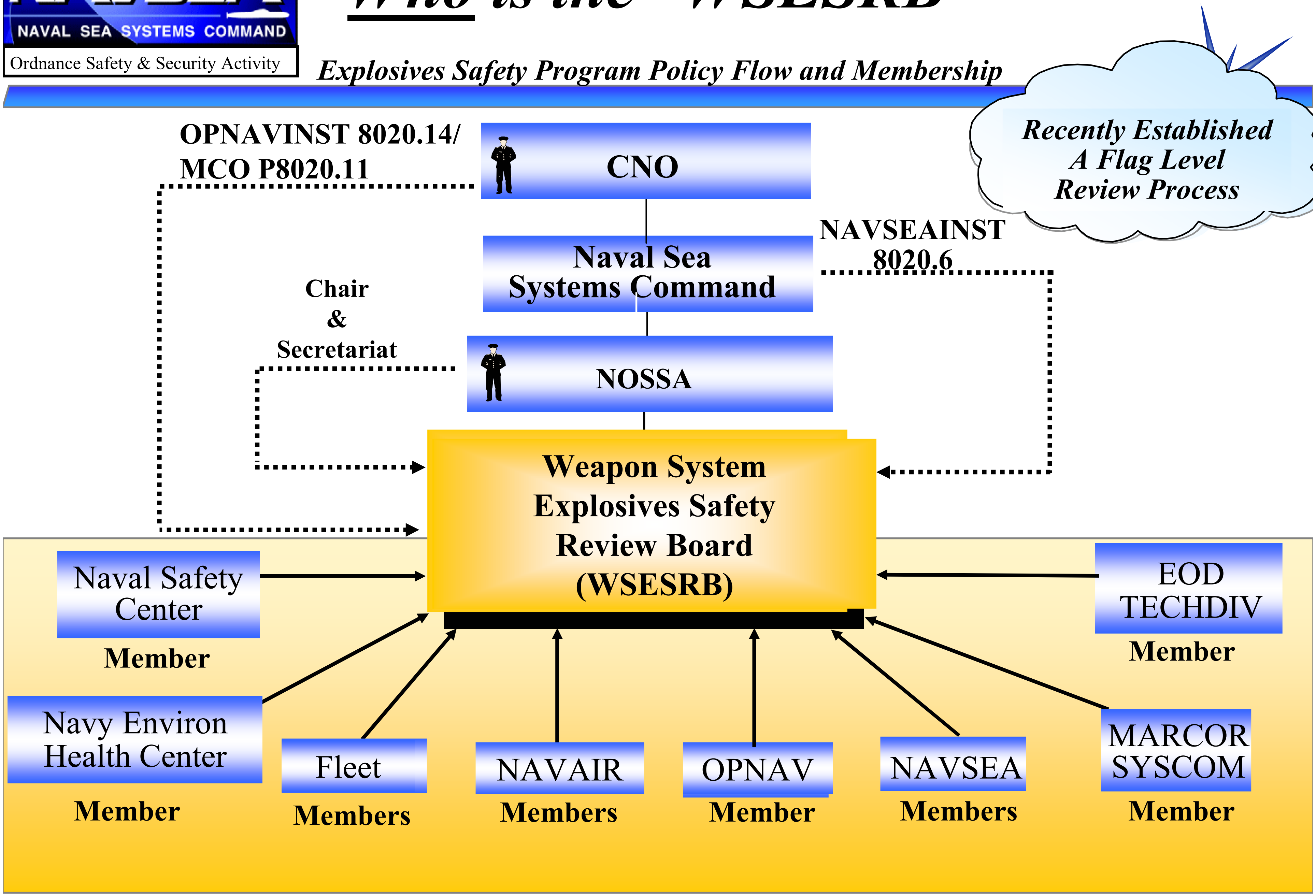
NAVSEAINST 8020.6D

- Defines WSESRB process and procedures

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

Who is the "WSESRB"

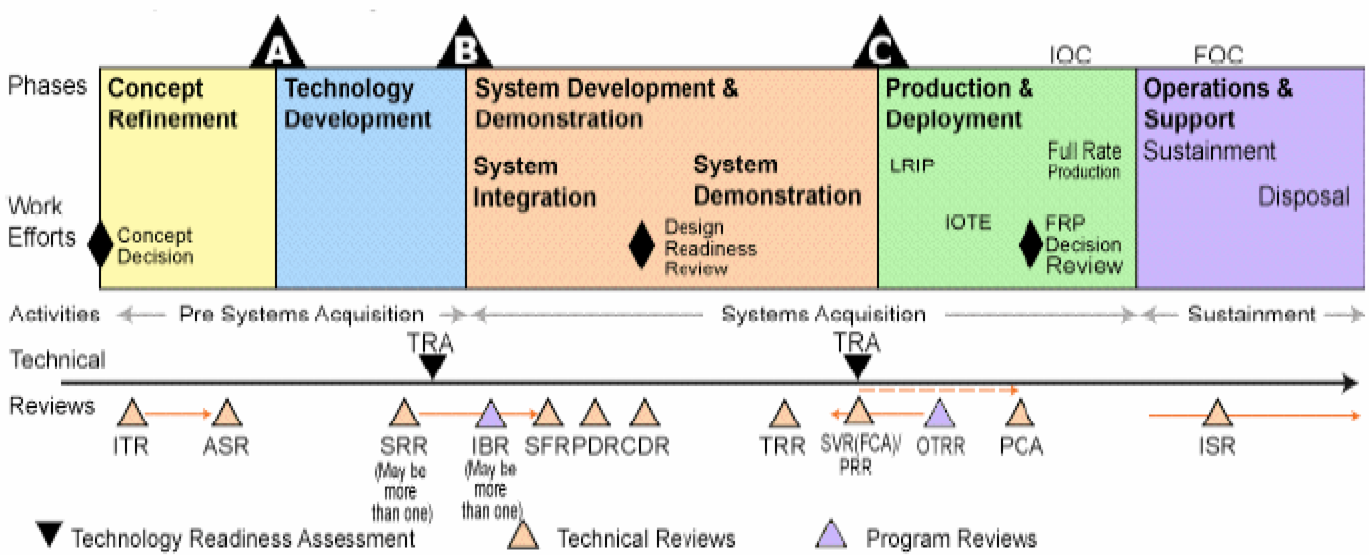
Explosives Safety Program Policy Flow and Membership



Ordnance Safety & Security Activity

Acquisition Life-Cycle

WSESRB reviews occur throughout that life-cycle



Transition to MIL-STD-882D

- Developed as result of acquisition reform
  - Converted to Standard Practice document
- Eliminated system safety tasks
  - “What to do” not “How to do it”
- Example Mishap Risk Index and defined High, Serious, Medium and Low risks
  - Agreement with DoDI 5000.2
  - Ability to tailor to specific programs
- Requirement for Closed Loop Hazard Tracking

MIL-STD-882D Process

- Eight basic steps to the MIL-STD-882D Standard Practice
  - Documentation of the System Safety approach
  - Identification of hazards
  - Assessment of mishap risk
  - Identification of mitigation measures
  - Reduction of mishap risk to acceptable level
  - Verification of mishap risk reduction
  - Acceptance of residual risk
  - Hazard tracking

NAVSEA NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

System Acquisitions

- MIL-STD-882D calls for System Safety Program, but eliminated tasks
  - No tasks to identify in solicitation
    "The bidder shall execute a system safety program in accordance with MIL-STD-882D"
    "System Safety Hazard Analysis shall be provided xx days prior to DRR"
  - Bidders propose safety programs for best competitive advantage
  - Proposals may vary widely in planned system safety program
  - Potential ambiguities between buyer and seller in program execution

System Acquisitions

- Lessons Learned
  - Solicitation needs to be as specific as possible and identify types of system safety efforts required of the developer (e.g., system safety program plan/POA&M, hazard analyses, hazard testing, certification requirements)
  - For Navy ordnance and weapon programs, there are many required tests and analyses that need to be identified in solicitation documents
  - Safety should to be part of Source Selection Criteria and participate in proposal evaluations

System Safety Program Planning

- DoDI 5000.2 only requires a PESHE
- MIL-STD-882D requires system safety program planning, but no longer identifies a task for the System Safety Program Plan (SSPP)
- Solicitation may or may not require an SSPP to be submitted with the proposal

NAVSEA NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

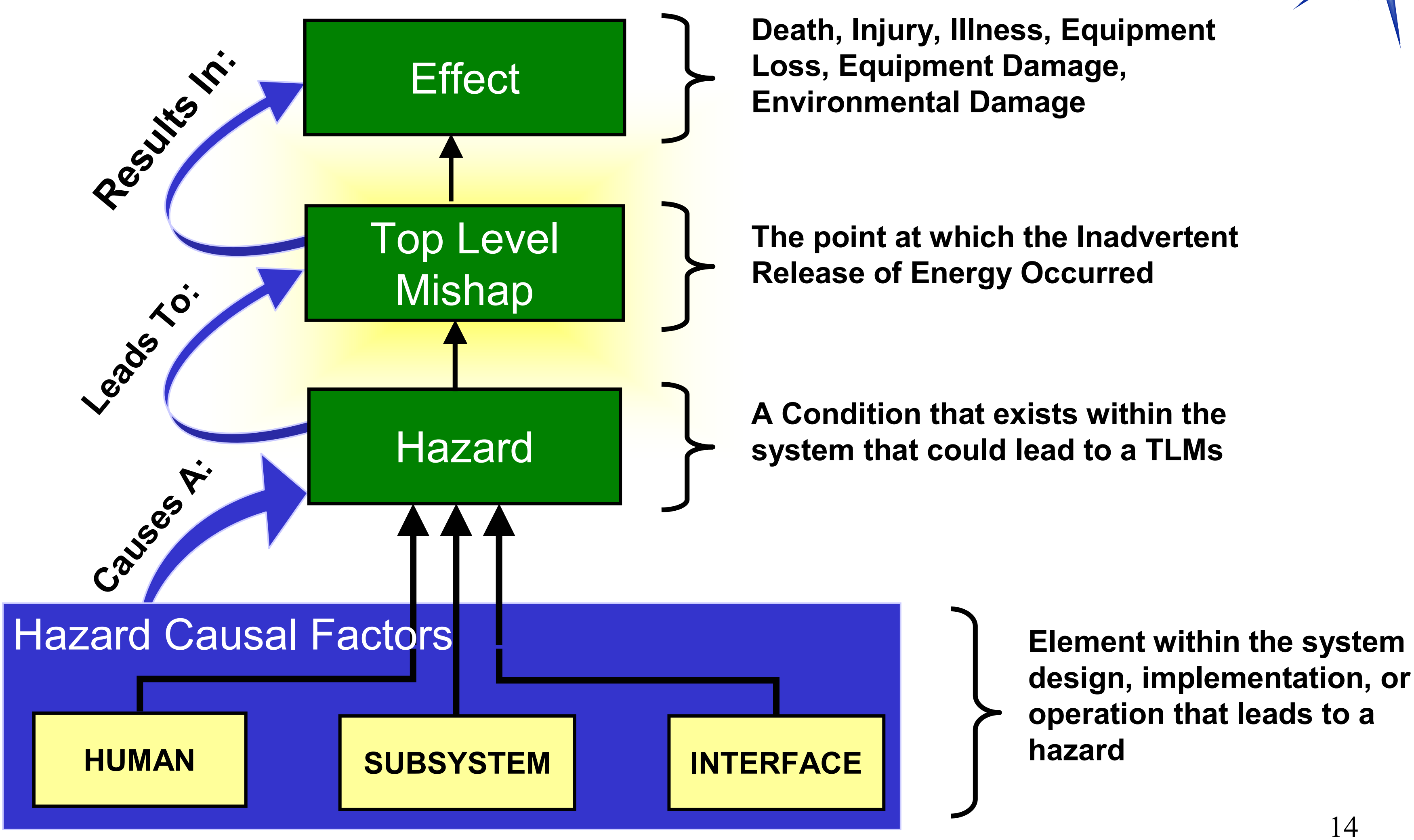
System Safety Program Planning

- Lessons Learned
  - A specific system safety plan needs to be developed for the program including identification of responsibilities, schedules, safety analyses, safety testing. Typically SSPPs are still being prepared.
  - For large complex programs, the Government should develop a System Safety Management Plan to identify how project safety efforts are aligned and integrated.

Safety Program Execution

- Integrated Product Process Development structure applied almost universally
- Concurrent engineering requires real time safety participation
  - Hazard identification
  - Hazard characterization
  - Prioritization of hazards
  - Identification of hazard mitigation
  - Implementation and verification of hazard risk mitigation
- Collaborative effort with Design IPTs

Mishap Relationships



Safety Program Execution

- Hazard Analysis tasks of MIL-STD-882C have been eliminated in MIL-STD-882D. However, these tasks lead the safety practitioner through a logical sequence of hazard identification/mitigation:
  - Preliminary Hazard List/Analysis (PHL/PHA) identifies top level hazards for further development
  - Safety Requirements/Criteria Analysis (SR/CA) identifies safety requirements that can be mapped to their allocated subsystems
  - Subsystem Hazard Analysis (SSHA) further evaluates hazards associated with identified subsystems
  - System Hazard Analysis (SHA) identifies hazards of interfacing subsystems/outside systems
  - Operating and Support Hazard Analysis (O&SHA) identifies those hazards associated with operations and maintenance

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

Safety Program Execution

- Lessons Learned
  - Safety practitioner needs to step back from day-to-day IPT activities to ensure that correct aspects of safety analyses are being conducted
  - Safety practitioner needs to ensure the scope of all the hazard analysis types has been covered within the program execution

Safety Program Execution

- Lessons Learned
  - Doing the system safety work doesn't necessarily mean producing the specific hazard analysis documents
  - Not having to produce the specific hazard analysis documents doesn't mean not having to do the system safety work

NAVSEA NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

Safety Program Execution

- Lessons Learned
  - Hazard tracking systems are becoming more important
    - Many are web based so everyone has access
    - Repository for all identified hazards
    - Real time tool that can capture work on-going within IPTs
    - Data base formats allow manipulation of data to produce information
    - Tool for development of System Safety Hazard Analysis deliverable documents

Safety Program Execution

- Software safety process heavily dependent on identification of safety-related requirements and assessment of criticality

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Ordnance Safety & Security Activity

Software Criticality Matrix

SOFTWARE CONTROL CATEGORY	MISHAP SEVERITY POTENTIAL			
	Catastrophic	Critical	Marginal	Negligible
Autonomous	SHRI 1	SHRI 1	SHRI 2	SHRI 4
Semi-Autonomous	SHRI 1	SHRI 2	SHRI 3	SHRI 4
Semi-Autonomous with Redundant Back-Up	SHRI 2	SHRI 3	SHRI 4	SHRI 4
Influential	SHRI 3	SHRI 3	SHRI 4	SHRI 4
No Safety Involvement	No Safety Analysis Required.			

High Risk – Safety verification requires requirements analysis, design analysis, code analysis and safety specific testing

Serious Risk – Requires requirements analysis, design analysis and in-depth safety specific testing

Medium Risk – Requires requirements analysis and safety specific testing

Low Risk – Requires requirements analysis and standard testing process

Software Integrity Matrix

Phase / SRI	DESIGN	CODE	UNIT TEST	INTEGRATING UNIT TEST	SYSTEM INTEGRATION
SRI 1 **High Risk**	• Design Team Review • Safety Review • SCF Linked To SW Rqmts • SCF Linked to Design Architecture • Fault Tolerant Design.	• Design Code Walkthrough • Independent Code Review • Safety Code Analysis • SCF Code Review • Safety Fault Detection, Fault Tolerance	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Thread Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review
SRI 2 **Serious Risk**	• Design Team Review • Prioritized Safety Review • SCF Linked To SW Rqmts • SCF Linked to Design Architecture.	• Design Code Walkthrough • Safety Code Analysis for Prioritized Modules • SCF Code Review • Safety Fault Detection, Fault Tolerance	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Thread Test • Safety Test Result Review		
SRI 3 **Medium Risk**	• Design Team Review • Limited Safety Review • Safety-Related Functions Linked to Design	• Design Code Walkthrough • Safety Code Analysis for Prioritized Modules • SCF Code Review • Safety Fault Detection, Fault Tolerance			
SRI 4 **Low Risk**	• Design Team Review • Minimal Safety Review • Normal Software Design Process IAW SDP				
SRI 5 **No Safety Risk**	• Normal Software Design Activity IAW the Software Development Plan	• Normal Software Code Activity IAW the Software Development Plan	• Normal Software Unit Test Activity IAW the Software Development Plan	• Normal Software Unit Integration Test Activity IAW the Software Development Plan	• Normal Software System Integration Test Activity IAW the Software Development Plan

EXAMPLE

Safety Program Execution

- Proposed revision to MIL-STD-882D introduces concept of relating safety criticality of software to safety integrity levels similar to DO 178B
- Different levels of rigor in the design, review, analysis and test efforts for varying levels of safety criticality

System Safety Risk Management

- MIL-STD-882D addresses Mishap Risk vice MIL-STD-882C Hazard Risk
- Higher level of abstraction associated with residual risk
  - Many hazards that can result in the same mishap

Mishap Risk Index

FREQUENCY OF OCCURRENCE	HAZARD CATEGORIES			
	I CATASTROPIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	1 (1A)	3 (2A)	7 (3A)	13 (4A)
(B) Probable	2 (IB)	5 (2B)	9 (3B)	16 (4B)
(C) Occasional	4 (1C)	6 (2C)	11 (3C)	18 (4C)
(D) Remote	8 (ID)	10 (2D)	14 (3D)	19 (4D)
(E) Improbable	12 (IE)	15 (2E)	17 (3E)	20 (4E)

HIGH (CAE (ASN-RDA))

SERIOUS (PEO)

MEDIUM (PM)

LOW (PM)

System Safety Risk Management

- Lessons Learned
  - Mishap Risk Index needs to be tailored for different applications, but most programs default to the identified MRI in MIL-STD-882D.
  - With Residual Risk being captured at the Mishap vice Hazard level, strategy for dealing with cumulative risk associated with many hazards should be identified.

Conclusions

- Acquisition reform and MIL-STD-882D have changed the way System Safety is performed
- Requires more understanding and thought up front to ensure the system safety program is properly structured
- Requires vigilance to ensure full scope of system safety effort is accomplished vice only those issues identified in IPT meetings
- Has fostered collaborative efforts between system safety, systems engineering, software engineering and design engineering on many programs


NOSSA:
Providing Ordnance Safety for our War Fighters.