NAVSEA
WARFARE CENTERS
DAHLGREN

System Safety in a System of Systems Environment

Janet G. McKinney, Code G72

October 2010

Approved By: Casey M. Clark, Code G72
Approved for Release By: Melissa A. Lederer, Code G70

NAVSEA
WARFARE CENTERS
DAHLGREN

Topics

- Background
  - Early History
  - Need for System of System (SoS) Safety
- Engineering Approach
- Lessons Learned
- Conclusion

USS Oriskany

- Oct 1966 shortly after combat operations
  - Fire broke out in hangar bay
  - Severely damaged 5 decks
  - Killed 44 personnel
- Cause of fire
  - Human error
  - Unsafe design of magnesium parachute flare
- Action taken
  - Increase manning to provide better supervision
  - Redesign flare

USS Forrestal

- July 1967 during combat operations
  - F-4 rocket accidentally fired
  - Struck fuel tank of another aircraft
  - JP-5 spewed on deck and under other fully loaded aircraft
- Final numbers
  - 134 sailors killed
  - 21 aircraft destroyed; 43 damaged
  - $72 million in damage
- Action taken
  - System Safety program established
    - Weapon System Explosives Safety Review Board (WSESRB)
    - Other supporting panels

System Safety Required for all Acquisition Programs

- Some Examples:
  - Weapon Systems
    - Guns
    - Missiles
    - Radars
  - Explosive Devices
    - Fuzes
    - Flares
    - Ordnance

NAVSEA WARFARE CENTERS
DAHLGREN

System Safety Process

PLANNING & MANAGEMENT

- Define safety approach methodology
- Establish SSWG
- Develop SSPP
- Establish Hazard Tracking System

HAZARD ANALYSIS & RISK REDUCTION PROCESS

PHL/ PHA

- Define safety functions, and I/Fs
- Define Top-Level mishaps, hazards, and causal factors
- Identify Potential System Hazard and Generate Hazard Worksheets

SRCA

- Identify safety critical requirements
- Determine SHRI
- Develop requirements verification Matrix
- Participate in Testing and Safety Verification

SSHA

- Identify hazards associated with:
1. Design of subsystems;
2. Component failure modes
3. Functional relationships between components

SHA

- Identify risk associated w/ passing of safety critical data between I/Fs
- Define and consider Operational Modes, system failures, training etc.

O&SHA

- Assess Safety Issues for Operator Impact
- Recommend Mitigations
- Write Mitigations
- Verify Implementation

HAZARD TRACKING DATABASE

Verify Hazard Mitigation Requirements → Generate MARs & Gain Risk Acceptance → Develop SAR and TDPs → Conduct Review Board Briefs

NAVSEA
WARFARE CENTERS
DAHLGREN

USS Nimitz Aircraft Carrier

NAVSEA
WARFARE CENTERS
DAHLGREN

Ticonderoga Class Aegis

NAVSEA WARFARE CENTERS
DAHLGREN

Calls for Combat System Safety

Date	System	Safety Review Board Requests/Direction
May 1999	Cooperative Engagement Capability	Recommend establish overall battleforce/combat systems safety program
Sept 1999	CEC	Safety integration and analysis between CSEs
July 2000	SSDS	Strongly recommends establish overall battleforce/combat systems safety program
May 2002	USS Nimitz	Directed to establish a Combat System Safety program
July 2003	Aegis Program	Determine mishap risk for entire combat system
Aug 2003	Aegis BMD	Address combat system
Jun 2004	Aegis 7P1	Present combat system analysis before fleet deployment
Oct 2005	VLS	Reevaluate hazards from a combat system perspective

Combat System Safety Program Objectives

- Address safety concerns driven by increasing complexity and integration of Combat Systems
  - Identification and resolution of hazards that fall outside of traditional Combat System Elements (CSEs) safety programs boundaries
    - Does not duplicate efforts at the CSE level
- Teamwork and coordination foundation of Combat System Safety Program
  - Safety team involves all CSEs that make up the Combat System
- Conduct safety analyses to identify Combat System integration hazards that fall beyond CSE boundaries
  - Risk characterization as Combat System hazards and threads within the Combat System
- Provide single safety POC concerning safety of Combat System configurations and associated certifications

Combat System Overview

- Combat System is a collection of the CSEs necessary to safely execute the capabilities and mission of the Combat System
  - Each CSE is treated as a subsystem from the Combat System point-of-view
  - All hardware and computer programs are allocated at the CSE level
    - Computer programs include software, firmware and programmable logic

Combat System: Another View

Combat System (CS): A collection of Combat System Elements (traditionally referred to as systems) integrated to perform overall situational awareness and Ship Self Defense through target search, air communications, electronic warfare, weapons control, and weapons firing. Integrated support systems, devices or interfacing systems to assist in crew training are included within the definition of Combat System.

Detect

- Radars
- IFF
- AIS
- EOIR
- EXCOMMS

Control

- C2 programs
- weapon system control programs
- ICOMS

Engage

- Guns
- Missiles
- Countermeasures

NAVSEA WARFARE CENTERS
DAHLGREN

Combat System Safety Process

PLANNING & MANAGEMENT

- Define **CS** safety approach methodology
- Establish **C**SSWG
- Develop **SSMP/**SSPP
- Establish Hazard Tracking System

HAZARD ANALYSIS & RISK REDUCTION PROCESS

PHL/ PHA

- Define safety functions, **CSEs**, and I/Fs
- Define Top-Level mishaps, hazards, and causal factors
- Identify Potential System Hazard and Generate Hazard Worksheets

SRCA

- Identify safety critical requirements
- Determine SHRI
- Develop requirements verification Matrix
- Participate in Testing and Safety Verification

SSHA

- Identify hazards associated with:
  1. Design of subsystems;
  2. Component failure modes
  3. Functional relationships between components

SHA

- Identify risk associated w/ passing of safety critical data between I/Fs
- Define and consider Operational Modes, system failures, training etc.

O&SHA

- Assess Safety Issues for Operator Impact
- Recommend Mitigations
- Write Mitigations
- Verify Implementation

HAZARD TRACKING DATABASE

Collect CSE known Safety Anomalies → **Assess CSE known Safety Anomalies for CS impact**

Verify Hazard Mitigation Requirements → **Generate MARs & Gain Risk Acceptance** → **Develop SAR and TDPs** → **Conduct SSTRP & WSESRB Briefs**

Major Differences

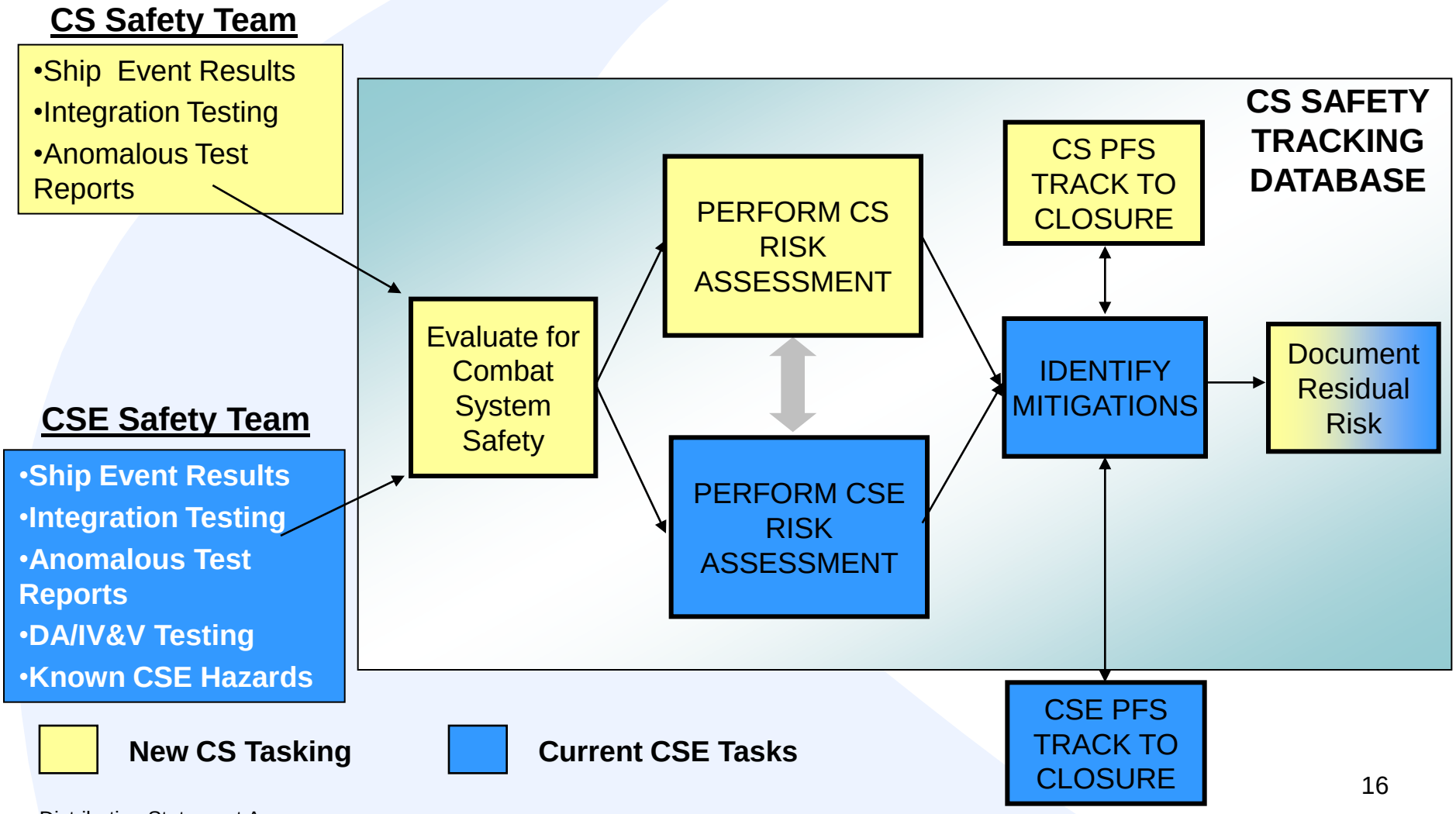
- Redefined scope
  - Combat System focuses on integration of elements
  - Combat System assesses issues that have an impact beyond the initiating element
- Collaboration
  - SoS safety requires safety engineering data from individual systems
  - SoS hazard definition and resolution requires collaborative engineering environment will all systems that make up the SoS

NAVSEA
WARFARE CENTERS
DAHLGREN

Combat System Safety Assessment Criteria

- Does the issue
  - involve an interface with another CSE?
  - impact the performance of a combat system safety function?
  - Map to a combat system Mishap, Hazard, CF?
- CSE issues that have impact beyond their element are considered on a case by case basis, including interaction with CSE PFS and design engineers as required

Combat System Risk Evaluation Process



NAVSEA
WARFARE CENTERS
DAHLGREN

Data Sharing

- New for Combat System Safety programs
- Critical to avoid duplication of effort
- Information requested from CSEs
  - Future capabilities and functionality
  - Known risk
- Information provided both directions
  - Safety and verification of products

Lessons Learned

- Dedicated CS PFS is required
  - Early involvement is critical
- CS safety cannot operate unilaterally
  - Must be cooperative effort with all stakeholders
    - Program Offices
    - CSE safety programs
    - Safety Boards
- CS safety program must execute a SE approach
  - More focus on analytical approach
  - Less focus on data gathering
- CS safety must be very involved in CS integration testing

Conclusion

- System of System environment is nothing new for the DoN
- Combat System Safety process designed for the SoS environment