System Safety in a System of Systems Environment

Janet G. McKinney, Code G72

August 2012

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

Distribution Statement A: Approved for Public Release; Distribution Unlimited
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
# 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

---

Distribution Statement A
USS Nimitz Aircraft Carrier
Ticonderoga Class Aegis
# Calls for Combat System Safety

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

<table>
<thead>
<tr>
<th><strong>Detect</strong></th>
<th><strong>Control</strong></th>
<th><strong>Engage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Radars</td>
<td>C2 programs</td>
<td>Guns</td>
</tr>
<tr>
<td>IFF</td>
<td>weapon system control programs</td>
<td>Missiles</td>
</tr>
<tr>
<td>AIS</td>
<td>ICOMS</td>
<td>Countermeasures</td>
</tr>
<tr>
<td>EOIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXCOMMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Combat System Safety Process

**PLANNING & MANAGEMENT**
- Define CS safety approach methodology
- Establish CSSWG
- 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

**Distribution Statement A**
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
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

CS Safety Team
- Ship Event Results
- Integration Testing
- Anomalous Test Reports

CSE Safety Team
- Ship Event Results
- Integration Testing
- Anomalous Test Reports
- DA/IV&V Testing
- Known CSE Hazards

New CS Tasking
Current CSE Tasks

PERFORM CS RISK ASSESSMENT
IDENTIFY MITIGATIONS
CS PFS TRACK TO CLOSURE
Document Residual Risk

CS SAFETY TRACKING DATABASE

PERFORM CSE RISK ASSESSMENT

CS PFS TRACK TO CLOSURE

CSE SAFETY TRACKING DATABASE

Distribution Statement A
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