System Safety in Systems Engineering
DAU Continuous Learning Module

NDIA Systems Engineering Conference
October 25, 2005

Amanda Zarecky
Booz Allen Hamilton
703-604-5468
zarecky_amanda@bah.com
Course Context - Drivers

- Increased DoD emphasis on safety
  - May 2003 SECDEF Memo
  - July 2003 Defense Safety Oversight Council
    - Joint Chiefs of Staff & Undersecretaries of the Services
    - Nine Task Forces

- April 2004 Acquisition and Technology Programs Task Force
  - Chair: Mr. Mark Schaeffer, USD (AT&L) Director of Systems Engineering
  - Focused on improving System Safety implementation
  - Linked efforts to Systems Engineering revitalization initiatives
  - 23 Sep 04 USD(AT&L) Memo "Defense Acquisition System Safety"
23 May 03 DoDI 5000.2 E7, Environment, Safety, and Occupational Health (ESOH)
- Strategy for integrating ESOH into Systems Engineering
- Identification of ESOH risks
- Acceptance of ESOH risks per "industry standard for system safety"
- NEPA/E.O. 12114 Compliance Schedule

23 Sep 04 USD (AT&L) Defense Acquisition System Safety memo
- Mandates integration of System Safety into Systems Engineering
- Mandates use of MIL-STD-882D

Oct 04 Defense Acquisition Guidebook
- Chapter 4, Systems Engineering
- Section 4.4.11, ESOH: "industry standard" = MIL-STD-882D
Course Development Team Effort

- USD (AT&L)/Systems Engineering
  - Col Warren Anderson, Program Manager
  - Ann Marie Choephel, Program Manager Support
  - DAU Course Developer contractors: MTC & CTC

- Subject Matter Experts from each Component and DAU
  - Trish Huheey, DUSD(I&E) (Team Lead)
  - Sherman Forbes, SAF/AQRE
  - Ben Mack, USMC (AOT, Inc.)
  - George Murnyak, US Army CHPPM
  - Paige Ripani, DUSD(I&E) (Booz Allen Hamilton)
  - Amanda Zarecky, CNO N45 (Booz Allen Hamilton)
Course Description

■ Course developed
  ▪ In response to need for training depicting how System Safety fits into the overall DoD Systems Engineering process throughout a system’s life cycle
  ▪ To teach the learning objectives and encourage active participation and coordination between System Safety Engineers and Systems Engineers

■ Top Level Outcomes
  ▪ Recognize the Defense Acquisition policy and guidance on System Safety in Systems Engineering
  ▪ Recognize System Safety methodology as the Systems Engineering approach for eliminating Environment, Safety, and Occupational Health (ESOH) hazards or minimizing ESOH risks across the system’s life cycle
Course Description (cont)

- Target Audience
  - Primary: Systems Engineers, Chief Engineers
  - Secondary: Program Managers, System Safety Engineers

- DAU Systems Engineering Elective - not required; no pre-requisites

- Counts towards 80 hours of DAWIA certified continual learning

- 3 ½ hours web-based training
Course Description (cont)

- Built around the Systems Engineering (SE) Process V-Model
- Identifies System Safety activities supporting each of the Systems Engineering activities in each phase of a systems life cycle
- Enables Systems Engineers and System Safety Engineers to understand what to expect, what to provide, and when
- Not intended to teach details of System Safety
- Assumes an understanding of Systems Engineering
Course Outline

- System Safety Overview
- System Safety Terminology
- Eight Mandatory Steps of System Safety
- Risk Assessment
- System Safety Order of Precedence
- Typical System Safety Tasks
- System Safety Throughout the System's Life Cycle
- Module Summary
System Safety Overview - Explains MIL-STD-882D methodology is DoD's SE approach for eliminating ESOH hazards or minimizing ESOH risks across the system's life cycle

Why Implement System Safety?

- Protects military and civilian personnel by reducing hazards/risk to personnel and equipment
- Reduces accidents proactively
- Improves warfighting capability and combat readiness
- Reduces total ownership costs
- Lowers the risk of environmental damage
- Prioritizes hazards for corrective action
- Reduces need for system retrofits
- Required by DoDI 5000.2 (May 2003) and USD(AT&L) Memo (Sep 23, 2004)
System Safety Terminology - Defines terms pertinent to use of system safety in the SE process

**System Safety Terminology**

*Directions:* Listed below are terms that are relevant to system safety and the systems engineering process. You may already be familiar with some of the terms. Please click each term below that is unfamiliar to you (or that you would like to review) to reveal its definitions.

<table>
<thead>
<tr>
<th>System</th>
<th>System Life Cycle</th>
<th>Systems Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Safety</td>
<td>System Safety Engineering</td>
<td>Environment, Safety, and Occupational Health (ESOH)</td>
</tr>
<tr>
<td>Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)</td>
<td>Human Systems Integration (HSI)</td>
<td>Hazard</td>
</tr>
<tr>
<td>Causal Factor</td>
<td>Mishap</td>
<td>Risk</td>
</tr>
<tr>
<td>Mitigation Measure</td>
<td>Residual Risk</td>
<td></td>
</tr>
</tbody>
</table>
Eight Mandatory Steps of System Safety - Describes application of each of
the steps in the system safety process outlined in MIL-STD-882D

Lesson Overview

1. Document the system safety approach
2. Identify hazards
3. Assess risk
4. Identify risk mitigation measures
5. Reduce risk to acceptable level
6. Verify risk reduction
7. Review hazards and accept residual risk by appropriate authority
8. Track hazards, their closures, and residual risk
Eight Mandatory Steps of System Safety – Knowledge Review

Drag-and-Drop Challenge

Directions: The following are the steps taken by the (fictitious) Marauder Howitzer Program Office team to mitigate the risk of extreme temperatures causing the gun barrel to warp, a round to jam in the barrel, followed by an in-bore explosion that severely injures or kills the operators and destroys the Howitzer. Arrange the activities in the order that accurately reflects the system safety process. Then click the Submit button. The Next button will return to the navigation bar when the answer is correct. Click here if you require a text-based version of this challenge.

- Discover potential round jamming hazard.
- Install LBDD to detect gun barrel warping.
- Document the system safety approach.
- Track rounds jamming in the gun barrel.
- Document PM acceptance of residual risk.
- Assign initial risk category as high.
- Verify residual risk following installation of LBDD.
- Identify alternatives for eliminating hazard or reducing risk.

Submit
Risk Assessment - Provides a systematic process for assessing risk and determining appropriate risk acceptance authority
Risk Assessment – Knowledge Review

**Risk Acceptance Authority, Cont.**

**Directions:** Use the Risk Assessment and Acceptance Matrix to answer each of the following challenges.

**Challenge:** Who is the acceptance authority if the severity category is marginal and the probability level is frequent? [Answer]

**Challenge:** Who is the acceptance authority if the severity category is catastrophic and the probability level is improbable? [Answer]

---

**Risk Assessment and Acceptance Matrix**

<table>
<thead>
<tr>
<th>PROBABILITY LEVEL</th>
<th>SEVERITY CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I CATASTROPHIC</td>
</tr>
<tr>
<td>(A) Frequent</td>
<td>1 (I A)</td>
</tr>
<tr>
<td>(B) Probable</td>
<td>2 (I B)</td>
</tr>
<tr>
<td>(C) Occasional</td>
<td>4 (I C)</td>
</tr>
<tr>
<td>(D) Remote</td>
<td>8 (I D)</td>
</tr>
<tr>
<td>(E) Improbable</td>
<td>12 (I E)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
<th>Category</th>
<th>Acceptance Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, 4, 5</td>
<td>HIGH</td>
<td>Component Acquisition Executive</td>
</tr>
<tr>
<td>6, 7, 8, 9</td>
<td>SERIOUS</td>
<td>Program Executive Officer</td>
</tr>
<tr>
<td>10, 11, 12, 13, 14, 15, 16, 17</td>
<td>MEDIUM</td>
<td>Program Manager</td>
</tr>
<tr>
<td>18, 19, 20</td>
<td>LOW</td>
<td>Program Manager</td>
</tr>
</tbody>
</table>
System Safety Order of Precedence - Identifies and explains application of DoD's system safety order of precedence for eliminating ESOH hazards or minimizing ESOH risks

<table>
<thead>
<tr>
<th>Most to Least Preferred Risk Mitigation Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Eliminate hazards through design selection</strong></td>
</tr>
<tr>
<td><strong>2. Incorporate safety devices</strong></td>
</tr>
<tr>
<td><strong>3. Provide warning devices</strong></td>
</tr>
<tr>
<td><strong>4. Develop procedures and training</strong></td>
</tr>
</tbody>
</table>

**Note:** For catastrophic or critical hazards, avoid using warning, caution, or other written advisory as the only risk reduction method.
### System Safety Order of Precedence (cont)

#### Marauder Howitzer SHA

**Risk Mitigation Measure 1b**

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Hazardous Effects</th>
<th>Causal Factors</th>
<th>IS</th>
<th>IP</th>
<th>IRV</th>
<th>IRC</th>
<th>Risk Mitigation</th>
<th>FS</th>
<th>FP</th>
<th>FRV</th>
<th>FRC</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round jams in barrel when fired</td>
<td>Round initiates causing in-bore explosion resulting in personnel death and weapon destruction</td>
<td>Warped gun barrel from a combination of extreme external temperature, e.g., in Desert Warfare, and high fire rate</td>
<td>I</td>
<td>B</td>
<td>2</td>
<td>High</td>
<td>Develop new barrel design using new technology composite material that will contain blast over pressure. New barrel design will minimize warping and is a line replaceable unit that costs $50K to minimize downtime in the event of an in-bore explosion. This design change allows only minor system damage and no injury to personnel.</td>
<td>III</td>
<td>D</td>
<td>14</td>
<td>Medium</td>
<td>Closed. The Program verified that new barrel design using the new technology composite material reduced the probability of warping (causal factor) and reduced the severity of the mishap occurring by being able to contain and dissipate the blast over pressure. The Program Manager formally accepted the FRC.</td>
</tr>
</tbody>
</table>

**Additional Notes**

- **IS** = Initial Risk Severity Category
- **FS** = Final Risk Severity Category
- **CAE** = Component Acquisition Executive
- **IP** = Initial Risk Probability Level
- **FP** = Final Risk Probability Level
- **IRV** = Initial Risk Value
- **FRV** = Final Risk Value
- **PEO** = Program Executive Officer
- **PM** = Program Manager
- **IRC** = Initial Risk Category
- **FRC** = Final Risk Category

---

**D**
System Safety Order of Precedence (cont)

<table>
<thead>
<tr>
<th>PROBABILITY LEVEL</th>
<th>SEVERITY CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I CATASTROPHIC</td>
</tr>
<tr>
<td>(A) Frequent</td>
<td>1</td>
</tr>
<tr>
<td>(B) Probable</td>
<td>2</td>
</tr>
<tr>
<td>(C) Occasional</td>
<td>4</td>
</tr>
<tr>
<td>(D) Remote</td>
<td>8</td>
</tr>
<tr>
<td>(E) Improbable</td>
<td>12</td>
</tr>
</tbody>
</table>

- High Risk
- Medium Risk
- Initial Risk
- Residual Risk

EXAMPLE ONLY
Drag-and-Drop Challenge

You are leading the Program Office team of the (fictitious) Marauder Howitzer. Please click round jamming hazard to review critical background information before completing the following challenge.

**Directions:** Listed below are four alternative measures to mitigate the round jamming hazard. Based on the system safety design order of precedence, indicate the order in which each alternative should be applied by placing the Number 1 beside the most preferred; the Number 2 beside the second preferred; etc. Then click the Submit button. The Next button will return to the navigation bar when the answer is correct. Click here if you require a text-based version of this challenge.

1. Train operators to routinely check for barrel warping.
2. Install alarm to alert operators to gun barrel warping.
3. Install safety interlock that prevents firing if the barrel is warped.
4. Change the design to preclude a round jamming in the barrel.

Submit
Typical System Safety Tasks - Provides detailed descriptions of several widely-used system safety analytical and assessment tools

<table>
<thead>
<tr>
<th>Safety Requirements/Criteria Analysis (SRCA)</th>
<th>Health Hazard Assessment (HHA)</th>
<th>Safety Assessment Report (SAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary Hazard List (PHL)</td>
<td>Preliminary Hazard Analysis (PHA)</td>
<td>Subsystem Hazard Analysis (SSHA)</td>
</tr>
<tr>
<td>System Hazard Analysis (SHA)</td>
<td>Operating &amp; Support Hazard Analysis (O&amp;SHA)</td>
<td>Sneak Circuit Analysis (SCA)</td>
</tr>
<tr>
<td>Fault Tree Analysis (FTA)</td>
<td>Failure Modes and Effects Analysis (FMEA)</td>
<td>Operational Trend Analysis</td>
</tr>
<tr>
<td>Threat Hazard Assessment (THA)</td>
<td>Failure Modes, Effects, and Criticality Analysis (FMECA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Safety Program Plan (SSPP)</td>
<td></td>
</tr>
</tbody>
</table>
System Safety Throughout the System's Life Cycle - Provides an overview of key system safety activities completed during each phase of the system life cycle.

**System Safety Activities Throughout the System Life Cycle**

**Directions:** Please click each of the five phases of the System Life Cycle to discover key safety activities completed by the system safety staff during that phase. After you have clicked each of the five phases, please click the Next button to continue.
System Safety Throughout the System's Life Cycle (cont)

Concept Refinement SE Chart

SE Chart Directions

INPUTS

- ICD
- AoA Plan
- Exit Criteria
- Alternative Maintenance & Logistics Concepts

Outputs

- Prelim Sys Spec
- T&E Strategy
- SEP
- Support & Maintenance Concepts & Technologies

Inputs to:
- draft CDD - TDS - AoA
- Cost/MANPOWER Est.

DECOMPOSE
Concept Performance into Functional
Definition & Verification Objectives

 trades

ASR

Analyze/Assess Concepts
Versus Defined User Needs &
Environmental Constraints

Analyze/Assess System
Concept Versus Functional
Capabilities

Analyze/Assess
Enabling/Critical Components
Versus Capabilities

Analyze/Assess
Enabling/Critical Technologies,
Constraints & Cost/Risk Drivers

Click each box to read the details
## Concept Refinement SE Chart

### SE Chart Directions

Alternate document containing all the information in the chart below.

### Inputs

<table>
<thead>
<tr>
<th>Inputs</th>
<th>System Safety Should:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Capabilities Document (ICD)</td>
<td>Provide inputs as requested</td>
</tr>
<tr>
<td>Analysis of Alternatives (AoA) Plan</td>
<td>Participate in AoA development</td>
</tr>
<tr>
<td>Exit Criteria</td>
<td>Provide the following exit criteria:</td>
</tr>
<tr>
<td></td>
<td>1. Preliminary Hazard List (PHL)</td>
</tr>
<tr>
<td></td>
<td>2. Strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk</td>
</tr>
<tr>
<td></td>
<td>management into the Systems Engineering Plan (SEP)</td>
</tr>
<tr>
<td>Alternative Maintenance and Logistics Concepts</td>
<td>Provide inputs as requested</td>
</tr>
</tbody>
</table>

### Objectives

- Develop Component Concepts, i.e., Enabling/Critical Technologies, Constraints & Cost/Risk Drivers

Click each box to read the details
Drag-and-Drop Challenge

**Directions:** Drag each of the system safety activities to the corresponding phase of the System Life Cycle. Then click the Submit button. The Next button will return to the navigation bar when the answer is correct. Click [here](#) if you require a text-based version of this challenge.

- **A** Evaluate each change to a fielded system for hazards
- **B** Review PCA for potential safety impacts
- **C** Present safety info at the SRR, SFR, PDR, CDR, TRR
- **D** Prepare the PESHE for Milestone B
- **E** Document the system safety approach

---

**Concept Refinement**
- Concept Decision

**Technology Development**

**System Development and Demonstration**
- Design Readiness Review

**Production and Deployment**
- LRIP/IOT&E
- FRP Decision Review

**Operations and Support**

Submit
Module Summary - Recaps essential information to reinforce attainment of the learning objectives of each lesson

Module Summary Organization

The module summary is organized by lesson. It presents the following for each lesson:

- Learning goal(s) of the lesson
- Summary of the key learning points needed to attain each learning goal

The Module Summary includes only the following lessons:

- System Safety Overview
- System Safety Terminology
- Eight Mandatory Steps of System Safety
- Risk Assessment
- System Safety Order of Precedence
- Typical System Safety Tasks
- System Safety Throughout the System's Life Cycle
Conclusion

- Continuous Learning Course helps students
  - Recognize the Defense Acquisition policy and guidance on System Safety in Systems Engineering
  - Recognize System Safety as the Systems Engineering approach for eliminating ESOH hazards or minimizing ESOH risks across the system life cycle

- Course (CLE009) available for registration at DAU’s website http://www.dau.mil/basedocs/continuouslearning.asp