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"

Course Context - DoD Policy

- 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

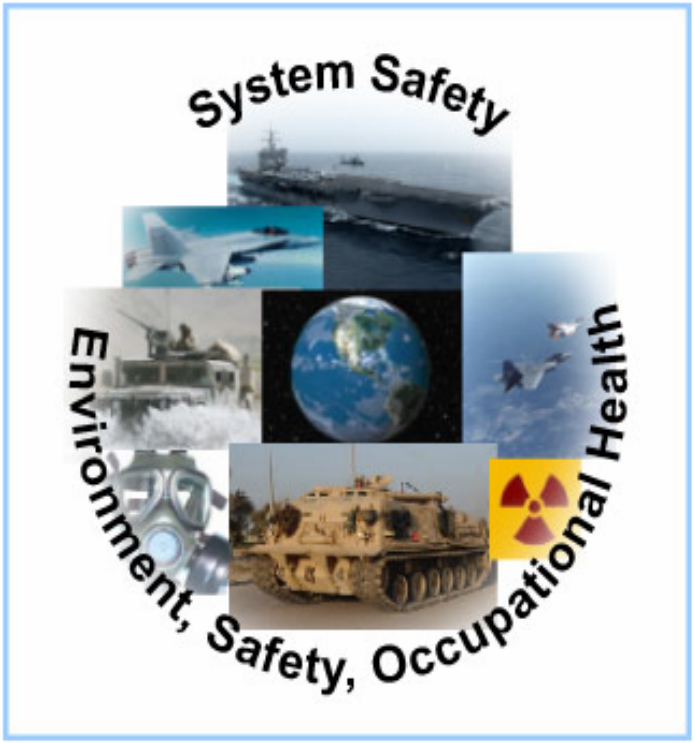
Course Outline

- 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)



D

System Safety Terminology - Defines terms pertinent to use of system safety in the SE process

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

MIL-STD-882D
10 February 2000

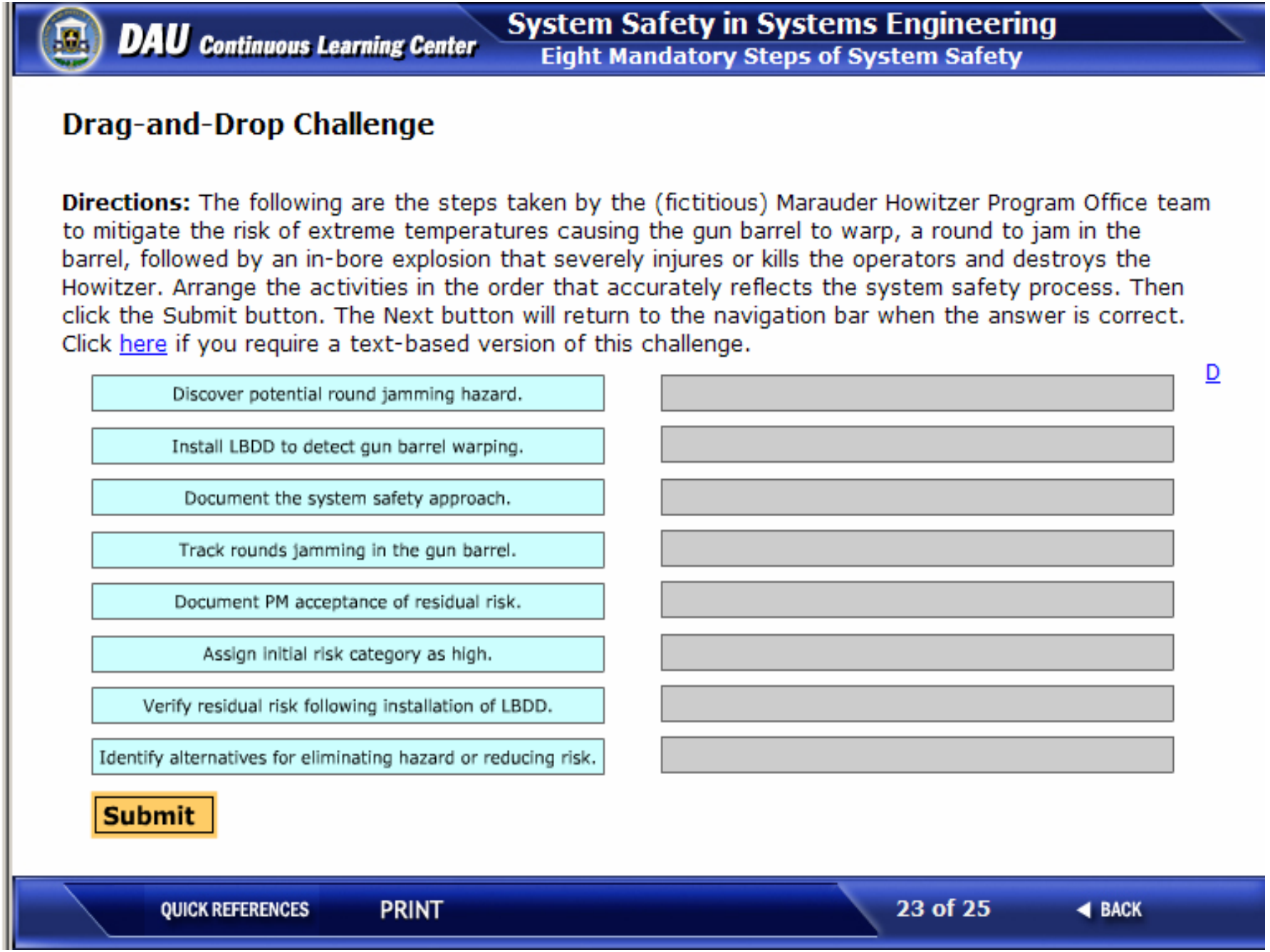
SUPERSEDING
MIL-STD-882C
19 January 1993

DEPARTMENT OF DEFENSE

STANDARD PRACTICE FOR
SYSTEM SAFETY

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



Risk Assessment - Provides a systematic process for assessing risk and determining appropriate risk acceptance authority

Overview of Mishap Assessment, Cont.

The following pages provide further details of each of these steps along with the three sample tables:

1. Severity Categories
2. Probability Levels
3. Risk Assessment and Acceptance Matrix (shown here)

MIL-STD-882D provides definitions for severity categories, probability levels, risk assessment values and risk assessment categories that will be used unless otherwise documented by the Program Office in the system safety approach.

Components of Step 1

D

Risk Assessment and Acceptance Matrix

PROBABILITY LEVEL	SEVERITY CATEGORY			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	1 (IA)	3 (IIA)	7 (IIIA)	13 (IVA)
(B) Probable	2 (IB)	5 (IIB)	9 (IIIB)	16 (IVB)
(C) Occasional	4 (IC)	6 (IIC)	11 (IIIC)	18 (IVC)
(D) Remote	8 (ID)	10 (IID)	14 (IIID)	19 (IVD)
(E) Improbable	12 (IE)	15 (IIE)	17 (IIIE)	20 (IVE)

Values	Category	Acceptance Authority
1, 2, 3, 4, 5	HIGH	Component Acquisition Executive
6, 7, 8, 9	SERIOUS	Program Executive Officer
10, 11, 12, 13, 14, 15, 16, 17	MEDIUM	Program Manager
18, 19, 20	LOW	Program Manager

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

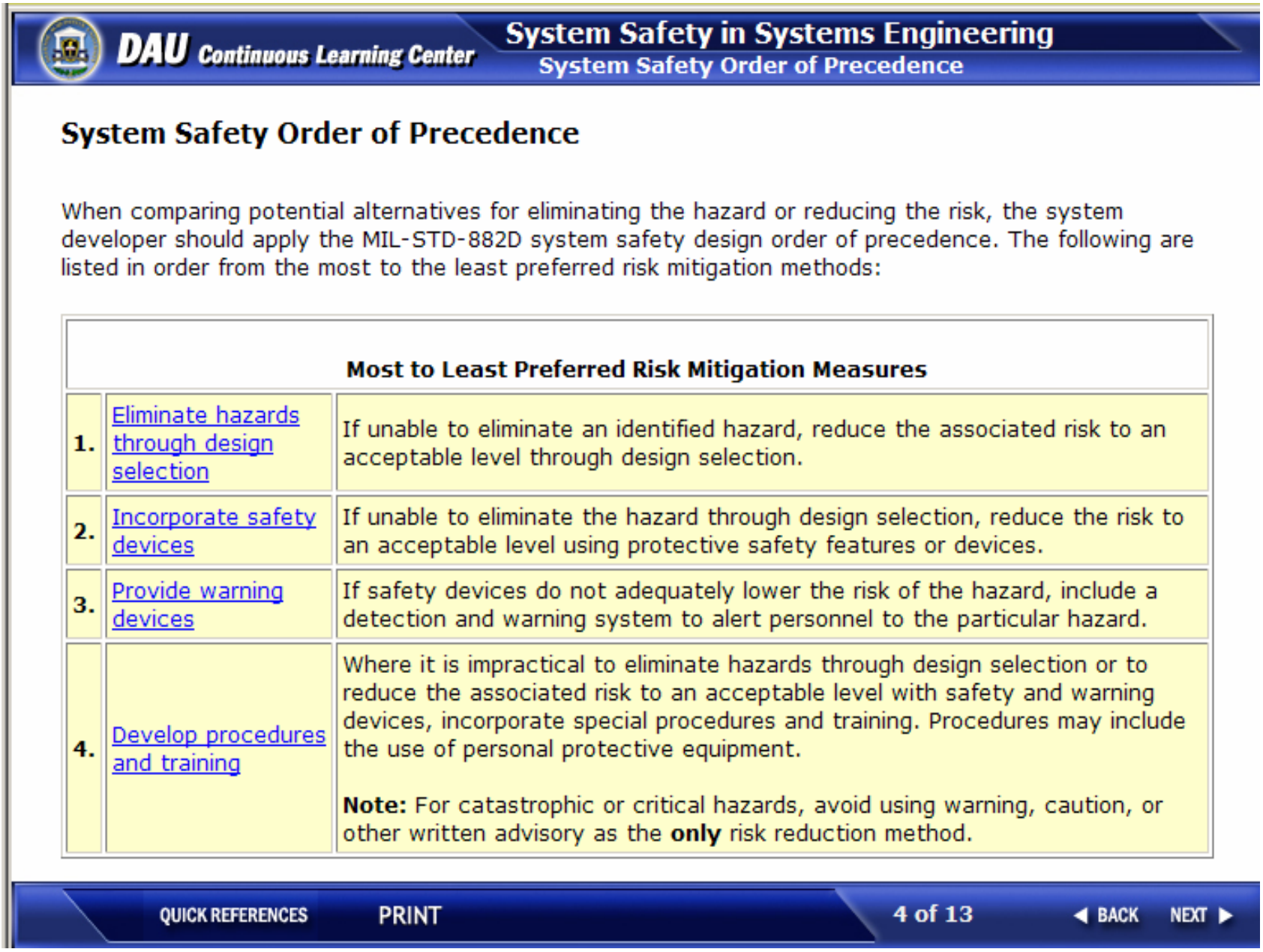
D

Risk Assessment and Acceptance Matrix

PROBABILITY LEVEL	SEVERITY CATEGORY			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	1 (IA)	3 (IIA)	7 (IIIA)	13 (IVA)
(B) Probable	2 (IB)	5 (IIB)	9 (IIIB)	16 (IVB)
(C) Occasional	4 (IC)	6 (IIC)	11 (IIIC)	18 (IVC)
(D) Remote	8 (ID)	10 (IID)	14 (IIID)	19 (IVD)
(E) Improbable	12 (IE)	15 (IIE)	17 (IIIE)	20 (IVE)

Values	Category	Acceptance Authority
1, 2, 3, 4, 5	HIGH	Component Acquisition Executive
6, 7, 8, 9	SERIOUS	Program Executive Officer
10, 11, 12, 13, 14, 15, 16, 17	MEDIUM	Program Manager
18, 19, 20	LOW	Program Manager

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



System Safety Order of Precedence

When comparing potential alternatives for eliminating the hazard or reducing the risk, the system developer should apply the MIL-STD-882D system safety design order of precedence. The following are listed in order from the most to the least preferred risk mitigation methods:

Most to Least Preferred Risk Mitigation Measures		
1.	Eliminate hazards through design selection	If unable to eliminate an identified hazard, reduce the associated risk to an acceptable level through design selection.
2.	Incorporate safety devices	If unable to eliminate the hazard through design selection, reduce the risk to an acceptable level using protective safety features or devices.
3.	Provide warning devices	If safety devices do not adequately lower the risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.
4.	Develop procedures and training	Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. **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

EXAMPLE ONLY

Example - Marauder Howitzer System Hazard Analysis Worksheet - Risk Mitigation Measure 1b

Hazard	Hazardous Effects	Causal Factors	IS	IP	IRV	IRC	Risk Mitigation	FS	FP	FRV	FRC	Status
Round jams in barrel when fired	Round initiates causing in-bore explosion resulting in personnel death and weapon destruction	Warped gun barrel from a combination of extreme external temperature, e.g., in Desert Warfare, and high fire rate	I	B	2	High	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.	III	D	14	Medium	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.

IS = Initial Risk Severity Category
FS = Final Risk Severity Category
CAE = Component Acquisition Executive

IP = Initial Risk Probability Level
FP = Final Risk Probability Level
PEO = Program Executive Officer

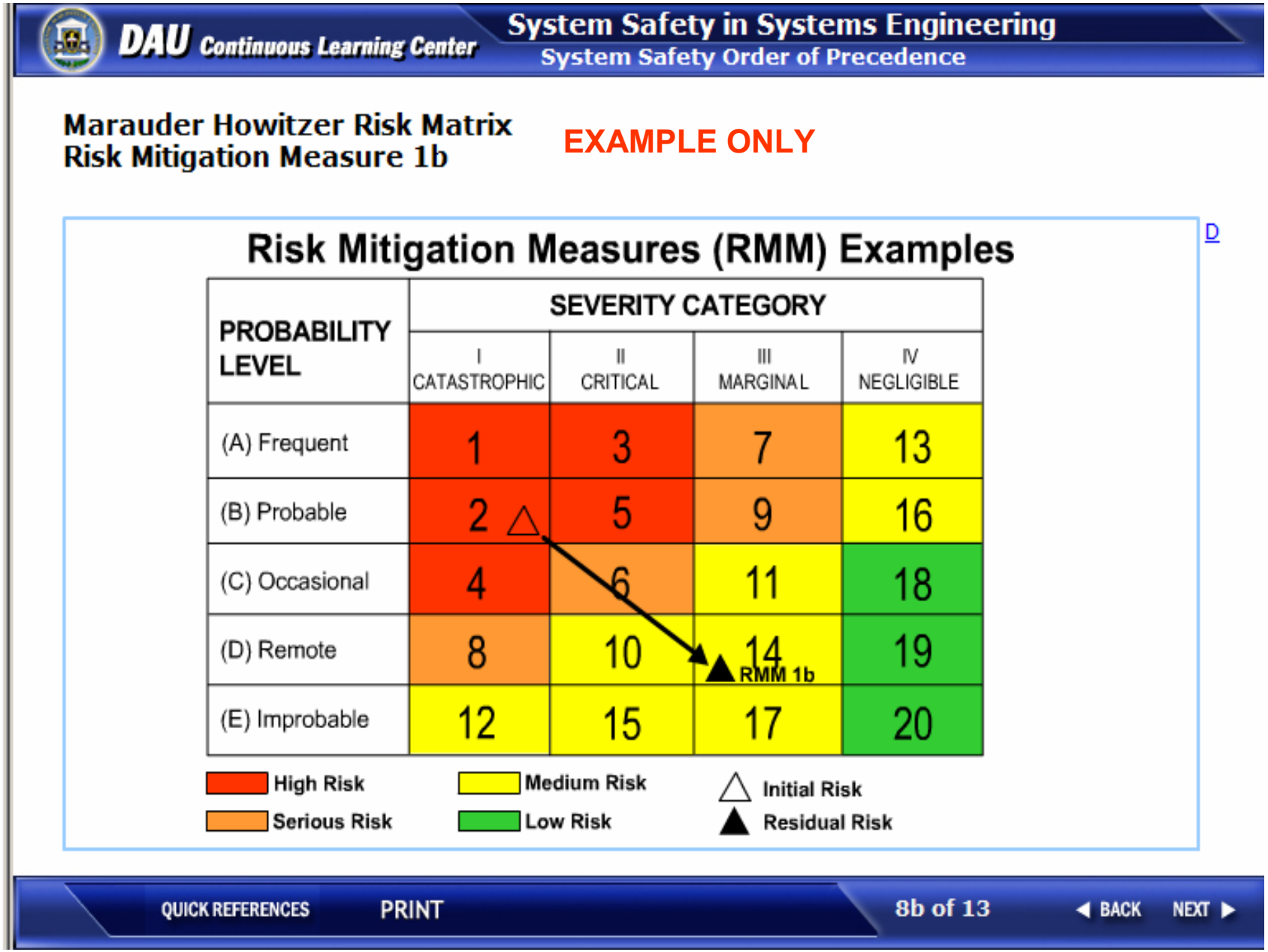
IRV = Initial Risk Value
FRV = Final Risk Value
PM = Program Manager

IRC = Initial Risk Category
FRC = Final Risk Category

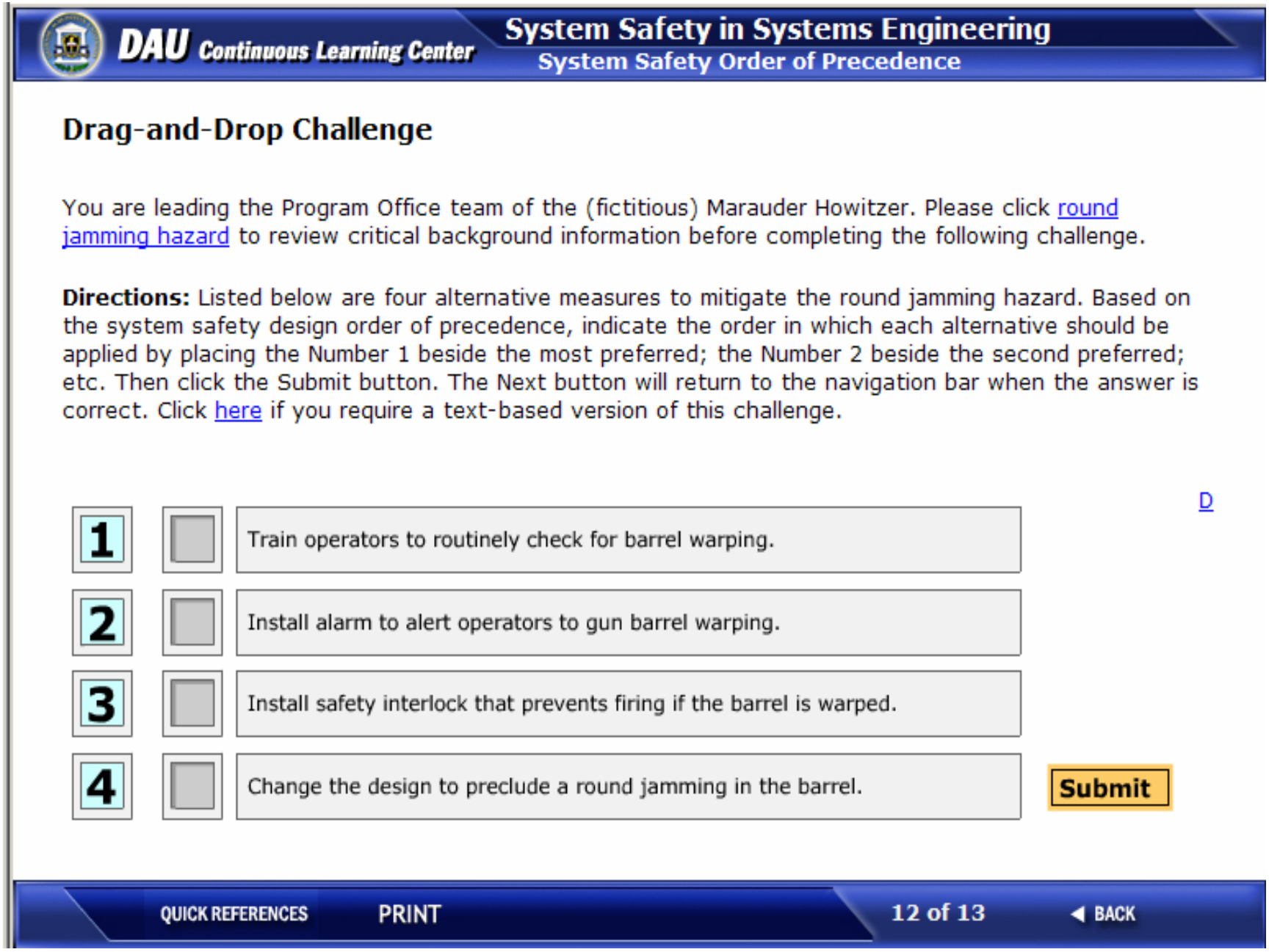
D

Close

System Safety Order of Precedence (cont)



System Safety Order of Precedence – Knowledge Review



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

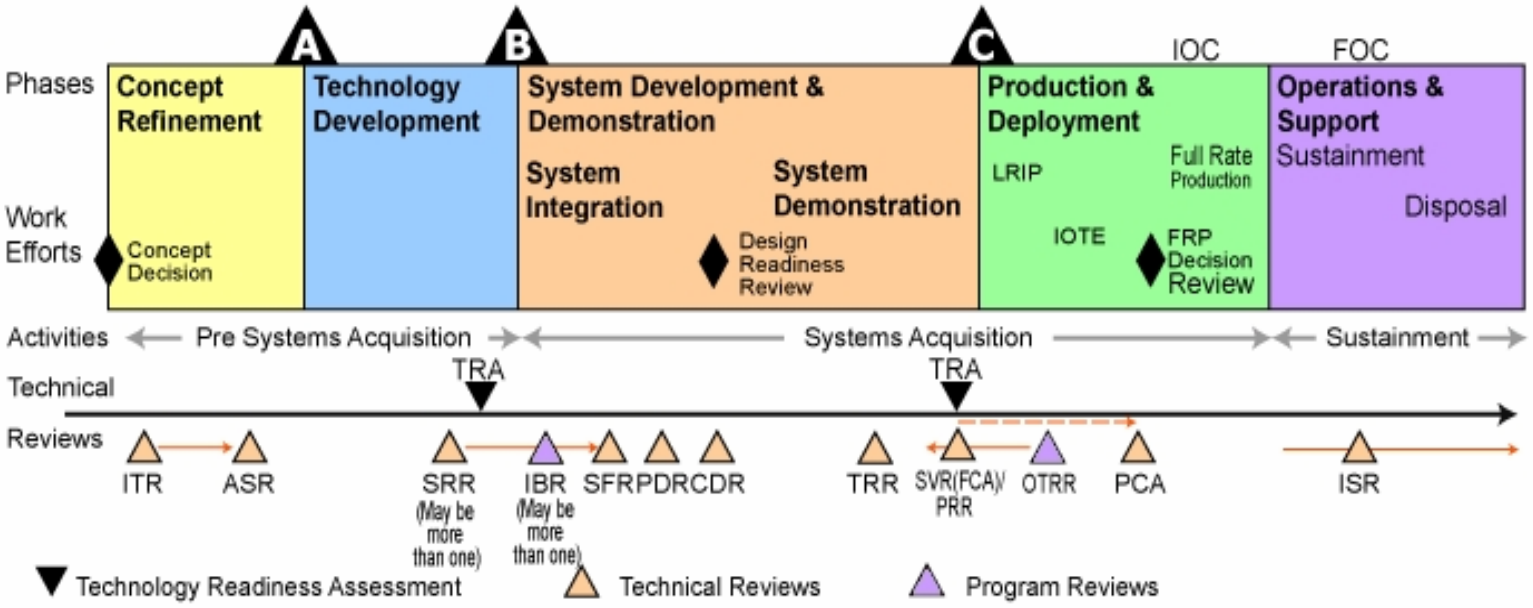
Typical System Safety Tasks, Cont.

Typical System Safety Tasks		
Safety Requirements/Criteria Analysis (SRCA)	Health Hazard Assessment (HHA)	Safety Assessment Report (SAR)
Preliminary Hazard List (PHL)	Preliminary Hazard Analysis (PHA)	Subsystem Hazard Analysis (SSHA)
System Hazard Analysis (SHA)	Operating & Support Hazard Analysis (O&SHA)	Sneak Circuit Analysis (SCA)
Fault Tree Analysis (FTA)	Failure Modes and Effects Analysis (FMEA) Failure Modes, Effects, and Criticality Analysis (FMECA)	Operational Trend Analysis
Threat Hazard Assessment (THA)	System Safety Program Plan (SSPP)	

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.

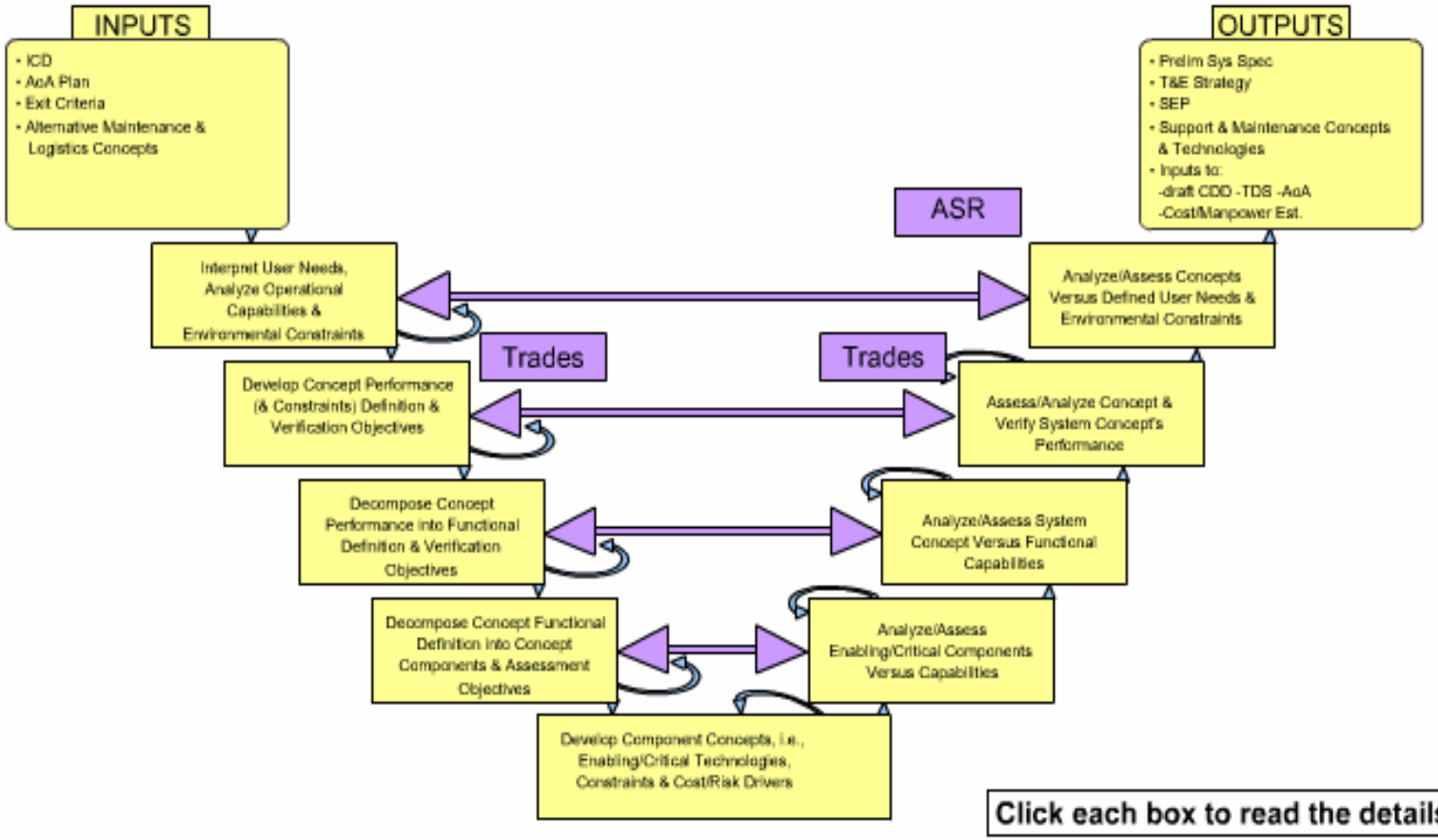


D

System Safety Throughout the System's Life Cycle (cont)

Concept Refinement SE Chart

SE Chart Directions Alternate document containing all the information in the chart below. D



Click each box to read the details

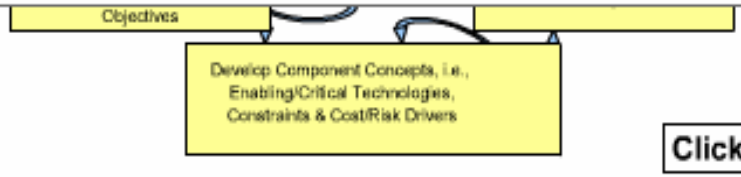
System Safety Throughout the System's Life Cycle (cont)

Concept Refinement SE Chart

SE Chart Directions **Alternate document containing all the information in the chart below.** D

X Close Window

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



Click each box to read the details

System Safety Throughout the System's Life Cycle – Knowledge Review

DAU Continuous Learning Center

System Safety in Systems Engineering

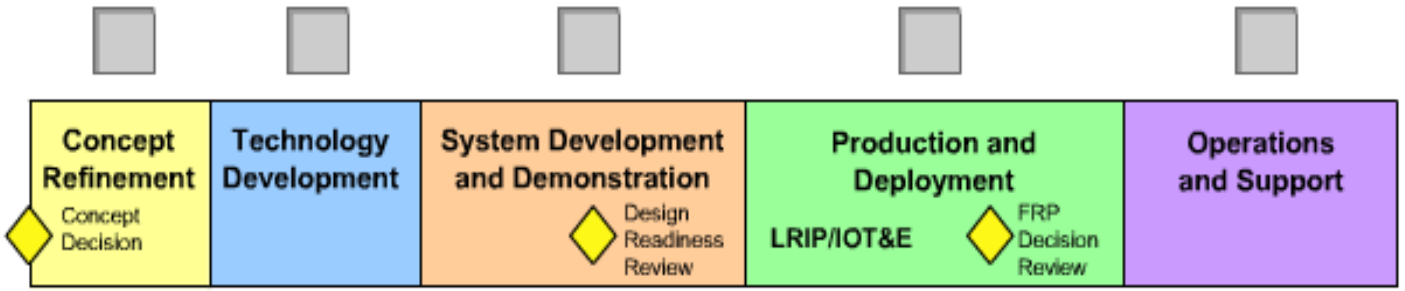
System Safety Throughout the System's Life Cycle

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.

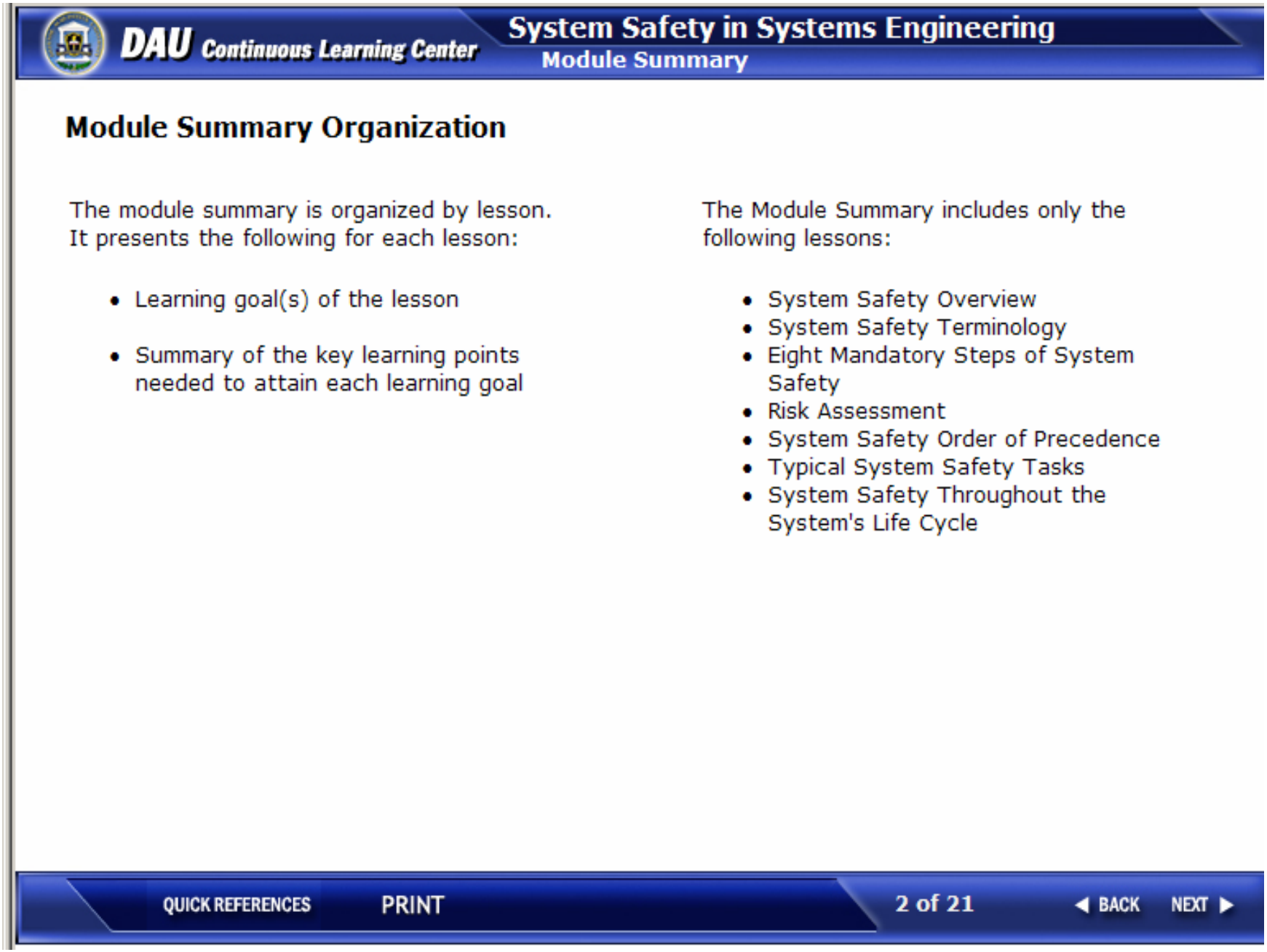
A Evaluate each change to a fielded system for hazards	**B** Review PCA for potential safety impacts	**C** Present safety info at the SRR, SFR, PDR, CDR, TRR	**D** Prepare the PESHE for Milestone B	**E** Document the system safety approach

D



Submit

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



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