Headquarters U.S. Air Force

Integrity - Service - Excellence

Using MIL-STD-882D to Integrate ESOH into SE

NDIA SE Conference
San Diego, CA
25 October 2005

Mr. Sherman G. Forbes
Office of the Deputy Assistant Secretary
(Science, Technology and Engineering)

U.S. AIR FORCE

U.S. AIR FORCE

Purpose

- **Discuss the deliberate, decade-long DoD-wide effort to integrate Environment, Safety, and Occupational Health (ESOH) Considerations into Systems Engineering (SE) using the System Safety risk management principles, with emphasis on**
  - **The benefits and challenges of institutionalizing System Safety within SE and the larger Acquisition System**
  - **Why DoD chose System Safety to be the methodology for integrating ESOH**
  - **The continuing focus on institutionalizing the "D" version of MIL-STD-882**

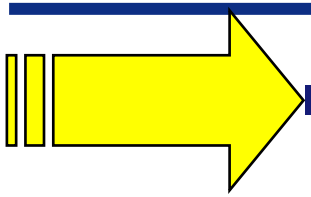
U.S. AIR FORCE

Overview

- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE
- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Overview



- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE
- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Acquisition Context

- **Defense Acquisition System -- provides effective, affordable, and timely systems to meet warfighting capability needs**
- **Systems Engineering (SE)**
  - **Translates capabilities into technical specifications**
    - **Optimizes total system performance**
    - **Minimizes total ownership cost**
  - **Employs interdisciplinary approach throughout life-cycle**
  - **Utilizes *Risk Management* to balance**
    - **External limitations, e.g,. technology, budget, *ESOH requirements***
    - **Design considerations & constraints, e.g., *ESOH***

U.S. AIR FORCE

Acquisition Context

- DoD chose System Safety as the methodology for effectively and efficiently integrating ESOH considerations into SE
  - Compatible with other SE risk management activities
  - Can consolidate and translate E, S, and OH requirements into manageable program risks
- System Safety process
  - Provides common approach for the E, S, and OH areas to interact with each other and SE
  - Needs to provide specific risk management products at key points on the SE process
  - Needs to integrate these System Safety products into overall program risk management
- DoD efforts focused on connecting E, S, and OH and SE using the System Safety process

U.S. AIR FORCE

Overview

- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE
- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Initial Breakthrough

- DoD 5000.2R (1996) integrated ESOH into Systems Engineering for the first time
  - Defined environmental compliance in risk management terms
  - Established System Safety hazard identification and risk assessment, mitigation, and acceptance requirements
  - Did not reference a standard of any kind
- PROBLEM: MIL-STD-882C (1993) was the only existing government-industry System Safety standard
  - DoD rejected it as too prescriptive
    - Defined "how to" in long list of System Safety tasks
    - Focused on multiple System Safety reports, not specific products that support program risk management
  - DoD would not allow Acquisition Programs to put MIL-STD-882C on contracts

U.S. AIR FORCE

Overview

- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE
- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Adapting MIL-STD-882

- DoD directed conversion of 882 into a performance-based Standard Practice to meet Acquisition PM needs
- Government & Industry team rewrote MIL-STD-882C
  - GEIA G-48 System Safety Committee had representatives from
    - OSD, the Services, FAA, NASA, and Coast Guard
    - All major defense corporations
  - AF published MIL-STD-882D on 10 Feb 00
    - Defined WHAT required -- 8 actions to integrate ESOH into SE
    - Focused on the process of hazard identification and risk assessment, mitigation, and acceptance -- not reports
    - Added guidance on how to apply risk management to Environmental issues
    - Approved for use on all DoD contracts without restriction

U.S. AIR FORCE

Adapting MIL-STD-882

- **MIL-STD-882D System Safety Process – 8 Actions**
  - **Document System Safety Strategy**
  - **Identify Hazards**
  - **Assess Mishap Risk**
  - **Identify Mitigation Measures**
  - **Reduce Mishap Risk to Acceptable Level**
  - **Verify Mishap Risk Reduction**
  - **Formally Accept Residual Risks**
  - **Track Hazards & Mishaps**

U.S. AIR FORCE

Adapting MIL-STD-882

Hazard Risk Index and Acceptance
DoDI 5000.2, E7.7 & MIL-STD-882D

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

HIGH(CAE)

SERIOUS (PEO)

MEDIUM (PM)

LOW (PM)

Adapting MIL-STD-882

MIL-STD-882D Severity Categories expanded to include Environmental Risk

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

U.S. AIR FORCE

Adapting MIL-STD-882

- **Risk acceptance levels defined IAW DoD Acquisition Policy**

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

- **PM puts 882D on contract to define WHAT required**
- **Contractor provides detailed plan of HOW to implement**
  - **Flexible implementation by contractor**
  - **Tailored to program size and complexity**

U.S. AIR FORCE

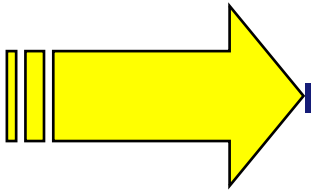
Adapting MIL-STD-882

- **Barriers to institutionalization of MIL-STD-882D**
  - **System Safety community resisted leaving 882C**
  - **G-48 Committee did not provide planned training for**
    - **System Safety Engineers and PMs**
  - **DoD lack of explicit emphasis or guidance on**
    - **Using 882D System Safety process for ESOH in SE**
    - **Connection between traditional Safety reporting and the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) document**
  - **DoD focused on PESHE as only DoD required ESOH report – issue of where to document ESOH risk data**
  - **Lack of Senior Leadership attention**

U.S. AIR FORCE

Overview

- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE



- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Institutionalizing System Safety

- 12 May 03 DoDI 5000.2, E7 laid groundwork for greater institutionalization and guidance
  - Carried over requirements from 1996 DoD 5000.2-R
  - Applies to ESOH risks identified by an Acquisition Program
    - Regardless of ACAT
    - Regardless of life cycle phase
  - Relies upon "industry standard for system safety"
- Oct 04 Defense Acquisition Guidebook (DAG)
  - ESOH discussion in Chapter 4, Systems Engineering
  - Detailed description of ESOH risk management process
  - Defines MIL-STD-882D to be the "industry standard"

U.S. AIR FORCE

Institutionalizing System Safety

- **May 2003 SECDEF Memo focused Senior Leadership attention on Safety**
  - **Established goal of 50% reduction in mishap rates**
  - **Led to creation of Defense Safety Oversight Council (DSOC)**
    - **Joint Chiefs of Staff & Undersecretaries of the Services**
    - **Eight supporting Task Forces (TF)**
- **DSOC Acquisition and Technology Programs (ATP) TF focused on System Safety**
  - **Chair: Mr. Mark Schaeffer, USD (AT&L) Director of Systems Engineering (SE)**
  - **ATP TF linked efforts to increase emphasis on System Safety to revitalization of Systems Engineering (SE)**

U.S. AIR FORCE

Institutionalizing System Safety

- 23 Sep 04 USD (AT&L) Defense Acquisition System Safety memo requires ALL DoD PMs to:
  - Integrate ESOH into SE using System Safety
  - Use MIL-STD-882D as the System Safety methodology
    - Extended debate on whether to refer to "D" exclusively
    - Firm decision by OSD and Services that "D" was most compatible with the overall Acquisition System approach
  - Incorporate ESOH integration strategy into the new Systems Engineering Plan (SEP)
  - Address ESOH risk acceptance decisions in technical and program reviews

U.S. AIR FORCE

Institutionalizing System Safety

- Connecting SE and System Safety Disciplines a key DSOC ATP TF effort
  - Oct 04 NDIA SE Conference Government & Industry Senior Level Panel on System Safety
  - Nov 04 PEO/SYSCOM Conference Senior Government Panel on System Safety
  - NDIA SE Division creation of System Safety Committee
    - Focus on implementation of 23 Sep 04 USD (AT&L) memo
    - Industry & Government Co-Chairs
  - Outreach to System Safety Society and G-48 Committee
    - Mark Schaeffer one of 4 Distinguished Speakers at the August 2005 International System Safety Conference

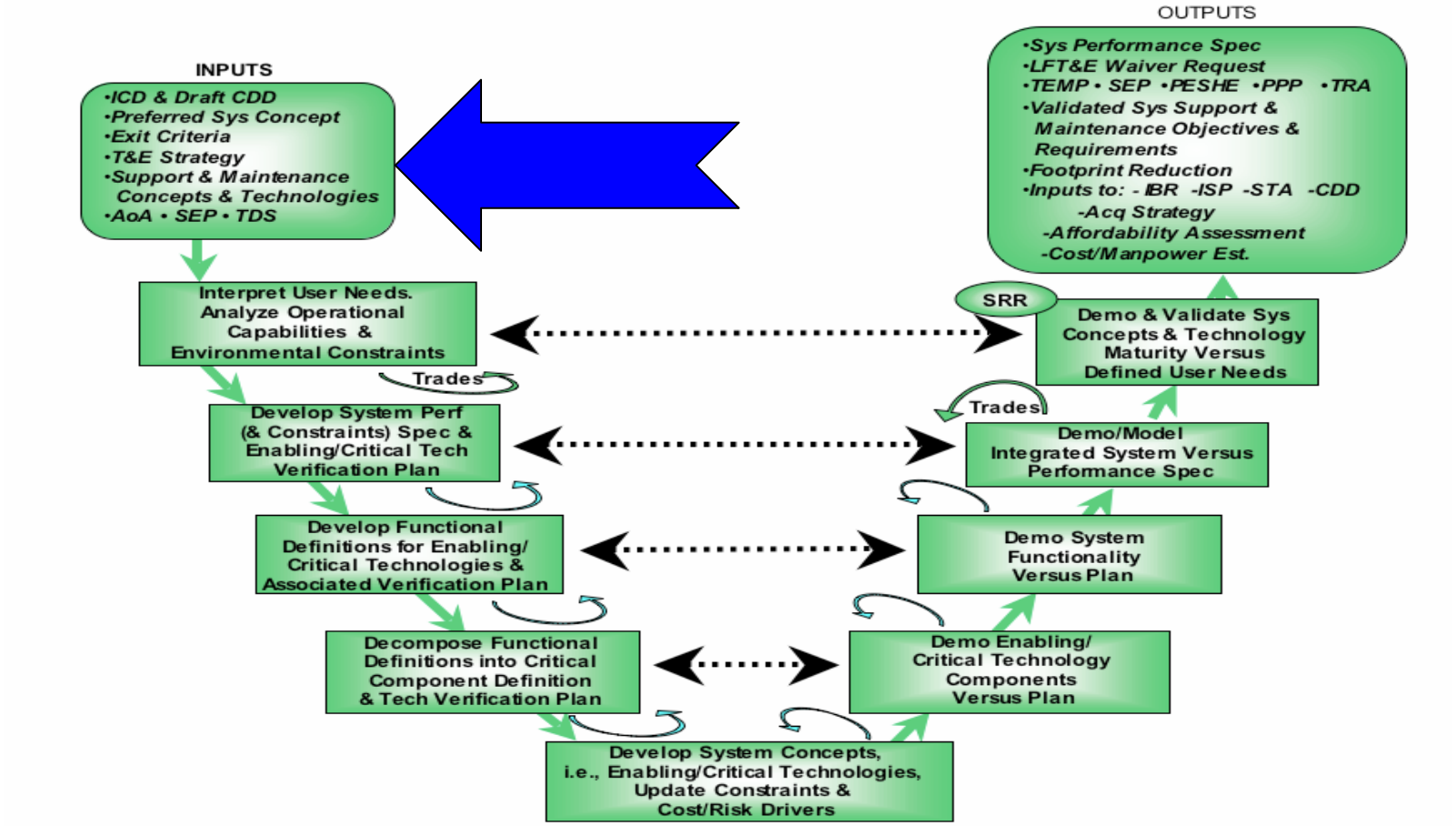
U.S. AIR FORCE

Institutionalizing System Safety

- **Defense Acquisition University (DAU) Continuous Learning Module (CLM) -- System Safety in Systems Engineering (SSSE)**
  - **Based on MIL-STD-882D**
  - **Subject Matter Experts (SMEs) from each service & industry worked together beginning in 2004**
  - **Feb 05: peer review of by government & industry practioners of SE, System Safety, Environmental Engineering, & Occupational Health**
  - **Apr 05: available to both industry & government**
  - **Maps System Safety activities into the SE V-Model**
  - **Maps government and industry relationships**

Institutionalizing System Safety

SSSE CLM Course Material - Technology Development Phase



Institutionalizing System Safety

U.S. AIR FORCE

SSSE CLM Course Material - Technology Development Phase

Inputs	System Safety Should:
Initial Capabilities Document (ICD) and Draft Capability Development Document (CDD)	Develop system safety criteria and requirements
Preferred System Concept	Evaluate system concept against identified system safety criteria
Exit Criteria	Provide the following exit criteria: 1. Update Preliminary Hazard List (PHL) 2. Update strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk management into systems engineering (SE)
Test and Evaluation (T&E) Strategy	1. Incorporate hazard risk mitigation test and verification methodologies 2. Provide approach toward obtaining safety release(s)
Support and Maintenance Concepts and Technologies	Provide inputs as requested
Analysis of Alternatives (AoA)	Characterize ESOH footprints or risks for AoA development
Systems Engineering Plan (SEP)	Update strategy for integrating ESOH risk management into SE
Technology Development Strategy (TDS)	1. Include strategy to identify hazards 2. Identify needed ESOH technology development

U.S. AIR FORCE

Institutionalizing System Safety

- 29 Jul 05 Air Force Instruction 63-101
  - Includes key System Safety (ESOH in SE) requirements from
    - 10 Feb 00 MIL-STD-882D
    - 12 May 03 DoDI 5000.2
    - 23 Sep 04 USD(AT&L) policy memo
    - 17 Oct 04 DoD Acquisition Guidebook
  - Key requirements include
    - Use of MIL-STD-882D to integrate ESOH into SE
    - ESOH documentation requirements
      - Acquisition Strategy
      - SEP
      - Risk Management Plan
      - Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)

U.S. AIR FORCE

Institutionalizing System Safety

- 29 Jul 05 AFI 63-101 Key Requirements (cont'd)
  - ESOH risk management data included in
    - Annual Expectation Management Reviews
    - Technical Reviews
    - Programmatic Reviews
  - Defines three types of ESOH risks (from DAG) due to
    - Routine operations and maintenance
    - System or subsystem failures (mishaps)
    - ESOH compliance on cost, schedule, & performance
  - Risk acceptance responsibilities

U.S. AIR FORCE

Overview

- Acquisition Context for System Safety
- Initial System Safety-ESOH-SE Breakthrough
- Adapting MIL-STD-882 to Support the DoD Acquisition System and SE
- Institutionalizing System Safety-ESOH-SE Integration
- Way Ahead

U.S. AIR FORCE

Way Ahead

- **Need to convert to a more traditional risk management 5X5 matrix of High-Medium-Low risks**
  - **Alignment with the rest of the Risk Management approaches in DoD Acquisition**
  - **Provide transparent communication about ESOH risks during technical and program reviews**
  - **More effective support to the customer – the PM**
- **Need to avoid going back to prescriptive 882**
  - **Drives unnecessary costs**
  - **Limits flexibility and innovation**
  - **Alternative ways to document traditional System Safety "tasks" to support System Safety engineers**

U.S. AIR FORCE

Way Ahead

- **ESOH Risk Acceptance role for Operational Commands -- not just Acquisition community decision**
  - **Needs greater definition & emphasis on existing guidance**
  - **Especially for Systems in Sustainment**
- **Improved clarification on relationships between PESHE & traditional System Safety documentation**
- **Standardized System Safety effectiveness evaluation criteria -- in work by the DSOC ATP TF**
  - **Already adopted in Defense Acquisition Executive Summary (DAES) for systems in Sustainment**
  - **Help clarify expectations for System Safety ESOH management as an integral part of SE process**

U.S. AIR FORCE

Summary

- **Institutionalizing System Safety within SE and the Acquisition System**
  - **Benefit - Makes System Safety directly useful and necessary to a DoD core business area**
  - **Challenge - Requires System Safety professionals to adapt their discipline to SE and Acquisition System expectations**
- **System Safety is <u>the</u> methodology for integrating ESOH because it can consolidate and translate E, S, and OH requirements into manageable program risks**
- **DoD will continue to focus on institutionalizing 882D**
  - **Compatible with prevailing Acquisition System approach**
  - **Hard-won policy and training infrastructure built around it**

BACK UP CHARTS

U.S. AIR FORCE

Risk Acceptance Authority

Hazard Risk Index and Acceptance
DoDI 5000.2, E7.7 & MIL-STD-882D

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

HIGH(CAE)

SERIOUS (PEO)

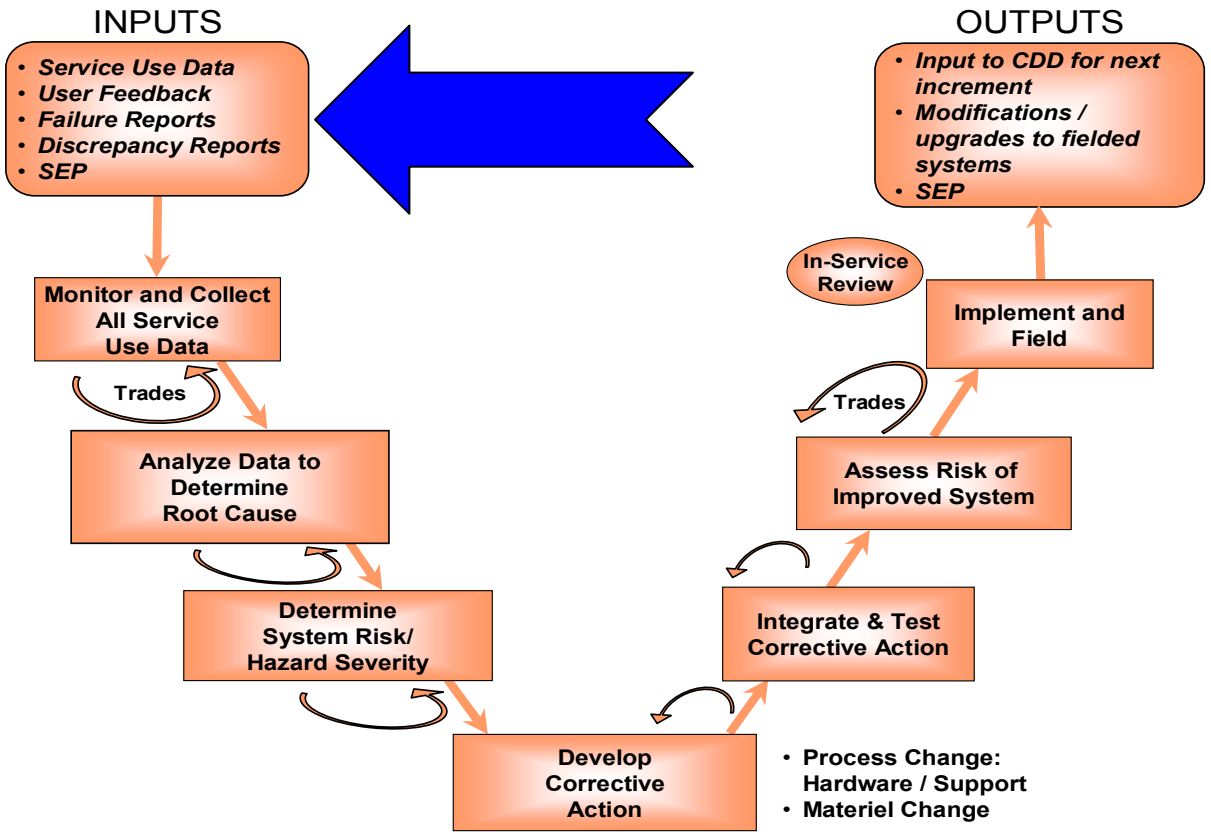
MEDIUM (PM)

LOW (PM)

Institutionalizing System Safety

U.S. AIR FORCE

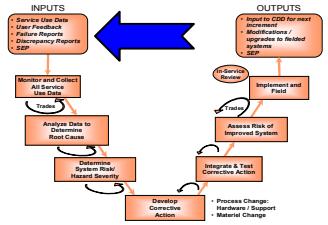
OPERATIONS AND SUPPORT PHASE



U.S. AIR FORCE

Institutionalizing System Safety

OPERATIONS AND SUPPORT PHASE



Inputs	System Safety Should:
Service Use Data	Review for system safety implications
User Feedback	Review for system safety implications
Failure Reports	1. Review Follow-On Operational Test & Evaluation (FOT&E) results for system safety implications 2. Review failure/mishap reports for causal factors or mitigation failures and recommend alternative mitigation measures 3. Assist in mishap investigations as requested
Discrepancy Reports	Review discrepancy reports for system safety implications
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval

U.S. AIR FORCE

ESOH Risk Management Keys

- Develop mitigation measures using System Safety Order of Precedence based on assessed risks
  - Higher the risk -- higher up the Order of Precedence
  - High & Serious Risks -- require more effective measures
    - Design or material changes to eliminate or reduce the risk
    - Control systems to prevent mishaps
  - Medium & Low Risks -- allow use of less effective and less expensive solutions to reduce the risk, if even necessary
    - Warning devices
    - Procedural changes and training

U.S. AIR FORCE

Risk-Based ESOH Management

- **Three types of ESOH risk to be identified and assessed**
  - **Potential for adverse impacts to ESOH from routine system use**
  - **Potential for adverse impacts to ESOH and mission readiness from system failures or mishaps**
  - **Potential for adverse impacts to program cost, schedule, and performance from ESOH compliance requirements**
- **Purpose of risk-based ESOH management approach**
  - **To determine what ESOH laws/regulations apply to the system**
  - **To prioritize Acquisition Program Office efforts to comply**
  - **To determine how Acquisition Program Office will comply**