Headquarters U.S. Air Force

Integrity - Service - Excellence

Using System Safety to Manage Acquisition ESOH Risks

U.S. AIR FORCE

PEO/SYSCOM Conference
16-17 November 2004

Mr. Terry Jaggers

Associate Deputy Assistant Secretary of the Air Force (Science, Technology and Engineering)

U.S. AIR FORCE

Context

- **Defense Acquisition System -- provides systems to meet warfighting capability needs**
- **Systems Engineering (SE)**
  - **Translates capabilities into technical specifications to**
    - **Optimize total system performance**
    - **Minimize total ownership cost**
  - **Balances**
    - **External limitations, e.g,. technology, budget, *ESOH requirements***
    - **Design considerations & constraints, e.g., *ESOH***

U.S. AIR FORCE

Policy Implementation

- **Integrate Environment, Safety, and Occupational Health (ESOH) considerations into the Systems Engineering (SE) process using the Standard Practice for System Safety, MIL-STD-882D**
  - **12 May 03 DoDI 5000.2, E7.7, ESOH**
  - **23 Sep 04 USD (AT&L) Defense Acquisition System Safety Policy Memo**
  - **14 Oct 04 DoD Acquisition Guidebook, Chapter 4, SE**

REQUIREMENT DATES BACK TO 1996 DoD 5000.2-R

U.S. AIR FORCE

What is System Safety?

"The application of engineering and management principles, criteria, and techniques

to achieve acceptable mishap risk

within the constraints of operational effectiveness and suitability, time and cost

throughout ALL phases

of the system life cycle."

- MIL-STD-882D

U.S. AIR FORCE

System Safety Process

1. Document System Safety Strategy
2. Identify Hazards
3. Assess Mishap Risk
4. Identify Mitigation Measures
5. Reduce Mishap Risk to Acceptable Level
6. Verify Mishap Risk Reduction
7. Formally Accept Residual Risks
8. Track Hazards & Mishaps

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)

U.S. AIR FORCE

Matrix Utility

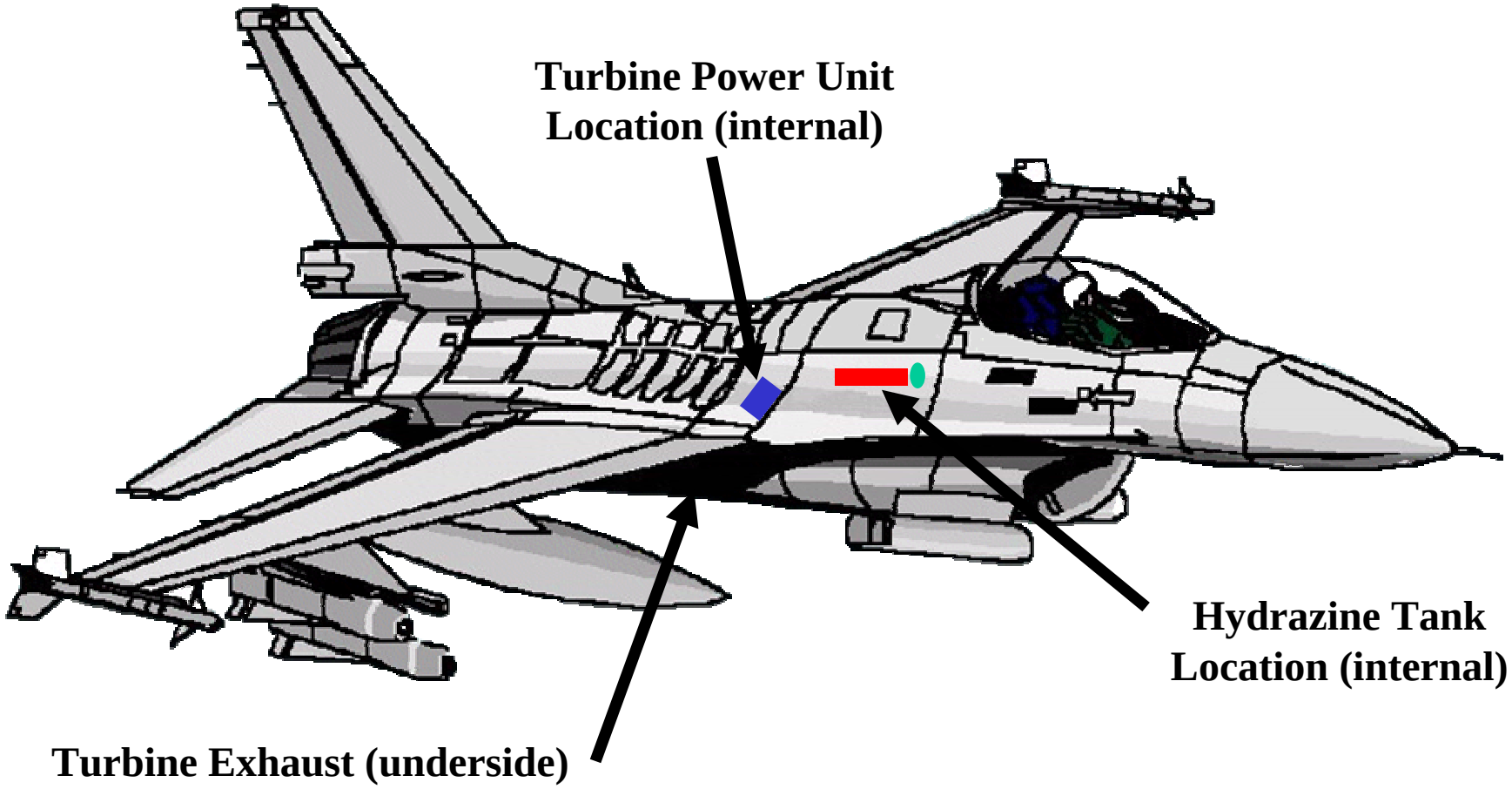
- Brings all 8 System Safety steps together
- Drives application of Order of Precedence
  - Red/Orange
    - High/Serious Risks
    - Design in Safety or Add controls or Accept by CAE/PEO
  - Yellow/Green
    - Medium/Low Risks
    - Warning Devices or Procedures/Training or Accept by PM
- Codifies Impacts
  - Routine use
  - Mission Readiness/Performance
  - Programmatic -- from ESOH compliance requirements

Strategy for ESOH Management

U.S. AIR FORCE

F-16 Use of Hydrazine

F-16 Emergency Power Unit (EPU)



F-16 EPU Hydrazine Operations and Maintenance - Field Developed Mitigation Measures

U.S. AIR FORCE

F-35 Joint Strike Fighter

- Strong ESOH management effort -- people, resources, leadership attention
- Focused on Hazardous Materials (HAZMAT)
  - E.G., ODS free system
  - Top ESOH priority by default
- Higher risks to program success posed by
  - Engine NOX emissions
  - Engine noise levels

U.S. AIR FORCE

AF Implementation -- Policy

- **PMs integrate System Safety into SE**
  - Incorporated in new AF Policy Directive (AFPD) 90-8
  - Incorporating in revised AF Instruction (AFI) 63-101
- **PMs use MIL-STD-882D**
  - Incorporated in new AFPD 90-8 & going into AFI 63-101
  - Emphasize in promulgation memo next month
- **PMs incorporate ESOH into SEP**
  - Lessons learned from SEP already submitted
  - Incorporating in revised AFI 63-101 and promulgation memo
- **PMs address ESOH decisions in tech/program reviews**
  - Incorporated in AFPD 90-8 & going into AFI 63-101
  - Emphasize in promulgation memo

U.S. AIR FORCE

AF Implementation -- Education & Training

- Work jointly through
  - DSOC ATP TF
  - DoD Acquisition ESOH IPT (since 1998)
- PEO/SYSCOM Conference
- NDIA Systems Engineering (SE) Conference
- NDIA SE Division & System Safety Society affiliation
- Criteria to assess Program Office System Safety
- DAU Continuous Learning Module *System Safety in Systems Engineering*
  - Unique contribution to grass roots implementation
  - Maps System Safety into SE V-Model

U.S. AIR FORCE

Summary

- AF committed to reducing operational mishaps thru disciplined SE process during development & sustainment
- AF implementing OSD (AT&L) memo thru policy promulgation, education, and training
- AF fully endorses MIL-STD-882D performance-based guidance to provide PMs flexible tools to manage ESOH risks

U.S. AIR FORCE

BACK UP CHARTS

U.S. AIR FORCE

Why MIL-STD-882D?

- **Performance-Based Standard Practice**
  - **Revised 10 Feb 00 as part of Specs & Standards Reform effort**
  - **Govt & Industry team rewrote 1993 MIL-STD-882C**
    - **Preparing Activity: Air Force Materiel Command**
    - **GEIA G-48 System Safety Committee**
  - **Eliminated proscriptive requirements**
  - **Added guidance on how to apply risk management to Environmental issues -- 1996 DoD 5000 requirement**
  - **Approved for use on all DoD contracts without restriction**

U.S. AIR FORCE

Why MIL-STD-882D?

- Defines WHAT REQUIRED, not HOW TO DO IT
  - Allows Program Offices & Contractors execution flexibility
  - Only Section 4, General Requirements, binding contractually
    - Only 8 mandatory steps
    - Define iterative, continuous process
  - Appendix provides detailed GUIDANCE, e.g.
    - System Safety Planning Subtasks
    - Safety Performance Requirements
    - Safety Design Requirements
    - Suggested Mishap Severity Categories and Probability levels
    - Example risk assessment matrix

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**

AF Implementation of 23 Sep 04 OSD System Safety Policy

- **Working as member of Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force and the DoD Acquisition Environment, Safety, and Occupational Health (ESOH) IPT on**
  - **17 Nov 04 System Safety Panel at the PEO/SYSCOM Conference**
  - **Defining criteria for assessing effectiveness of Program Office System Safety efforts as part of the overall SE effort**
  - **Developing Defense Acquisition University Continuous Learning Module on "System Safety Integration into SE"**