Headquarters U.S. Air Force

Integrity - Service - Excellence

18001 — ESOH Risk Management for Fielded Systems

U.S. AIR FORCE

Mr. Sherman Forbes
SAF/AQRE
sherman.g.forbes.civ@mail.mil
703-254-2480
ESOH Track - 4B6
29 October 2015
Version 8

U.S. AIR FORCE

Bottom Line Up Front (BLUF)

- DoDI 5000.02 ESOH formal risk acceptance policy designed to protect people, equipment, and the environment from exposure to known hazards without formal acceptance of the hazard mishap risk by appropriate level of Service management
- However, this policy creates an impossible situation for fielded systems when a new hazard is identified or an existing risk level has to be increased based on new information – this results in the need to either obtain instantaneous formal risk acceptance or suspend use of the entire system until get formal risk acceptance
- US Air Force just published new Acquisition policy to manage this fielded system situation
  - Special emphasis placed on dealing with a new High risk or a risk level raised to High for a fleet of fielded aircraft
  - DoDI policy requires grounding the aircraft fleet until the Component Acquisition Executive (CAE) accepts the High risk

U.S. AIR FORCE

Overview

- DoD ESOH Risk Management Policy
- MIL-STD-882E User Representative Definition
- MIL-STD-882E ESOH Risk Management Methodology
- Fielded System ESOH Risk Management Challenge
- US Air Force Response

U.S. AIR FORCE

DoD ESOH Risk Management Policy-1

- **DoDI 5000.02, 7 January 2015, Enclosure 3, Section 16, Environment, Safety, and Occupational Health (ESOH)**
  - **"…As part of risk reduction, the Program Manager will eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. The Program Manager will use the methodology in MIL-STD-882E, 'DoD Standard Practice for System Safety'"**
  - **"Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the Program Manager will document that the associated risks have been accepted by the following acceptance authorities: the Component Acquisition Executive for high risks, Program Executive Officer-level for serious risks, and the Program Manager for medium and low risks."**

U.S. AIR FORCE

DoD ESOH Risk Management Policy-2

- **DoDI 5000.02, 7 January 2015 Enclosure 3, Section 16, Environment, Safety, and Occupational Health (ESOH)**
  - **"The user representative, as defined in MIL-STD-882E, must be part of this process throughout the life cycle and will provide formal concurrence prior to all serious-risk and high-risk acceptance decisions."**

DoD formalized the role of the user representative in the decision whether to accept a High or Serious ESOH risk. This ensures that the system users (operators and maintainers) can prevent acceptance of a risk that they find unacceptable. This is necessary because it is the users, not those in the Acquisition chain, that will be exposed to the risk if accepted.

NOTE: This process only applies to system-related ESOH risks, not operational risks. Operational Commanders have the authority to accept operational risks without acquisition inputs.

U.S. AIR FORCE

MIL-STD-882E
User Representative Definition

- **For fielding events, the User Representative is a Command or agency that has been formally designated in the Joint Capabilities Integration and Development System (JCIDS) process to represent single or multiple users in the capabilities and acquisition process.**
- **For non-fielding events, the User Representative is the Command or agency responsible for the personnel, equipment, and environment exposed to the risk.**
- **For all events, the User Representative will be at a peer level equivalent to the risk acceptance authority.**

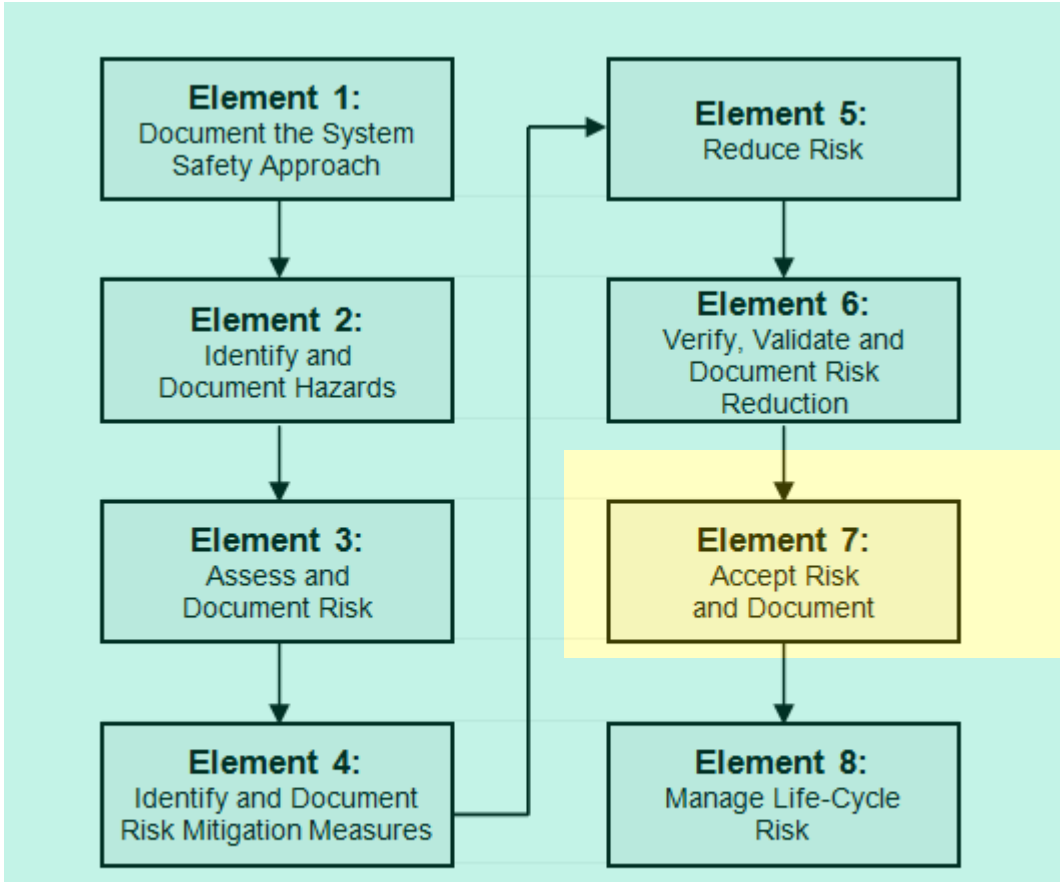
Fielding Events = Initial Operating Capability (IOC), Full Operating Capability (FOC), Bed down, etc.

Non-Fielding Events = Development Test (DT), Operational Test and Evaluation (OT&E), Field User Evaluations (FUEs), Air Shows, etc.

Peer Level = General Officer to General Officer, SES to SES, General Officer to SES, etc.

MIL-STD-882E ESOH Risk Management Methodology-1

Risk Assessment Elements in Blue



Risk Acceptance Element in Yellow

FIGURE 1. Eight elements of the system safety process

MIL-STD-882E ESOH Risk Management Methodology-2

- **Element 1: Document the System Safety approach – for Program Offices this should occur in the Systems Engineering Plan (SEP) beginning at Milestone A**
- **Element 2: Document identified hazards in a Hazard Tracking System (HTS)**
  - **Core of the MIL-STD-882E System Safety Process**
  - **Repository for all pertinent data related to ESOH hazards, their mitigation(s), and risks**
  - **Updated throughout life cycle as data changes**
  - **Government publishes HTS or HTS data in the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) document — part of the SEP beginning at Milestone B**

U.S. AIR FORCE

MIL-STD-882E ESOH Risk Management Methodology-3

Assessed risks are expressed as a Risk Assessment Code (RAC) which is a combination of one severity category and one probability level, e.g. RAC of 1C. Table III assigns a risk level of High, Serious, Medium, or Low for each RAC, e.g., a RAC of 1C is a High level.

TABLE III. Risk assessment matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

U.S. AIR FORCE

Fielded System ESOH Risk Management Challenge

- DoDI 5000.02 requirement for formal risk acceptance prior to exposing people, equipment, or the environment to known hazard
  - Fielded System already in use
  - If identify new, previously unknown, or changed (increased) risk, policy requires obtaining immediate risk acceptance or suspending use ("ground") the system to avoid exposing people, equipment, or environment to this known risk without formal risk acceptance by specified authority
- Real issue occurs when the risk is High
  - Risk acceptance required by Component Acquisition Executive (CAE) with the prior concurrence of the User Representative of equivalent rank (General Officer or SES)
  - If User Representative and CAE do not agree to accept the risk, the system should not be used until the risk is lowered to an acceptable level or Operational Commanders accept risk

U.S. AIR FORCE

US Air Force Response-1

- Published in USAF acquisition program policy on 18 Sep 2015
- When a Program Manager identifies a High risk that does not have acceptance, the Program Manager must notify the CAE and Lead Command's Commander (User Representative) within 24 hours
- Notification establishes automatic Interim Risk Acceptance for a period of time specified by the Program Manager, typically on the order of several days
  - Unless either the CAE or User Representative objects
  - Interim Risk Acceptance period to allow Program Manager to
    - Notify field units using the system
    - Identify any short term mitigations (procedural changes) that may be possible to lower the RAC, but not the risk level
    - Submit more detailed description of risk assessment and proposed risk management to CAE and User Representative

U.S. AIR FORCE

US Air Force Response-2

- Before end of Interim Risk Acceptance period, Program Manager must submit a more detailed request for risk acceptance for another, longer, specified period of time to
  - Determine if there are any materiel changes that could eliminate or lower the risk to Serious, Medium, or Low
  - Identify funding requirements, and establish an implementation schedule for the mitigations
- Program Manager would return to CAE and User Representative prior to end of this second risk acceptance period to
  - Request extension of risk acceptance period as necessary
  - Specify whether or not materiel changes can eliminate or lower the risk and time required to implement these materiel changes
  - If no further risk reduction possible, risk acceptance extension would be for remaining life of the system

U.S. AIR FORCE

US Air Force Response-3

- For High risks on fielded aircraft systems, the Program Manager may recommend temporary grounding of an aircraft fleet to avoid loss of life or aircraft until implementation of mitigation measures
  - As part of the initial High risk notification and Interim Risk Acceptance procedure
  - Within 24 hours of receipt of initial High risk notification and grounding recommendation, the CAE must notify the Lead Command's Commander and all Using Command Commanders of whether the CAE supports the grounding recommendation
- If CAE does not support grounding, the CAE must accept the High risk if the User Representative first concurs
- If the CAE and User Representative agree to accept the High risk, aircraft operations may continue

U.S. AIR FORCE

US Air Force Response-4

- Each aircraft system Using Command's Commander would have to decide whether to ground their portion of the aircraft fleet or accept the High risk in order to continue to operate the system if
  - The CAE is unwilling to accept the High risk and supports grounding the aircraft fleet, or
  - The CAE is willing to accept the High risk, but the User Representative is not

The key points are the following:

1. Neither the Program Manager nor the CAE has the authority to ground an aircraft fleet – they can only recommend grounding

2. The User Representative cannot ground an aircraft fleet, but has to agree with High risk acceptance before the CAE can accept a High risk

3. Only an Operational Command's Commander may ground the portion of an aircraft fleet under their command

U.S. AIR FORCE

Summary

- DoDI 5000.02 requires formal ESOH risk acceptance before exposing people, equipment, or the environment to a known hazard
- ESOH risk acceptance requirement focused on systems in development, not fielded systems
- On fielded systems, when a Program Manager identifies a new hazard or determines that the risk assessment of a known hazard is too low, the DoDI 5000.02 ESOH risk acceptance policy creates impossible situation requiring
  - Instantaneous risk acceptance, or
  - Removing entire system from use
- This is especially important for a new or revised High risk on an aircraft fleet
- Out of necessity, Air Force established policy on how to manage this situation