MIL-STD-882E:
ESOH Risk Acceptance Requirements and Scenarios

Karen Gill, Booz Allen Hamilton
NDIA Systems Engineering Conference
San Diego, CA
October 24, 2012

Agenda

- DoD Policy
- Definitions
- Risk Acceptance Scenarios
  - Test or Demonstration
  - Single or Joint Service, Low and Medium Risks
  - Single Service Serious and High Risks
  - Joint Program Serious and High Risks
  - Fielding
  - Post Fielding
  - Summary

DoD Policy – DoD Instruction 5000.02, E12.6, ESOH

- "The PM shall integrate ESOH risk management into the overall systems engineering process for all developmental and sustaining engineering activities. As part of risk reduction, the PM shall eliminate ESOH hazards where possible, and manage ESOH risks where hazards cannot be eliminated. **The PM shall use the methodology in MIL-STD-882D (now "E"), DoD Standard Practice for System Safety".**
  - MIL-STD-882E provides a matrix and defines probability and severity criteria to determine ESOH risk levels (Low, Medium, Serious, High)

- "**Prior to exposing people, equipment, or the environment to known system-related ESOH hazards**, the PM shall **document that the associated risks have been accepted by the following acceptance authorities**: the CAE for High risks, PEO-level for Serious risks, and the PM for Medium and Low risks. The **User Representative shall be part of this process throughout the life cycle** and shall **provide formal concurrence prior to all Serious and High risk acceptance decisions**."

DoD Policy, Continued

- What does the policy mean?
  - **Identifies WHEN** risks must be formally accepted:
    - Prior to exposing people, equipment, or the environment to known system-related hazards, ESOH risks must be formally accepted, which includes formal concurrence from the User Representative for Serious and High risks.
    - Because of this requirement, there may be a need for multiple risk acceptances for the same hazard for different events if the risk has increased
    - Risk acceptances are valid for a given system configuration and operational parameters and environment
  - **Identifies WHO** the acceptance authorities are for risks:
    - Based on risk level as assessed using MIL-STD-882E process
    - Program Manager for Low and Medium, PEO-level for Serious, and the Component Acquisition Executive (CAE) for High risks
  - **Requires USER REPRESENTATIVE involvement** in the risk assessment and acceptance process:
    - Must be part of this process throughout the life cycle
    - Provides formal concurrence prior to all Serious and High risk acceptance

Definitions – MIL-STD-882E

- Three types of ESOH risk:
  - Initial Risk. The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard.
  - Event Risk. The risk associated with a hazard as it applies to a specified hardware/software configuration during an event. Typical events include Developmental Testing/Operational Testing (DT/OT), demonstrations, fielding, post-fielding tests.
  - Target risk. The projected risk level the PM plans to achieve by implementing mitigation measures consistent with the design order of precedence described in 4.3.4.

  NOTE: 882E eliminated the term “residual risk” in response to the DoD policy stating WHEN risks must be accepted
- Acceptable Risk. Risk that the appropriate acceptance authority (as defined in DoDI 5000.02) is willing to accept without additional mitigation.
- Risk. A combination of the severity of the mishap and the probability that the mishap will occur.
- Risk Level. The characterization of risk as either High, Serious, Medium, or Low.

Risk Acceptance – Test or Demonstration

- Prior to each test event or series of events where the system and test environment are in the same configuration:
  - Test plans and the system test configuration must be reviewed for potential hazards and the associated risks assessed
  - There may be unique hazards or mitigation measures present during the test or demonstration
  - Each associated risk must be formally accepted with User Representative concurrence if Serious or High risk level
- Must be accomplished as part of the PMs Safety Release for Testing

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Single or Joint Service, Medium and Low Risks

- Risks must be formally accepted “prior to exposing people, equipment, or the environment to known system-related hazards”
- Risk acceptances are valid for a given system configuration and operational parameters and environment
- User involvement in the process is required over the life cycle; for Joint programs, users from each Participating Service must be involved
- Program Manager is the required management level for acceptance of Low and Medium risks

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Single Service, Serious and High Risks

- ESOH risks must be formally accepted “prior to exposing people, equipment, or the environment to known system-related hazards”
- Risk acceptances are valid for a given system configuration and operational parameters and environment
- For Serious and High risks, formal concurrence by the User Representative is required prior to risk acceptance by the risk acceptance authority
  - Formal concurrence should be made at a management level comparable to that of the acceptance authority
  - Formal concurrence is a recommendation to the acceptance authority but the acceptance authority can decide against accepting the risk
- PEO is the required management level for acceptance of Serious risks
- CAE is the required management level for acceptance of High risks

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Joint Service, Serious and High Risks

- ESOH risks must be formally accepted “prior to exposing people, equipment, or the environment to known system-related hazards”
- Risk acceptances are valid for a given system configuration and operational parameters and environment
- For Serious and High risks, formal concurrence from the User Representative is required
  - User representatives from each Participating Service provide formal concurrence for both Serious and High risks
    - Formal concurrence should be made at a management level comparable to that of the acceptance authority
    - Formal concurrence is a recommendation to the acceptance authority but the acceptance authority can decide against accepting the risk
- PEO is the management level for acceptance of Serious risks
- CAE of the Lead Component should be the management level for acceptance of High risks

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Fielding

- ESOH risks must be formally accepted “prior to exposing people, equipment, or the environment to known system-related hazards”
- Risk acceptances are valid for a given system configuration and operational parameters and environment
- Prior to fielding the system, all risks should be accepted at their “current” risk level
  - Current risk level is the actual risk level for hazards as the system is configured when fielded
  - May or may not be the Target risk level depending on whether all mitigations are in place and have been verified/validated
- For Serious and High risks, formal concurrence from the User Representative is required prior to risk acceptance
- DoDI 5000.02, E12.6 identifies the required management level for ESOH risk acceptance (CAE for High, PEO for Serious, and PM for medium and low)

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Post Fielding (Operations & Support Phase)

- After a system is fielded, a mishap, a deficiency report, or some other mechanism may result in the identification of an incorrect risk assessment or a previously unrecognized or new hazard
  - If a risk level increases for an identified hazard, a new risk acceptance is required prior to continuing to expose people, equipment, or the environment to the increased risk
  - If a previously unrecognized or new hazard is identified, it must be assessed and accepted in accordance with DoD policy prior to continuing to expose people, equipment, or the environment to the increased risk
  - In both cases:
    - It may be necessary to accept the existing risk for a period of time to allow implementation of mitigation measures across the fleet needed to lower the risk to the desired Target level
    - The alternative is to “ground the fleet” until the desired mitigations are implemented across the fleet; generally, this unacceptable to the warfighter due to mission requirements

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Risk Acceptance – Post Fielding (Operations & Support Phase), Continued

- In the situation where it is necessary to accept a newly identified risk for a known, previously unrecognized, or new hazard, to avoid "grounding the fleet," the User and Risk Acceptance Authority should require the following:
  - A specified time period to obtain funding and implement mitigation measures to lower the risk to the desired Target risk level
  - Immediate implementation of a combination of signage, procedures, training, and PPE to inform the system operators and maintainers of the new risk and possibly achieve minimal risk reduction
- The operational risk management process and the system's Program Office ESOH risk management process overlap in the case of fielded systems.
  - In effect, the operational risk management risk acceptance decision becomes the User concurrence (or non-concurrence) for High and Serious system risks assessed using the MIL-STD-882E process.
  - However, formal risk acceptance authority remains within the Acquisition chain.

Based on DoDI 5000.02 and the draft Defense Acquisition Guidebook

Summary

- Systems engineering uses the MIL-STD-882E process to identify hazards and assess risks as Low, Medium, Serious, or High
- Prior to exposing people, equipment, or the environment to known system-related hazards ESOH risks must be formally accepted
  - The User Representative must be part of the process over the life cycle
  - Risk acceptances are valid for a given system configuration and operational parameters and environment
  - If a risk level increases for a hazard, a new risk acceptance is required
- The required management levels for ESOH risk acceptance are the PM for Low and Medium, PEO for Serious, and the CAE for High risks
  - For Joint programs, the CAE of the Lead Component should be the acceptance authority for High risks
  - For Joint programs, the User Representative from each Participating Service must provide formal concurrence prior to Serious and High risk acceptance
- Fielded systems present potentially complicated risk acceptance scenarios, which require flexible and expandable hazard tracking systems to manage

Questions

Karen Gill
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202
Phone: (703) 412-7436
gill_karen@bah.com