16267 - MIL-STD-882E: Implementation Challenges

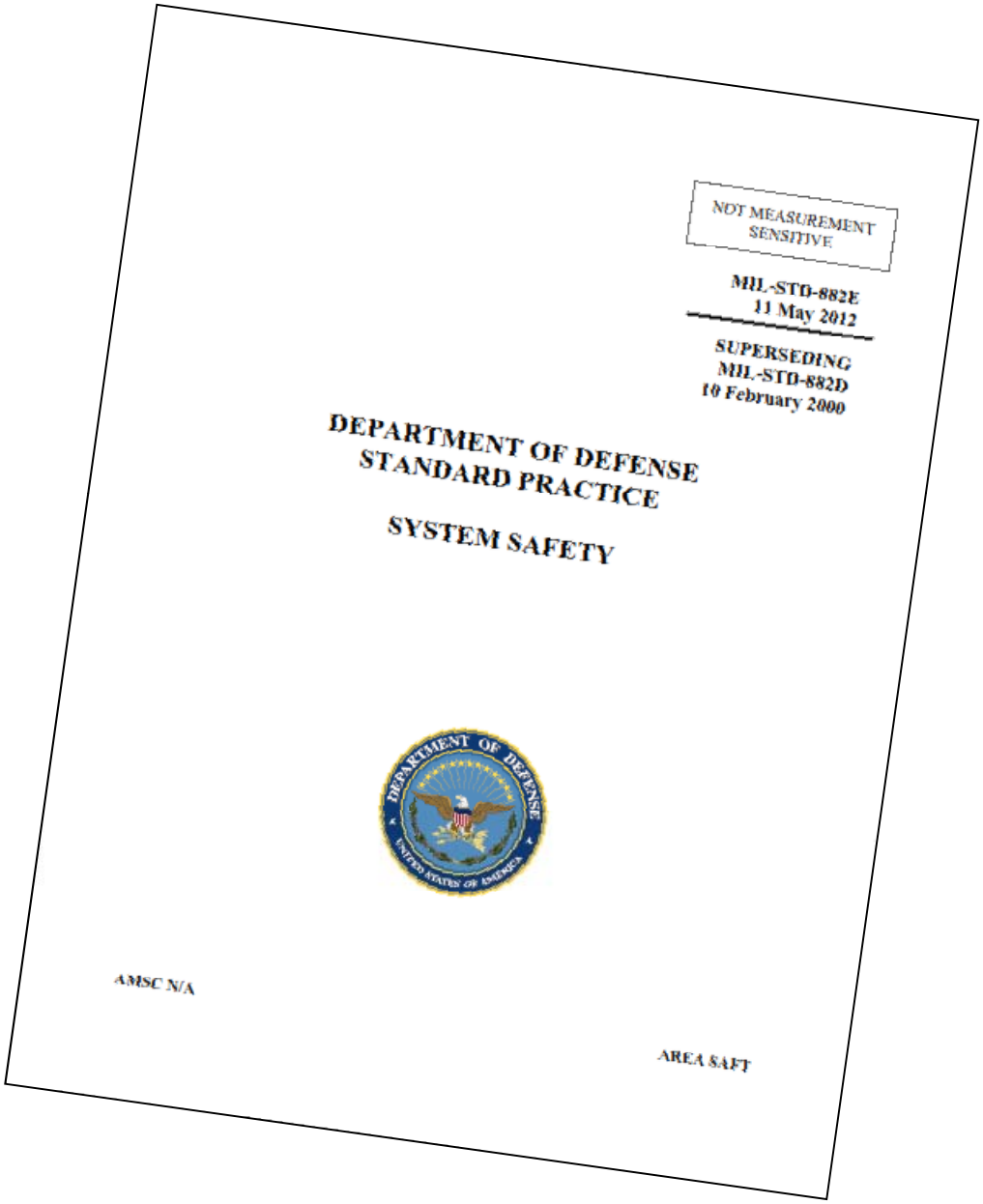
Jeff Walker, Booz Allen Hamilton
NDIA Systems Engineering Conference
Arlington, VA
October 30, 2013

Agenda

- Introduction
- MIL-STD-882 Background
- Implementation Issues
  - Risk Severity Category - Monetary Threshold
  - Risk Severity Category - Environmental Thresholds
  - Risk Probability Level - “F – Eliminated”
  - Risk Acceptance Authority
  - Hazard Tracking System
  - Software (SW) System Safety

Introduction

- Revision E published 11 May 2012
  - Update of Revision D started in 2003
  - Consensus development with representatives from each Service and OSD – challenging and time-consuming
  - Expands the emphasis of the System Safety process on Environment and Health issues to comply with DoDI 5000.02 requirements to integrate ESOH into Systems Engineering using the MIL-STD-882 process
  - Issues/Queries since publication from
    - Interested Organizations
    - Users


NOT MEASUREMENT SENSITIVE

MIL-STD-882E
11 May 2012

SUPERSEDING
MIL-STD-882D
10 February 2000

DEPARTMENT OF DEFENSE
STANDARD PRACTICE

SYSTEM SAFETY

AMSC N/A

AREA SAFT

Background

- **MIL-STD-882E Structure**
  - Foreword
  - 1. Scope
  - 2. Applicable Documents
  - **3. Definitions**
  - **4. General Requirements**
  - 5. Detailed Requirements
  - 6. Notes
  - Tasks
    - 100 Series – Management
    - 200 Series – Analysis
    - 300 Series – Evaluation
    - 400 Series – Verification
  - Appendices
    - A – Guidance for the System Safety Effort
    - B – Software System Safety Engineering and Analysis

What's New in 882E Compared to 882D

- Clarified that when this Standard is required in a solicitation or contract, but no specific task is identified, only Sections 3 and 4 are mandatory
- Clarified and mandated definitions (Section 3)
- Incorporated the eight elements of system safety from 882D with added details on process execution and increased emphasis on post-fielding risk management
- Added mandatory data fields to Hazard Tracking requirement
- Updated Severity Categories, Probability Levels, and Risk Matrix
- Emphasized risk acceptance in accordance with DoDI 5000.02
- Added Software contribution to risk (Section 4)
- Incorporated and revised task descriptions from 882C and added new tasks
- Updated Appendix A – Guidance for the System Safety Effort
- Added Appendix B – Software System Safety Engineering and Analysis

TABLE I. Severity categories

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

TABLE II. Probability levels

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

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			

Implementation Issues

- **Issue 1: Risk Severity Category - Monetary Threshold**
  - **Issue:** Risk is a combination of mishap severity and probability
    - Severity is determined based on the degree of personnel injury, environmental impact, or monetary loss
    - The “Catastrophic” monetary threshold in Table I – Severity Category is now $10M
    - A question was posed about what is included in the monetary loss definition. For example, an aircraft engine has a turbine defect that costs $11M to fix fleet-wide. However, most of the repair cost is borne by the engine manufacturer warranty. DOD pays $3M, and the engine manufacturer pays $8M. Does this still fall under the Catastrophic hazard due to the total cost of $11M?
  - **Resolution:** The monetary thresholds in MIL-STD-882E severity category definitions are only associated with the loss due to a potential mishap resulting from the hazard
    - For the scenario identified, one potential mishap that could result from the turbine defect is aircraft crash. If the aircraft is unmanned, the severity category would likely be based on the replacement cost of the aircraft. If manned, loss of life (death) from a crash is a credible potential outcome and would drive a Catastrophic severity category.
    - The cost of eliminating or reducing risk associated with a hazard has no bearing on the severity category determination

Implementation Issues

- **Issue 2: Risk Severity Category - Environmental Thresholds**
  - **Issue:** Risk is a combination of mishap severity and probability
    - Severity is determined based on the degree of personnel injury, environmental impact, or monetary loss
    - The environmental criteria for determining severity category uses the terms “irreversible significant” (Catastrophic), “reversible significant” (Critical), “reversible moderate” (Marginal), and “minimal” (Negligible) to describe potential environmental impacts
    - Users raised several questions about the definitions and guidance on using these terms and whether environmental costs should be considered part of the monetary loss
  - **Resolution:** The environmental terminology is well understood by environmental subject matter experts who should assess environmental risks
    - The definitions reside in the National Environmental Policy Act (NEPA) and its supporting information regarding assessment of environmental impacts
    - Several DoD contractors have successfully applied these terms, especially the General Dynamics, Electric Boat division that has made several presentations on this subject at previous Systems Engineering conferences
    - Any environmental impact associated costs, e.g., remediation, would be included separately in the assessment of monetary loss

Implementation Issues

- **Issue 3: Risk Probability Level - “F – Eliminated”**
  - **Issue:** Risk is a combination of mishap severity and probability
    - MIL-STD-882E added a new probability level of “F – Eliminated”
    - Contractors are inappropriately applying the "F - Eliminated" probability level
  - **Resolution:** The “F” probability level is applicable in only two scenarios, 1) the hazard or causal factor was identified as a possibility but was determined not to be credible, or 2) the hazard or causal factor was identified and confirmed as designed out
    - No one should apply the “F” level to any hazard that still exists
    - A Government program office requiring a contractor to use MIL-STD-882E is responsible for validating the contractors risk assessments prior to obtaining the required Government risk acceptance
    - A Government program office requiring a contractor to use MIL-STD-882E has this authority because IAW 882E, the program office owns the data
    - As with all hazards in a program’s hazard tracking system, those assigned probability “F” should be reviewed as necessary in response to design changes, mishaps, etc.
    - No change to MIL-STD-882 is necessary

Implementation Issues

- **Issue 4: Risk Acceptance Authority**
  - **Issue:** Risk acceptance is a primary function of a system safety program
    - Mandated in DoDI 5000.02 and MIL-STD-882
    - Risk acceptance authority determined by level of risk
    - A question was posed regarding identification of the risk acceptance authority in a joint service program involving contracting for flight operations
  - **Resolution:** DoDI 5000.02 applies to procurement activities associated with system development or sustainment, not to system operations
    - The most directly applicable DoD risk management policy for contracting flight operations would be operational risk management which requires that the “appropriate management level” accept a given risk
      - The “appropriate management level” would be the first office in the direct chain of command of the operation being assessed that has the authority to not accept the risk, thereby cancelling the operation, and the authority to direct the allocation of resources necessary to mitigate the risk to an acceptable level by that same management level
      - Typically, this would be the Commander that directed the operation take place

Implementation Issues

- **Issue 5: Hazard Tracking System**
  - **Issue:** MIL-STD-882E mandates use of a hazard tracking system (HTS)
    - Primary vehicle for managing ESOH risks through the system's lifecycle
    - A question was posed regarding a mismatch of HTS fields listed in Section 4.3.1.d and Task 106, Hazard Tracking System
  - **Resolution:** Section 4.3.1.d defines the minimum essential HTS data elements that any HTS must contain; the optional Task 106 contains an expanded list of data elements
    - Section 4.3.1.d lists the following data elements: identified hazards, associated mishaps, risk assessments (initial, target, event(s)), identified risk mitigation measures, selected mitigation measures, hazard status, verification of risk reductions, and risk acceptances
    - A program office my decide to mandate the expanded list of data elements in Task 106 to ensure a contractor will collect and maintain all necessary hazard data
    - If a program office is confident in the contractor's system safety expertise, it would not be necessary to put Task 106 on contract in addition to MIL-STD-882E
      - Just putting MIL-STD-882E on contract only requires compliance with Sections 3 & 4
      - To mandate any of the optional tasks, e.g., Task 106, requires the contract to specifically list the task

Implementation Issues

- **Issue 6: Software (SW) System Safety**
  - **Issue:** MIL-STD-882E introduces standard practices for determining the contribution of software to system risks as a mandatory element of the overall system safety methodology because most DoD systems are now heavily reliant on software
    - Section 4.4, Software Contribution to System Risk, is based on the Joint Software Systems Safety Engineering Handbook
    - Multiple inquiries have been received in regard to application of the new software system safety process
  - **Resolution:** Referring people to MIL-STD-882E Appendix B, Software System Safety Engineering and Analysis, the Joint Software Systems Safety Engineering Handbook, and the Joint Software Safety Working Group that wrote Appendix B and the Handbook
    - The application of the software system safety methodology requires personnel with the appropriate expertise, as do each of the ESOH functional areas
    - The basic software system safety methodology focuses on assessing the potential software contribution to an identified mishap risk

TABLE IV. Software control categories

SOFTWARE CONTROL CATEGORIES		
Level	**Name**	**Description**
1	**Autonomous (AT)**	• Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard. *(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and safety-critical functions that are time critical.)*
2	**Semi-Autonomous (SAT)**	• Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. *(This definition includes the control of moderately complex system/software functionality, no parallel processing, or few interfaces, but other safety systems/mechanisms can partially mitigate. System and software fault detection and annunciation notifies the control entity of the need for required safety actions.)* • Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence. *(This definition assumes that the safety-critical display information may be time-critical, but the time available does not exceed the time required for adequate control entity response and hazard control.)*
3	**Redundant Fault Tolerant (RFT)**	• Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition. *(This definition assumes that there is adequate fault detection, annunciation, tolerance, and system recovery to prevent the hazard occurrence if software fails, malfunctions, or degrades. There are redundant sources of safety-significant information, and mitigating functionality can respond within any time-critical period.)* • Software that generates information of a safety-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	**Influential**	• Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap.
5	**No Safety Impact (NSI)**	• Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data.

TABLE V. Software safety criticality matrix

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

TABLE VI. Relationship between SwCI, risk level, LOR tasks, and risk

RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK		
Software Criticality Index (SwCI)	**Risk Level**	**Software LOR Tasks and Risk Assessment/Acceptance**
SwCI 1	High	• If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	Serious	• If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	Medium	• If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	Low	• If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	Not Safety	• No safety-specific analyses or testing is required.

Summary

- MIL-STD-882E expanded and refined the application of the system safety methodology to all aspects of ESOH, to include software safety
- Provided a standard practice for the various ESOH functional area to use in assessing and managing risks in support of program offices and in compliance with DoDI 5000.02
- Individual users and organizations are raising issues and concerns about the application of MIL-STD-882E methodology
  - Utilizing the severity and probability definitions to assess risk levels
  - Complying with the requirement for formal risk acceptance prior to exposing people, equipment or the environment to known hazards
  - Documenting the results in a Hazard Tracking System
  - Applying the software system safety methodology

Questions

Jeff Walker
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202
Phone: (703) 412-7418
walker_jefferson@bah.com