14788
MIL-STD-882E:
Overview of Development and Objectives of Rewrite

Jeff Walker, Booz Allen Hamilton
NDIA Systems Engineering Conference
San Diego, CA
October 24, 2012

Purpose

- Provide an overview of MIL-STD-882E, 11 May 12
  - Background
  - Objectives
  - Developmental Timeline
  - What's New in 882E Compared to 882D
- List of Today's MIL-STD-882E Presentations

Background

- MIL-STD-882D – “DoD Standard Practice for System Safety”
  - Performance based Standard Practice: What, not how
    - Published 10 Feb 00
    - Converted from prescriptive 882C per acquisition reform
  - 23 Sep 04 AT&L Policy memo required the use of 882D “in all developmental and sustaining engineering activities”
  - 8 Dec 08 DoDI 5000.02 incorporated requirement to use 882D process for Environment, Safety, and Occupational Health (ESOH) risk management

Initial Objectives of Rewrite

- Be evolutionary, not revolutionary
- Support implementation of 8 Dec 08 DoDI 5000.02
- Emphasize integration into Systems Engineering (SE)
- Incorporate optional tasks to put on contract
  - Update and revise task descriptions from 882C
  - Create new task descriptions to apply across ESOH
- Improve standardization by creating mandatory definitions
- Add software system safety techniques and practices

Clarifying Objectives from DASD(SE)

- DASD(SE)
  - Owns DoD Systems Engineering (SE) policy and is the Defense Standardization Executive
  - Recognizes MIL-STD-882 as:
    - A key element of SE
    - A standard practice for all DoD acquisition programs
- Required 882E be a “standard, generic method for the identification, classification, and mitigation of hazards” that “can be practically applied by not only system safety professionals, but also by other functional disciplines, such as fire protection engineers, occupational health professionals, and environmental engineers.” (7 January 2011)

Developmental Timeline

- 2000 – DoD published MIL-STD-882D
- 2003 – DoD initiated effort to update MIL-STD-882D
- 2004 to 2010 – Multiple Drafts
- April 2010 – Final DoD Draft
- May to June 2010 – Industry Comment Period
- July 2010 to January 2011 – Resolved Industry and DoD comments
- 7 January 2011 – DASD(SE) provided clarifying objectives for revising MIL-STD-882D that drove end-to-end review and extensive changes

Developmental Timeline, Continued

- January to July 2011 – Extensive rewrite of draft
  - Multiple meetings held with each Service providing one voting representative and subject matter experts
  - Paragraph by paragraph review with unanimous agreement on changes required by voting representatives
- 20 July 2011 to 13 September 2011 - DoD Draft posted on ASSIST-Online for final review and comment by Industry and Government
- Oct 2011 to April 2012 – Adjudicated Industry and Government comments using the same rules of engagement, unanimous agreement of Service voting representatives
- 11 May 2012 – MIL-STD-882E published

What's New in 882E Compared to 882D

- Facilitates use of 882 by multiple functional disciplines as an integral part of SE to improve consistency of hazard management practices across programs
- 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

✓ Definitions clarified and mandated (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

What's New in 882E Compared to 882D, Continued

- Monetary loss values increased in Severity Categories
- ✓ Probability levels
  - Quantitative values removed from Table II
  - "Eliminated" description added
- Risk Assessment Matrix
  - Removal of Risk Assessment Values (1-20) from Risk Matrix
  - Addition of "Eliminated"
- ✓ Emphasized risk acceptance in accordance with DoDI 5000.02
- ✓ Software contribution to risk
  - Included in Section 4 (mandatory section)
  - Based on DoD Joint Software Systems Safety Engineering Handbook

What's New in 882E Compared to 882D, Continued

- Incorporated and revised optional task descriptions from 882C
- Included additional tasks
  - Task 103 – Hazard Management Plan (alternative to SSPP)
  - Task 108 – Hazardous Materials Management Plan
  - Task 208 – Functional Hazard Analysis
  - Task 209 – System-of-Systems Hazard Analysis
  - Task 210 – Environmental Hazard Analysis
  - Task 302 – Hazard Management Assessment Report (alternative to SAR)

What's New in 882E Compared to 882D, Continued

- Updated Appendix A – Guidance for the System Safety Effort
  - Task application matrix updated
  - Example probability levels table includes quantitative values
- Added Appendix B – Software System Safety Engineering and Analysis
  - Additional detail on software system safety techniques and practices
  - Based on DoD Joint Software System Safety Engineering Handbook

List of Today's 882E Presentations

Wednesday October 24 Track 9 – ESOH Chair: Bob Smith		
TIME	TITLE	SPEAKER
8:00 - 8:35	14797-Acquisition ESOH: An OSD Perspective	Asiello
8:35 - 9:10	14756-Driving Affordability with Sustainability Analysis	Risz
9:10 - 9:45	14788-MIL-STD-882E: Overview of Development and Objectives of Rewrite	Walker
BREAK		
10:15 - 10:50	14789-MIL-STD-882E: Eight Element Process Changes – Highlight the New Details and Requirements	Gill
10:50 - 11:25	14794-MIL-STD-882E: Software System Safety Process in MIL-STD-882E	Smith
11:25 - 12:00	14790 - MIL-STD-882E: Mandatory Definitions	Rodriguez
LUNCH		
1:30 - 2:05	14863-MIL-STD-882E: Quantitative vs. Qualitative ESOH Risk Assessments Using the 882E Risk Matrix	Smith
2:05 - 2:40	14791-MIL-STD-882E: Risk Acceptance Requirements and Scenarios	Gill
2:40 - 3:15	14793-MIL-STD-882E: 882E Hazard Tracking System Requirements and Options	Thacker
BREAK		
3:45 - 4:20	14792 - MIL-STD-882E: Putting 882E on Contract	Walker
4:20 - 4:55	14818-Architecting for Disaster Preparedness	Dam
4:55 - 5:30	14541-Test and Evaluation of Black Swan Risks in Early Development for Maximum Effectiveness: A Case Study of Lightning Protection of Insensitive High Explosives	Sanders
END OF DAY		
Thursday October 25 Track 9 – ESOH Chair: Bob Smith		
8:00 - 8:35	14840-NEPA and Systems Engineering: Managing the Environmental Risk	Evans
8:35 - 9:10	14843-NEPA Compliance Challenges for Joint Acquisition Programs: US Air Force Perspective	Brown
9:10 - 9:45	New Concept for PESHE and NEPA/EO 12114 Compliance Schedule (REPLACES 14844)	Rodriguez
END OF TRACK		

Questions?

Jeff Walker
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202-4158
Walker_Jefferson@bah.com

BACKUP

ASSIST-Online Comments (July – Sept 2011)

- 522 comments received
  - 382 submitted through ASSIST-Online
  - 140 submitted via other comment matrices or attached files to Preparing Activity
- Characterization of comments
  - Range of comments from essential to administrative
  - Most comments similar to those already reviewed by 882 Working Group
    - Definition and terminology conflicts
    - Concern with the probability levels / orders of magnitude
    - Update to the risk matrix
    - Further clarity needed for the software safety guidance
  - All comments reviewed and dispositioned by the 882 Working Group

7 JAN 2011 – ASD(R&E)/SE/MA Guidance

- “Since the practice of system safety is a key element of Systems Engineering, the responsibility to update this document ultimately resides within the Mission Assurance directorate within USD(AT&L)/DDR&E/SE. Additionally, since it is a standards document, it falls under the purview of the DoD Standardization Office. Both of these areas are within my functional responsibility.”
- “MIL STD 882, the Standard Practice for System Safety, is a key document within the overarching systems engineering discipline. This document provides a standard, generic method for the identification, classification, and mitigation of hazards but, historically, has served as an engineering standard only for the system safety professionals since 1969. The tools and processes outlined within the standard, however, can be practically applied by not only system safety professionals, but also by other functional disciplines, such as fire protection engineers, occupational health professionals, and environmental engineers.”

7 JAN 2011 – ASD(R&E)/SE/MA Guidance (cont)

- “A spectrum of functional disciplines can, and should, use the standard processes, practices, and definitions contained within this standard. Those processes, practices and definitions must remain generic for the practice of system safety.”
- “Functional areas are welcome to apply the standard tools, definitions and practices, however, it is not appropriate to alter or place adjectives in front of fundamental definitions, processes, practices and other nouns used within the standard. For example, the term "hazard" must remain generic, not be defined in this standard practice as an ESOH hazard, a fire hazard, an HSI hazard, etc.”

7 JAN 2011 – ASD(R&E)/SE/MA Guidance (cont)

- “An exception to the requirement to use generic nouns without functional discipline adjectives occurs through the introduction of functional tasks that are clearly focused on a specific functional discipline through use of system safety practices; these focused tasks are reasonable to be incorporated within the standard. It is expected that the exception will clearly support a specific discipline in the use of the standard practices, and standard, generic definitions. For example, Task 107, Hazardous Material Management Plan, is a focused task. Another example is Task 210, Environmental Hazard Analysis, which uses the hazard analysis practice but focuses it for the functional discipline of environment.”
- “Compliance with this adjudication guidance will allow the single focused intent of the standard, i.e. the identification, classification, and mitigation of any type of hazard, not just ESOH hazards, to be realized and allow all safety-related disciplines to adopt this generic, standard practice.”

What's New Compared to 882D (cont)

- Software contribution to risk included in Section 4 (mandatory section)
  - Based on Joint Software Systems Safety Engineering Handbook
  - Includes software control categories
  - Provides software safety criticality matrix of Software Criticality Indices (SwCIs)
  - Defines relationships between SwCIs, risk levels, and Levels of Rigor

Assess SwCI for software as it relates to an identified hazard and software control

Determine level of rigor required to mitigate the software contribution to risk

Determine level of risk based on whether the level of rigor applied

In accordance with DASD(SE) Direction