Update on Revisions to MIL-STD-882

NDIA 11th Annual Systems Engineering Conference
System Safety – ESOH & HSI Session 3C4
San Diego, CA

Robert E. Smith, CSP

October 22, 2008

Contents

- Introduction
- MIL-STD-882 history
- Purpose of revision
- Highlight of changes
- Coordination process
- Conclusion

Introduction

- MIL-STD-882 is DoD's standard practice for system safety
- Considered the system safety "bible" for DoD Acquisition Programs
- Identifies system safety practices for both the program manager and contractor
- In existence since 1969 and has been revised several times
- Last revision (MIL-STD-882D) occurred Feb 2000

MIL-STD-882 History[1]

- MIL-STD-882 - July 1969
  - First DoD system safety standard
  - System safety program became mandatory on all DoD-procured products and systems
- MIL-STD-882A - June 1977
  - Centered on the concept of risk acceptance as a criterion for system safety programs
  - Required introduction of hazard probability and established categories for frequency of occurrence to accommodate the long-standing hazard severity categories
- MIL-STD-882B - 30 March 1984
  - Continued evolution of detailed guidance in both engineering and management requirement
  - More emphasis on facilities and off-the-shelf acquisition was added, and software was addressed in some detail for the first time

[1] Clifton Ericson II, *A Short History of System Safety*, Journal of System Safety, May-June 2006.

MIL-STD-882 History[1] (cont)

- MIL-STD-882B, Notice 1 - 1 July 1987
  - Expanded software tasks and the scope of the treatment of software by system safety
- MIL-STD-882C - 19 Jan 1993
  - Integrated the hazard and software system safety efforts
  - Individual software tasks were removed
  - Safety analysis would include identifying the hardware and software tasks together in a system
- MIL-STD-882C, Notice 1 - 19 Jan 1996
  - Corrected some errors and revised the Data Item Descriptions
- MIL-STD-882D - 10 Feb 2000
  - Under the Military Specifications and Standards Report (MSSR) initiative, MIL-STD-882D was considered important to continue, as long as it was converted to a performance-based standard practice – *what you want vs. how to do it*
  - Task descriptions removed

Average time between revisions: ~ 8 yrs

Purpose of Revision

- Initial drivers:
  - Government and Industry wanted to bring back the Task Descriptions from MIL-STD-882C to make them readily available for call out in contract documents
  - Align with current OSD Acquisition Systems Engineering policy changes
- Subsequent drivers:
  - Adjust the organizational arrangement of information to clarify the basic elements of a system safety program and the process flow among them
  - New tasks
  - Support DoD strategic plans and goals

Highlight of Changes

- Update will be referred to as MIL-STD-882D, Revision 1
- Subtitle added to emphasize ESOH integration into Systems Engineering
  - "ESOH Risk Management Methodology for Systems Engineering"
- Standardized definitions
- Rewrote task descriptions to clarify and dissociate from each other
  - 100-series tasks - program management and control
  - 200-series tasks - design and integration
  - 300-series tasks - design
  - 400-series tasks - compliance and verification
- Emphasized the identification and derivation of applicable ESOH technical requirements
- Added Hazardous Material Management Process (HMMP) task

Highlight of Changes (cont)

- Matrix description updated
  - For severity, dollar value on losses increased for today's program dollars and logarithmic progression applied
  - For probability, finite period of time or cycles added; "Eliminated" level added
  - Matrix rearranged to have ascending severity on x-axis
    - » Mishap risk assessment values and categories unchanged, but graphically looks different than current matrix
- More emphasis on:
  - Establishing a collaborative ESOH effort using the system safety process
  - Providing coordinated ESOH input to systems engineering to maximize performance by minimizing the environmental "footprint" of the system and improving safety of personnel and the system itself
- "Appendix A - Guidance for Implementation of an ESOH Effort" has been updated
  - Additional detail on hazard definitions and assessing top level mishaps
  - Software safety techniques and principles reintroduced

Coordination Process

- DoD ACQ ESOH IPT
  - 882 Working Group complete IPT recommended draft
  - Review and comments
  - Resolution of comments
  - Provide the IPTs recommended Draft to SAF/AQRE
- NDIA SE Division
  - Review and comments
  - Resolution of comments
- Formal DoD Coordination
  - Standardization community

Current Estimated Completion Date: Mid 2009

Conclusion

- Clarifies terminology, incorporates current policy and defines task descriptions to improve system safety practices
- Strengthens integration across Environment, Safety, and Occupational Health and into Systems Engineering during the acquisition process
- Improves consistency of system safety practices between programs

Questions?

Robert E. Smith, CSP
Booz Allen Hamilton
1550 Crystal Drive, Suite 1550
Arlington, VA 22202-4158
703-412-7661
smith_bob@bah.com

MIL-STD-882D, Rev 1 – Severity Categories

TABLE 1. Severity Categories

Severity Category	Severity Level	Environment, Safety, and Occupational Health Mishap Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $10M, or irreversible significant environmental impact.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $1M but less than $10M, or reversible significant environmental impact.
Marginal	III	Could result in injury or occupational illness resulting in 10 or more lost work days, loss exceeding $100K but less than $1M, or reversible moderate environmental impact.
Negligible	IV	Could result in injury or illness resulting in less than 10 lost work days, loss less than $100K, or minimal environmental impact.

Dollar value on losses changed:

- ***Increased for today's program dollars***
- ***Logarithmic progression applied***

Current MIL-STD-882D Definition

MIL-STD-882D, Rev 1 – Probability Levels

TABLE 2. Probability Levels

Probability Name	Probability Level	Description*
Frequent	A	Likely to be experienced several times by a system within a 12 month period; a probability of occurrence greater than 10^{-1} over 12 months.
Probable	B	Likely to be experienced by a system within a 12 month period; a probability of occurrence less than 10^{-1} but greater than 10^{-2} over 12 months.
Occasional	C	May be experienced by a system within a 12 month period; a probability of occurrence less than 10^{-2} but greater than 10^{-3} over 12 months.
Remote	D	Unlikely, but possible to be experienced by a system within a 12 month period; a probability of occurrence less than 10^{-3} but greater than 10^{-6} over 12 months.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced by a system within a 12 month period; a probability of occurrence of less than 10^{-6} over 12 months.
Eliminated	F	Incapable of occurrence. This category is used when potential hazards are identified and later eliminated.

- ***Finite period of time or cycles added to description***
- ***"Eliminated" level added***

Current MIL-STD-882D Definition

MIL-STD-882D, Rev 1 – Risk Matrix

TABLE 3. ESOH Risk Assessment Values

		Severity			
		Negligible IV	Marginal III	Critical II	Catastrophic I
Probability	Frequent (A)	13	7	3	1
	Probable (B)	16	9	5	2
	Occasional (C)	18	11	6	4
	Remote (D)	19	14	10	8
	Improbable (E)	20	17	15	12
	Eliminated	21			

TABLE 4. Risk Categories

Risk Assessment Value	Risk Category	Risk Acceptance Level
1 – 5	High	In accordance with DoD policy
6 – 9	Serious	
10 – 17	Medium	
18 – 20	Low	
21	N/A (eliminated)	

- ***Matrix rearranged to have ascending severity on x-axis***
- ***Risk assessment values and categories unchanged***

Current MIL-STD-882D Definition

Backups

MIL-STD-882 Eight Mandatory System Safety Steps

1. Document the system safety approach
2. Identify ESOH hazards
3. Assess the risk
4. Identify risk mitigation measures
5. Reduce risk to an acceptable level
6. Verify risk reduction
7. Review hazards and accept risk by appropriate authority
8. Track ESOH hazards, their resolution, and residual risk throughout the system lifecycle

Current MIL-STD-882D Severity Definitions

TABLE A-I. **Suggested mishap severity categories.**

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Current MIL-STD-882D Probability Definitions

TABLE A-II. **Suggested mishap probability levels.**

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

*Definitions of descriptive words may have to be modified based on quantity of items involved.

**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

Current MIL-STD-882D Risk Assessment Matrix

TABLE A-III. **Example mishap risk assessment values.**

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

TABLE A-IV. **Example mishap risk categories and mishap risk acceptance levels.**

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

*Representative mishap risk acceptance levels are shown in the above table. Mishap risk acceptance is discussed in paragraph A.4.4.7. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.