MIL-STD-882E:

Eight Element Process Changes – Highlights of New Details and Requirements

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

Agenda

- Comparison of 882D to 882E Elements
- Eight Elements of the System Safety Process in 882E
  - Document the System Safety Approach
  - Identify and Document Hazards
  - Assess and Document Risk
    - Table I: Severity Categories
    - Table II: Probability Levels
    - Table III: Risk Assessment Matrix
  - Identify and Document Risk Mitigation Measures
  - Reduce Risk
  - Verify, Validate, and Document Risk Reduction
  - Accept Risk and Document
  - Manage Life Cycle Risk
- Summary of Software Contribution to System Risk

Comparison of 882D to 882E Elements

882D	882E
1. Documentation of the system safety approach	1. Document the system safety approach
2. Identification of hazards	2. Identify and document hazards
3. Assessment of mishap risk	3. Assess and document risk
4. Identification of mishap risk mitigation measures	4. Identify and document risk mitigation measures
5. Reduction of mishap risk to an acceptable level	5. Reduce risk
6. Verification of mishap risk reduction	6. Verify, validate, and document risk reduction
7. Review and acceptance of residual mishap risk by the appropriate authority	7. Accept risk and document
8. Tracking hazards and residual mishap risk	8. Manage life cycle risk

Fundamentals of the 882D system safety process unchanged, 882E provides more detail

Eight Elements of the System Safety Process in 882E
Element 1: Document the System Safety Approach

- The PM and contractor shall document the system safety approach for managing hazards as an integral part of the SE process. The minimum requirements for the approach include:
- Describing the risk management effort and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure.
- Identifying and documenting the prescribed and derived requirements applicable to the system.
- Defining how hazards and associated risks are formally accepted by the appropriate risk acceptance authority and concurred with by the user representative in accordance with DoDI 5000.02.
- Documenting hazards with a closed-loop Hazard Tracking System (HTS) – see HTS presentation 14793 at 2:40 pm today.

Eight Elements of the System Safety Process in 882E
Element 2: Identify and Document Hazards

- Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment.
- Consider and use mishap data; relevant environmental and occupational health data; user physical characteristics; user knowledge, skills, and abilities; and lessons learned from legacy and similar systems.
- The hazard identification process shall consider the entire system life-cycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment.
- Identified hazards shall be documented in the HTS.

Eight Elements of the System Safety Process in 882E
Element 3: Assess and Document Risk

- The severity category and probability level of the potential mishap(s) for each hazard across all system modes are assessed using the definitions in Tables I & II.
- To determine the appropriate severity category as defined in Table I for a given hazard at a given point in time, identify the potential for death or injury, environmental impact, or monetary loss. A given hazard may have the potential to affect one or all of these three areas.
- To determine the appropriate probability level as defined in Table II for a given hazard at a given point in time, assess the likelihood of occurrence of a mishap.
  - Probability level F is used to document cases where the hazard is no longer present.
  - No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap probability to level F.

Eight Elements of the System Safety Process in 882E
Element 3: Assess and Document Risk, Continued

- When available, the use of appropriate and representative quantitative data that defines frequency or rate of occurrence for the hazard, is generally preferable to qualitative analysis.
  - The Improbable level is generally considered to be less than one in a million.
  - See Appendix A for an example of quantitative probability levels - see presentation 14863 at 1:30 pm today.
- In the absence of such quantitative frequency or rate data, reliance upon the qualitative text descriptions in Table II is necessary and appropriate.
- Assessed risks are expressed as a Risk Assessment Code (RAC) which is a combination of one severity category and one probability level.
- The definitions in Tables I and II, and the RACs in Table III shall be used, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy.
- Assessed risks shall be documented in the HTS.

Eight Elements of the System Safety Process in 882E
Element 3: Assess and Document Risk, Continued
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 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 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 week days, reversible moderate environmental impact, or monetary loss exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness resulting in less than 1 lost week day, minimal environmental impact, or monetary loss less than $100K.

Increased dollar value on losses logarithmically to account for today's program dollars
Removed "that violates law or regulation" from descriptions of environmental damage

Eight Elements of the System Safety Process in 882E
Element 3: Assess and Document Risk, Continued
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 on 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.

Added a sixth Description / Level – "Eliminated" / "F"

Removed quantitative probability definition, now strictly qualitative in Section 4

Appendix A has example of quantitative definition derived from 882D

Eight Elements of the System Safety Process in 882E
Element 3: Assess and Document Risk, Continued
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			

Added matrix depicting risk levels (H,S,M,L), eliminated risk assessment values (1-20), added Risk Assessment Code (RAC), e.g., 1A, 3C

Eight Elements of the System Safety Process in 882E
Element 4: Identify and Document Risk Mitigation Measures

- Potential risk mitigation(s) shall be identified, and the expected risk reduction(s) of the alternative(s) shall be estimated and documented in the HTS.
- The goal should always be to eliminate the hazard if possible.
- When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence.
- The system safety design order of precedence identifies alternative mitigation approaches and lists them in order of decreasing effectiveness.

Eight Elements of the System Safety Process in 882E
Element 4: Identify and Document Risk Mitigation Measures, Con't

- The System Safety Design Order of Precedence:

  1. Eliminate hazards through design selection
  2. Reduce risk through design alteration
  3. Incorporate engineered features or devices
  4. Provide warning devices
  5. Incorporate signage, procedures, training, and PPE

Note: For hazards assigned Catastrophic or Critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.

Eight Elements of the System Safety Process in 882E
Element 5: Reduce Risk

- Mitigation measures are selected and implemented to achieve an acceptable risk level.
- Consider and evaluate the cost, feasibility, and effectiveness of candidate mitigation methods as part of the SE and Integrated Product Team (IPT) processes.
- Present the current hazards, their associated severity and probability assessments, and status of risk reduction efforts at technical reviews.

Eight Elements of the System Safety Process in 882E
Element 6: Verify, Validate and Document Risk Reduction

- Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, demonstration, or inspection.
- Document the verification and validation in the HTS.

Eight Elements of the System Safety Process in 882E
Element 7: Accept Risk and Document

- Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority as defined in DoDI 5000.02.
  - The system configuration and associated documentation that supports the formal risk acceptance decision shall be provided to the Government for retention through the life of the system.
  - The definitions in Tables I and II, the RACs in Table III, and the criteria in Table VI for software shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved in accordance with DoD Component policy.
  - The user representative shall be part of this process throughout the life cycle of the system and shall provide formal concurrence before all Serious and High risk acceptance decisions.

Eight Elements of the System Safety Process in 882E
Element 7: Accept Risk and Document, Continued

- After fielding, data from mishap reports, user feedback, and experience with similar systems or other sources may reveal new hazards or demonstrate that the risk for a known hazard is higher or lower than previously recognized. In these cases, the revised risk shall be accepted in accordance with DoDI 5000.02.

Note: A single system may require multiple event risk assessments and acceptances throughout its life-cycle. Each risk acceptance decision shall be documented in the HTS.

Note: See presentation 14791 at 2:05 pm today on risk acceptance.

Eight Elements of the System Safety Process in 882E
Element 8: Manage Life Cycle Risk

- After the system is fielded, the system program office uses the system safety process to identify hazards and maintain the HTS throughout the system's life-cycle.
- This life-cycle effort considers any changes to include, but not limited to, the interfaces, users, hardware and software, mishap data, mission(s) or profile(s), and system health data.
- Procedures shall be in place to ensure risk management personnel are aware of these changes, e.g., by being part of the configuration control process.
- The program office and user community shall maintain effective communications to collaborate, identify, and manage new hazards and modified risks.
- If a new hazard is discovered or a known hazard is determined to have a higher risk level than previously assessed, the new or revised risk will need to be formally accepted in accordance with DoDI 5000.02.
- In addition, DoD requires program offices to support system-related Class A and B (as defined in Department of Defense Instruction 6055.07) mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors.

Summary of Software Contribution to System Risk
882E Section 4.4

- Section 4.4 is in addition to the Eight Elements in Section 4.3

- 882E added Software assessments to Section 4 to provide the approach to be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware.

- Note: see the next presentation 14794 on the Software System Safety Process for more details

Questions

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