14790
MIL-STD-882E:
Mandatory Definitions

Lucy Rodriguez, Booz Allen Hamilton
NDIA Systems Engineering Conference
San Diego, CA
October 24, 2012

Agenda

- Purpose
- Rationale for Including Mandatory Definitions
- Overview of 882D to 882E Definitions
- List of Terms Defined in Section 3 of 882E
- Key 882E Definitions
- Eliminated Residual Mishap Risk in 882E
- Conclusion

Purpose

- To provide an overview of the Mandatory Definitions as specified in MIL-STD-882E Section 3.2 – Definitions

Rationale for Including Mandatory Definitions

- Ensures consistent terminology usage across the Department of Defense and its contractors
  - Establishes a common baseline for communication
  - Facilitates application by Joint programs
  - Supports consistent hazard tracking and risk reporting
  - Provides standardized terminology for communications with risk acceptance authorities

Overview of 882D to 882E Definitions

- Changed from 14 to 49 definitions
- Included definitions for software system safety from the Joint Software Systems Safety Engineering Handbook (JSSSEH)
  - Added definitions to facilitate the use of MIL-STD-882E to analyze environmental hazards
  - Provided definitions that support the risk acceptance requirements in DoDI 5000.02
- Eliminated or revised definitions no longer consistent with DoDI 5000.02 or the changes to the system safety process

List of Terms Defined in Section 3 of 882E

Acceptable risk	Level of rigor (LOR)	Safety-related
Acquisition program	Life-cycle	Safety-significant
Causal factor	Mishap	Severity
Commercial-off-the-shelf (COTS)	Mitigation measure	Software
Contractor	Mode	Software control category
Environmental impact	Monetary Loss	Software re-use
ESOH	Non-developmental item (NDI)	Software system safety
Event risk	Probability	System
Fielding	Program Manager (PM)	System-of-systems (SoS)
Firmware	Re-use items	System safety
Government-furnished equipment (GFE)	Risk	System safety engineering
Government-furnished information (GFI)	Risk level	System safety management
Government-off-the-shelf (GOTS)	Safety	System/subsystem specification
Hazard	Safety-critical	Systems Engineering
Hazardous material (HAZMAT)	Safety-critical function (SCF)	Target risk
Human systems integration (HSI)	Safety-critical item (SCI)	User representative
Initial risk		

Key 882E Definitions

- Definitions that were critical to reaching consensus on 882E

ESOH	Initial Risk
Environmental Impact	Event Risk
Hazard	Target Risk
Mishap	Severity
Risk	Probability
Risk Level	Risk Assessment Code

Key Definitions, Continued

ESOH – “An acronym that refers to the combination of disciplines that encompass the processes and approaches for addressing laws, regulations, Executive Orders (EO), DoD policies, environmental compliance, and hazards associated with environmental impacts, system safety (e.g., platforms, systems, system-of-systems, weapons, explosives, software, ordnance, combat systems), occupational safety and health, hazardous materials management, and pollution prevention.”

- Significance: To define the scope of applicability of the 882E system safety process as required in DoDI 5000.02 for ESOH risk management

Key Definitions, Continued

Environmental Impact – “An adverse change to the environment wholly or partially caused by the system or its use.”

- Significance: This is to discriminate from the traditional definition of environmental impact that includes positive changes to the environment

Key Definitions, Continued

Hazard – “A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.”

- Significance: Added “unplanned” to emphasize that typically mishaps are not planned events

Mishap – “An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this Standard, the term “mishap” includes negative environmental impacts from planned events.”

- Significance: Added “negative environmental impacts from planned events” to enable the environmental community to use the 882E methodology for risk assessment

Key Definitions, Continued

Risk (formerly mishap risk) – “A combination of the severity of the mishap and the probability that the mishap will occur.”

- Significance: Removed “mishap” for consistency with DoDI 5000.02

Risk Level – “The characterization of risk as either High, Serious, Medium, or Low.”

- Significance: To label the High, Serious, Medium, and Low terms used for grouping Risk Assessment Codes (RAC), e.g. 1D, 3B…

Key Definitions, Continued

Initial Risk – "The first assessment of the potential risk of an identified hazard. Initial risk establishes a fixed baseline for the hazard."

- Significance: To define a common term for the initial assessment of risk

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."

- Significance: To support the DoDI 5000.02 requirement to accept risk prior to exposing people, equipment, or the environment to known system hazards

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: Section 4.3.4 is "Identify and document risk mitigation measures."*

- Significance: To define a common term for the anticipated risk after all planned mitigations have been implemented, verified, and validated

Key Definitions, Continued

Severity – “The magnitude of potential consequences of a mishap to include: death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss.”

- Significance: 882D did not include a definition of severity

Probability – “An expression of the likelihood of occurrence of a mishap.”

- Significance: 882D did not provide a definition of probability

Key Definition from Section 4

Risk Assessment Code (RAC) – "A combination of one severity category and one probability level."

- Significance: Adopted a single term to refer to the combination of severity and probability vice the Risk Assessment Value (1-20) or Hazard Risk Index

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			

- Example RAC=3D

Eliminated Residual Mishap Risk in 882E

Residual Mishap Risk (from 882D) – “The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence.”

- Significance: DoD changed the risk acceptance policy on 7 March 2007 to require risk acceptance prior to any exposure of people, equipment, or the environment to a known system hazard. The residual mishap risk concept was inconsistent with this policy requirement because the residual mishap risk concept only required risk acceptance at one point. In addition, the residual mishap risk concept supported the “closing” of hazards which resulted in failure to continue to seek further risk reductions throughout the life cycle.

Conclusion

- The 882E Working Group spent a significant amount of time to reach agreement on the mandatory definitions to use in the system safety process
- Mandatory definitions ensure consistent terminology usage across the Department of Defense and its contractors
- One key definition was probability. The next presentation will address how the definitions of probability levels can be employed.

Questions?

Lucy Rodriguez
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202-4158
703-412-7685
rodriguez_lucy@bah.com

Robert E. Smith, CSP
Booz Allen Hamilton
1550 Crystal Drive, Suite 1100
Arlington, VA 22202-4158
703-412-7661
smith_bob@bah.com

BACK UP SLIDES

Detailed Definitions

Acceptable Risk –

Risk that the appropriate acceptance authority (as defined in DoDI 5000.02) is willing to accept without additional mitigation

Risk Level	Acceptance Authority
High	Component Acquisition Executive (CAE)
Serious	Program Executive Office (PEO)
Medium	Program Manager (PM)
Low	Program Manager (PM)

882E 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

882E 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 numbering schema, now strictly qualitative in Section 4

Appendix A has example of quantitative derived from 882D

Key Differences Compared to 882C/882D

- 882D has 14 definitions; 882E has 49 definitions
- New definitions
- Ones that have been modified
- Eliminated: residual risk…[drives risk acceptance at events…and eliminate idea of “closing” hazards]
- 882D Mishap Risk; 882E Risk
- 882E contains multiple types of risk: acceptable risk, initial risk, event risk
- Definition of Mishap

Mishap risk – An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence

Risk – A combination of the severity of the mishap and the probability that the mishap will occur

Significant Changes Between 882D & 882E

882D	882E
14 Total Definitions	49 Total Definitions
Mishap risk -- An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence	Risk -- A combination of the severity of the mishap and the probability that the mishap will occur