SYSTEM SAFETY

Evolution of MIL-STD-882E

Bob McAllister, USAF
Jimmy Turner, Raytheon

History

- Long ago
  - Analyses done after the fact
- Ballistics Sys Div Exhibit 62-41 (1962)
  - Ballistic missiles
- MIL-S-38130A (June 1966 and March 1967)
  - Aircraft, space, & electronics
- MIL-STD-882 (July 1969)
  - Mgmt emphasis & industry involvement
- MIL-STD-882A (June 1977)
  - Hazard probabilities and risk acceptance
- MIL-STD-882B (Mar 1984 and July 1987)
  - Individual tasks
- MIL-STD-882C (Jan 1993 and Jan 1996)
  - Integrated hardware and software tasks
- MIL-STD-882D (Feb 2000)
  - Acquisition reform

Risk Levels & Matrices

- Mil-S-38130A
  - No levels nor matrix
- MIL-STD-882
  - No matrix. Defined hazard levels
- MIL-STD-882A
  - No matrix – reversed hazard levels.
  - New qualitative probability levels
- MIL-STD-882B
  - Qualitative risk matrices in appendix
- MIL-STD-882C
  - Qualitative and quantitative matrices in Appendix.
  - Established risk acceptance levels
- MIL-STD-882D
  - Qualitative matrix, but quantitative probability levels.
- MIL-STD-882E (draft)
  - Multiple matrices and risk levels

Qualitative matrix (-882B)

FREQUENCY OF OCCURRENCE	HAZARD CATEGORIES			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	V NEGLIGIBLE
(A) FREQUENT	1A	2A	3A	4A
(B) PROBABLE	1B	2B	3B	4B
(C) OCCASIONAL	1C	2C	3C	4C
(D) REMOTE	1D	2D	3D	4D
(E) IMPROBABLE	1E	2E	3E	4E

Quantitative Matrix (-882C)

HAZARD CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2 CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT (X > 10-1)*	1A	2A	3A	4A
(B) PROBABLE (10-1 > X > 10-2)*	1B	2B	3B	4B
(C) OCCASIONAL (10-2 > X > 10-3)*	1C	2C	3C	4C
(D) REMOTE (10-3 > X > 10-6)*	1D	2D	3D	4D
(E) IMPROBABLE (10-6 > X)*	1E	2E	3E	4E

* Example of quantitative criteria

Qualitative Matrix (-882D)

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

Probability Levels (-882D)

• Frequent	more than 10^{-1}
• Probable	between 10^{-2} and 10^{-1}
• Occasional	between 10^{-3} and 10^{-2}
• Remote	between 10^{-6} and 10^{-3}
• Improbable	less than 10^{-6}

882D: Numbers are for individual item, not fleet

882C: Doesn't specify

Origin of numbers?

- Done by committee (like a camel)
- Not enough probability levels to change single order of magnitude (skipped ahead from 10^{-3} to 10^{-6})
- Why 10^{-6}?
  - Originated in munitions world
  - Seemed ‘unapproachable. (‘Not one in a million!’)

Why 882E

- MIL-STD-882D complied with Acquisition Reform
  - Tells ‘what’ to do, not ‘how’
  - Specifies eight generic system safety steps
    - = Have a plan
    - = Identify hazards
    - = Assess their risks
    - = Take action on the risks
    - = Accept residual risks
  - 882 D removed the 882C System Safety Tasks
  - Considered to be too ‘watered-down’
- We overdid it, so need a more robust standard

MIL-STD-882E Drafts

- Mid 2004, first draft MIL-STD-882E
  - Re-instated System Safety Tasks
  - Re-instated software criticality matrix
  - Changed Mishap Risk Assessment Value (MRAV) to Mishap Risk Index (MRI)
- Early 2005, Second draft
  - Add new Tasks on Safety Critical Functions and FHAs, etc
  - Re-instate Task usage matrices
  - Re-instate "F" probability level (designed out/impossible)
  - Revised the risk matrices
    - = $10K to $20K
    - = Expanded 'Low risk range'

Next?

- Summer 2005, third draft
  - Re-structuring for better logic flow
  - Multiple risk matrices – upper right is High
  - New precedence step – added Engineering Safety Features

    (Examples include the emergency core cooling system of a nuclear reactor and loss-of-tension braking for elevators; full-time, on-line redundant paths; interlocks; ground-fault circuit interrupters and uninterruptible power supplies)
  - Five system safety 'Elements; instead of 8 Steps
- Being coordinated by GEIA G-48 (System Safety) Panel
- Publish, fall/winter 2005

Questions?