Defining a Generic ESOH Hazard Tracking Database for Future Programs

NDIA 11th Annual Systems Engineering Conference
System Safety – ESOH & HSI Session 3B4 - 7211
San Diego, CA

Jeff Walker

October 22, 2008

Contents

- Requirements
- MIL-STD-882
- Generic Database Fields

USD(AT&L) Policy Memorandums

- Defense Acquisition System Safety, September 23, 2004
  - Use Standard Practice for System Safety, MIL-STD-882D to manage ESOH risk
  - Report ESOH risk status and acceptance decisions at technical and program reviews
- Reducing Preventable Accidents, November 21, 2006
  - Address status of each High and Serious ESOH risk and compliance with applicable safety technology requirements at all program reviews
- Defense Acquisition System Safety – ESOH Risk Acceptance, March 7, 2007
  - Formal acceptance of ESOH risks prior to exposing people, equipment, or the environment to a known system-related ESOH hazard
  - User Representative Formal Concurrence for High and Serious ESOH risks

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

Hazard Description

- More detail is better – may be clarified as details emerge
- Includes three items:

Hazard – (Source) A source or condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap.

Causal Factor – (Mechanism) One or several mechanisms that trigger the hazard.

Mishap – (Outcome) Unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Hazard Description Examples:

- *Laceration (outcome) from unprotected skin exposure (mechanism) to a sharp edge (source)*
- *Ship damage (outcome) from collision with foreign object (mechanism) due to degraded vision (source)*

Hazard Identifiers/Discriminators

- Entries to help track a hazard and supplement the hazard description
- Enable sorting and searches by characteristics

Hazard Number – Unique identifier – may be coded

Hazard Type – Safety, Environmental, Occ. Health (one or more)

Common Hazard Code – Track similar hazards across programs

Mode – Operation, Maintenance, Transport, Storage (one or more)

Source – Analysis, Test, User, Lessons Learned

System/Subsystem – Applicable to some programs

Point of Contact – Applicable to some programs

Risk Assessments

- Each risk assessment based on mishap severity and mishap probability - other fields determined based on established criteria

Mishap Severity – Defined in MIL-STD-882

Mishap Probability – Defined in MIL-STD-882

Risk Assessment Code (RAC) – IA through IVE

RAC Index – 1 through 20

RAC Level – High, Serious, Medium, Low

- Multiple risk assessments are recognized
  - Initial Risk
  - Target Risk
  - Current Risk
  - Event Risk
  - Residual Risk

Mitigation Efforts

- ESOH SMEs identify mitigation alternatives
- Implementation decisions made as part of systems engineering effort based on cost, schedule, performance and risk acceptability

Recommended Mitigation – Clearly defined action

Actionee – Person and function responsible for taking action

Estimated Completion Date – Date all activities complete

Status – Submitted, Approved, Disapproved, In Progress, Complete (others as defined by program)

Status Comments – Running commentary on progress of mitigation to include verification of mitigation effects (consider automated time-stamping)

Hazard Status

- Overall status of hazard resolution
- Must account for weakest link in mitigation process
  - Hazard not closed until all mitigations applied or risk accepted

Status – Open, Closed (others as defined by program)

Status Comments – Hazard-level comments

Risk Acceptance / User Concurrence

- Mechanism to document each risk acceptance/ user concurrence event
  - Requires snap-shot in time of risk and status of mitigation efforts for each hazard
  - Becomes historical record and should be protected from deletion/alteration

Date – Date of risk acceptance

Event – (e.g., test, urgent field, basing)

User Signatory – Multiple if Joint Program

Risk Acceptance Signatory – Dependent on highest risks

Generic Database Field List

- Hazard Number
- Hazard Type
- Common Hazard Code
- Safety POC
- Mode
- Source
- System/Sub-system
- Hazard
- Causal Factor
- Mishap
- Status

- Recommended Mitigation(s)
- Estimated Completion Date
- Mitigation Actionee
- Mitigation Status
- Mitigation Status Comments

- Initial Severity
- Initial Probability
- Initial RAC
- Initial RAC Index
- Initial RAC Level

- Current Severity
- Current Probability
- Current RAC
- Current RAC Index
- Current RAC Level

- Target Severity
- Target Probability
- Target RAC
- Target RAC Index
- Target RAC Level

- Residual Severity
- Residual Probability
- Residual RAC
- Residual RAC Index
- Residual RAC Level

Risk Acceptance/User Concurrence

- Date
- Event
- User Signatory
- Risk Acceptance Signatory

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

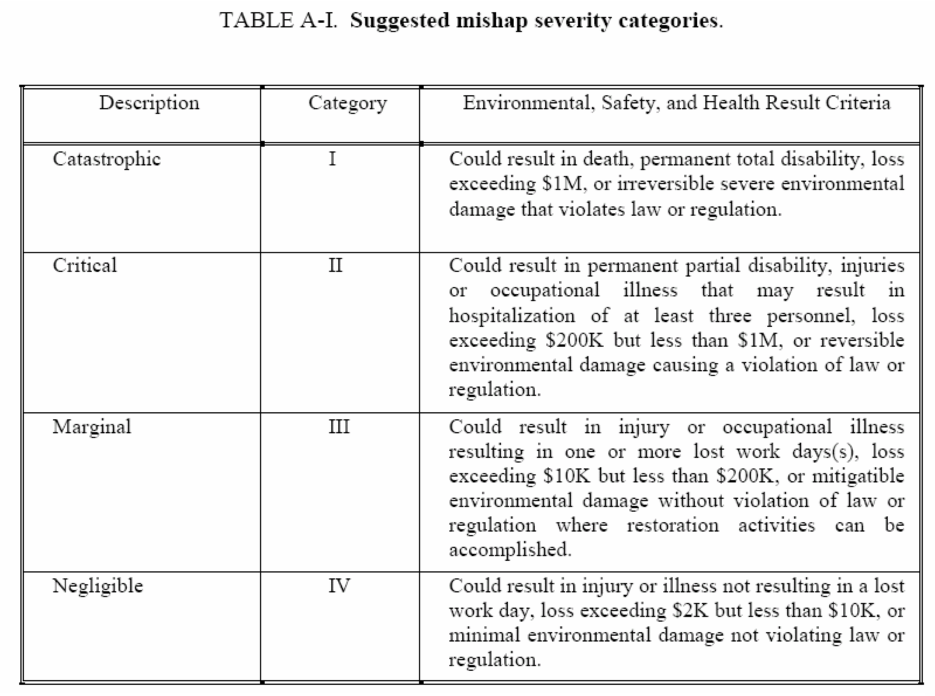

TABLE A-I. **Suggested mishap severity categories.**

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.

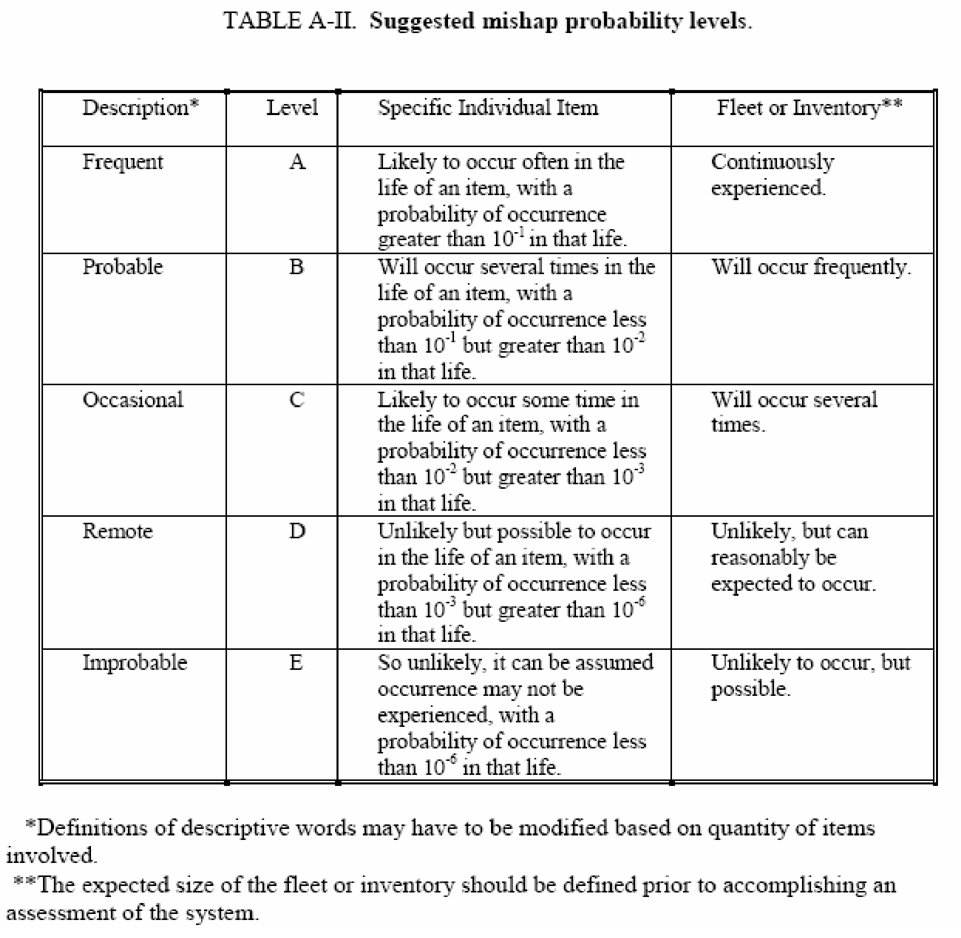

TABLE A-II. **Suggested mishap probability levels.**

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.

MIL-STD-882D (cont)

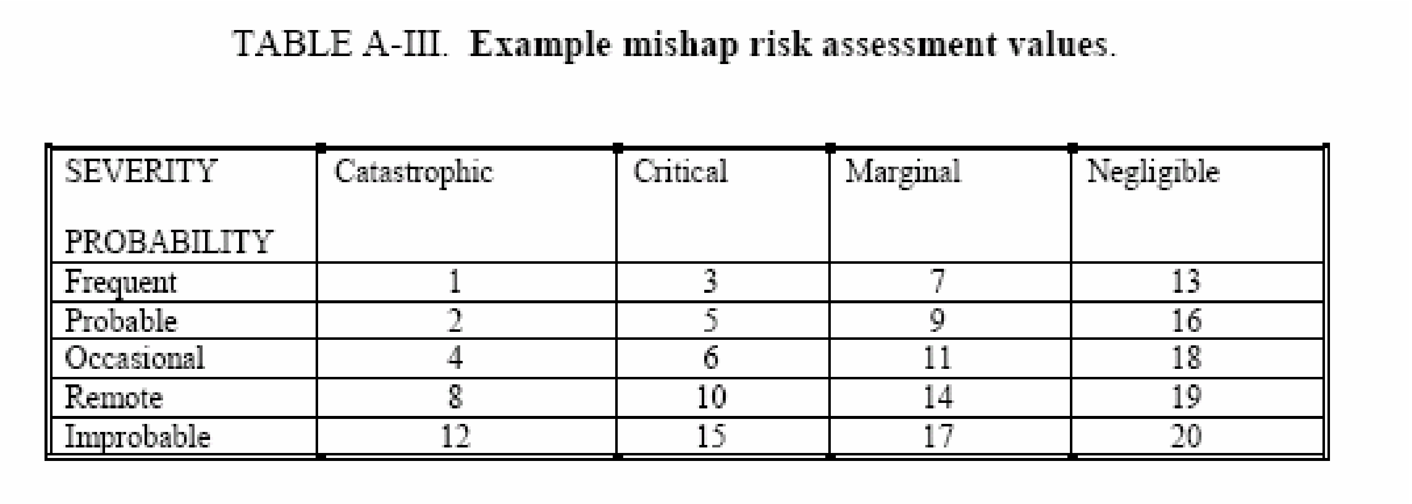

TABLE A-III. **Example mishap risk assessment values.**

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

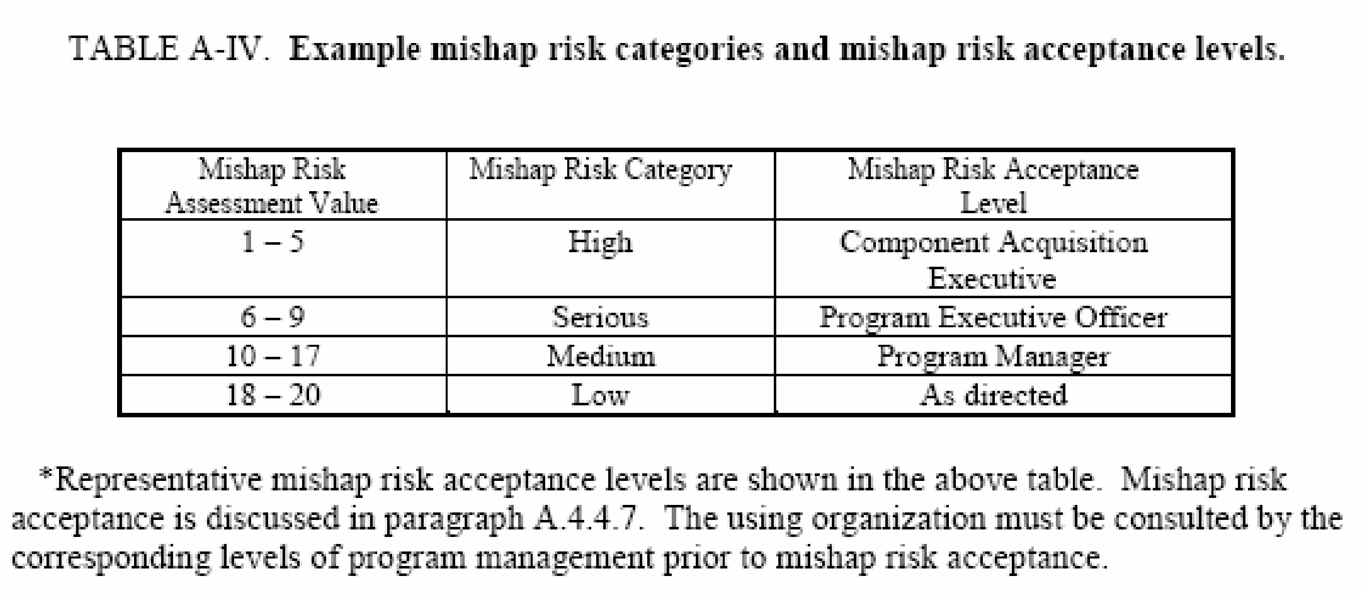

TABLE A-IV. **Example mishap risk categories and mishap risk acceptance levels.**

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.