



**System Reliability Center**  
 201 Mill Street  
 Rome, NY 13440-6916  
 888.722-8737  
 or 315.337.0900  
 Fax: 315.337.9932

## 882D "Lite" – System Safety – Mishap Risk Assessment

In general, MIL-STD-882D has been simplified, proscriptive requirements have been eliminated and guidance has been added on how to apply risk management. This tool is intended primarily to acquaint the reader with significant changes in the latest revision of the subject document.

**System Safety** is now defined as: The application of engineering and management principles, criteria, and techniques **to achieve acceptable mishap risk**, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

In MIL-STD-882D, the first step in the "Standard Practice for System Safety" is the identification of hazards through a systematic hazard analysis. Then, a "mishap risk assessment" is undertaken. This concept of "**mishap risk**", as used in revision "D", is somewhat different than the "hazard" approach utilized in the "C" version. MIL-STD-882D defines "mishap risk assessment" in Appendix A, simply by using four key parameters and their appropriate matrices:

- Mishap Severity Categories
- Mishap Qualitative Probability Levels
- Mishap Risk Assessment Values
- Mishap Risk Acceptance Levels

**Mishap Severity Categories** are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table 1. The dollar values shown in this table should be established on a system by system basis depending on the size of the system being considered to reflect the level of concern.

Table 1. 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 day(s), loss exceeding \$10K but less than \$200K, or mitigatable 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.



## 882D "Lite" – System Safety – Mishap Risk Assessment (Cont'd)

**Mishap Qualitative Probability** is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table 2.

Table 2. Mishap Qualitative 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 on quality of items.

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

**Mishap Risk Assessment** is the potential negative impact of the hazard on personnel, facilities, equipment, operations, the public, and the environment, as well as on the system itself. Mishap risk classification by mishap severity and mishap probability can be performed by using a mishap risk assessment matrix. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is then often used to rank different hazards as to their associated mishap risks. A hypothetical example of a mishap risk assessment matrix is shown at Table 3.

Table 3. 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



**System Reliability Center**  
201 Mill Street  
Rome, NY 13440-6916  
888.722-8737  
or 315.337.0900  
Fax: 315.337.9932

## 882D "Lite" – System Safety – Mishap Risk Assessment (Cont'd)

**Mishap Risk Acceptance.** Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table 4 includes a hypothetical example listing of mishap risk categories and the associated assessment values. In the hypothetical example, the system management has determined that mishap risk assessment values 1 through 5 constitute "High" risk while values 6 through 9 constitute "Serious" risk, etc.

Table 4. Mishap Risk Categories and Mishap Risk Acceptance Levels

<b>Mishap Risk Assessment Value</b>	<b>Mishap Risk Category</b>	<b>Mishap Risk Acceptance Level</b>
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 Table 4. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

Copyright © 2005 Alion Science and Technology. All rights reserved.

**Source:**

- MIL-STD-882D, "Standard Practice For System Safety", February 10, 2000, Appendix A, Pages 18-20.

**For More Information:**

- "Defense Acquisition Guidebook", Defense Acquisition University <http://akss.dau.mil/dag/> (Formerly "Defense Acquisition Deskbook") Deskbook Joint Program Office, Wright-Patterson Air Force Base, Ohio.
- "System Safety Analysis Handbook", System Safety Society Unionville, VA, <http://www.system-safety.org/ProductsResourcesBooks.htm>.