

ATTACHMENT 008
SYSTEM SAFETY PROGRAM GUIDE

1. SYSTEM SAFETY PROGRAM GUIDANCE.

1.1 System safety program. The contractor shall establish and maintain a system safety program to support efficient and effective achievement of overall system safety objectives.

1.1.1 Management system. The contractor shall establish a safety management system to implement provisions of this standard commensurate with the program contractual requirements. The contractor program manager shall be responsible for the establishment, control, incorporation, direction and implementation of the system safety program policies and shall assure that mishap risk is identified and eliminated or controlled within established program risk acceptability parameters. The contractor shall establish internal reporting systems and procedures for investigation and disposition of system related mishaps and safety incidents, including potentially hazardous conditions not yet involved in a mishap/incident. Report such matters to the Managing Activity (MA) as required by the contract.

1.1.2 Key system safety personnel. The contractor shall establish and maintain a key system safety position for each program. The individual in this position shall be directly responsible to the contractor program manager for safety matters and shall meet the minimum qualifications specified by the MA.

1.1.3 Conflicting requirements. When conflicting requirements or deficiencies are identified within system safety program requirements or with other program requirements, the contractor shall submit notification, with proposed solutions or alternatives and supporting rationale, to the MA for resolution.

1.2 System safety program objectives. The system safety program shall define a systematic approach to make sure that:

- a. Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- b. Hazards associated with each system are identified, tracked, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the MA throughout the entire life cycle of a system. Risk shall be described in risk assessment terms (see paragraph 4.5 below).
- c. Historical safety data, including lessons learned from other systems, are considered and used.
- d. Minimum risk is sought in accepting and using new technology, materials or designs; and new production, test and operational techniques.
- e. Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.
- f. Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during research, technology development for and acquisition of a system.
- g. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA.
- h. Consideration is given early in the life cycle to safety and ease of disposal (including explosive ordnance disposal), and demilitarization of any hazardous materials associated with the system. Actions should be taken to minimize the use of hazardous materials and, therefore, minimize the risks and life cycle costs associated with their use.

ATTACHMENT 008
SYSTEM SAFETY PROGRAM GUIDE

1.3 System safety design requirements. The contractor shall establish safety design criteria derived from all applicable data including the preliminary hazard analyses if available. These criteria shall be the basis for developing system specification safety requirements. Some general system safety design requirements are:

- a. Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the life cycle of the system.
- b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.
- c. Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points).
- d. Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).
- e. Design to minimize risk created by human error in the operation and support of the system.
- f. Consider alternate approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail safe design, system protection, fire suppression, and protective clothing, equipment, devices, and procedures.
- g. Protect the power sources, controls and critical components of redundant subsystems by physical separation or shielding.
- h. When alternate design approaches cannot eliminate the hazard, provide safety and warning devices and warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These shall be standardized in accordance with commonly accepted industry or military practice or with MA requirements for conditions in which prior standards do not exist. The MA shall be provided copies of all warnings, cautions and distinctive markings proposed for review and comment.
- i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.
- j. Design software controlled or monitored functions to minimize initiation of hazardous events or mishaps.
- k. Review design criteria for inadequate or overly restrictive requirements regarding safety. Recommend new design criteria supported by study, analyses, or test data.

1.4 System safety precedence. The order of precedence for satisfying system safety requirements and resolving identified hazards shall be as follows:

1.4.1 Design for minimum risk. Eliminating hazards should be the goal from the initial design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection.

1.4.2 Incorporate safety devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA

ATTACHMENT 008
SYSTEM SAFETY PROGRAM GUIDE

through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

1.4.3 Provide warning devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.

1.4.4 Develop procedures and training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver from the MA, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards (as defined in paragraph 4.5.1 below). Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the MA. Tasks and activities judged to be safety critical by the MA may require certification of personnel proficiency.

1.5 Risk assessment. Decisions regarding resolution of identified hazards shall be based on assessment of the risk involved. To aid the achievement of the objectives of system safety, hazards shall be characterized as to hazard severity categories and hazard probability levels, when possible. Since the priority for system safety is eliminating hazards by design, a risk assessment procedure considering only hazard severity will generally suffice during the early design phase to minimize risk. When hazards are not eliminated during the early design phase, a risk assessment procedure based upon the hazard probability, hazard severity, as well as risk impact, shall be used to establish priorities for corrective action and resolution of identified hazards.

1.5.1 Hazard severity. Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as shown at Table 1.

Table 1
HAZARD SEVERITY CATEGORIES

Description	Category	Definition
CATASTROPHIC	I	Death, system loss, or severe environmental damage.
CRITICAL	II	Severe injury, severe occupational illness, major system or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

1.5.2 Hazard probability. The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is shown at Table 2.

Table 2

**ATTACHMENT 008
SYSTEM SAFETY PROGRAM GUIDE
HAZARD PROBABILITY LEVELS**

Description	Level	Specific Individual Item	Fleet or Inventory
FREQUENT	A	Likely to occur frequently	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 of 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 that it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

1.6 Action on identified hazards. Action shall be taken to eliminate identified hazards or reduce the associated risk to a level defined by or acceptable to the MA. Catastrophic, critical and other hazards specified by the MA shall not rely solely on warnings, cautions or procedures/training for control of risk. If this is impossible or impractical, alternatives shall be recommended to the MA.

1.6.1 Residual risk. The risk associated with significant hazards for which there are no known control measures, no plans to control or incomplete control measures will be considered residual risk. The contractor will document each residual risk along with the reason(s) for incomplete resolution and notify the MA. The residual risks will be accepted for the Army as noted in Table 3.

Table 3

PROBABILITY	SEVERITY			
	1 Catastrophic	2 Critical	3 Marginal	4 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
1A, 1B, 1C, 2A, 2B	HIGH	Risk accepted by Component Acquisition Executive		
1D, 2C, 3A, 3B	SERIOUS	Risk accepted by the PEO		
1E, 2D, 2E, 3C, 3D, 3E, 4A, 4B	MEDIUM	Risk accepted by the Program Manager		
4C, 4D, 4E:	LOW	Risk accepted by the Program Manager		