BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 91-118

18 JANUARY 1994

Safety

SAFETY DESIGN AND EVALUATION CRITERIA FOR NUCLEAR WEAPON SYSTEMS

OPR: HQ AFSA/SENA
(Lt Col John D. Waskiewicz)
Supersedes AFR 122-10, 14 May 90

Certified by: HQ USAF/SE
(Brig Gen James L. Cole, Jr.)
Pages: 52
Distribution: F

This manual contains the minimum criteria for designing, developing, or modifying a nuclear weapon system and outlines criteria to evaluate systems, equipment, and software for nuclear safety certification. It applies to all organizations that design, develop, modify, evaluate, or operate a nuclear weapon system. It does not apply to Air Force Reserve and Air National Guard. Send recommendations for improvements to HQ AFSA/SENA, 9700 Avenue G, Kirtland AFB NM 87117-5670.

SUMMARY OF REVISIONS

This is the initial publication of AFMAN 91-118, incorporating the requirements and procedures formerly in AFR 122-10.

Chapter 1— GENERAL STANDARDS AND CONTROL **6**

Section 1A Responsibility and Scope 6

1.1. Terms and Definitions. 6

1.2. Department of Defense (DoD) Safety Standards. 6

1.3. Air Force Criteria: 6

Section 1B Deviations to Criteria 6

1.4. Requests for Deviations: 6

Chapter 2— DESIGN CRITERIA FOR NUCLEAR WEAPON SYSTEMS **7**

Section 2A General Philosophy and Criteria 7

2.1. Nuclear Weapon Safety Design Philosophy. 7

2.2. Nuclear Weapon System Safety Design Philosophy. 7

2.3. Critical Function Numerical Requirements. 9
2.4. Safety Features and Procedures. 9
2.5. Explosive Ordnance Disposal. 9
2.6. Physical and Internal Security. 10
2.7. Environmental Parameters. 10
2.8. Safe and Arm (S&A) and Arm/Disarm (A/D) Devices. 10
2.9. Protection of Friendly Territory. 10
2.10. Single Component Malfunction or Operation. 10
2.11. Human Engineering. 10

Section 2B Automata and Software 10

2.12. General Design Requirements. 10
2.13. Memory Characteristics: 12
2.14. Critical Command Messages. 12
2.15. Operating System (OS) and Run-Time-Executive (RTE). 12
2.16. Critical Function Routine Design: 13

Section 2C Electrical Subsystems and Hazards 13

2.17. Electrical Subsystem General Design Criteria. 13
2.18. Wiring and Cabling: 14
2.19. Electrical Connectors. 14
2.20. Electrical Current Considerations. 15
2.21. Electromagnetic Radiation (EMR). 15

Section 2D Arming and Fuzing (A&F) Systems 16

2.22. General Criteria. 16
2.23. System Devices: 16
2.24. System Design Features: 16

Section 2E Ground-Launched Missile Systems 17

2.25. Criteria Applicability. 17
2.26. Launch Control System. 17
2.27. Reentry System, Reentry Vehicle, or Payload Section A/D Device. 18
2.28. Monitor Systems: 18
2.29. Command and Control Communications: 18

2.30. Mobile Launch Points and Launch Control Points. 19

Section 2F Aircraft and Air-Launched Missiles 19

2.31. Criteria Applicability. 19
2.32. General Design Criteria. 20
2.33. Nuclear Weapon Suspension and Release Systems. 20
2.34. Nuclear System Controls and Displays: 21
2.35. Multiplace Aircraft Consent Functions. 22
2.36. Aircrew Cautions. 22
2.37. Nuclear Weapon Status Monitoring. 23
2.38. Interface Unit and Weapon Power Control. 23
2.39. Multifunction Controls and Displays. 23
2.40. Multiplexed (MUX) Systems: 24
2.41. Air-Launched Missiles. 25

Section 2G Test Equipment and Training Devices 25

2.42. Test Equipment. 25
2.43. Training Devices. 27

Section 2H Technical Order (TO) Procedures 27

2.44. General Criteria. 27
2.45. Operational Certification Procedures. 27
2.46. Training Procedures. 27
2.47. Cargo Aircraft Loading Procedures. 27

Chapter 3— DESIGN CRITERIA FOR NONCOMBAT DELIVERY VEHICLES AND SUPPORT EQUIPMENT 28

Section 3A General Design Criteria 28

3.1. Design Philosophy. 28
3.2. Structural Load Definitions: 28
3.3. Structural Design Criteria. 28
3.4. Data Sources. 29

Section 3B Ground Transportation Equipment 29

3.5. Criteria Applicability. 29
3.6. General Criteria: 29

3.7. Trailers and Semitrailers. 30
3.8. Tow Vehicles. 30
3.9. Self-Propelled Vehicles. 30
3.10. Rail-Based Vehicles. 30
3.11. Forklifts and Weapon Loaders. 30

Section 3C Hoists, Cranes, and Similar Devices 31

3.12. Criteria Applicability. 31
3.13. Safety Features and Controls: 31
3.14. Structural Design: 31

Section 3D Handling and Support Fixtures 32

3.15. General Criteria. 32
3.16. Weapon Containers. 32
3.17. Pallet Standards. 32

Section 3E Cargo Aircraft Systems 32

3.18. General Cargo Aircraft Criteria. 32
3.19. Restraint Configuration Criteria. 32

Table 3.1. Nuclear Weapon Restraint Configuration G-Load for Cargo Aircraft. 33

Chapter 4— EVALUATION CRITERIA FOR NUCLEAR WEAPON SYSTEMS 34

Section 4A General Criteria 34

4.1. Criteria Applicability. 34

Section 4B Specific Criteria 36

4.2. Automata and Software: 36
4.3. Electrical Subsystems. 37
4.4. Arming and Fuzing (A&F) Systems. 38
4.5. Ground-Launched Missile Systems. 38
4.6. Aircraft and Air-Launched Missiles: 39
4.7. Test Equipment: 40

Chapter 5— EVALUATION CRITERIA FOR NONCOMBAT DELIVERY VEHICLES AND HANDLING EQUIPMENT 42

Section 5A Criteria and First Article Verification 42

5.1. Evaluation Criteria. 42
5.2. First Article Verification. 42
Section 5B Ground Transportation Equipment 42
5.3. General Criteria. 42
5.4. Trailers and Semitrailers. 43
5.5. Tow Vehicles. 43
5.6. Self-Propelled Vehicles. 44
5.7. Rail-Based Vehicles. 44
5.8. Forklifts and Weapon Loaders. 44
Section 5C Hoists, Cranes, and Similar Devices 45
5.9. Safety Features and Controls. 45
5.10. Safety Factor Verification. 45
Section 5D Handling and Support Fixtures 45
5.11. Handling Equipment, Suspended Load Frames, and Support Fixtures. 45
5.12. Weapon Containers. 45
5.13. Pallet Standards. 45
Section 5E Cargo Aircraft Systems 46
5.14. Tiedown Patterns. 46
5.15. Load Configurations. 46
Section 5F Production Article Verification 46
5.16. Fail-Safe Features. 46
5.17. Proof Tests. 46
5.18. Environmental Tests. 46
5.19. Hoist Tests. 46
Attachment 1—GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS 47

Chapter 1

GENERAL STANDARDS AND CONTROL

Section 1A—Responsibility and Scope

1.1. Terms and Definitions. AFI 91-101, (formerly AFR 122-1), defines all terms used in this manual.

1.2. Department of Defense (DoD) Safety Standards. The DoD Nuclear Weapon System Safety Standards form the basis for the safety design and evaluation criteria for nuclear weapon systems. The DoD Nuclear Weapon System Safety Standards state that:

- There shall be positive measures to prevent nuclear weapons involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield.
- There shall be positive measures to prevent DELIBERATE prearming, arming, launching, firing, or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority.
- There shall be positive measures to prevent INADVERTENT prearming, arming, launching, firing, or releasing of nuclear weapons in all normal and credible abnormal environments.
- There shall be positive measures to ensure ade-quate security of nuclear weapons, pursuant to DoD Directive 5210.41.

1.3. Air Force Criteria: To comply with the DoD safety standards, the Air Force has implemented a set of minimum design and evaluation criteria for their nuclear weapon systems. These criteria do not invalidate the safety requirements in other DoD publications, but Air Force activities are required to apply the more stringent criteria. Since the criteria in this manual are not design solutions and are not intended to restrict the designer in the methods and techniques used to meet operational design requirements, they are not all-inclusive. Air Force nuclear weapon system designers may add feasible and reasonable safety features, as needed. The goal is to design a system that significantly exceeds these safety criteria.

Section 1B—Deviations to Criteria

1.4. Requests for Deviations: If the design of an Air Force nuclear weapon system does not meet the requirements contained in this manual, a deviation must be obtained according to the requirements of AFI 91-107. Exceptions to this manual, as evidenced by some current and older designs, do not constitute a precedent to deviate from the criteria.

Chapter 2

DESIGN CRITERIA FOR NUCLEAR WEAPON SYSTEMS

Section 2A—General Philosophy and Criteria

2.1. Nuclear Weapon Safety Design Philosophy. The Department of Energy (DOE) designs nuclear weapon safety devices to withstand credible abnormal environments for a longer time than the weapon's critical arming components or until the weapon is physically incapable of providing a nuclear detonation. The design of Air Force nuclear weapon systems must consider the DOE nuclear weapon design concepts:

2.1.1. Exclusion Region. This region contains the firing set and weapon detonator system. It also has the necessary packaging and safety devices to exclude electrical energy, for other than intended use, from the firing set and weapon detonator system.

2.1.2. Strong Links. Safety devices (such as system prearm devices and environmental or trajectory sensing devices) called strong links provide the signal path to the firing set for the arming and firing signals. Strong links provide energy isolation in an abnormal environment and operate in the normal mode only when used.

2.1.3. Weak Links. A weak link is a selected functional unit (such as a capacitor or transformer) vital to operating the firing set and weapon detonator system and whose function is not likely to be duplicated or bypassed. Weak links respond predictably to certain levels and types of abnormal environments by becoming irreversibly inoperative and thus rendering the system inoperable at levels less than those at which the strong links fail to keep electrical isolation. Weak links and strong links are collocated so as to experience essentially the same environment at the same time.

2.2. Nuclear Weapon System Safety Design Philosophy. The guidance in this chapter is for use by Air Force and Air Force-contracted designers and evaluators. Air Force nuclear weapon system designs implement critical function control to provide adequate protection against premature detonation of a nuclear weapon in both normal and credible abnormal environments.

2.2.1. Critical Function Control Concepts. Criteria for adequately controlling some critical functions depend on the specific nuclear safety design concept of the weapon system. Older nuclear weapons and weapon systems use the energy control (or removal) concept. However, many currently deployed systems and those in development use the information control concept or a combination of both concepts.

2.2.1.1. Energy Control Concept. Limiting the entry of energy into the weapon system control the critical functions.. Devices that execute critical functions are designed to require high- energy signals for operation. Other functions require signals with very low energy and occur as infrequently as possible. Reliability requires that the weapon system respond when the specified high-energy command signals are present at the weapon interface. Therefore, safety levels of weapon systems using this design concept depend on the safety controls that block application of those high-energy signals to the weapon interface until the controls are properly removed.

2.2.1.2. Information Control Concept. Critical functions are commanded by uniquely encoded information or data words. Safety levels depend on the uniqueness of the command or data word and are evaluated based on the assumptions of worst-case power levels.

2.2.2. Critical Functions. These functions are critical:

2.2.2.1. Authorization. The weapon system must have one or more devices to control authorization to use the weapon. These devices must prevent prearming or arming (or both) of a bomb or warhead in aircraft-carried weapons and thelaunch of a ground-launched missile until authorization to prepare to use the weapon is received through the command and control system. A ground-launched missile may have an authorization control device that prevents warhead prearming or arming (or both). Examples of these controls are the enable device in the Minuteman weapon system and the permissive action link (PAL) in many nuclear bombs.

2.2.2.1.1. The authorization device, which meets the numerical standards for protection against unauthorized actions, must operate on the information control concept. A secure method must provide the information through command and control channels.

2.2.2.1.2. The system must have built-in positive design features to prevent inadvertent operation of the data entry control. The positive features must protect against inadvertent operation of the authorization device and an attack on, or bypass of, the device. The system design must reveal the attack on the device. If remotely monitored, the weapon system operators or control point must receive an attack indication. The indication (either local or local and remote) must be latching and must be protected from the attacker to prevent reset.

2.2.2.1.3. The authorization device must not prevent any safing or relocking function, regardless of the state of the authorization device.

2.2.2.2. Prearming. The prearm command signals the weapon that the weapon system operators want it to function as designed and produce a nuclear detonation. Once commanded to the prearm state and presented with proper arming stimuli, the weapon will arm. The weapon system design must keep the prearming function separate and independent from the authorization function. Weapon design features must preclude prearming in the absence of the prearm command signal and prevent bypass of any prearming device that would permit arming without prearming.

2.2.2.2.1. For weapons whose design is based on the information control concept, use uniquely coded prearm command signals. The information needed to generate the unique signal must be physically unavailable to the unique signal generator until its use is required.

2.2.2.2.2. For weapons whose design is based on the energy control concept, physically and electrically isolate the prearm command signal line from all other circuits. Avoid the use of common routing, cabling, or connectors with the prearm command signal line and any wire likely to carry enough power to operate the prearm device. Give special design consideration to credible abnormal environments.

2.2.2.3. Launching. Operation of a rocket motor propulsion system (control of launch) is controlled through two independent functions: the ignition system arm or safe command and the ignition command. The weapon system must have a safe and arm device or equivalent design to protect the ignition system. Without the arm command, propulsion system ignition will not occur even if the ignition command is sent. Design features must preclude accidental or deliberate unauthorized transmission of the arm and ignition commands. The design must also prevent any fail-

ure from allowing bypass of the ignition safing device that would permit ignition when the device is safed.

2.2.2.4. Releasing. Operation of the release system for aircraft-carried weapons is controlled through two independent functions: the release system unlock command and the release command. Without the unlock command, separation of the weapon from the combat delivery aircraft will not occur even if the release command is sent. Design features must preclude accidental transmission of the unlock and release commands and must also prevent any failure from allowing bypass of the lock device that would permit release of the weapon when the device is locked. For air-launched missiles, the ignition system arm and the release system unlock must be separate and independent functions.

2.2.2.5. Arming. If the weapon is prearmed, arming will be the design response of the weapon to sensing that the environment is within the limits defined for operational use (after launch or release). Design features must include measurements of the environment so environments other than "intended use" are discriminated against to the greatest extent possible. If a missile has self-contained guidance, include a good guidance signal (paragraph **2.9.1.**) as a measurement of the proper operational environment. The armed condition allows the selected fuze signal (such as radar, contact, or timer) to detonate the warhead. Design features must preclude arming unless the proper operational environment is sensed; prevent erroneous transmission of the good guidance signal; and preclude bypass of the arming system that would permit nuclear detonation of the warhead without arming.

2.2.2.6. Targeting. Targeting is a critical function for ground-launched missiles. It includes the preparation, weapon system processing, and transmission of targeting data to missile guidance and arming and fuzing systems. Targeting data consists of the flight control and fuzing constants needed to deliver and detonate the weapons within the designated target area. The weapon system design must prevent erroneous targeting functions and accidental or unauthorized changes to targeting data.

2.2.3. Reversible Operations. Ensure the operation of devices for authorization, prearming, propulsion system ignition arming, and aircraft release system unlocking is reversible.

2.3. Critical Function Numerical Requirements. The numerical requirements specified in AFM 91-107 apply to ground-launched missile and combat delivery aircraft systems to show that, in normal environments, the calculated probability of occurrence of inadvertent prearming, launching, releasing or jettisoning, arming, or erroneous targeting of nuclear weapons is unlikely to occur during the system lifetime. Although numerical specifications for credible abnormal environments are only defined for DOE bombs and warheads, Air Force nuclear weapon system designers will incorporate positive safety features for these environments into the design of combat delivery vehicles to protect against inadvertent critical function activation.

2.4. Safety Features and Procedures. Ensure the nuclear safety features eliminate or minimize the dependence of safety and security on administrative procedures.

2.5. Explosive Ordnance Disposal. Design aircraft and missile systems to permit emergency access to those components and circuits required to carry out render-safe procedures. Develop render-safe procedures with the intent of meeting the numerical requirements of AFI 91-107.

2.6. Physical and Internal Security. According to the fourth DoD Nuclear Weapon System Safety Standard, a physical security system must prevent access to nuclear weapons and protect critical equipment and secure data. In support of the second DoD standard, nuclear weapon systems and nuclear weapons must incorporate internal security features to prevent unauthorized use.

2.7. Environmental Parameters. Consider nuclear safety design features over the full range of normal and credible abnormal environments to which the system could be subjected. Since specific normal and abnormal environmental parameters are system dependent, use the parameters specified in appropriate bomb and warhead STS and MC documents and in the weapon system specifications.

2.8. Safe and Arm (S&A) and Arm/Disarm (A/D) Devices. Ensure these devices meet the design criteria in MIL-STD-1512. If the devices are electrically actuated, they must arm only in response to an externally generated unique signal. The safing signal must differ from the arming signal to reduce the risk of arming during attempted safing. If a monitor signal is used, it must also be different from the arming signal.

2.9. Protection of Friendly Territory. Design weapon systems to prevent nuclear detonations, except within specified target boundaries.

2.9.1. Good Guidance Signal. Missile systems, including guided missiles launched from aircraft, must receive a good guidance signal from the guidance and control unit before nuclear warhead arming can occur. The good guidance signal must be withheld if a final guidance accuracy check shows the weapon will impact outside the specified target boundaries.

2.9.2. Target Boundaries. The boundaries for airborne release and delivery systems vary with the number of weapons, weapon yield and type, methods of use, geographical location, and operational needs. Consequently, the DoD weapon system program managers, with coordination from the operating command and the appropriate nuclear safety evaluation agency, must specify target boundaries.

2.10. Single Component Malfunction or Operation. Ensure the malfunction or accidental operation of a single component does not result in prearming, launching, or releasing of a nuclear weapon; arming of a prearmed weapon; or authorization to use a nuclear weapon system. This criterion applies before any of these functions are initiated or when more than one event remains in the operational sequence leading to function initiation.

2.11. Human Engineering. Design the system so no two independent human errors or acts will cause prearming, arming, launching, or releasing of a nuclear weapon in an operational weapon system or will authorize the use of a ground-launched missile system. This criterion applies only before initiation of actions required to complete the desired operation. The design must minimize the number of points within the system where human actions could degrade nuclear safety or security. The design must also stress positive measures to prevent deliberate unauthorized or accidental operation of controls that could degrade nuclear safety or security.

Section 2B—Automata and Software

2.12. General Design Requirements. These design safety criteria apply to automata and software that receive, store, process, or transmit data to monitor, target, prearm, arm, launch, release, or authorize the

use of a nuclear weapon. Design such equipment and software to provide the greatest extent of protection against accidental or deliberate unauthorized operation of critical functions.

2.12.1. Software Specifications. Follow DoD-STD-2167A and translate system requirements into program design in a systematic "top down" method. Incorporate the applicable nuclear safety design requirements of this manual as well as the derived design implementation requirements, into the appropriate software specifications.

2.12.2. Higher-Order Language (HOL). Base the software development or modification principally on the use of an Air Force-approved HOL. Use code development in assembly or machine language only when the HOL does not provide adequate capability for time-critical or hardware-interfacing functions. Ensure all software verification checks (of nuclear critical variables, flags, data, etc.) that can be made in the HOL are done before calling assembly or machine language routines (paragraph **2.14.2.**). Unless specifically approved in the nuclear surety impact statement defined in AFI 91-103, do not modify critical software functions in a language other than the source code for that software.

2.12.3. Hierarchical Design. Design the software in a hierarchical structure of identifiable programs, subprograms, modules, procedures, and routines. The highest level of control logic must reside at the top levels, and the computational or algorithmic functions must reside at the lower levels. Set up the levels so lower levels do not call on higher levels. Use structured program techniques to the greatest extent, consistent with the programming language selected. Modules performing critical functions must be single- purpose modules.

2.12.4. Hardware Check. Design the automata to provide self-check, confidence, or test routines to verify the integrity and proper state of hardware devices that affect or execute critical functions. Critical failure modes or illegal states must result in operator notification of the problem and the status of any automated actions taken.

2.12.5. Fault Tolerance and Error Handling. Design the computer system to revert to a predictably safe state when a critical function system fault is detected. The computer system must be "fault tolerant" to the effects of temporary power outages and protected against the harmful effects of electromagnetic and electrostatic interference. Ensure the automated response to critical system errors and faults does not result in any weapon command state change and is displayed to the system operator.

2.12.6. Interrupts. Define specific priorities and responses for routines that interrupt program execution or disable interrupts.

2.12.7. Idle Operations. Software must not use a STOP or HALT instruction or cause a CPU (central processing unit) WAIT state. The unit must always be executing, whether idle or actively processing. Provide techniques for deadlock (waiting for a particular event that will not occur) prevention, detection, or resolution.

2.12.8. Instruction Alterations. Prevent software from modifying its own instruction set or the program instruction set of ancillary programs.

2.12.9. Hardware Initialization and Shutdown. Ensure critical function hardware, which is controlled or monitored by software and automata memory containing nuclear critical information, is initialized or verified to be in a known and predictably safe state (paragraph **2.12.4.**). Upon system shutdown or program termination, the software must ensure all settable, nonvolatile devices and relays are set to a known and safe state.

2.13. Memory Characteristics:

2.13.1. Memory Volatility. Design automata system to ensure operational use does not alter or degrade memory content over time. Storage of critical function programs and data in nonvolatile and nondestructive read-only memory is preferred. Memory with volatile characteristics must have provisions to ensure erroneous data, resulting from power removal or other phenomena, does not affect any critical function or component.

2.13.2. Hardware Faults. Ensure the system inhibits any memory changes due to hardware failures. A single hardware fault must not cause a memory change that could initiate a critical function.

2.13.3. Memory Integrity Verification. Protect memory containing critical function routines and data with an error-detection memory controller, and ensure errors are resolved only by reloading programs or data from a memory image file located on a nonvolatile storage device. Do not perform error correction on memory locations containing nuclear critical routines or data.

2.13.4. Memory Accessibility. Include provisions to protect the accessibility of memory locations containing nuclear critical routines and data. Partition critical function routines and data base elements so any allowable memory segment address, which is allowed by the system for noncritical functions or data base elements, cannot specifically address critical data base elements or critical function routines.

2.13.5. Memory Declassification. Provide a method to erase or obliterate any clear-text secure codes from memory.

2.13.6. Memory Initialization. Initialize to a pattern all memory not used for initial program and data load, which is available to any processor capable of executing critical function routines. If executed as an instruction, this pattern must not initiate any critical functions or change the state of critical safety features or meters. Initialization may be done for all memory at system startup or for only unused memory after completion of program and data loading.

2.14. Critical Command Messages. Design the system to prevent program execution or continuation until all program instructions or data (or both) are loaded and verified. Display the results of the program load verification to system operators.

2.14.1. Command Verification Protocol. For aircraft and air-launched nuclear weapons, ensure the verification of critical commands transferred to remote units for processing or execution. If a communication error occurs, the command sequence must be reset to its initial state.

2.14.2. Validity Checks. Ensure all critical command transmissions originate with manual operator inputs (paragraph **2.16.1.**). Before transmission, system operators must verify the state of all applicable preconditions and inhibits to be in the correct state.

2.15. Operating System (OS) and Run-Time-Executive (RTE). Ensure only the OS and RTE are able to call critical function routines and modules. The operating system software, while working on a fixed stack size with accumulated depth in applications use, must not overflow or overwrite other program instructions or data or be unable to correctly return all previous calls. An erroneous entry into a critical function routine or sequence (paragraph **2.16.3.**) must terminate function execution and notify the operator of the error.

2.16. Critical Function Routine Design:

2.16.1. Operator Interface. Ensure nuclear critical functions cannot be initiated without operator intervention or by a single operator action (two or more actions, such as keystrokes, are required). For ground-launched missiles, crewmember initiation of critical functions requires separate and independent action. The software must provide detection and notification of improper operator entries, except for authorization and unique signal information. Operator cancellation of nuclear critical function processing requires a minimum number of safely accomplished operator actions.

2.16.2. Single Function Routines. Ensure routines are not capable of performing more than one nuclear critical command. Each nuclear function routine must have a single unique entry point and a single unique exit point.

2.16.3. Critical Function Call and Entry Checks. Ensure critical function command routines cannot be called until all proper conditions exist. All entries into nuclear critical function routines must have checks to ensure such entries are both authorized and approved (operator action is accomplished and all preconditions are met).

2.16.4. Command and Data Word Format. Select decision logic data values that require a specific binary data pattern of "ones" and "zeros" (not all "ones" or all "zeros") to reduce the likelihood of hardware or automata malfunctions that satisfy the decision logic for critical function initiation or propagation.

Section 2C—Electrical Subsystems and Hazards

2.17. Electrical Subsystem General Design Criteria. A major part of a nuclear weapon system is composed of electrical subsystems designed to monitor, target, prearm, arm, launch, release, or authorize the use of nuclear weapons. Design these subsystems to preclude accidental operation, single component failure, or electrical disturbance from performing or degrading critical functions.

2.17.1. Electromagnetic Interference (EMI). Design all electronic and electrical subsystems or equipment within or associated with nuclear weapon systems to minimize undesired responses and emissions. (Refer to MIL-B-5087, MIL-B-6051, MIL-STD-461, and MIL-STD-462.) The design of wires, switches, cable connectors, junction points, and other system elements must minimize undesirable radiated and conducted interference or transients when such EMI could cause a nuclear hazard or ordnance ignition.

2.17.2. Isolation. In general, electrically isolate any critical circuit, either power or control, from other critical and noncritical circuits (consider signals transmitted on either time- or frequency-domain multiplexed transmission lines to be electrically isolated). The purpose of this requirement is to prevent faults or common mode malfunctions from operating critical circuits or explosive components in all environments. These requirements apply to all nuclear weapon systems:

- Do not use wire or cable shields as current-carrying conductors and cover shields with an insulation layer.
- Ensure electroexplosive circuitry, which affects or is affected by critical functions, conforms to MIL-STD-1512.
- Within the weapon interface control units, use crush-resistant shielded compartments and separate wiring bundles to isolate critical function circuits from power, noncritical circuits, and other critical circuits.

- For hardwire systems, ensure electrical functions unique to the aircraft monitoring and control (AMAC) and release systems do not share an electrical connector with nonnuclear functions.
- Isolate critical from potential sources of unintended electrical power.

2.17.3. Switching. Switch the supply side or power side of switchable circuits. For critical circuits, switch both the supply and return sides.

2.18. Wiring and Cabling:

2.18.1. Routing and Installation. Install and secure electrical wiring to minimize vibration and chafing. Cable design and routing must minimize electromagnetic coupling between circuits and the potential for damage during maintenance operations.

2.18.2. Shields. Terminate cable shields at a connector backshell that provides for peripheral bonding of the shield. When shielded wires and cables contained within an overall cable shield terminate with pigtails, the cable shield pigtails must not exceed 6 inches. Connector backshells must have conductive finishes to minimize shield termination impedance.

2.18.3. Grounds. Use a common ground reference connection for signal returns common to two or more circuits. Select ground wire or shield braid gauge to ensure the largest current expected during system operation or credible failure either does not offset the ground plane reference voltage or offsets it by an order of magnitude less than the level at which system operation or logic state could change or ground-loop symptoms could occur.

2.18.4. Power Cable Terminations. Except for weapon and warhead interface connectors, electrical power wiring must end in female connectors at the power source side.

2.18.5. Mechanical Support. Provide critical circuit wiring with mechanical support that is an integral part of the connector at the entry point into the electrical connector. Mechanical support should provide strain relief during mating and demating.

2.19. Electrical Connectors. Ensure all hardwire electrical connectors associated with aircraft nuclear weapon circuits conform to MIL-C-38999. This requirement does not apply to electrical connectors used within armament system black boxes.

2.19.1. Alignment and Mating. Design electrical connectors to prevent misalignment of connector components, bent pins during mating, and mating of wrong connectors. Use only one wire for each pin and minimize the number of spare pins. Do not use these pins for mechanical support. Provide adequate access for connector mating and demating operations. If possible, make the mating and demating processes visible.

2.19.2. Sealing. Use environmentally sealed connectors. If used in electrical connectors, potting compounds must positively preclude reversion.

2.19.3. Mandated Use Isolation Exception. If possible, design the circuits within a single connector to meet the isolation requirements of paragraph **2.17.2.** If all the requirements cannot be met due to the mandated use of nonconforming weapons or equipment, connector pin mapping must ensure no single bent or misaligned pin can result in the application of sufficient power to cause critical function activation.

2.19.4. Nonelectrical Connections. Ensure connectors do not contain both critical electrical circuits and lines carrying liquids (such as coolant solutions, fuels, and hydraulic fluids).

2.20. Electrical Current Considerations. Limit monitoring and testing current to a value at least an order of magnitude below the maximum no-fire level of the most sensitive ordnance device or firing circuit component in a nuclear weapon system.

2.21. Electromagnetic Radiation (EMR). Provide for maximum practical protection against the hazards of EMR, including electromagnetic pulse and EMR from lightning. Also, provide protection from direct lightning strikes to the weapon system for all ordnance devices and firing circuits. Ensure the design of nuclear weapon systems protects against the inherent susceptibility to EMR of electroexplosives, semiconductors, and other devices.

2.21.1. EMR Environment Levels. Although a complete survey of the EMR environment weapons will encounter is not available, the ground-based and airborne radio transmitters and radar sets now in the Air Force inventory can generate peak power densities of about 75dB(mW/m2), equivalent to 3440 volts per meter, in the near vicinity of the antenna. These average and peak values or those specified in the STS (whichever is greater) are the minimum levels considered in designs for EMR protection.

2.21.2. Shielding Design. Ensure critical function components are protected against EMR-induced component damage or functional upset. If feasible, use an integral shielded volume design consisting of shielded enclosures and wire and cable shielding.

2.21.2.1. Shielded Enclosures. Locate critical function components within shielded enclosures that provide sufficient attenuation of external electromagnetic fields and surface currents to preclude electronic component damage or functional upset. The shielded enclosure design must provide radio frequency gasketing for enclosure doors; minimize gap, joint, and aperture sizes; and provide transient suppression for unshielded line penetrations into the shielded enclosure. Where conductive aircraft or missile skin surfaces form part of the shielded enclosure, ensure skin joints have low-resistance contacts with fastener spacing designed to minimize gap sizes. Design monitor circuits to not conduct or couple EMR energy into the shielded volume.

2.21.2.2. Cable Shielding. Refer to paragraph **2.18.2.**

2.21.2.3. Use terminal protection devices (TPD) (such as filters and surge suppressors) to provide additional circuit protection where shielding alone does not provide sufficient attenuation. Also, use TPDs on unshielded line penetrations into the shielded volume.

2.21.2.4. Shield electroexplosive devices (EED) firing circuits using a twisted wire configuration with the case of the initiator electrically bonded to the structure. A single ground point must be common to all firing circuits. When exposed to the EMR environments specified in the STS or 50dB(mW/m2) average (whichever is greater), the maximum RMS (root mean square) current in its bridgewire must be 20dB below the maximum no-fire current of the EED. EED male connectors are in an open-circuited configuration, install shielding caps that have electrical continuity from shield to case with no gaps or discontinuities in the shielding configuration.

Section 2D—Arming and Fuzing (A&F) Systems

2.22. General Criteria. An A&F system is the sum of components, devices, and design features that cause weapon prearming, arming, fuzing, and firing as well as those components and features that protect against deliberate unauthorized or accidental prearming, arming, fuzing, and firing. Both DoD and DOE subsystems are normally a part of the total nuclear weapon system A&F design, and the DOE design satisfies many of the requirements in this section. An effective design incorporates the components and design concepts described in the following criteria to satisfy the criteria in paragraph **2.2.1.**

2.23. System Devices:

2.23.1. Prearm Device. Design the A&F system to provide a unique prearming signal for the strong-link prearm device in the warhead or bomb. Derive this signal from some part of the weapon system under direct human control. If operational considerations permit, the function provided by human action must be reversible up to the time of launch or release.

2.23.2. Environmental or Trajectory Sensing Device (E/TSD). Include an E/TSD in the A&F system design. This device (preferably a strong link located in the warhead or bomb) prevents arming until proper environment is sensed and responds only to an environment unique to flight of the weapon. Because this stimulus may occur as a result of the release of a bomb or the launch and programmed flight of an air-launched or ground-launched missile, prevention of premature release or launch of the weapon is essential. Operating the prearm function will normally be a prerequisite to activating the E/TSD.

2.23.3. Launch or Release Sensing Device. Include a device in the A&F system that prevents power from being applied to the A&F system (or applicable components within the system). For aircraft systems, this device (such as a pullout switch or breakaway connector) must sense launch or release of the weapon. For ground-launched missiles, this device (such as a lanyard or a pressure-actuated valve) must sense the proper launch environment. The design of these devices must protect against accidental or inadvertent operation.

2.24. System Design Features:

2.24.1. Abnormal Environment Protection. Include protective features in the A&F system to prevent prearming and arming in all credible abnormal environments specified in the STS document and in the applicable weapon system specifications.

2.24.2. Dual Signal Arming. Incorporate at least two separate and independently derived signals, which cannot be generated by a single signal at any point, to arm the weapon. These signals are interrupted by one or more strong-link devices located within the nuclear bomb or warhead. Ensure at least one of the signals is continuous after application (required for multiple power sources).

2.24.3. Energy Discharge. Design the A&F system to provide for automatic discharge of stored energy in the A&F energy storage devices (such as capacitors and activated batteries) if arming power is interrupted.

2.24.4. Lightning Protection. Incorporate lightning protection to protect critical A&F circuits.

2.24.5. Nondestructive Testing Compatibility. Ensure exposure to standard Air Force nondestructive testing environments (X-ray, ultrasonic, magnetic, and similar tests) specified for use in the weapon system does not degrade nuclear safety for the A&F system.

2.24.6. Chemical Compatibility and Reversion. Ensure all material used in the design is chemically compatible in all STS environments. Do not use materials that could increase the high-explosive sensitivity, generate an explosive gas, cause an electrical short or reversion, or create similar results.

2.24.7. Monitoring:

- •Provide the capability (always placed on the A&F system) to monitor the state of at least one strong link in all weapon system configurations. Also, develop requirements for the weapon system to use the capability to complement the employment concept.
- •Ensure the monitoring function design prohibits the possibility of introducing energy from any source that might operate an A&F critical function if a system fault or credible abnormal environment occurs (**2.20.**paragraph 2.20). If feasible, consider nonelectrical monitor systems.

2.24.8. Input and Output Isolation. Isolate the electrical inputs to nuclear safety devices from the outputs, and use other methods (such as incompatible signals) to minimize the possibility of bypassing the safety devices.

Section 2E—Ground-Launched Missile Systems

2.25. Criteria Applicability. Apply the design criteria in this section to ground-launched missile systems, and apply the noncombat delivery vehicle criteria in **Chapter 3**chapter 3 to ground mobile combat delivery vehicles.

2.26. Launch Control System. This system consists of the hardware, firmware, software, and secure codes used to authorize a missile launch and to launch the missile.

2.26.1. System Design. Apply these criteria:

- •Missile launch must occur only through intentional operation of the authorization and launch control devices. No other system or subsystem, in either its operational or failure mode, must be able to authorize a missile launch, start a launch sequence, launch a missile, or operate the propulsion system.
- •Controlled launching requires both launch authorization and launch control functions. Design the weapon system to detect and resist tampering with the launch control system. Continuous visual and audible indications to all launch control points (LCP) must occur when an attempt is made to operate the launch control system, and the indications must remain until the system operators acknowledge and reset them.
- •The launch control system must remain in, or return to, a safe state when component failure or electrical power loss occurs.
- •Arm (operate) and safe (off) critical command signal functions must not be complementary functions; that is, the absence of "arm" will not be construed as "safe" or vice versa.

2.26.2. Propulsion System Ignition Protection. Protect the rocket propulsion system with an S&A or A/D device (or equivalent protection) that can be electrically armed by a directly applied unique signal (whose generator is not located in the missile) and can be electrically and manually safed (paragraph **2.8.**). Generation of the unique signal requires some physical or electrical action unlikely to occur in a credible abnormal environment.

2.26.3. Multiplex Control Systems. Use multiplex control systems, if feasible, for critical signals within or between LCPs and launch points (LP); within the missile; and between the missile and reentry system or nuclear payload. These safeguards apply:

- A single component failure or system fault must not cause inadvertent transmission of critical signals or inadvertent operation of critical functions.
- The system design must stop a change of state or an output of a critical signal if data synchronization is lost.
- The multiplex system design must be compatible with system hazard and fault analyses so that the polling time interval and automation logic will not mask any critical function activation or fault between successive polls. If this requirement cannot be done for all credible environments, provide a means for dedicated reporting, automatic shutdown, or priority interrupts.

2.27. Reentry System, Reentry Vehicle, or Payload Section A/D Device. For each ground-launched missile, incorporate an A/D device in the reentry system, reentry vehicle, or payload section to interrupt all power (except monitor power) to any warhead interface (paragraph **2.8.**) and make it possible to safe this device for all weapon system configurations. The A/D device is not needed if it can be shown that a single component failure will not apply power to any warhead interface; the device is not needed to meet the criterion of table 2.2 for inadvertent application of power or signals to the bomb or warhead interface; and provisions exist for removing power to the missile if a failure occurs that could contribute to power being inadvertently applied to any warhead interface.

2.28. Monitor Systems:

2.28.1. Monitor Requirements. Provide systems that allow the operator to continuously monitor the safe status of the missile propulsion system; warhead or warheads (paragraph **2.24.7.**); reentry system, reentry vehicle, or payload section A/D device; and launch control system. When the operator cannot continuously monitor these components, provide for on-demand monitoring of the safe status; however, ensure the weapon control system continuously monitors each of these devices. Also, ensure the operator receives a positive and timely indication of any change in the safety status of these continuously monitored systems.

2.28.2. Power Removal. Provide for automatic removal of electrical power that could cause accidental prearming or arming of the nuclear weapon or launching of the missile if an unsafe condition is indicated and cannot be corrected.

2.28.3. Monitor Electrical Current Limitations. Refer to paragraph **2.20.**

2.29. Command and Control Communications:

2.29.1. National Command Authorities to LCP:

2.29.1.1. The launch crew must not have the secure code necessary to authorize the launch of or to launch a missile until launch authority is granted. This withheld code may be used to satisfy the unique signal input requirement for all ignition protection devices. A code that authorizes the use of a warhead must be different from the code used to authorize the launch of a missile.

2.29.1.2. For systems with a selective launch capability, the launch control system must be secured to allow launch of one or more missiles without revealing or compromising any of the codes for the other missiles or military forces.

2.29.1.3. Policies and procedures that govern the authentication and safeguarding of nuclear control orders are in Joint Publication 1-04.

2.29.2. LCP to LP Communications and Code Devices:

2.29.2.1. Ensure nuclear command and control communications meet the numerical standards that specify the minimum degree of protection required against the threat or commission of unauthorized launch actions by third parties or cognizant agents. For any device operated by the withheld secure code discussed in paragraph **2.29.1.1.**, allow only a limited number of attempts at operation using incorrect codes or include some other antitamper feature. Also, include a device or system to detect tampering. The system must maintain the numerical requirements until tampering is detected and stopped.

2.29.2.2. Secure critical command and status message transmissions against tampering, monitoring, and substituting. If LCP and LP locations make physical security measures impractical, encrypt the messages and authenticate the status by cryptographic means. The communications system must alarm the LCPs if tampering with the system occurs.

2.29.2.3. An LP may respond to launch commands from a single LCP. For a tactical nuclear weapon system, ensure one or more LCPs monitor and are able to take compensatory action if an unauthorized critical command message or status is detected. For a strategic nuclear weapon system, ensure the critical LP status is monitored at the primary LCP and at least one other location. Each location must be able to take compensatory action if an unauthorized critical command message or status is detected.

2.29.2.4. The LCP will ensure that even after all secure codes are available, at least two people must actively cooperate to command authorization and launch.

2.29.2.5. Design the LCP and LP secure code storage devices to resist bypass or code readout, and ensure access to the storage device memory is controlled to prevent unauthorized code changes. Prohibit the use of maintenance tools or other devices that can change the memory to a standard unclassified code, except when the tool or device will stop use of the code storage device for its intended purpose and cause positive indications to be received at the LCP.

2.29.2.6. Make the signal commands for controlling the critical functions of prearming and launching unique, and do not store them in the weapon control system in a directly usable form. Also, prevent inadvertent and deliberate unauthorized use of the unique signals by such means as deriving unique signals from secure code commands, storing the signals in permuted form, and storing parts of the signals in separate locations.

2.30. Mobile Launch Points and Launch Control Points. For movement of a fully assembled missile and reentry system or nuclear payload, add safety devices to maintain the safe state of missile propulsion and A&F systems in normal and credible abnormal environments.

Section 2F—Aircraft and Air-Launched Missiles

2.31. Criteria Applicability. Apply the design criteria in this section to aircraft delivery, launch, suspension, release, and weapon monitor and control systems. The safety devices these criteria require may also be used for nonnuclear stores, except where their use is specifically restricted.

2.32. General Design Criteria. Design the aircraft nuclear weapon system to meet these criteria:

2.32.1. AMAC and Release System Electrical Power:

- Ensure critical functions will not occur by opening a circuit breaker or other circuit protective device. Also, do not connect operating power or control functions to a device (such as a semiconductor) whose major failure mode could cause activation of a critical function. Aircraft electrical power failure must not jeopardize the safe condition of a weapon.
- Power the monitor and control functions, unlocking devices, S&A and A/D devices from an electrical bus that can be automatically powered from a secondary or backup power source if the primary power source is lost.

2.32.2. Prearmed Bomb Release. For a prearmed bomb release (not jettison), apply electrical power on one or more designated pins (identified in AMAC specifications) of the weapon interface connector before and during electrical separation of the weapon from the aircraft.

2.32.3. Inadvertent Power at Weapon Interface. Ensure malfunction or accidental operation of a single component does not result in application of unintended power to the bomb or missile interface.

2.32.4. Cable and Connector Design. Make connector pin assignment to protect against inadvertent application of prearm and arming power to the bomb or warhead as the result of damaged cables and connectors. Thus, the design will guard against cable or connector selection and cable routing susceptible to damage during assembly, maintenance, and test operations.

2.33. Nuclear Weapon Suspension and Release Systems. Design the suspension and release system to prevent weapon separation, release, ejection, launch, or jettison by any means other than proper operation of control devices. Protect all mechanical cables in the system from accidental operation and withhold electrical power to suspension and release components until release preparation begins.

2.33.1. Suspension Lock Monitor. Ensure the latched and locked condition of suspension devices is observable while the aircraft is on the ground. Also, ensure the locked condition can be determined electrically while the aircraft is on the ground or in the air.

2.33.2. In-Flight Reversible Lock. Provide an in-flight reversible lock that, when locked, prevents weapon release, even if the releasing force is generated and transmitted to the release system. Make the lock and its control independent of the nuclear weapon release system and the electrical connections between the aircraft and the weapon. The in-flight reversible lock system must:

- Mechanically restrain the releasing device.
- Stop release or launch if maximum available release force is accidentally applied in the release mechanism.
- Fail safe in the event a failure occurs when the lock is locked.
- Disable all means of release when in the locked position.
- Permit ground personnel to visually check the locked state. For direct visual inspection, the locking device itself must present an unmistakable indication of the locked state.
- Be protected from accidental operation.
- Provide a method in the crew compartment to show tampering with the aircrew's controls of the in-flight reversible lock.

- •Provide the aircrew with a remote indication of the fully locked or unlocked (or both) positions of the in-flight lock. If using a single indication for the locked state, reflect only the fully locked position of the in-flight reversible lock. If using a single indication for the unlocked state, reflect every state other than a fully locked state. The remote indication system must not allow an apparent indication to the aircrew of a locked state if an unlocked state exists.
- •Ensure the safety lock mechanically restrains the suspension and release linkage if hooks are used in the suspension and release linkage. When using hooks that can be individually latched or unlatched, the safety lock must mechanically restrain each hook.
- •Relock if unlock power is removed (accidentally or intentionally) while the lock is unlocked.

2.33.3. Pylon Jettison. Ensure pylons carrying nuclear weapons are either not jettisonable or the pylon jettison system includes a lock that meets the criteria for the nuclear weapons lock, as stated in paragraph **2.33.2.** If feasible, use a single lock for both the weapon and the pylon.

2.33.4. Unlock and Release Signal Isolation. When using discrete (energy control) signals, physically and electrically isolate the discrete signals for unlocking the in-flight lock and releasing the weapon to the greatest extent possible. A release system fault must not be able to operate the in-flight reversible lock, and an in-flight reversible lock fault must not be able to cause a release.

2.34. Nuclear System Controls and Displays:

2.34.1. Prearm and Safe Controls. Ensure application of a prearm or safing command to a weapon requires a control or control setting unique to the selected nuclear weapon. The control or control setting must require a separate and deliberate act by the weapon system operator.

2.34.1.1. Prearm Command. Design the prearm control as a unique signal generator (USG) command signal according to the proper specification for the aircraft-to-weapon interface. Do not have the information that defines the unique signal pattern within the stores management system (SMS) software, and make the information totally defined through crewmember action. Use the crew input for both the sequence of unique signal events and the definition of those events (such as data words). An insertable (by some physical action) read-only memory is the preferred method of unique signal data entry to the SMS. Initiation or application of the prearm command must not occur in the event of an accident.

2.34.1.2. Prearm Consent. The function of prearm consent is to inhibit prearming until direct crew action provides the required consent signal. Design the prearm consent control to reveal unauthorized operation or tampering (paragraph **2.35.**).

2.34.1.2.1. Electrical Interface (Non-MIL-STD-1760). Make the prearm consent function a hardwired control that interrupts power to the prearm circuit controlling the intent strong link.

2.34.1.2.2. Digital AMAC Electrical Interface (MIL-STD-1760). The design may implement prearm consent through software inhibits and controls. However, the consent signal must originate only through crew action. Removal of prearm consent must result in terminating the prearm or release functions in process and must inhibit prearm and release until consent is reestablished. Any change in consent status must also be sent to the weapon, which will then inhibit any critical function processing under missile system control.

2.34.2. Release and Launch Controls:

2.34.2.1. Release Consent. In the operating controls for the release system, include a nuclear consent function to inhibit unlocking the release system unless consent is given. Nuclear release consent must be a hardwired function. Neither the application nor reapplication of nuclear release consent must unlock or inhibit the locking of the in-flight reversible lock. Removal of nuclear release consent must relock the in-flight reversible lock.

2.34.2.2. In-flight Reversible Lock. Design the system controlling release or launch of a nuclear weapon with a unique hardware or software control or control setting for locking and unlocking the in-flight reversible lock. Make this control separate from the release and launch controls and the release consent.

2.34.2.3. Release Control or Control Setting. In addition to the control for the in-flight reversible lock and the release consent, ensure release systems have at least one separate hardware or software control or control setting unique to the release or launch of nuclear weapons and nuclear weapon training items. This control or setting must not be used to release or launch nonnuclear weapons.

2.34.2.4. Crewmember Release Input. For aircraft designed to release multiple nuclear stores, implement a crewmember input to the release system controls before each release of a nuclear weapon on a target or series of releases on a target complex. A one-time activation of nuclear release consent does not satisfy this requirement. The intent is to specifically preclude the automated delivery of numerous weapons without further crewmember input once authorization, nuclear consent (prearm and release), and prearm are accomplished.

2.34.2.5. Jettison and Emergency Release. Jettison is defined as the release of an unarmed weapon. If implemented, design the jettison function to only permit jettison of a nuclear weapon in a safe configuration. If emergency release is required during a combat situation, the weapon may be released in the prearmed state.

2.35. Multiplace Aircraft Consent Functions. Design multiplace aircraft AMAC and release systems with separate controls for both prearm and release consent. Each consent function must require the physically separate and independent actions of two crewmembers. The functioning of these controls is called "nuclear consent." A multiplace aircraft used in combat by one person may have provisions for prearming and release by a single person if a bypass is done before flight. Design this bypass so a person cannot do it in flight (paragraph **2.34.1.2.**).

2.36. Aircrew Cautions. Ensure aircrews are aware of these events:

2.36.1. Uncommanded Unlock. Unlocking of, or an unlock signal going to, the in-flight reversible lock when normal operation of controls has not commanded unlocking.

2.36.2. Uncommanded Prearm. Prearming of a weapon when normal operation of controls has not commanded weapon prearming.

2.36.3. Indeterminate Weapon State. Warning function that occurs when the aircrew cannot positively determine the safe state of the weapon. A delay may be designed into this function so the aircrew will not receive a caution during weapon change of state from safe to prearm or from prearm to safe.

2.36.4. Uncommanded Release. Nuclear weapon release signals occurring when normal operation of controls has not commanded release.

2.37. Nuclear Weapon Status Monitoring. Explicitly indicate the safe or prearmed state of each weapon through continuous or on-demand monitoring. Ensure continuous monitoring is provided when a weapon is in a state other than "OFF." Periodic monitoring on a multiplex bus communication system may satisfy this requirement.

2.37.1. Monitor and Control Circuit Isolation. Ensure monitor circuits are electrically isolated from power and control circuits and monitor functions are done independently of weapon control functions.

2.37.2. Weapon Monitor States. The weapon states are SAFE and PREARM, with a "not safe" condition while in transition. Define the corresponding monitor states as follows: SAFE - safe monitor true; ARM - arm monitor true; and ENABLE - PAL monitor line true. Paragraph **2.36.3.** discusses the conditions where both arm and safe monitors are true or both are false.

2.38. Interface Unit and Weapon Power Control. Control of power to interface units and weapon interfaces will require these actions and controls:

•Positive action to supply power to the interface unit (logic and power switching assemblies).

•Separate control that removes power from the interface unit (logic and switching assemblies).

•Positive action to supply power at the weapon interface.

•Separate control that removes power from the weapon interface.

2.39. Multifunction Controls and Displays. In addition to the other control and display criteria of this chapter, these criteria also apply to a software- driven display system:

2.39.1. Legends and Controls. Screen legends next to control buttons must only display if the control button is active (capable of initiating a function). Conversely, all active controls must have legends to indicate the active control function. All AMAC and rack lock and unlock commands require separate controls; for example, MONITOR will not become SAFE and LOCK will not become UNLOCK by subsequent activation of the same button. For aircraft (with more than one crewmember) that do not meet this requirement, only one crewmember at a time will have control over weapon system functions. Provide a capability to transfer this control function to another crewmember (such as a "TAKE" command).

2.39.2. Dedicated Display. When power is applied to a nuclear weapon, one crewmember must have control of nuclear weapon functions and at least one display must be dedicated to monitoring weapon status. Generally, the monitoring station will also be the control station. Implement scrolling where operational considerations make dedication impractical, and design the scrolling implementations in conjunction with a thorough advisory system that will alert the aircrew to anomalous nuclear weapon system conditions when the display is not present. If control is associated with the scrolled display, ensure return of control is clear and immediate. The software must not permit inadvertent control of the nuclear weapon system while the display is scrolled away.

2.39.3. Combined AMAC and Release Displays. AMAC and delivery functions may be combined on the same screen display, but screen formats must clearly differentiate the functions. Software pro-

tocols (inhibits and critical function preconditions) must minimize the possibility of executing an erroneously selected function.

2.39.4. Allowable Command State Transitions. Except for the SAFE-OFF state transition, each nuclear weapon must transition to a new command state from an adjacent command state (a command state is the last state the weapon was commanded to take). The adjacent states are defined according to this sequence: OFF-MONITOR-SAFE-ARM. The appropriate AMAC specification must define these command states. Change of state will occur only by a crewmember's explicit command, and such transition commands must be independent of the monitored state. The SMS design must ensure these control rules are followed when weapons are selected for a state change. In the event of weapon system faults or failures, this requirement would not prevent removing all power from the weapon interface (paragraph **2.38.**).

2.40. Multiplexed (MUX) Systems:

2.40.1. Time-Division Multiplexing (TDM). Whenever possible, use TDM for standardization purposes (preferred method according to MIL-STD-1553).

2.40.2. Discrete Signal Isolation. All hardwired discrete signals in the MUX AMAC system must meet the requirements of a totally hardwired AMAC system.

2.40.3. Data Communication and Transfer:

2.40.3.1. Only the correct stations, as determined by the system programming or control source, will transmit or receive data on the SMS MUX bus. Data transfer, change of state, or control signals must not occur until the correct stations are successfully connected.

2.40.3.2. Unauthorized stations transmitting or receiving data must not affect the nuclear weapon interface.

2.40.3.3. The MUX system must inhibit any change of state or output of a remote MUX unit if data communication has been lost.

2.40.4. Powerup and Shutdown. The MUX AMAC and logic power subsystems designs must ensure that, after applying logic power to a MUX terminal unit, a startup routine will verify correct operation before the station is capable of output to the weapon or release system. Each MUX station must operate safely during any change, application, or removal of power from any part of the MUX system.

2.40.5. Abnormal Environment Protection:

2.40.5.1. Internal MUX Unit Isolation. Physically separate opposing critical functions (such as safe and prearm) as far apart as possible within each MUX terminal unit (paragraph 2.17.2.3). Within MUX units, provide break-beforemake action between changes of state of all critical signals applied to the nuclear weapon interface.

2.40.5.2. Logic Power Levels. Voltage and current levels required to operate MUX station logic must be sufficiently below operating levels to minimize the probability of operating critical functions if these voltages and currents are inadvertently applied to the nuclear weapon interface.

2.40.5.3. Nonvolatile Memory. Nonvolatile, nondestructive read-only memory units are required to store MUX AMAC operational programs and algorithms for MUX control and AMAC and release logic processing. Ensure a deliberate, manually controlled action is required to alter the

contents of those memory units. If the MUX AMAC operational programs and logic processing routines are stored in a common memory unit shared with other functions, take special precautions to protect the AMAC and release portion.

2.40.6. Built-in Test. Self-testing must not interfere with normal MUX operation nor cause the generation of any consent signal or critical signal at the nuclear weapon interface. Also, ground testing must not degrade nuclear safety.

2.40.7. Operator MUX Control:

2.40.7.1. Only positive operator control over the MUX bus must generate prearm and separation control signals to the nuclear weapon interface. Critical functions must not occur as a result of either automatic action of one MUX station or the absence of data from the MUX bus.

2.40.7.2. The aircrew must always have control of the MUX AMAC system and be informed of failures or changes in MUX system capabilities.

2.41. Air-Launched Missiles. Until launched or released, an air-launched missile is an extension of the aircraft. Therefore, apply the same criteria applicable to combat delivery aircraft (such as connector design, electromagnetic radiation protection, electrical subsystems, and A&F systems) to the missile. These criteria also apply:

2.41.1. A&F System. The A&F system must contain:

- A unique signal S&A or A/D device for arming and safing the missile part of the A&F system (paragraph **2.8.**). The warhead prearm switch must not serve as the missile system arming and safing device.
- A launch or release sensing device (paragraph **2.23.3.**) to isolate the missile A&F system electrically and mechanically from any arming power source until a mechanical force is applied to the device during launch operation (such as a pull-out switch).

2.41.2. S&A and A/D Devices (Propulsion or A&F Systems). These requirements apply:

- Ensure each S&A or A/D device requires a weapon system operator to apply safing power.
- Incorporate the capability to monitor the missile S&A or A/D devices for the safe condition, either continuously or on demand. Ground personnel must be capable of visually monitoring the state of the devices.
- If used with the propulsion system S&A or A/D devices, locate manual positive locks where they can be removed at the last practical point in the missile loading sequence.

Section 2G—Test Equipment and Training Devices

2.42. Test Equipment. The following criteria apply to test equipment used to verify the proper operation, safe state, and control of critical nuclear functions:

2.42.1. Fail-Safe Requirements. The test equipment design must prevent these conditions:

- Faults in the test equipment or test circuits that could operate critical functions or apply unintended power to the weapon interface.
- Faults within a tester that could degrade the nuclear safety of the equipment to be tested.

- •Introduction of signals, voltages, or currents into the weapon system that could degrade nuclear safety.
- •Operation or firing of an item under test, except when specifically designed for that purpose.

2.42.2. End-of-Test Safe State. Test equipment must ensure a weapon system component, which has been operated during testing, is in the safe or inactivated position when the test ends. A positive indication verifies the safe position of such components. Test equipment failures or shutdowns should leave the components under test in a safe condition.

2.42.3. Built-In Test Equipment (BITE). Subsystems or system features that require frequent periodic testing must have built-in test modes or equipment, where possible. BITE for nuclear weapon systems must comply with all design and safety requirements that apply to nuclear weapon systems. With nuclear weapons attached, BITE must not operate any nuclear critical function nor energize any critical circuits.

2.42.4. Test Procedures. The following criteria apply to equipment used to test the control, launch, or release systems:

- •Use test equipment only where necessary to set up and verify system operation, reliability, and safety. Minimize the amount of testing done after mating the nuclear weapon to the combat delivery vehicle.
- •Keep the interval between required tests on nuclear weapons or weapon systems to the maximum needed to maintain a high confidence level in the system operation and safety.

2.42.5. Periodic Maintenance. The test equipment design agency must provide periodic maintenance, inspection, and test requirements and procedures for the test equipment so the equipment will continue to meet the original specifications.

2.42.6. Functionality and Safety Checks. The test equipment design must include conducting a self-test before use. Based on weapon system requirements, design the test equipment to show system faults (such as improper wiring, line-to-line and line-to-ground shorts, unintended voltage, and improper system operation).

- •Preloading tests must show faults in any of the critical functions.
- •Preflight, postflight, and periodic testing must occur from any connector interfacing with the weapon to the furthest termination in the combat delivery vehicle (end-to-end check).
- •When possible, isolation resistance tests of the combat delivery vehicle must occur during the routine time-phase testing mentioned in paragraph 2.42.4.2.
- •Isolation resistance tests of all critical circuits external to the weapon must occur periodically.
- •Where redundant features are present in the weapon system (such as parallel circuits), test provisions or BITE must indicate the integrity of both the redundancy and the function.

2.42.7. Component Failures. Electrical test equipment (including BITE) used with nuclear weapons must not cause or allow one component failure to result in:

- •Generating of release or launch signals.
- •Initiating of a critical function.
- •Negating of Two-Person Concept control.
- •Unlocking the in-flight reversible lock.

•Operating an S&A or A/D device.

2.42.8. Automated Test Software. Automata and software used for testing or checkout must meet the provisions in **Section 2B** of this chapter.

2.42.9. Electromagnetic Effects. Control of interference and susceptibility within test equipment is needed to prevent undesired responses and emissions. The design of wires, switches, cable connectors, junction points, and other electrical system elements (as appropriate) must prevent undesired radiated and conducted interferences or transients.

2.43. Training Devices. Training weapons or missiles and their components must be explicitly identified as training items. Personnel must not use a war reserve nuclear bomb or warhead as a test or training device for initial qualification or component exchange. Nuclear weapon training devices and equipment require operation of controls and must provide responses so the training does not differ from actual weapon system operations.

Section 2H—Technical Order (TO) Procedures

2.44. General Criteria. The criteria in this section apply to developing or modifying TO procedures that pertain to system and equipment operational certification, training, and cargo aircraft loading.

2.45. Operational Certification Procedures. Before mechanically attaching and electrically connecting a nuclear weapon with an aircraft or a warhead to a missile, operationally certify the weapon system. These procedural requirements apply:

- •Ensure procedures used to test the weapon system critical functions define a sufficient set of tests necessary to verify system operability and safety.
- •Keep test requirements to a minimum after the nuclear weapon is mated to the combat delivery vehicle. The interval between required tests on nuclear weapons or weapon systems must be the maximum needed to maintain a high confidence level in system functionality and safety.
- •Ensure test equipment used to verify system and equipment functionality is within applicable calibration intervals and is in fully serviceable condition before being used with the weapon system. The design agency must provide procedures for periodic maintenance, inspection, and testing to ensure the test equipment will continue to meet the original specifications.

2.46. Training Procedures. Operations involving nuclear weapon training devices and equipment will not differ from the operational procedures, except nuclear weapons must not be involved.

2.47. Cargo Aircraft Loading Procedures. Loading procedures for mixed loads of nuclear and nonnuclear cargo must minimize the movement of the nuclear cargo and must position the nonnuclear cargo where it will not collide with nuclear cargo.

Chapter 3

DESIGN CRITERIA FOR NONCOMBAT DELIVERY VEHICLES AND SUPPORT EQUIPMENT

Section 3A—General Design Criteria

3.1. Design Philosophy. The design of noncombat delivery vehicles and equipment used to transport, store, support, load, and unload nuclear weapons must incorporate positive safety features. The vehicles and equipment must meet appropriate structural, environmental, stability, and mobility requirements. The STS document defines modes of transportation. The safety design factors must allow for uncertainties in predicting operational conditions; uncertainties or variations in material strength and manufacturing techniques; and uncertainties introduced by simplified design and test procedures. The criteria in this section supplement good industrial design practices, standards, and features and are not intended to prohibit the use of any commercial design of nonspecialized equipment (such as trucks, truck tractors, semitrailers, trailers, and cranes) that meet the stated criteria.

3.2. Structural Load Definitions:

3.2.1. Rated Load. Base the rated load on the combination of load forces the basic equipment must support or resist in a static state. This static load consists of one or more weapons and the associated handling and restraint equipment and is the nuclear-certified load.

3.2.2. Dynamic Load. Determine the dynamic load by using the rated load and factor in the loads and accelerations in all directions encountered during ground and air transport and the shock load associated with mate, demate, load, and unload operations.

3.2.3. Design Load. Base the design load on the rated load multiplied by a factor of 3 or the dynamic load multiplied by a factor of 2, whichever is greater. This design load is considered the minimum load for attaining the design stress levels.

3.3. Structural Design Criteria. In addition to meeting the design load requirements of paragraph **3.2.3.**, ensure the design will not be subject to a primary failure mode. A primary failure mode is any material failure that degrades support or control of a nuclear weapon and could result in weapon damage. These are typical failure mode classifications:

3.3.1. Elastic Failure. Exhibited by excessive deflection that could result in weapon damage.

3.3.2. Plastic Failure. Exhibited by material yielding (yield is experienced when stress levels exceed the minimum yield strength of the material, as specified in MIL-HDBK-5 or other applicable standards).

3.3.3. Buckling Failure. Exhibited by excessive and quick deformations (collapse) with a loss of operational capability.

3.3.4. Fatigue Failure. Exhibited by fracture incurred by the cyclic application of loads.

3.3.5. Composite Failure. Exhibited by any composite material failure (such as delamination under compressive load) that could result in weapon damage.

3.3.6. Ultimate Failure. Exhibited by material fracture.

3.4. Data Sources. In determining allowable stresses for equipment, select the material and allowable stress specified in government publications (such as MIL-HDBK-5) and national standards (such as those produced by the Society of Automotive Engineers or the American Society for Testing and Materials). In cases where both an average and a minimum stress are specified, use the minimum stress.

Section 3B—Ground Transportation Equipment

3.5. Criteria Applicability. In addition to the general criteria of this section, apply the following criteria to trailers and semitrailers, self- propelled (nontowed) ground vehicles, forklifts, and weapon loaders used to transport nuclear weapons on their basic structure.

3.6. General Criteria:

3.6.1. Frame Support. Design this equipment to support nuclear loads on the basic frame of the equipment rather than by lift arms, cables, or hydraulic systems. This requirement does not apply to equipment used only to position or transfer nuclear weapons within a designated area (such as a weapons storage area). Hydraulic or pneumatic shock absorber systems between the basic frame and the nuclear weapon are acceptable.

3.6.2. Static Grounding. Provide grounding provisions for equipment designed for specific nuclear weapon systems to prevent static electrical discharge through the weapon.

3.6.3. Fire Propagation Potential. Design the equipment to minimize the potential for fire propagation due to electrical or fuel system failure.

3.6.4. Shock Isolation. Design the equipment to minimize mechanical shock transmission to a nuclear weapon.

3.6.5. Restraints. Ensure restraint provisions for ground transport of all nuclear weapons are capable of restraining the design load, as defined in **Section 3B** of this chapter.

3.6.6. Engine-Transmission Interlock. Ensure the engine start switch will operate only when the clutch is disengaged or the automatic transmission is in the "neutral" or "park" position.

3.6.7. Brakes. All equipment capable of freewheeling, except locomotives and railcars (paragraph **3.10.1.**), must have parking brakes designed to hold the fully loaded equipment on an 11.5-degree incline when headed either up or down.

3.6.8. Stability. Ensure the equipment does not have an unsafe tendency to tip, tilt, yaw, sway, skid, or jackknife while loaded in the most adverse load configuration and while undergoing maximum performance maneuvers (such as emergency braking and obstacle avoidance).

3.6.9. Mobility. Comply with mobility requirements of applicable military standards, and meet the mobility requirements based on operational conditions.

3.6.10. Identification Plates. Identify the rated load and gross vehicle weight on all vehicles.

3.6.11. Roadability. Ensure the equipment meets the minimum roadability requirements in the STS, ORD, MNS, or weapon system specifications.

3.6.12. Adverse Environments. Demonstrate the equipment's ability to operate safely in the most adverse environments (as specified in the STS, ORD, MNS, or weapon system specifications).

3.7. Trailers and Semitrailers. In addition to the general criteria of **Section 3A** and paragraph **3.6.** include these design features in trailers and semitrailers:

3.7.1. Service Brakes. Ensure service brake systems meet the requirements of MIL-STD-1784.

3.7.2. Emergency Brakes. Design trailers using towbars with an emergency brake system that will activate automatically and bring the trailer to a controlled stop in case of inadvertent towbar disconnect.

3.7.3. Mobility. Comply with the mobility requirements of MIL-STD-1784.

3.8. Tow Vehicles. In addition to the general criteria of **Section 3A** and paragraph **3.6.**, tow vehicles (such as trucks, tugs, and tractors) must have these design features:

3.8.1. Brake System. Make the brake system functionally compatible with the towed vehicle brake system. The towing vehicle must not jackknife under maximum performance maneuvers, and brake performance must comply with Federal Motor Vehicle Regulations.

3.8.2. Parking Brakes. Ensure that the parking brakes, together with the towed vehicle parking brakes, can hold a fully loaded towing and towed vehicle combination on an 11.5-degree incline when headed either up or down.

3.8.3. Tug-Trailer Interconnect. Make the vehicle connecting device compatible with the towed vehicle and ensure it meets the structural design criteria of **Section 3A**.

3.8.4. Fifth Wheel. Equip the fifth wheel (if used) with a safety latch designed to allow a visual check of the locked condition.

3.9. Self-Propelled Vehicles. In addition to the general criteria of **Section 3A** and paragraph **3.6.**, ensure nontowed vehicles (such as trucks, vans, and high lift trucks) comply with the service brake performance requirements in Federal Motor Vehicle Regulations.

3.10. Rail-Based Vehicles. In addition to the general criteria of **Section 3A** and paragraph **3.6.**, apply these criteria to railroad locomotives, railcars, and similar equipment:

3.10.1. Parking Brakes. Ensure the locomotive parking brakes, with the railcar parking brakes, can hold a fully loaded railcar and locomotive combination on a 3-degree incline when headed either up or down.

3.10.2. Railroad Standards. Comply with all applicable standards of the American Association of Railroads.

3.10.3. Railbed Requirements. Use only classes 3 through 6 on rail-based vehicles carrying nuclear weapons.

3.11. Forklifts and Weapon Loaders. In addition to the general criteria of **Section 3A** and paragraph **3.6.**, include the following design features in equipment such as conventional forklifts, bomb-lift and high-lift trucks, munitions handling trailers with lifting devices, and 463L loading and unloading trucks:

3.11.1. Lift Systems. Design the lift system so it maintains safe control of the rated load if electrical, hydraulic, or pneumatic system failure occurs. Include pressure relief valves or regulators in hydraulic

and pneumatic systems to prevent overpressure. To prevent weapon damage, limit internal leakage in lift system hydraulic components so the maximum drift rate does not exceed 0.5 inch per hour.

3.11.2. Tines and Adapters. Design tines and adapters for forklifts or bomb- lift trucks to safely meet all nuclear weapon operational requirements for the equipment. Ensure the equipment center of gravity and the rated load center of gravity are compatible.

3.11.3. Movement Controls. Provide for positive control of the nuclear weapon at all times in the lifting and handling modes. Apply these criteria:

- •Make all movement controls self-centering (except for such devices as the parking brake, steering control, transmission selectors, power takeoff, and hydraulic pump).
- •Add mechanical stops or electrical switches to prevent overtravel in all directions of the lift control.
- •Include in the weapon loader a capability for small increments of movement (inching) in both reverse and forward directions.
- •If more than one power-operating component in a mechanically parallel system is used to lift the weapon, the components may be individually controlled to provide weapon attitude adjustments. However, make the components capable of synchronization to provide a uniformly controlled lifting attitude.

3.11.4. Parking Brakes. Ensure forklift parking brakes can hold a forklift with rated load on an 8. 5-degree incline in both forward and reverse directions. Weapon loader service and parking brakes must be able to independently hold a fully loaded weapon loader on an 11.5-degree incline with the loader headed either up or down.

Section 3C—Hoists, Cranes, and Similar Devices

3.12. Criteria Applicability. The criteria in this section apply to hoists, cranes, winches, and similar devices. In addition to the more stringent applicable military specifications or the general criteria of **Section 3A**, design such equipment to have the features and controls in paragraph **3.13.** as a minimum.

3.13. Safety Features and Controls:

3.13.1. Positive Control. System controls must ensure the load is under positive operator control. The design must have automatic stops in the absence of operator control or if the operating mechanism fails; synchronized operations; and mechanical stop or fail-safe limit switches to prevent overtravel of a hoist on rails and stop the chain or wire rope when the hook reaches its upper limit.

3.13.2. Lift Capacity. The lift system must have limits and rates identified for maximum lift capacity and positioning.

3.13.3. Hooks. Hooks used with the lift system must have throat-opening safety devices.

3.14. Structural Design:

3.14.1. Rope. Blocks and rope falls, fiber rope, and webbing require a minimum safety factor of 10 based on ultimate strength.

3.14.2. Chains and Accessories. Load chains and all accessory parts (such as hooks, rings, shackles, slings, and wire rope) require a minimum safety factor of 5 based on the ultimate strength.

Section 3D—Handling and Support Fixtures

3.15. General Criteria. Design items such as load frames, hoist trolleys, test and storage stands, and handling units to meet the structural design criteria in **Section 3A**. Ensure test and storage stands and handling units, if castered, meet the mobility requirements of applicable military standards and operational requirements.

3.16. Weapon Containers. Use the design criteria in MIL-STD-209 and MIL- STD-648 for containers used for storing and transporting weapons.

3.17. Pallet Standards. Pallets used with nuclear weapons must conform to MIL-STD-1366.

Section 3E—Cargo Aircraft Systems

3.18. General Cargo Aircraft Criteria. Design air transportable delivery vehicles and support equipment to meet the general specifications of MIL STD-1791.

3.19. Restraint Configuration Criteria. In addition to the general criteria of paragraph **3.18.**, the nuclear cargo restraint configurations must comply with these criteria:

- •Not impose a reaction load in excess of that calculated using table.
- •Limit one restraint device to one aircraft or pallet tiedown ring, and require each end of each restraint device to end at one attachment point without going through any other attachment point.
- •Consist of symmetrical tiedown patterns parallel to the longitudinal axis of the aircraft. If symmetrical tiedown patterns cannot be used, evaluate the restraint configuration to ensure adequate restraints are provided.
- •Require at least four restraint devices on each item and use only tiedown devices that meet MIL-T-25959 for chains and MIL-T-27260 for straps with nuclear weapons.
- •Not exceed allowable cargo floor or deck roller loads identified in applicable -9 technical orders.
- •Be compatible with weapon design to prevent inadvertent activation of environmental sensing devices.

Table 3.1. Nuclear Weapon Restraint Configuration G-Load for Cargo Aircraft.

RULE	A LOAD DIRECTION	B G-LOAD
1	Forward	3.0
2	Aft	1.5
3	Laterial	1.5
4	Vertical (Down)	4.5
5	Vertical (Up)	3.7

Chapter 4

EVALUATION CRITERIA FOR NUCLEAR WEAPON SYSTEMS

Section 4A—General Criteria

4.1. Criteria Applicability. This chapter outlines the minimum evaluation criteria engineering agencies must apply to combat aircraft, missiles, associated software, technical order procedures, and subsystems before HQ AFSA/SEN will grant nuclear safety design certification according to AFI 91-103.

4.1.1. Organizational Responsibilities. The Air Force organization with engineering responsibility for each specific system or subsystem must develop the evaluation plan and conduct the tests and analyses needed to demonstrate the adequacy of nuclear safety features. In addition to the evaluation criteria in this chapter, the responsible engineering office must define supplemental criteria (based on system and subsystem specifications pertaining to nuclear safety design requirements) applicable to the unique design features of the system being developed or modified. This requirement also applies to Air Force organizations with responsibility for providing engineering and compatibility guidance for a system or subsystem developed by an allied country for use with US nuclear weapons. The organization with engineering responsibility and the appropriate nuclear safety evaluation agency must determine the adequacy of proposed and completed tests and analyses to meet nuclear safety requirements.

4.1.2. Evaluation Source Data:

4.1.2.1. The data from tests and analyses are essential in making nuclear safety evaluations. Both qualitative and quantitative analyses provide a basis for these evaluations. The analyses must consider and be compatible with the concept used to design the system; that is, energy control or information control (or both).

4.1.2.2. When military specifications or standards exist that satisfy nuclear safety requirements, the responsible agency can meet the test and analysis requirements by showing that those specifications or standards have been met.

4.1.3. Numerical Evaluations. This manual includes numerical design criteria given in probabilistic terms for certain undesired events. Tests or analyses (or both) may be used to establish that these numbers are met. However, demonstrating by test or analysis that a numerical criterion is satisfied is not sufficient in itself be to establish the adequacy of the design. An assessment of the safety features of the weapon system, using the applicable qualitative design criteria that implement the positive measures required by the DoD Nuclear Weapon System Safety Standards, will support the evaluation against the numerical criteria.

4.1.4. System-Level Evaluations. The primary concerns of nuclear weapon system safety analyses are unauthorized or accidental nuclear detonation; accidental prearming of a nuclear weapon; accidental launch, release, or jettison of a nuclear weapon; accidental power applied to the nuclear weapon interface; and circumvention of the Two-Person Concept (where applicable) for authorization, launch, prearm, or unlock. For analysis purposes, express accident rates for both the warhead and delivery system in the same units. Use worst-case generic failure rate data for these required analyses:

4.1.4.1. Fault Hazard Analysis. This analysis starts during the demonstration and validation phase. It provides component-level information on failure modes, effects, causes, and com-

mon-cause susceptibilities within a given subsystem. The information is used in fault-tree and common-cause analyses.

4.1.4.2. Operating and Support Hazard Analysis. This analysis starts during the demonstration and validation phase. It evaluates the hazard potential due to procedural flaws or personnel errors during each phase of the STS. Hazards that contribute to the primary concerns listed in paragraph **4.1.4.** are the primary focus of the analysis. The information is used in fault-tree and common-cause analyses.

4.1.4.3. Fault-Tree Analysis. This analysis starts during the full-scale engineering development phase. It provides qualitative and quantitative measures of nuclear safety relative to the primary concerns listed in paragraph **4.1.4.**

4.1.4.4. Common-Cause Analysis. This analysis starts during the full-scale engineering development phase after the fault tree is constructed. It uses the fault-tree minimal cut sets (or prime implicants) to qualitatively assess system susceptibility to potential common-cause failure mechanisms.

4.1.5. Design and Procedural Priorities. Comply with safety requirements in this order:

4.1.5.1. Ensure safety through incorporation of proper design features.

4.1.5.2. Use additional safety devices when safety requirements cannot be met by the basic design.

4.1.6. Explosive Ordnance Disposal. Evaluate aircraft and missile systems to ensure adequate emergency access is permitted to those components and circuits as required to carry out render-safe procedures. Analyze the systems to ensure render-safe procedures meet the requirements of paragraph **2.5.**

4.1.7. Environmental Criteria. Derive the environ-mental requirements for each nuclear weapon system from the predicted normal and credible abnormal operational environments.

4.1.7.1. Nuclear Weapon Systems. Use the STS as the basic document to define operational environments, both normal and credible abnormal, for bombs and warheads. The DoD-DOE Environmental Data Bank is another source of data.

4.1.7.2. Support Equipment. Generally derive the environmental testing requirements for support equipment from the STS and other military equipment standards. Use the more stringent of either the military standard requirements or the predicted environments for the environmental criteria.

4.1.8. S&A and A/D Devices. Test and evaluate these devices according to MIL-STD-1512.

4.1.9. Protection of Friendly Territory. Evaluate and test the weapon system design for its adequacy to prevent accidental or deliberate unauthorized changes in targeting. Also, evaluate the system to ensure adequate safety design features exist to prevent nuclear detonations, except within the boundaries of the designated target area.

4.1.10. Human Engineering. Using accepted human engineering factors and methods, conduct error analyses and error-reduction studies to identify weapon system modes that may cause hazardous conditions. Use these studies to add features that minimize the potential for human errors or deliberate unauthorized acts and limit their consequences when they occur.

Section 4B—Specific Criteria

4.2. Automata and Software:

4.2.1. Automated Test Equipment (ATE). The follow-ing evaluation criteria apply to ATE and the associated software and firmware that perform those functions identified in **Section 2G** of **Chapter 2** and require nuclear safety design certification according to AFI 91-103. The nuclear certification plan for ATE must specify analyses and tests sufficient to verify ATE capability, as specified in paragraph **4.2.1.1.** and paragraph **4.2.1.2.**, of the unit under test and to verify the safe state of the unit upon test completion. The evaluation program must fulfill these objectives for all environmental conditions within which the ATE is designed to operate and must include at least one test of a production or production-like ATE.

4.2.1.1. For aircraft weapon system components, the ATE-required capability is used to determine proper functioning of system components.

4.2.1.2. For ground-launched missile systems, ATE is used to accomplish functional testing for operational certification. Functional tests verify the unit under test operates in the intended manner.

4.2.2. Critical Function Automata. Base the evaluation program for critical function automata and software on the design certification requirements of AFI 91-103. The nuclear surety impact statement or nuclear software certification plan required by AFI 91-103 must define a sufficient set of tests and analyses to verify design compliance with the criteria of **Section 4B** of this chapter. In addition to the system-unique design features, the evaluation program must ensure compliance with these criteria:

4.2.2.1. Software Function Analysis. Accomplish a description and analysis of the software logic path to demonstrate compliance with the structural and single-purpose criteria; initialization, fault and error handling, and critical function processing and transmission requirements; and the single-point entry and exit requirements for critical function routines. Show the validity checks that must be satisfied before calling a critical function routine and those checks within a critical function routine that must be satisfied before executing a critical function.

4.2.2.2. Critical Data Element Analysis. The software analysis must define the modules and routines that change or evaluate the data elements (such as constants, variables, and flags) that contribute to critical function execution and must also define the chronological sequence of data element changes and evaluations. The data element analysis must define the minimum conditions required for critical function execution. This data set defines the susceptibility of critical function routines to data element alteration.

4.2.2.3. Memory Characteristics:

4.2.2.3.1. Verification. Conduct a demonstration or analysis of the memory to show that any single change in a volatile memory could not cause a critical function to occur and a single hardware fault will not result in a memory change that could initiate a critical function.

4.2.2.3.2. Memory Loading and Change. Demonstrate that errors will be detected and operators notified; reset or synchronization functions are operable; automatic operation will not start until all valid and correct data are loaded and verified; reloading or changing that part of memory involving critical functions will stop unless the proper means for entry is used; improper

reload or change will be rejected and indicated to the operator; and the block of proper program data or instructions to be transferred fills each section of memory.

4.2.2.3.3. Memory Declassification. Demonstrate the method used to erase or obliterate clear-text secure codes from memory. The National Security Agency must approve all declassification procedures.

4.2.2.4. Processor Deviations. Demonstrate the capability to detect manually started commands, message errors, and deviations causing an erroneous entry to a critical routine. The demonstration must show the automata will stop transmitting critical commands upon detecting errors and deviations and will recycle, self-test, or perform automatic shutdown while displaying associated crew indications.

4.2.2.5. Fault Detection. Demonstrate the fault detection capability of the system. For ground-launched missiles, this may be accomplished with an analysis.

4.2.2.6. Hardware Checks:

- Conduct a demonstration of the self-check, confidence, or test routines.
- Evaluate the hardware to ensure it meets current National Security Agency TEMPEST (Radiation of Unintentional Intelligence-Bearing Electronic Signals) requirements according to MIL-STD-461. This requirement does not apply to functional areas that do not process secure codes.

4.2.2.7. Ancillary Equipment. Ancillary equipment provides the interface between the operator and the automata. Check this equipment for the extent of control it exerts on the weapon system and its susceptibility to unauthorized control.

4.2.2.8. Software Certification:

4.2.2.8.1. Critical Software. To ensure system nuclear safety integrity, the software used to process the data for, provide the status of, or which can exercise automated or automatic control over any critical nuclear weapon system function may undergo a Nuclear Safety Cross-Check Analysis, be designated a critical component, and be certified according to AFI 91-103.

4.2.2.8.2. Noncritical Software. Software not designated as a critical component is certified according to AFI 91-103.

4.3. Electrical Subsystems. In addition to the weapon system evaluation requirements of paragraph **4.4.** and paragraph **4.5.**, accomplish these additional electrical subsystem analyses:

4.3.1. Electromagnetic Radiation (EMR) Evaluation Requirements. DoD Directive 3222.3/Air Force Supplement 1 (formerly AFR 80-23) outlines responsibilities to ensure electromagnetic compatibility (EMC) of all military communications-electronics equipment, subsystems, and systems during conceptual, design, acquisition, and operational phases. Before the system is certified, the evaluation agency must produce data that cover EMR hazards to electro-explosive, semiconductor, and other devices. The evaluation must include these data as a minimum:

4.3.1.1. Data attesting to system design adequacy to the effects of static electricity, EMC, external EMR, EMI, and lightning. Demonstrate system tolerance to these potential hazards by full-scale or scale-model tests or through analyses.

4.3.1.2. EMR susceptibility data and results that verify the shielding effectiveness of the total system. Demonstrate the tolerance of the total (includes combat delivery vehicle and nuclear weapon) nuclear weapon system to continuous wave and pulse fields throughout the entire STS, over the frequency range of 100 KHz to 40 GHz.

4.3.2. Isolation Requirements. Conduct the tests and analyses needed to ensure compliance with the electrical isolation requirements.

4.4. Arming and Fuzing (A&F) Systems. These criteria supplement the aircraft or missile system evaluation criteria. The evaluation of the A&F subsystem design must include:

4.4.1. A&F System Devices and Safety Features. The A&F subsystem evaluation must include a summary description of the A&F design and a qualitative assessment of the primary design safety features in the prearming, arming, and fuzing functions.

4.4.2. Component Failure Analysis:

4.4.2.1. The A&F evaluation must identify any critical component failure modes that could contribute to premature prearming or arming. For each critical component failure mode, determine a nominal probability of occurrence (along with the associated tolerance or confidence level) and give the basis for the probability estimates in each case.

4.4.2.2. Accomplish a thermal analysis on each component that can be thermally operated, all thermal-protective components and design features, and all explosive components. Document each analysis in a graphic "temperature- time" presentation, showing relative component temperature as a function of exposure time.

4.4.2.3. For each critical component, define both normal and credible abnormal environmental levels for all operate and no-operate response characteristics.

4.4.2.4. Accomplish bent pin and connector mismating and misalignment analyses for each connector containing energy-control prearm and arming circuits.

4.4.3. Nuclear Safety Analysis. As a minimum, a nuclear safety analysis of the system must determine the probability of the following events in normal and credible abnormal environments:

•Premature nuclear detonation during storage and logistics operations (system not prearmed).

•Premature nuclear detonation for each stage of prearming and arming.

•Premature nuclear detonation after the system is armed.

4.5. Ground-Launched Missile Systems. The design evaluation of ground- launched missile systems must ensure nuclear safety and security requirements are met. When the implementation of system or equipment specifications will result in hazards, the system manager must conduct a trade-off study to achieve maximum nuclear safety consistent with operational requirements. In addition to the general requirements of paragraph **4.1.**, conduct these tests and analyses:

4.5.1. Preliminary Hazard Analysis. Early in the design phase, conduct a complete, qualitative, and nonmathematical assessment of the software and hardware safety features. This analysis can provide the basis for determining other required analyses.

4.5.2. System and Subsystem Hazards Analysis. From the conceptual through postdesign phases, perform general analyses of each subsystem and major component; their relationship to each other and their interfaces; environments that could affect them; and hazards they could cause.

4.5.3. Circuit Logic Analysis. Conduct a circuit logic analysis during developmental and postdesign phases to determine the possibilities of accidental operation of critical circuits. Include studies of electrical and electronic systems to determine the effects of component failures on the circuit operation.

4.5.4. Bent Pin Analysis. If not covered by any other analysis, perform a bent pin analysis to study pin assignments and power sources before final approval of pin assignments to minimize the probability of critical functions occurring due to bent connector pins.

4.5.5. Analysis of Susceptibility to Unauthorized Launch (UL). Perform an analysis of the nuclear weapon system's UL susceptibility according to AFI 91-106 (formerly AFR 122-6). The objectives are to identify possible ways to accomplish a UL by negating the nuclear safety design safeguards of a nuclear weapon system and to assess the means of detecting a UL attempt and what countermeasures to apply. The analysis may reveal design deficiencies in the system involving human actions or component failures.

4.5.6. Safety Testing. Where required by the system, subsystem, and equipment specifications, perform the following safety validation tests and consider them an integral part of the development and acceptance tests or the demonstration tests:

- •Laboratory tests, functional mockups, models, or simulations to demonstrate partial verification of safety characteristics or procedures.
- •Safety tests on critical devices and components to determine the degree of hazard or margin of safety.
- •Induced failure tests to demonstrate the failure mode of critical components.
- •Evaluations of support equipment for nuclear logistics movement and ground mobile combat delivery vehicles according to **Chapter 5**.

4.6. Aircraft and Air-Launched Missiles:

4.6.1. Nuclear Safety Design Certification. Design certification of an aircraft nuclear weapon system is based on satisfying the requirements in AFI 91-103. Procedures for obtaining nuclear safety design certification will consist of a design evaluation by test and analysis (where applicable) of the weapon system to assure the system complies with the nuclear safety design criteria in this manual.

4.6.2. Design Certification Analysis. The system evaluation must integrate the general analyses (paragraph **4.1.**); automata and software analyses (paragraph **4.2.**); electrical subsystem assessment (paragraph **4.3.**); A&F subsystem requirements (paragraph **4.4.**); and test and training analysis requirements (paragraph **4.7.**). The integrated system evaluation must also include these analyses and documentation:

4.6.2.1. Nuclear System Definition. The evaluation must document a listing of all critical function software and assemblies, wires, connectors, and other hardware that, when considered totally, define the aircraft monitoring and control (AMAC) and nuclear suspension and release systems. This evaluation defines the nuclear system configuration and the interfaces and functional interaction between the nuclear weapon system and other aircraft systems.

4.6.2.2. Hazard Analyses. The integrated assessment must also identify nonnuclear system operational or failure hazards that could degrade the safety and functionality of the nuclear system or a loaded nuclear store.

4.6.2.3. Requirements Compliance Summary. The evaluation analysis must summarize the applicable design requirements of **Chapter 2** and show how these requirements were developed into lower-tier specifications and allocated to hardware and software components of the nuclear system. For **Chapter 2** and lower-tier requirements, the evaluation must contain a compliance matrix that correlates the design requirements with the system design safety features (hardware or software) that satisfy the requirement.

4.6.3. Design Certification Tests. Conduct these tests and demonstrations:

4.6.3.1. A functional test of the nuclear system on a production aircraft. The demonstration (using production aircraft and test load devices) must verify the capability of the AMAC and release systems to meet these design requirements: voltage, current, switching characteristics, signal timing and sequencing, and worst load conditions as defined in the AMAC specifications.

4.6.3.2. Circuit isolation tests to ensure the nuclear configuration meets design criteria for electrical isolation of the unlock, release, launch, and AMAC circuits.

4.6.3.3. EMR and EMI tests to ensure on-board emitters and switching functions cannot initiate critical functions.

4.6.3.4. Testing of suspension and release equipment, as prescribed by MIL- T-7743 or determined by flight conditions, whichever is more stringent.

4.7. Test Equipment:

4.7.1. Criteria Applicability. These criteria apply to nuclear weapon system BITE, AMAC test equipment, release or launch test equipment, nuclear bomb or warhead testers, component testers (for racks, line replaceable units, and similar items), and general test equipment when used to test nuclear critical circuits.

4.7.2. Evaluation Objective. The primary purpose of the evaluation is to confirm the test equipment accurately verifies the functionality of the nuclear weapon system or a system component and the system or system component is left in a safe state upon completion of the test.

4.7.3. Evaluation Criteria. In addition to the customary industrial standards, the Air Force evaluation agency must require the following tests, analyses, demonstrations, and data to assure the test equipment meets the objectives of paragraph **4.7.2.** in all normal operating environments:

4.7.3.1. Environmental Tests. Verify the ability of the test equipment to perform its intended function in all environmental conditions identified in paragraph **4.1.8.**

4.7.3.2. Required Analyses:

- Circuit analyses of the tester operating with the circuits of the equipment to be tested.
- Failure modes, effects, and criticality analysis of the test device to ensure faults within the device will not degrade the nuclear safety of the equipment to be tested.
- Analysis of the tester interface with the weapon system to verify the test concept.

- •Compatibility. Perform a fit-and-function demonstration to ensure the mechanical and electrical designs are both compatible with the weapon system to be tested.
- •Demonstration. Demonstrate operations and procedures at the field level and take appropriate corrective action in problem areas. Verify each applicable section of each procedural document.
- •Technical Data. Use the evaluation to verify the adequacy of maintenance and inspection procedures on the test equipment and to ensure the tester's integrity can be verified before use.

Chapter 5

EVALUATION CRITERIA FOR NONCOMBAT DELIVERY VEHICLES AND HANDLING EQUIPMENT

Section 5A—Criteria and First Article Verification

5.1. Evaluation Criteria. This chapter defines the minimum evaluation criteria applicable to noncombat delivery vehicles and handling equipment that support, lift, or transport nuclear weapons. Evaluation requirements for certification according to AFI 91-103 must consist of analysis, examination, and testing (as appropriate) by the responsible Air Force agency. Agencies may evaluate nonspecialized equipment for nuclear safety adequacy according to appropriate standards, specifications, and designated tests defined in this chapter.

5.2. First Article Verification. Use one or more of the following methods to prove the adequacy of the prototype structural design (paragraph **3.2.**):

5.2.1. Analysis. Perform a detailed stress analysis and supplement it with selective structural tests. Correlate the test results to the stress analysis results.

5.2.2. Nondestructive Tests. Perform an abbreviated stress analysis to determine all critical stress points, and apply the test design load to the structure with suitable instrumentation at all critical stress points. This test should not result in a primary failure mode (paragraph **3.3.**).

- Use mobility or functional test results (or both) to verify the dynamic load.
- Use the verified dynamic load multiplied by a factor of 2 or the rated load multiplied by a factor of 3 (whichever is greater) for the test design load.
- Apply the lateral and longitudinal test loads statically (with the equipment simultaneously loaded to its rated capacity) and apply the vertical test load statically and independently.
- Correlate the test results to the abbreviated stress analysis results to determine if the structure meets design requirements.

5.2.3. Destructive Tests. Apply test loads simultaneously to the test article along the appropriate axes until the item exhibits a critical failure mode (paragraph **3.3.**). The test loads at this point must exceed the design load in each appropriate axis.

Section 5B—Ground Transportation Equipment

5.3. General Criteria. In addition to the criteria in paragraph **5.1.** and paragraph **5.2.**, include the following tests and analyses in the design verification:

5.3.1. Frame Load Support. Analyze the equipment to ensure the weapon is supported by the basic frame of the equipment during both air and ground transport, rather than by lift arms, cables, or hydraulic systems. This requirement does not apply to equipment used solely to position or transfer weapons nor to hydraulic or pneumatic shock absorber systems.

5.3.2. Performance Evaluations:

- Subject the equipment to maximum performance maneuvers to evaluate stability.

- •Perform an analysis to ensure the equipment meets the minimum roadability requirements specified in the STS, ORD, MNS, or weapon system specifications.
- •Ensure mobility requirements of applicable military standards or requirements based on operational conditions are met. Accomplish mobility testing to verify structural integrity, stability, and safety.
- •Test brake systems while transporting or towing simulated loads that represent the worst load conditions expected in service (such as maximum weight and extreme center of gravity).

5.3.3. Environmental and General Hazard Evaluations:

- •Analyze the equipment to minimize the potential for fire propagation due to electrical or fuel system failure.
- •Test or analyze the equipment to ensure mechanical shock transmission to the nuclear weapon is within weapon design tolerances.
- •Test tiedown provisions for ground movement of nuclear weapons to verify the equipment's capability to restrain the design load.
- •Conduct environmental tests, as required by the Air Force organization with engineering evaluation responsibility, to verify safe operation at extreme operating environments (such as temperature and EMI extremes) with the equipment loaded to its rated capacity.
- •Perform tests or analyses to determine if the equipment has adequate provisions for static grounding.
- •Inspect the equipment to ensure rated load and gross weight are clearly identified.

5.4. Trailers and Semitrailers. In addition to the general test and analysis requirements, subject trailers and semitrailers to these tests:

5.4.1. Service Brakes. Test the service brake system according to MIL-STD-1784.

5.4.2. Parking Brakes. Test parking brakes to verify the parking brake system's capability to hold the vehicle on an 11.5-degree incline when headed either up or down.

5.4.3. Emergency Brakes. Test the emergency braking system of trailers using towbars to verify trailer performance during accidental towbar disengagement by full-scale testing or by limited testing and analysis. Conduct the full-scale testing while towing the fully loaded trailer over a straight, smoothly paved road at the maximum operating speed expected. Testing will consist of disengaging the towbar from the tow vehicle and observing the emergency braking action of the trailer. When testing the emergency brake system, consider these conditions:

- •Distance from the point of towbar disengagement to final stop.
- •Lateral distance of travel from the point of towbar disengagement to final stop.
- •Attitude of the trailer at the time of stop.
- •Damage incurred by the trailer or load as a result of disengagement.

5.4.4. Mobility Requirements. Comply with the mobility requirements of MIL-STD-1784.

5.5. Tow Vehicles. In addition to the general test and analysis requirements, tow vehicles must be subjected to specific tests.

5.5.1. Vehicle and Brake Performance. Accomplish the following tests with the most adverse configuration of tow and towed vehicles to verify functional compatibility:

- Evaluate the towing vehicle performance to ensure it does not have tendencies to tip, tilt, yaw, sway, skid, or jackknife under maximum performance maneuvers.
- Ensure brake performance meets the requirements of the Federal Motor Vehicle Regulations. Also, test the tow vehicle by progressively increasing the speed from which stops are made, in increments of 5 miles per hour, up to the maximum rated speed of the vehicle. Continue this procedure until failure occurs or the maximum safe speed is attained, whichever occurs first. Conduct the initial tests on a dry, brushed, level concrete surface. Stop the vehicle by operating the brake system to produce maximum braking force (panic stops) and repeat the procedure on surfaces similar to the worst condition expected during the operational life of the vehicle. In each test, determine the maximum safe speed and record (as a minimum) these brake performance data: damage or excessive wear, stopping distances, speed range, and contact of wheels with the ground.

5.5.2. Parking Brakes. Conduct tests to verify the capability of the towing and towed vehicle combination parking brakes to hold on an 11.5-degree incline when headed either up or down.

5.5.3. Connecting Device. Test the vehicle connecting device to ensure compliance with the structural design criteria (paragraph **3.3.**).

5.5.4. Fifth-Wheel Safety Latch. Ensure visual check capability for the fifth-wheel safety latch.

5.5.5. Engine Start Switch. Verify by test that the engine start switch will only operate in neutral, park, or with the clutch disengaged (as applicable).

5.6. Self-Propelled Vehicles. In addition to the general test and analysis requirements, subject nontow vehicles to brake system tests to ensure compliance with the Federal Motor Vehicle Regulations.

5.7. Rail-Based Vehicles. In addition to the general test and analysis requirements (paragraph **5.2.**), subject rail-based vehicles to these tests and analyses:

5.7.1. Brake System Verification. Test the brake system's capability to hold the locomotive and railcar combination on a 3-degree slope when headed either up or down. Demonstrate by analysis that the locomotive and railcar combination will not jackknife under maximum braking.

5.7.2. Standards Compliance. Demonstrate that the locomotive and railcar combination complies with all applicable standards of the American Association of Railroads.

5.8. Forklifts and Weapon Loaders. In addition to the general test and analysis requirements, subject forklifts and weapon loaders to these tests:

5.8.1. Brake System Tests. Test the forklift's parking brakes on an 8.5-degree incline while loaded to its rated capacity. Test the weapon loader's service brakes and parking brakes to verify the capability to hold the vehicle on an 11.5-degree incline when headed either up or down while loaded to its rated capacity.

5.8.2. Movement and Positioning Controls. Conduct these demonstrations:

- Safe control of the rated load must be maintained if electrical, hydraulic, or pneumatic system failure occurs.

- •Appropriate movement controls are self-centering.
- •Positive control of nuclear weapons is maintained in all operations. If used, test the attachment points and straps.
- •Capability for small increments of movement compatible with required usage.
- •Overtravel prevention capability.
- •Capability to uniformly control lifting attitude.

5.8.3. Lift System. Conduct these demonstrations:

- •Prevention of overpressure in hydraulic and pneumatic systems. Test the drift rate at ambient and extreme temperature conditions to verify safe operation based on the requirements of the loader.
- •Tine and adapter compatibility with the rated load center of gravity in the worst-case environment to which the vehicle will be subjected.

Section 5C—Hoists, Cranes, and Similar Devices

5.9. Safety Features and Controls. In addition to the general criteria (paragraph **5.2.**), evaluate these areas:

5.9.1. Automatic Stop Features. Test the device at 125 percent of the rated load to verify automatic stop in the absence of operator control and if the operating mechanism fails or power is lost. Also, verify synchronized operations and proper functioning of stop or limit switches that prevent overtravel of a hoist on rails and stop the chain or rope when the hook reaches its travel limit.

5.9.2. Capacity Identification Plates. Ensure limits and rates for maximum lift capacity and positioning are clearly identified.

5.9.3. Hooks. Ensure hooks are fitted with throat-opening safety devices.

5.10. Safety Factor Verification. Test blocks, rope falls, fiber rope, and webbing to verify a minimum safety factor of 10 based on ultimate strength. Test load chains and all accessory parts (such as hooks, rings, shackles, slings, and wire rope) to verify a minimum safety factor of 5 based on the ultimate strength.

Section 5D—Handling and Support Fixtures

5.11. Handling Equipment, Suspended Load Frames, and Support Fixtures. Evaluate handling and support fixtures (such as load frames, hoist trolleys, test and storage stands, and handling units) according to paragraph **5.2.** to ensure compliance with the structural design requirements of paragraph **3.3.**

5.12. Weapon Containers. Test or analyze (or both) containers as necessary to verify compliance with MIL-STD-209 and MIL-STD-648.

5.13. Pallet Standards. Test or analyze (or both) pallets as necessary to verify compliance with MIL-STD-1366.

Section 5E—Cargo Aircraft Systems

5.14. Tiedown Patterns. Structurally test or verify the tiedown patterns (by analysis) according to the g-load factors in **Table 3.1.** When tested, secure pallet loads to a simulated aircraft system and apply simulated loads according to paragraph **3.19.**

5.15. Load Configurations. Evaluate load positioning configurations of nuclear weapons to ensure appropriate orientation and to prevent inadvertent activation of environmental sensing devices.

Section 5F—Production Article Verification

5.16. Fail-Safe Features. If used, evaluate or test (or both) fail-safe features to determine if the procedures provide safe control of the weapon in the event of system failure.

5.17. Proof Tests. Perform operational equipment proof tests on at least one fully configured production article (and other designated samples as necessary) to determine if the item will function properly with specified limit loads.

5.18. Environmental Tests. Perform selected environmental tests on production articles, as required, after considering the intended use of the vehicle or support equipment.

5.19. Hoist Tests. Test all hoists in their final installed configuration to 125 percent of the rated capacity.

JAMES L. COLE, JR., Brig Gen, USAF
Chief of Safety

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

DoD Directive 3150.2, *Safety Studies and Reviews of Nuclear Weapon Systems*

DoD Directive 4540.5, *Movement of Nuclear Weapons by Noncombat Delivery Vehicles*

DoD Directive S-5200.16 (S), *Objectives and Minimum Standards for Communications Security Measures Used in Nuclear Command and Control Communications*

DoD Directive 5210.41, *Security Criteria and Standards for Protecting Nuclear Weapons*

DoD 5210.41-M (C), *Nuclear Weapon Security Manual*

DoD-STD-2167A, *Defense System Software Development*

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*

JP 1-04 (S-FRD), *Policy and Procedures Governing JCS Positive Control Material and Devices*

KAG-30A/TSEC (S-NOFORN), *Compromising Emanation Standard for Cryptographic Equipment* (National Security Agency Publication)

AFR 80-18, *Department of Defense Engineering for Transportability* (Joint Service)

DOD Directive 3222.3/AF Sup 1 (formerly AFR 80-23), *The US Air Force Electromagnetic Compatibility Program*

AFI 91-101, *Air Force Nuclear Weapons Surety Program*

AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*

AFI 91-103, *Air Force Nuclear Safety Certification Program*

AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*

AFI 91-105, *Critical Components*

AFI 91-106, *Unauthorized Launch and Launch Action Studies*

AFI 91-107 (formerly AFR 122-10), *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*

AFI 91-201 (formerly AFR 127-100), *Explosives Safety Standards*

AFI 21-205 (formerly AFR 136-2), *Logistic Movement and Handling of Nuclear Cargo*

AFI 31-101 (formerly AFR 207-1) (C), *The Air Force Physical Security Program*

AFI 91-202 (formerly AFR 127-2), *The US Air Force Mishap Prevention Program*

NOTE: The following Military Handbooks, Specifications, Standards, and Technical Orders publications do not include applicable suffixes; use the current issue of the document.

MIL-HNDBK-5, *Metallic Materials and Elements for Aerospace Vehicle Structures*

MIL-STD-209, *Slinging and Tiedown Provisions for Lifting and Tying Down Military Equipment*

MIL-STD-461, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*

MIL-STD-462, *Electromagnetic Interference Characteristics, Measurement of*

MIL-STD-463, *Definition and System of Units, Electromagnetic Interference Technology*

MIL-STD-648, *Design Criteria for Specialized Shipping Containers*

MIL-STD-882, *System Safety Program Requirements*

MIL-H-904, *Hoists, Chains, Hand Operated, Hook and Trolley Suspension*

MIL-STD-1365, *General Design Criteria for Handling Equipment Associated With Weapons and Weapon Systems*

MIL-STD-1366, *Packaging, Handling, Storage, and Transportation System Dimensional Constraints, Definition of*

MIL-STD-1472, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities*

MIL-STD-1512, *Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods*

MIL-STD-1522, *Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems*

MIL-STD-1553, *Aircraft Internal Time-Division Command/Response Multiplex Data Bus*

MIL-STD-1760, *Aircraft/Store Electrical Interconnection System*

MIL-STD-1784, *Mobility, Towed and Manually Propelled Support Equipment*

MIL-STD-1791, *Designing for Internal Aerial Delivery in Fixed Wing Aircraft*

MIL-STD-2088, *Bomb Rack Unit (BRU), Aircraft, General Design Criteria for*

MIL-B-5087, *Bonding, Electrical, and Lightning Protection for Aerospace Systems*

MIL-E-6051, *Electromagnetic Compatibility Requirements, Systems*

MIL-A-8421, *Air Transportability Requirements, General Specification for*

MIL-A-8591, *Airborne Stores, Suspension Equipment and Aircraft-Store Interface (Carriage Phase), General Design Criteria for*

MIL-A-8860, *Airplane Strength and Rigidity, General Specification for*

MIL-S-8512, *Support Equipment, Aeronautical, Special, General Specifications for the Design of*

MIL-S-45152, *Semitrailer, Lowbed, Commercial*

MIL-H-19925, *Hoist, Wire Rope, Electric Powered*

MIL-T-7743, *Testing, Stores Suspension and Release Equipment, General Specification for*

MIL-T-21868, *Truck, Lift, Fork, Diesel, Shipboard and General Purpose, General Specification for*

MIL-T-21870, *Truck, Lift, Fork, Gasoline, General Specification for*

MIL-T-25959, Tie Down, Cargo, Aircraft

MIL-T-27260, *Tie Down, Cargo, Aircraft, CGU-1/B*

MIL-T-45333, *Trailer, Flat Bed, 10-Ton 4-Wheel, M345*

MIL-T-45382, *Trailer, Lowbed, 4-Wheel 2- to 7-Ton*

MIL-C-22137, *Cranes, Overhead Traveling, Overrunning Bridge and Trolley, Electrical Powered*

MIL-C-25200, *Cable Assembly, Special Weapon, Electrical, General Requirements for*

MIL-C-28546, *Crane, Overhead Traveling, Underhung, Electric Powered*

MIL-C-38999, *Connector, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded, and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for*

MIL-W-5088, *Wiring, Aerospace Vehicle*

TO 11A-1-33, *Handling and Maintenance of Explosives Loaded Aircraft*

TO 11A-1-46, *Firefighting Guidance, Transportation and Storage Management Data and Ammunition Complete Round Chart*

TO 11N-20-11 (C-RD), *General Firefighting Guidance*

TO 11N-45-51, *Transportation of Nuclear Weapons Material*

TO 31Z-10-4, *Electromagnetic Radiation Hazards*

Sandia National Laboratories, Drawings and Technical Reports, and AMAC Specifications:

Drawing No. 173837, *Basic Design Specification, Bomber System A*

Drawing No. 173838, *Basic Design Specification, Fighter System A*

Drawing No. 185435, *Permissive Action Link (PAL) Fighter A*

Drawing No. 185475, *Basic Interface Requirement, System I*

Drawing No. 186990, *Basic Design Specification, PAL Fighter System B*

Drawing No. 306562, *Category D PAL AMAC Requirements*

Technical Report SAND 77-0777, *Barrier Technology Handbook*

Nuclear Regulatory Commission Publication NUREG 0492, *Fault Tree Handbook*

Abbreviations and Acronyms

A/D—Arm/Disarm

A&F—Arming and Fuzing

AFI—Air Force Instruction

AFM—Air Force Manual

AFSA—Air Force Safety Agency

AMAC—Aircraft Monitoring and Control

ATE—Automated Test Equipment

BIT—Built-in Test

BITE—Built-in Test Equipment

CPU—Central Processing Unit

DoD—Department of Defense

DOE—Department of Energy

EED—Electroexplosive Devices

EMC—Electromagnetic Compatibility

EMI—Electromagnetic Interference

EMR—Electromagnetic Radiation

E/TSD—Environmental or Trajectory Sensing Device

HOL—Higher-Order Language

JCS—Joint Chiefs of Staff

JP—Joint Publication

LCP—Launch Control Point

LP—Launch Point

MAJCOM—Major Command

MC—Military Characteristics

MNS—Mission Need Statement

MUX—Multiplexed Systems

OPDD—Operational Plan Data Document

ORD—Operational Requirements Document

OS—Operating System

PAL—Permissive Action Link

RTE—Run-Time-Executive

S&A—Safe and Arm

SA-ALC—San Antonio Air Logistics Center

SMS—Stores Management System

STS—Stockpile-to-Target Sequence

TDM—Time-Division Multiplexing

TNT—Trinitrotoluene

TO—Technical Order

TPD—Terminal Protective Devices

UL—Unauthorized Launch

USG—Unique Signal Generator