BY ORDER OF THE
SECRETARY OF THEAIR FORCE

AIR FORCE MANUAL 91-118

4 AUGUST 2010

Incorporating Change 1, 21 JUNE 2011

Safety

SAFETY DESIGN AND EVALUATION CRITERIA FOR NUCLEAR WEAPON SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available digitally on the AFDPO WWW site at: **www.e-publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFSC/SEWN

Certified by: AF/SE (Maj Gen Frederick Roggero)

Supersedes: AFMAN91-118, 18 January 1994

Pages: 60

This Manual implements AFPD 91-1, *Nuclear Weapons and Systems Surety*. This Manual contains the minimum criteria for designing, developing or modifying a nuclear weapon system to include nuclear weapon maintenance, handling and storage facilities. This Manual outlines criteria to evaluate these systems for nuclear safety design certification. It applies to all organizations that design, develop, modify, evaluate or operate a nuclear weapon system. This Manual is applicable to Air National Guard and Air Force Reserve units performing nuclear missions. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate (MAJCOM) publications/forms manager. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Send recommendations for improvements to Headquarters Air Force Safety Center (AFSC/SEWN), 9700 G Avenue SE, Kirtland AFB, NM 87117-5670.

SUMMARY OF CHANGES

This interim change (IC) provides policy guidance for the design and nuclear safety design certification of aircraft delivery systems that may deliver guided bombs. A margin bar indicates newly revised material.

Chapter 1

GENERAL STANDARDS AND CONTROL

Section 1A—Responsibility and Scope

1.1. 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:

1.1.1. There shall be positive measures to prevent nuclear weapons involved in accidents or incidents or jettisoned weapons, from producing a nuclear yield.

1.1.2. There shall be positive measures to prevent DELIBERATE prearming, arming, launching or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority.

1.1.3. There shall be positive measures to prevent INADVERTENT prearming, arming, launching or releasing of nuclear weapons in all normal and credible abnormal environments.

1.1.4. There shall be positive measures to ensure adequate security of nuclear weapons, pursuant to DoDD O-5210.41, *Security Policy for Protecting Nuclear Weapons*.

1.2. 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. Refer to AFI 63-125 for nuclear certification procedures.

Section 1B—Deviations to Criteria

1.3. Request for Deviation. If the design of an Air Force nuclear weapon system does not meet the requirements contained in this manual, a deviation request shall be obtained according to the requirements of AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*. Exceptions to this manual, as evidenced by some current and older designs, do not constitute a precedent to deviate from the criteria.

1.4. Currency of Standards and Guidance. Standards and guidance referenced in this document are current as of the date of publication. In the event of cancellation or modification of the referenced standards or guidance, contact AFSC/SEWN for requirements.

1.5. Existing Systems. Existing systems are not required to be modified solely to meet new or changed requirements in this manual. If an existing system is modified, the modified system shall meet new requirements established through guidance or standards as referenced in **attachment 1**. Deviations if the design of a modified system is not expected to meet the requirements contained in this manual, shall be obtained according to the requirements of AFI

91-107, Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems.

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 shall consider these DOE nuclear weapon safety 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 functional 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 permit the transmission of functional energy to the firing set for the arming and firing signals (following the receipt of the appropriate unique signal information sequence at the appropriate time) and provide threat energy isolation in an abnormal environment. *Functional energy* includes the proper energy type(s) and level(s), which are required to achieve the intended functional operation of the weapon (i.e., significant nuclear yield). *Threat energy* encompasses unintended temporal patterns of energy type(s) and level(s) that can lead to an unintended state of the weapon up to and including unintentional significant nuclear yield.

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 inoperable and thus rendering the system inoperable at levels less than those at which the strong links fail to keep energy 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 or the information control concept. Many currently deployed systems use the information control concept or a combination of both concepts.

2.2.1.1. Energy Control Concept. The energy control concept involves limiting the entry of threat energy into the weapon system devices that control the operation of the critical functions. Critical functions are designed to require functional energy signal(s) for operation. Reliability requires that the weapon system respond as intended when the functional energy signal(s) are present at the weapon interface. Therefore, safety levels

(IAW AFI 91-107) of weapon systems using this design concept depend on the safety controls that block application of those functional energy signal(s) to the weapon interface until the controls are properly removed.

2.2.1.2. Information Control Concept. Critical prearm functions are commanded by a unique signal that provides indication of an unambiguous human intent to detonate the weapon. Safety levels depend upon the uniqueness of a carefully designed sequence of bi-valued events and are evaluated based on the assumptions of worst-case power levels. *Worst-case power levels* involve temporal patterns of energy type(s) and level(s) needed to transmit bi-valued events which can be discriminated by the strong link and can lead to an unintended establishment of the transmission path through the strong link barrier that allows passage of either functional or threat energy.

2.2.2. **Critical Functions.** These functions are critical:

2.2.2.1. Authorization. The weapon system shall have one or more devices to control authorization to use the weapon. These devices shall prevent prearming or arming (or both) of a nuclear bomb or warhead in aircraft-carried weapons and the launch of a ground-launched missile until authorization to prepare to use the weapon is received through the command and control system. 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 requirements specified in AFI 91-107, for protection against unauthorized actions, shall operate on the information control concept. A secure method shall provide the information through command and control channels.

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

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

2.2.2.2. Prearming. The prearm command provides an unambiguous indication of human intent to 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 shall arm. The weapon system design shall keep the prearming function separate and independent from the authorization function. Weapon design features shall 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 shall 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 shall have a safe and arm device or equivalent design to protect the ignition system. Without the arm command, propulsion system ignition shall not occur even if the ignition command is sent. Design features shall preclude accidental or deliberate unauthorized transmission of the arm and ignition commands. The design shall also prevent any failure 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 shall not occur even if the release command is sent. Design features shall preclude accidental transmission of unlock and release commands and shall also prevent any failure from allowing bypass of the lock device that would permit release of the weapon when the device is locked. Aircraft delivery system controls for release of guided weapons shall provide for the protection of friendly territory to the greatest extent possible (i.e., combination of system design features and procedural controls). For air-launched missiles, the ignition system arm and the release system unlock shall be separate and independent functions.

2.2.2.5. Arming. If the weapon is prearmed, arming shall 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 shall 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 (refer to paragraph 2.9.1.1) as a measurement of the proper operational environment. Bombs with self contained guidance shall include a good guidance signal prior to release as a measurement of the proper operational environment. Bombs with active self contained guidance** released from aircraft shall include a good guidance signal (refer to paragraph 2.9.1.2) 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 shall 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, targeting data transmission to missile guidance, and arming and fuzing systems. Targeting data consists of the flight control and fuzing constants needed to deliver and detonate the weapon within the designated target area. The weapon system design shall 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.

2.2.4. Targeting for air-delivered systems. Targeting is not a critical function for air-delivered systems. However, air delivered missiles or bombs with self contained guidance require positive measures as defined in AFI 91-101 to ensure the protection of friendly territory to the greatest extent possible. (refer to paragraphs 2.9.1 and 2.9.2).

2.3. Critical Function Numerical Requirements. The numerical requirements specified in AFI 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 nuclear bombs and warheads, Air Force nuclear weapon system designers shall 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. A physical security system shall prevent access to nuclear weapons and protect critical equipment and secure data (refer to paragraph **1.1.4**). Nuclear weapon systems and nuclear weapons shall incorporate internal security features to prevent unauthorized use (refer to paragraph **1.1.2**).

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 the appropriate nuclear bomb and warhead Stockpile-to-Target Sequence (STS) and Military Characteristics (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-HDBK-1512, *Electro-explosive Subsystems, Electrically Initiated, Design Requirements and Test Methods*. If the devices are electrically actuated, they shall arm only in response to an externally generated unique signal. The safing signal shall differ from the arming signal to reduce the risk of arming during attempted safing. If a monitor signal is used, it shall 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:

2.9.1.1. Missile systems and guided missiles launched from aircraft shall receive a good guidance signal from the guidance and control unit before nuclear warhead arming can occur. The good guidance signal shall be withheld if a final guidance accuracy check shows the weapon shall impact outside specified target boundaries.

2.9.1.2. Bombs with self contained guidance shall incorporate a good guidance signal prior to release. Bombs with active self contained guidance shall also incorporate a good guidance signal for arming which shall be withheld if the weapon cannot be guided to detonate within specified target boundaries (refer to paragraph 2.9.2).

Active self contained guidance is defined as a weapon that has capability to update position and navigate to the target.

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, shall specify target boundaries.

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

2.11. Human Engineering. Design the system so no two independent human errors or acts shall cause prearming, arming, launching or releasing of a nuclear weapon in an operational weapon system or shall 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 shall minimize the number of points within the system where human actions could degrade nuclear safety or security. The design shall also stress positive measures to prevent deliberate unauthorized or accidental operation of controls that could degrade nuclear safety or security.

2.12. Commercial off-the-shelf (COTS) Equipment.

2.12.1. **Non-specialized COTS.** Non-specialized COTS equipment is nuclear safety design certified as prescribed in AFI 91-103, *Air Force Nuclear Safety Design Certification Program*.

2.12.2. **Integrated COTS Equipment/Item.** COTS items that are used or integrated as part of an item that requires nuclear safety design certification as defined in AFI 91-103 (e.g., multi-meters integrated as part of a certified tester, etc.) are considered specialized and shall be evaluated in accordance with this manual.

Section 2B—Automata, Software, Firmware and Hardware Generated Using Software

2.13. General Design Criteria. All automata, software, firmware and integrated circuits generated using software that receives, stores, processes or transmits data to monitor, target, prearm, arm, launch, release or authorize the use of a nuclear weapon shall comply with the design and evaluation criteria specified in AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software*. An example of an integrated circuit being generated using software is the use of Very-High-Speed Integrated Circuits (VHSIC) Hardware

Description Language (VHDL) to design, simulate and synthesize an Application Specific Integrated Circuit (ASIC).

2.13.1. Circuitry Designed with Automated Tools. Critical circuitry designed with automated tools (e.g. synthesized from VHDL) shall be verified IAW AFMAN 91-119.

2.13.2. Reprogrammable Circuitry. Reprogrammable circuitry (e.g. the contents of a Field Programmable Gate Arrays (FPGA)) shall be protected IAW AFMAN 91-119.

2.13.3. Circuits with Embedded Software**.** Critical circuits with embedded software or firmware are subject to AFMAN 91-119.

2.13.4. Electronic Circuits Controlling Critical Signals or Performing Critical Functions. The integrity of critical functions implemented with electronic circuits must be protected IAW AFMAN 91-119.

2.13.5. Programmable Logic Devices. Critical circuitry incorporating FPGA's or other logic devices subject to a single event upset shall employ redundancy or other discipline to protect the integrity of the critical function for all credible environments. Reliability goals specified in AFI 91-107 are sufficient for systems incorporating programmable logic devices.

Section 2C—Electrical Subsystems and Hazards

2.14. 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.

2.14.1. 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-STD-461, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment* and MIL-STD-464, *Requirements for Systems Electromagnetic Environmental Effects*,). The design of wires, switches, cable connectors, junction points and other system elements shall minimize undesirable radiated and conducted interference or transients when such EMI could cause a nuclear hazard or ordnance ignition.

2.14.2. 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:

2.14.2.1. Do not use wire or cable shields as current-carrying conductors and cover shields with an insulation layer.

2.14.2.2. Ensure electro-explosive circuitry, which affects or is affected by critical functions, conforms to MIL-HDBK-1512.

2.14.2.3. 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.

2.14.2.4. 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.

2.14.2.5. Isolate critical circuits from potential sources of unintended electrical power.

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

2.15. Wiring and Cabling.

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

2.15.2. 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 shall not exceed 6 inches. Connector backshells shall have conductive finishes to minimize shield termination impedance.

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

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

2.15.5. 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 of connectors.

2.16. Electrical Connectors. Ensure all hardwire electrical connectors associated with nuclear weapon circuits conform to MIL-DTL-38999-XX series, *General Specification for Connector, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded, and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts*. This requirement does not apply to electrical connectors used within a line replaceable unit.

2.16.1. Alignment and Mating. Design electrical connectors to prevent misalignment of connector components and bent pins during mating. Use diverse connector designs to ensure connectors are compatible with the intended connection only and incompatible with other 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.

2.16.1.1. Connector Pin Mapping. Connector pin mapping should minimize the likelihood of bent pins resulting in the inadvertent activation of a critical function.

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

2.16.3. Mandated Use Isolation Exception. If possible, design the circuits within a single connector to meet the isolation requirements of paragraph **2.14.2**. If all the requirements cannot be met due to the mandated use of nonconforming weapons or equipment, connector pin mapping shall ensure no single bent or misaligned pin can result in the application of sufficient power to cause critical function activation.

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

2.17. Electrical Current Considerations. Limit monitoring and testing current of ordnance devices 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.

2.18. 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 EMR susceptibility to electro-explosives, semiconductors and other devices.

2.18.1. EMR Environment Levels. Although a complete survey of the EMR environment weapons shall 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 milliwatt per square meter (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 weapon's STS (whichever is greater) are the minimum levels considered in designs for EMR protection.

2.18.2. 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.

2.18.2.1. 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 shall 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 so they do not conduct or couple EMR energy into the shielded volume.

2.18.2.2. Cable Shielding. Refer to paragraph **2.15.2**.

2.18.2.3. Terminal Protection Devices (TPD). Use TPDs 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.

2.18.2.4. Electro-explosive Devices (EED). Shield all EED firing circuits using a twisted wire configuration with the case of the initiator electrically bonded to the structure. A single ground point shall 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 root mean square current in its bridgewire shall be 20dB below the maximum no-fire current of the EED. EED male connectors that are in an open-circuited configuration must 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

2.19. General Design 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. 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**.

2.20. System Devices.

2.20.1. Prearm Device. Design the A&F system to provide a unique prearming signal for the strong link prearm device in the warhead or nuclear bomb. Derive this signal from some part of the weapon system under direct human control to provide an unambiguous indication of human intent to use the weapon. The function provided by human action shall be reversible up to the time of launch or release for aircraft systems or commitment to launch for ground-launched missiles.

2.20.2. 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 nuclear bomb or warhead) prevents arming until the proper environment is sensed and responds only to an environment unique to the flight of the weapon. Because this stimulus may occur as a result of the release of a nuclear 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 shall normally be a prerequisite to activating the E/TSD.

2.20.3. 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 until a weapon launch or release is detected. For aircraft systems, this device (such as a pullout switch or breakaway connector) shall sense launch or release of the weapon. For ground-launched missiles, this device (such as a lanyard or a pressure-actuated valve) shall sense the proper launch environment. The design of these devices shall protect against accidental or inadvertent operation.

2.21. System Design Features.

2.21.1. 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.

2.21.2. 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).

2.21.3. 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.

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

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

2.21.6. 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 or electrically conductive gas, cause an electrical short or reversion or create similar results.

2.21.7. Monitoring.

2.21.7.1. Provide the capability (always placed on the A&F system) to monitor the weapon state status in all weapon system configurations.

2.21.7.2. Ensure the monitoring function design prohibits the possibility of introducing energy from any source that might operate an A&F critical function or prevent the transition of a weapon from a prearm state to a safe state if a system fault or credible abnormal environment occurs (refer to paragraph **2.17**). If feasible, consider non-electrical monitor systems.

2.21.8. 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

2.22. General Design Criteria. Apply the design criteria in this section to ground-launched missile systems and apply the noncombat delivery vehicle criteria in **Chapter 3** to ground mobile combat delivery vehicles.

2.23. 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.

2.23.1. System Design. Apply these criteria:

2.23.1.1. Missile launch shall occur only through intentional operation of the authorization and launch control devices. No other system or subsystem, in operational or failure mode, shall be able to authorize a missile launch, start a launch sequence, launch a missile or operate the propulsion system.

2.23.1.2. 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) shall occur when an attempt is made to operate the launch control system and the indications shall remain until the system operators acknowledge and reset them.

2.23.1.3. The launch control system shall remain in or return to a safe state when component failure or electrical power loss occurs.

2.23.1.4. Arm (operate) and safe (off) critical command signal functions shall not be complementary functions; that is, the absence of "arm" shall not be construed as "safe" or vice versa.

2.23.2. 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 (refer to paragraph **2.8**) and manually safed. Generation of the unique signal requires some physical or electrical action unlikely to occur in a credible abnormal environment.

2.23.3. 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:

2.23.3.1. A single component failure or system fault shall not cause inadvertent transmission of critical signals or inadvertent operation of critical functions.

2.23.3.2. The system design shall stop a change of state or an output of a critical signal if data synchronization is lost.

2.23.3.3. The multiplex system design shall be compatible with system hazard and fault analyses so that the polling time interval and automation logic shall not mask any critical function activation or fault between successive polls. If this requirement cannot be met for all credible environments, provide a means for dedicated reporting, automatic shutdown or priority interrupts.

2.24. Reentry System, Reentry Vehicle or Payload /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 (refer to 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 shall not apply power to any warhead interface; the device is not needed to meet the criterion of (AFI 91-107 Table 2 Rule 2) for inadvertent application of power or signals to the nuclear 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.

2.25. Monitor Systems.

2.25.1. Monitor Requirements. Provide systems that allow the operator to continuously monitor the safe status of the missile propulsion system; warhead or warheads (refer to paragraph **2.21.7**); 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 while ensuring 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.

2.25.2. 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 whenever an unsafe condition is indicated. Power can be restored when the unsafe condition is corrected.

2.25.3. Monitor Electrical Current Limitations. Refer to paragraph **2.17**.

2.26. Command and Control Communications.

2.26.1. Launch Control Points.

2.26.1.1. The launch crew shall 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 shall be different from the code used to authorize the launch of a missile.

2.26.1.2. For systems with a selective launch capability, the launch control system shall 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.

2.26.1.3. Policies and procedures that govern the authentication and safeguarding of nuclear control orders are in DoDD (S) 5210.81, *United States Nuclear Weapons Command and Control, Safety, and Security* and AFI 11-299, *Nuclear Airlift Operations* (for airlift operations).

2.26.2. Launch Control Points to Launch Points Communications and Code Devices.

2.26.2.1. 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 cognizant agents or third parties. For any device operated by the withheld secure code discussed in paragraph **2.26.1.1**, allow only a limited number of attempts at operation using incorrect codes or include some other anti-tamper feature. Also, include a device or system to detect tampering.

2.26.2.2. 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 shall alarm the LCPs if tampering with the system occurs.

2.26.2.3. An LP may respond to launch commands from a single LCP. Ensure the critical LP status is monitored at the primary LCP and at least one other location. Each location shall be able to take compensatory action if an unauthorized critical command message or status is detected.

2.26.2.4. The LCP shall ensure that even after all secure codes are available; at least two people shall actively cooperate to command authorization and launch.

2.26.2.5. 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 shall stop use of the code storage device for its intended purpose, which must cause an alarm and positive indications to be received at the LCP.

2.26.2.6. 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 access and 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.

2.27. Mobile Launch Points and Mobile 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

2.28. 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.

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

2.29.1. Aircraft Monitor and Control (AMAC) and Release System Electrical Power.

2.29.1.1. Ensure critical functions shall 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 shall not jeopardize the safe condition of a weapon.

2.29.1.2. 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.

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

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

2.29.4. Cable and Connector Design. Make connector pin assignments to protect against inadvertent application of prearm and arming power to the nuclear bomb or warhead as the result of damaged cables and/or connectors. The design shall guard against cable or connector selection and cable routing susceptible to damage during assembly, maintenance and test operations.

2.30. 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.

2.30.1. Suspension Lock Monitor. Ensure the latched and locked condition of suspensiondevices 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.

2.30.2. 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 shall:

2.30.2.1. Mechanically restrain the releasing device.

2.30.2.2. Stop release or launch if maximum available release force is accidentally applied in the release mechanism.

2.30.2.3. Fail safe in the event a failure occurs when the lock is locked.

2.30.2.4. Disable all means of release when in the locked position.

2.30.2.5. Permit ground personnel to visually check the locked state. For direct visual inspection, the locking device itself shall present an unmistakable indication of the locked state.

2.30.2.6. Be protected from accidental operation.

2.30.2.7. Provide a method in the crew compartment to show tampering with the aircrew's controls of the in-flight reversible lock.

2.30.2.8. 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 shall not allow an apparent indication to the aircrew of a locked state if an unlocked state exists.

2.30.2.9. Ensure the safety lock mechanically restrains the suspension and release linkage if hooks are used in the suspension and release linkage. The safety lock shall mechanically restrain each hook that can be individually latched or unlatched.

2.30.2.10. Relock if unlock power is removed (accidentally or intentionally) while the lock is unlocked.

2.30.3. 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 **2.30.2** If feasible, use a single lock for both the weapon and the pylon.

2.30.4. Unlock and Release Signal Isolation. Physically and electrically isolate the discrete energy control signals for unlocking the in-flight lock and releasing the weapon to the greatest extent possible. A release system fault shall not be able to operate the in-flight reversible lock and an in-flight reversible lock fault shall not be able to cause a release.

2.31. Nuclear System Controls and Displays.

2.31.1. 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 shall require a separate and deliberate act by the weapon system operator.

2.31.1.1. 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 aircrew member action. Use aircrew 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 shall not occur in the event of an accident.

2.31.1.2. Prearm Consent. The function of prearm consent is to inhibit prearming until direct aircrew action provides the required consent signal. Design the prearm consent control to reveal unauthorized operation or tampering.

2.31.1.2.1. Electrical Interface Non-(MIL-STD-1760, *Aircraft/Store Electrical Interconnection System*). Make the prearm consent function a hardwired control that interrupts power to the prearm circuit controlling the intent strong link.

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

2.31.2. Release and Launch Controls.

2.31.2.1. 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 shall be a hardwired function. Neither the application nor reapplication of nuclear release consent shall unlock or inhibit the locking of the in-flight reversible lock. Removal of nuclear release consent shall relock the in-flight reversible lock.

2.31.2.2. 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.

2.31.2.3. 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 control (hardware or software) or control setting unique to the release or launch of nuclear weapons. This control or setting shall not be used to release or launch nonnuclear weapons.

2.31.2.4. Aircrew Member Release Input. For aircraft designed to release multiple nuclear stores, implement an aircrew member 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 aircrew member input once authorization, nuclear consent (prearm and release) and prearm are accomplished.

2.31.2.5. 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. For emergency release where normal jettison procedures cannot be accomplished, at least one distinct human action shall be required to separate a prearmed weapon in as safe a state as possible to preclude weapon detonation. The intent of this distinct human action is to provide a signal to exercise available options for returning the weapon to a safe state.

2.32. Multi-crew Aircraft Consent Functions. Design multi-crew aircraft AMAC and release systems with separate controls for both prearm and release consent. Each consent function shall require the physically separate and independent actions of two aircrew members. The functioning of these controls is called "nuclear consent." A multi-crew 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.

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

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

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

2.33.3. Indeterminate Weapon State. Warning 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 shall not receive a caution during weapon change of state from safe to prearm or from prearm to safe.

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

2.34. 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.

2.34.1. Monitor and Control Circuit Isolation. Ensure monitor circuits are electrically isolated from power and control circuits; and monitor functions are independent of weapon control functions.

2.34.2. 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 true

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

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

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

2.35.3. Positive action to supply power at the weapon interface.

2.35.4. Separate control that removes power from the weapon interface.

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

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

2.36.2. Dedicated Display. When power is applied to a nuclear weapon, one aircrew member shall have control of nuclear weapon functions and at least one display shall be dedicated to monitoring weapon status. Generally, the monitoring station shall 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 shall 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 shall not permit inadvertent control of the nuclear weapon system while the display is scrolled away.

2.36.3. Combined AMAC and Release Displays. AMAC and delivery functions may be combined on the same screen display; however screen formats shall clearly differentiate the functions. Software protocols (inhibits and critical function preconditions) shall minimize the possibility of executing an erroneously selected function.

2.36.4. Allowable Command State Transitions. Except for the SAFE-OFF state transition, each nuclear weapon shall 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 shall define these command states. Change of state shall occur only by an aircrew member’s explicit command and such transition commands shall be independent of the monitored state. The SMS design shall 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.

2.37. Multiplexed (MUX) Systems.

2.37.1. Time-Division Multiplexing (TDM). Whenever possible, use TDM for standardization purposes (preferred method according to MIL-STD-1553, *Digital Time-Division Command/Response Multiplex Data Bus*).

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

2.37.3. Data Communication and Transfer.

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

2.37.3.2. Unauthorized stations transmitting or receiving data shall not affect the nuclear weapon interface.

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

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

2.37.5. Abnormal Environment Protection.

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

2.37.5.2. Logic Power Levels. Voltage and current levels required to operate MUX station logic shall 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.

2.37.5.3. Non-volatile Memory. Non-volatile, nondestructive read-only memory units are required to store MUX AMAC operational programs, algorithms for MUX control, 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.

2.37.6. Built-in Test. Self-testing shall not interfere with normal MUX operation, cause the generation of any consent signal or critical signal at the nuclear weapon interface. Also, ground testing shall not degrade nuclear safety.

2.37.7. Operator MUX Control.

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

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

2.38. 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:

2.38.1. A&F System. The A&F system shall contain:

2.38.1.1. A unique signal S&A or A/D device for arming and safing the missile part of the A&F system. The warhead prearm switch shall not serve as the missile system arming and safing device.

2.38.1.2. A launch or release sensing device 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).

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

2.38.2.1. Ensure each S&A or A/D device requires a weapon system operator to apply safing power.

2.38.2.2. Incorporate the capability to monitor the missile S&A or A/D devices for the safe condition, either continuously or on demand. Ground personnel shall be capable of visually monitoring the state of the devices.

2.38.2.3. 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.

2.39. General Design Criteria. Apply the design criteria in this section to test equipment used to verify the proper operation, safe state and control of critical nuclear functions.

2.39.1. Fail-Safe Requirements. The test equipment design shall prevent these conditions:

2.39.1.1. Faults in the test equipment or test circuits that could operate critical functions or apply unintended power to the weapon interface.

2.39.1.2. Faults within a tester that could degrade the nuclear safety of the equipment to be tested.

2.39.1.3. Introduction of signals, voltages or currents into the weapon system that could degrade nuclear safety.

2.39.1.4. Operation or firing of an item under test, except when specifically designed for that purpose.

2.39.2. Safe State at End-of-Test. Test equipment shall 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.

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

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

2.39.4.1. 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.

2.39.4.2. 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.

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

2.39.6. Functionality and Safety Checks. The test equipment design shall 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) using the following tests:

2.39.6.1. Preloading tests shall test the functionality, as defined by the AFNWC and AFSC/SEWN, of the entire DoD/DOE interface.

2.39.6.2. Preflight, post-flight and periodic testing shall occur from any connector interfacing with the weapon to the furthest termination in the combat delivery vehicle (end-to-end check).

2.39.6.3. When possible, isolation resistance tests of the combat delivery vehicle shall occur during the routine time-phase testing.

2.39.6.4. Isolation resistance tests of all critical circuits external to the weapon shall occur periodically.

2.39.6.5. Where redundant features are present in the weapon system, test provisions or BITE shall indicate the integrity of both the redundancy and the function.

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

2.39.7.1. Generating of release or launch signals.

2.39.7.2. Initiating of a critical function.

2.39.7.3. Negating of Two-Person Concept control.

2.39.7.4. Unlocking the in-flight reversible lock.

2.39.7.5. Operating an S&A or A/D device.

2.39.8. Test Automata, Software, Firmware and Hardware Generated Using Software. All automata, software, firmware and integrated circuits used for testing or checkout shall meet the provisions in AFMAN 91-119. This criterion applies to software that receives, stores, processes, or transmits data to monitor, target, prearm, arm, launch, release or authorize the use of a nuclear weapon.

2.39.9. 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) shall prevent undesired radiated and conducted interferences or transients.

2.39.10. Test Equipment. Test equipment intended to test the AMAC functions at DoD/DOE interface shall incorporate parameter limits defined by the appropriate AMAC system specification and interface control documents.

Section 2H—Technical Order (TO) Procedures.

2.40. 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. Any technical order change that may impact a Nuclear Certified design or configuration should be reviewed by a Chief Engineer or designated representative IAW TO 00-5-3, *AF Technical Order Life Cycle Management* and AFI 63-1201, *Life Cycle Systems Engineering*.

2.41. 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:

2.41.1. Ensure procedures used to test the weapon system critical functions define a sufficient set of tests necessary to verify system operability and safety.

2.41.2. 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 shall be the maximum needed to maintain a high confidence level in system functionality and safety.

2.41.3. 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 shall provide procedures for periodic maintenance, inspection and testing to ensure the test equipment shall continue to meet the original specifications.

2.42. Cargo Aircraft Loading and Restraint Procedures. Loading procedures for mixed loads of nuclear and nonnuclear cargo shall minimize the movement of the nuclear cargo and shall position the nonnuclear cargo where it shall not collide with nuclear cargo (refer to MIL-

DTL-25959, *Aircraft Cargo Tie Down, Tensioners,* MIL-DTL-6458, *Aircraft Cargo Single Leg Tie Down Chain Assemblies* and SAE-AS8905, *Aircraft Floor Fittings and Tie Down Cargo Rings,*). Tiedown patterns and configurations require review by AFNWC engineering.

Section 2I—Nuclear Weapons Maintenance, Handling and Storage Facilities.

2.43. Criteria Applicability. Apply the applicable Unified Facilities Criteria (UFC) design criteria and the criteria in this section to new and existing facilities that are capable of supporting nuclear weapon maintenance, handling and storage operations. These criteria shall apply to US owned facilities.

2.43.1. Existing Facilities. Existing facilities and facility systems are not required to be modified solely to meet the requirements of this chapter.

2.43.2. New Facilities and Facility Modifications. Any new facility, as well as, any proposed, planned, required modification or upgrade to existing facilities or essential facility systems shall require nuclear design safety certification action in accordance with AFI 91-103, *Air Force Nuclear Safety Design Certification Program*.

2.44. General Design Criteria. Facilities (as part of the nuclear weapon system) shall be certified before conducting operations with nuclear weapons IAW AFI 91-103 *Air Force Nuclear Safety Design Certification Program*, AFPD 91-1 *Nuclear Weapons and Systems Surety*, AFI 91-101 *Air Force Nuclear Weapons Surety Program* and DoDD 3150.2, *DoD Nuclear Weapon System Safety Program*. **2I** and **4H** of this manual establish the Air Force design and evaluation criteria, respectively, for facility subsystems that can directly support maintenance, handling and storage operations for nuclear weapons. A systems engineering approach is essential for nuclear certification of facilities. Facilities and the essential facility systems (EFS), listed below in paragraph **2.45**, shall be designed and built to preclude potential electrical, mechanical, thermal, electromagnetic radiation and chemical insult to nuclear weapon systems, assuming the occurrence of severe natural phenomena (e.g., lighting, tornadoes, earthquake), an explosive detonation or other abnormal event (e.g., facility power surge, electromagnetic radiation, fire, blast, dropping, striking, etc). These EFSs and any subsequent modifications or upgrades to these EFSs shall comply with the criteria below. In addition, all interface or connectivity between essential facility subsystems shall be designed to ensure that the nuclear surety environment has not been degraded or eliminated (e.g. the interface between fire alarm and the Blast Containment Management System (BCMS) software at Kirtland Underground Munitions Maintenance Storage Center). These criteria apply to all US owned facilities that maintain a capability to support nuclear weapon storage, maintenance and handling operations.

2.45. Design of Essential Facility Systems.

2.45.1. Lightning Protection System (LPS). Facilities shall be provided with a LPS in accordance with NFPA 780, *Standard for the Installation of Lightning Protection Systems*, AFMAN 91-201, *Explosives Safety Standards* AFI 32-1065, *Grounding Systems* and UFC 3-520-01, *Interior Electrical Systems*. Underground facilities (excludes Earth Covered Magazines [Igloos]) do not require conventional air terminal or down conductor LPSs, but shall have a counterpoise grounding system that meets the requirements of NFPA 70, *National Electrical Code*, AFMAN 91-201, AFI 32-1065 and UFC 3-520-01.

2.45.2. Nuclear Weapons Side Flash Protection Requirements.

2.45.2.1. Default Safe Separation Distance (SSD). Nuclear weapons, during intrusive maintenance operations, shall be protected from lightning side flash by maintaining a minimum 7-foot separation distance between a weapon and the walls, ceiling, hoists, structural supports and metallic conductors of the facility in accordance with AFMAN 91-201. This is commonly referred to as the "7-foot rule". If the facility (either above ground or underground) is capable of supporting intrusive maintenance operations, implementation plans and procedures for ensuring compliance with the 7-foot rule shall be documented. Also, a physical demarcation (i.e., paint or tape) shall be readily visible and clearly indicate the area in which intrusive maintenance operations can be accomplished. When not in use, overhead hoists will have designated parking outside the 7-foot stand-off area, away from where maintenance operations are conducted.

2.45.2.2. Alternative to 7-Foot Standoff. The required separation distance of the 7-foot rule can be significantly reduced by implementing the design feature known as a "Faraday Shield" (referred to as a "metallic cage" by NFPA 780) including electrically bonding penetrations to the Faraday Shield and installing proper surge suppression. In this approach, the facility shall be tested and analyzed to determine the effectiveness of the facility Faraday-like Shield characteristics. Based on the specific test results, the side flash and associated SSD within the facility may be reduced. This process is referred to as facility characterization.

2.45.2.2.1. Facility Characterization Design Criteria. To accomplish a facility characterization, the following measures, in order, are required in addition to the customary standards for LPS (refer to paragraph **2.45.1**):

2.45.2.2.1.1. Define the Faraday-like Shield boundary of the facility based on facility construction.

2.45.2.2.1.2. In addition to the bonding requirements in NFPA 780, AFMAN 91-201 and AFI 32-1065, provide upgraded or additional bonding of all metallic penetrations at the point of entry to the defined Faraday-like Shield using a methodology approved by the Authority Having Jurisdiction (AHJ) prior to implementation. Bond lengths shall be kept as short as practical, ideally less than 4 inches and if possible/practical should go downward from the penetration to the Faraday-like Shield. Bonds exceeding 4 inches in length shall require additional calculations of impedance, voltage and side flash corresponding to the current of a lightning strike traveling through the bond to determine the final SSD.

2.45.2.2.1.3. Surge suppression shall be installed on all incoming service conductors and on low voltage systems. Surge protection shall have the capability to interrupt the energy levels of the established "one percentile" lightning strike. This is defined as the 99 percent severity level in the DOE baseline STS. When it is not practical to install suppression on communications and data circuits capable of interrupting the energy levels of the established one percentile lightning strike, alternatives approved by the AHJ shall be in place to mitigate the possibility of the lightning energy from entering the facility through these conductors.

2.45.2.2.1.4. Perform the transfer impedance testing of the facility to determine the Faraday-like Shield characteristic (i.e., determine how closely the facility demonstrates Faraday-like Shield characteristics – electrical connectivity of reinforcing steel and facility structural members in the floor, walls and ceiling) and associated SSD.

2.45.3. Facility Power Systems. Facility power systems shall incorporate an auxiliary power system to insure adequate power is maintained to subsystems that maintain safety or security of nuclear weapons at all times. Normal and auxiliary power systems for maintenance, handling and storage facilities shall be designed to meet the requirements of AFMAN 91-201 *Explosive Safety Standards.* Emergency power systems shall meet the requirements of AFI 32-1063, *Electric Power Systems,* chapter 5.

2.45.4. Fire Protection Systems. Fire suppression and alarm systems shall be incorporated in the design of the facility. Automated fire suppression systems meeting the requirement of NFPA 13, *Standard for the Installation of Sprinkler Systems* shall be provided unless a Fire Hazards Analysis (FHA) clearly indicates that an appropriate alternative to a fire suppression system is justified.

2.45.5. Hoist, Cranes and Similar Devices**.** Refer to the design criteria in **Section 3C** of this AFMAN.

2.45.6. Security Systems. Security systems are designed and implemented IAW AFMAN 31-108 *The Air Force Nuclear Weapon Security Manual*. Consider the safety risks from the possibility of exposing a nuclear weapon (either inadvertently or by deliberate unauthorized acts) to abnormal environments. Security systems that directly control access to nuclear weapons shall be designed to prevent unintended or deliberate unauthorized access. The possibility of unintended or deliberate unauthorized access shall be adequately mitigated through a combination of design and procedural means.

2.45.7. Facility Security System Automata and Software Design. Ensure automata and software design is compatible with other facility safety and security systems IAW AFMAN 91-119.

2.45.8. Blast Containment/Isolation Features. Design blast containment and isolation features IAW AFMAN 91-201 *Explosive Safety Standards* and DoDD 6055.9E, *Explosives Safety Management and the DoD Explosives Safety Board*. A key element of the design is to mitigate contamination of facilities and weapons by limiting radiation transport mechanisms such as explosions/blast and fires. Blast isolation design of the facility shall incorporate blast zones/areas for the purpose of limiting the spread of contamination and consequential damage to the facility and stored critical assets. Design of blast containment/isolation systems shall consider such factors as siting requirements, blast zones, blast pressures, isolation requirements, drainage requirements and heating, ventilating, air-conditioning (HVAC). Compatibility between these factors, when incorporated, shall be assured. Ensure that the blast mitigation design prevents sympathetic detonation of nearby weapons by blast, fragment or thermal insult.

2.45.9. Electromagnetic Radiation (EMR) Environment. An EMR environment in a facility results from the combination of installed and portable equipment that emits EMR. These EMR sources in facilities include unintentional emitters such as lighting, motors, monitors, communication equipment, etc., as well as intentional emitters such as radio transmitters. All equipment installed or used within the facility, individually and collectively, shall not result in an overall EMR environment that exceeds the weapons STS levels (IAW AFMAN 91-201, chapter 9).

2.45.10. Radiation Monitoring. Design maintenance, handling and storage facilities with the ability to monitor for both plutonium and tritium. This design shall work in conjunction with other facility systems, especially the blast containment/isolation system, HVAC systems, and the fire alarm and suppression systems, to minimize collateral effects to both the rest of the facility and the local environment.

2.46. Essential Facility System Automata and Software. Ensure automata and software design that is unique and developed specifically to control essential facility systems is compatible with other facility safety and security systems IAW AFMAN 91-119.

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 shall incorporate positive safety features. The vehicles and equipment shall meet appropriate structural, environmental, stability and mobility requirements. The STS document defines modes of transportation. The safety design factors shall 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. Good industrial design practices, standards and features can be used to substantiate nuclear safety design certification of any commercially designed non-specialized equipment as identified in AFI 91-103. At locations outside the United States and territories, non-US design standards (i.e. European Specifications and Approvals) may be used in lieu of the listed US standards.

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 rated load consists of one or more weapons and the associated handling and restraint equipment and is the nuclear-certified load.

3.2.2. Design Load. The loads used to initiate the design of equipment shall be based on the rated load multiplied by a factor of three (3), unless higher factors are required due to dynamic loading. Some examples of dynamic loading are accelerations encountered during air transport or towing operations.

3.2.3. Stress Levels. The stress level, under the static rated load condition, at any point in the structure shall be limited to a level that provides a factor of safety of three (3) against permanent deformation. Where dynamic factors induce loads that exceed 1.5 times the rated load, as defined in paragraph **3.2.2**, then the stress level at any point in the structure shall be limited to a level that provides a factor of safety of two (2) against permanent deformation.

3.3. Structural Design Criteria. In addition to meeting the design load requirements of paragraph **3.2.2**., ensure the design shall 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. The interfacing of loading between systems shall be considered. These are typical failure mode classifications:

3.3.1. Elastic Failure. Elastic failure is exhibited by excessive deflection.

3.3.2. Plastic Failure. Plastic failure is exhibited by material yielding (yield is experienced when stress levels exceed the minimum yield strength of the material, as specified in applicable standards).

3.3.3. Buckling Failure. Buckling failure is exhibited by excessive and quick deformations (collapse) with a loss of operational capability. Buckling load shall not exceed 1/2 yield strength of material.

3.3.4. Fatigue Failure. Fatigue failure is exhibited by a fracture incurred by the cyclic application of loads.

3.3.5. Composite Failure. Composite failure is exhibited by any composite material failure such as material delaminating under compressive load.

3.3.6. Ultimate Failure. Ultimate failure is exhibited by material fracture.

3.4. Data Sources. In determining allowable stresses for equipment, select the material and allowable stress specified in government publications 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 ground vehicles, forklifts and weapon loaders used to transport nuclear weapons on their basic structure.

3.6. General Criteria.

3.6.1. Frame Load Support. Design 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.

3.6.4. Shock Isolation. Design the equipment to minimize mechanical shock transmission to a nuclear weapon. This would include a Shock Response Spectra analysis for the system under load.

3.6.5. Restraints. Ensure restraint provisions for ground transport of all nuclear weapons are capable of restraining the design load with accelerations from paragraph **3.19**.

3.6.6. Engine Start Switch. Ensure the engine start switch shall 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 (refer to paragraph **3.10.1**), shall have parking brakes designed to hold the maximum operational load on an 11.5-degree incline when headed both up and down, for a minimum of 15 minutes each.

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 maximum operational 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/or applicable commercial standards, whichever is more stringent, and meet the mobility requirements based on operational conditions. Guidance can be found in MIL-HDBK-1784, *Mobility*, *Towed and Manually Propelled Support Equipment* and commercial standard SAE-AS8090, *Equipment*, *Towed Aerospace Ground*, *Mobility*.

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, Capability Development Document (CDD), Capability Production Document (CPD) 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, CDD, CPD and 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: (does not apply to commercial semi-trailers considered nuclear certified in accordance with AFI 91-103).

3.7.1. Service Brakes. Ensure service brake systems meet the requirements derived from MIL-HDBK-1784.

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

3.7.3. Mobility. Comply with the mobility requirements derived from MIL-HDBK-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) shall have these design features: (does not apply to commercial semi-trailers considered nuclear certified in accordance with AFI 91-103).

3.8.1. Brake System. The brake system shall be functionally compatible with the towed vehicle brake system. The towing vehicle shall not jackknife under maximum performance maneuvers. Brake performance shall comply with applicable industry standards and meet the failure criteria for towed vehicles in MIL-HDBK-1784.

3.8.2. Parking Brakes. Ensure that the parking brakes, together with the towed vehicle parking brakes, can hold a maximum operational load and towed vehicle combination on an 11.5-degree incline when headed both up and down for a minimum of 15 minutes each.

3.8.3. Tow Vehicle to Trailer Interconnect Device. Make the vehicle connecting device compatible with the towed vehicle and ensure it meets the structural design criteria of **Section 3A** or commercial standards, whichever is more stringent.

3.8.4. Fifth Wheel Safety Latch. Equip the fifth wheel with a safety latch designed to allow a visual check of the locked condition.

3.8.5. Vehicle Structure. The tow vehicle structure should be designed to accept loads induced by including the item in tow, tow bar and not exceed the stress levels in paragraph **3.2.3**

3.9. Self-Propelled Vehicles. In addition to the general criteria of **Section 3A** and paragraph **3.6**, ensure vehicles (such as trucks, vans and high lift trucks) comply with the brake performance requirements in paragraph **3.8.1**.

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 both up and down for a minimum of 15 minutes each.

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

3.10.3. Rail Bed 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: (For European forklifts, see paragraph 3.11.5)

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 that the equipment center of gravity and the rated load center of gravity are compatible.

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

3.11.3.1. Make all movement controls self-centering (except for such devices as the parking brake, steering control, transmission selectors, power takeoff and hydraulic pump).

3.11.3.2. Add mechanical stops or electrical switches to prevent over travel in all directions of the lift control.

3.11.3.3. Include in the weapon loader a capability for small increments of movement (inching) in both reverse and forward directions.

3.11.3.4. 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 shall be able to independently hold a maximum operational load on an 11.5-degree incline with the weapon loader headed either up or down.

3.11.5. European Forklifts. European forklifts are considered nuclear certified provided the standards listed in the tables below have been met. Any updates to these standards will require review by the process owners to ensure there are no significant changes that would invalidate their nuclear certification.

The following European Union (EU) standards apply to the process of manufacturing nuclear certified European forklifts:

Name	**Title**
Directive 98/37/EC	*Directive 98/37/EC of the European Parliament and of the Council of 22June 1998 on the Approximation of the Laws of the Member States Relating to machinery*
EN1726-1	*Safety of industrial trucks, self-propelled trucks up to and including 10000kg capacity and industrial tractors with a drawbar pull up to and including 20000 N-part 1: General requirements*
EN1551	*Safety of industrial trucks, self-propelled trucks over 10,000 kg capacity*

The following directives apply to electric forklifts:

Name	Title
Directive 89/336/EEC	*Council Directive of 3 May 1989 on the Approximation of the Laws of the Member States Relating to Electromagnetic compatibility*
EN 1175-1	*Safety of industrial trucks, electrical requirements, general requirements for battery powered trucks*
EN12895	*Industrial trucks, electromagnetic compatibility*
EN60204-1	*Safety of machinery, electrical equipment of machines, specification for general requirements*

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**, as a minimum design such equipment to have the features and controls in paragraph **3.13**.

3.13. Safety Features and Controls.

3.13.1. Positive Control. System controls shall ensure the load is under positive operator control. The design shall 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 over travel of a hoist on rails and stop the chain or wire rope when the hook reaches its upper limit.

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

3.13.3. Hooks. Hooks used with the lift system shall 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 Design 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**. Design weapon stands to remain stable when equivalent force equal to the weight of the stand and supported load are applied laterally at the center of gravity of this configuration.

3.15.1. Mobility. Ensure test and storage stands and handling units with casters meet the mobility requirements of applicable military standards and operational requirements.

3.15.2. Stability. All handling and support structures shall show that they are stable (no excessive movement or tendency to tip or buckle) while laterally loaded to a minimum acceleration of 1/2 G. This can be shown by test or analysis or a combination of testing and analysis.

3.16. Weapon Containers. Use the design criteria in MIL-STD-209, *Lifting and Tiedown Provisions* and MIL-STD-648, *Design Criteria for Specialized Shipping Containers* for containers used for storing and transporting weapons.

3.17. Pallet Standards. Pallets used with nuclear weapons shall conform to MIL-STD-1366, *Transportability Criteria*.

Section 3E—Air or Ground Transport Systems, General Use Tiedowns and Restraints.

3.18. General Air or Ground Transport Design Criteria. Design air transportable delivery vehicles and support equipment to meet the general specifications of MIL-HDBK-1791, *Designing for Internal Aerial Delivery in Fixed Wing Aircraft*.

3.18.1. Pallet Lock Systems. Pallet lock systems on cargo shall fail-safe (i.e., a single point failure of an active component shall not result in an uncommanded release of the pallet).

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

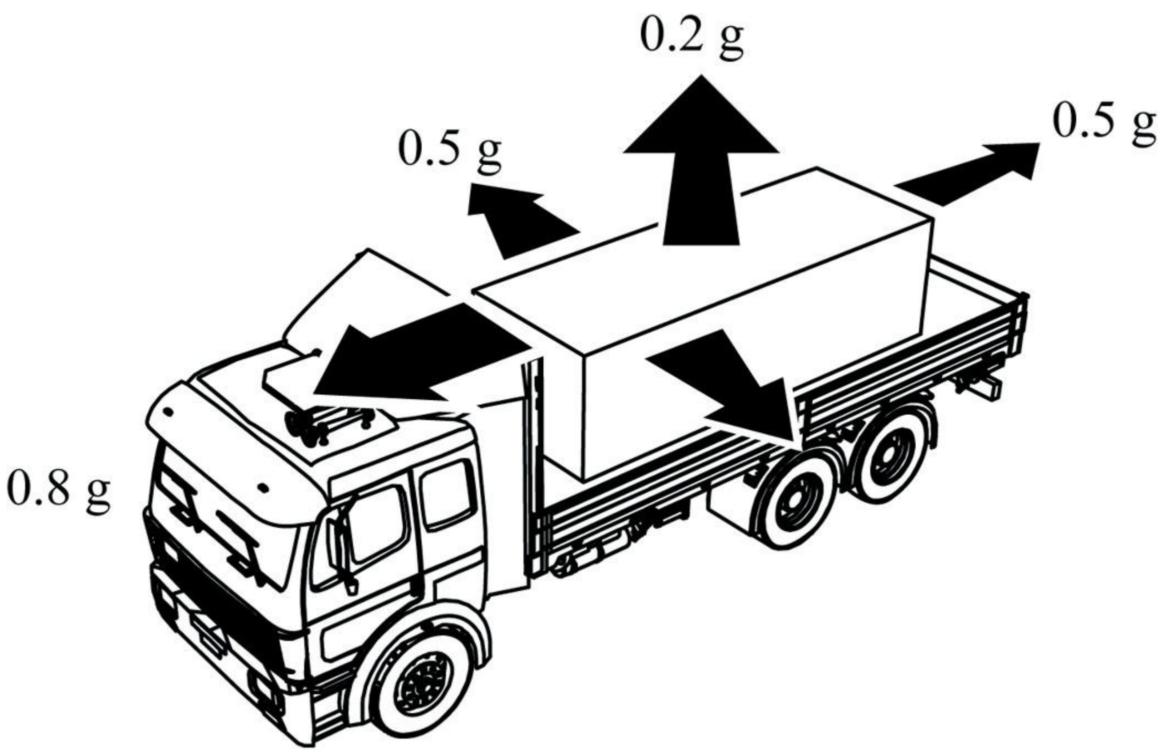
3.19.1. Minimum Tiedown Provision Condition. Industry working load of tiedown equipment should be used for determining the items working load rating.* Restraints must be loaded appropriately for comparison to be valid. As an example chains, wire rope and fabric straps cannot be loaded in compression, they only function in tension. Thus, a summation of force calculation must be performed on the tiedown device to determine the tiedown device load.

3.19.2. Ground Transport Requirements. Ground transport envelopes are based on North American Cargo Securement Standard Ground transport directional accelerations (refer to Figure 3.1). Each directional load is evaluated without friction between the trailer decking and the cargo. Evaluate statically and independently using the restraining device rated working load. Furthermore, the restraint assembly must remain connected when not under tension.

Vertical Upwards	0.2g
Vertical Down	Not Considered

Forward	0.8g
Aft	0.5g
Lateral	0.5g

Figure 3.1. Ground Transport Directional Accelerations.



Tiedown restraining devices consist of the following:

Synthetic webbing	Chain	Clamps and latches
Webbing ratchet	Wire rope	Grab hooks
Shackles	D-rings	Binders

To identify a tiedown for a load in the forward direction, first determine the load on the restraint device in the forward direction by using a summation of forces to determine tiedown device load.

Accelerating Mass x 0.8g = Forward load.

Repeat the calculation for the other directional accelerations. Use the forward load to choose a tiedown device by finding a tiedown restraint with a manufacturer rated working load greater than or equal to the calculated load. This criterion is derived from MIL-HDBK-1791 and MIL-STD-209 and commercial ground transport standards.

3.19.3. Air Transport Requirements. Air transport envelopes are based on directional accelerations (refer to Figure 3.1). Each directional load is evaluated to the material ultimate strength (breaking strength) statically and independently with a safety factor of 1.5 applied. Fiber straps are not permitted for air transport.

Vertical Upwards	3.7g	Note: Effectively 2.7g when opposing gravity
Vertical Down	4.5g	Note: This includes standard gravity of 1g, otherwise 3.5g.
Forward	3.0g	
Aft	1.5g	
Lateral	1.5g	

To identify a tiedown for a load in the forward direction, first determine the load on the restraint device in the forward direction by using a summation of forces to determine tiedown device load.

$$Accelerating\ Mass \times 3.0g \times 1.5 = Forward\ Load$$

Repeat the calculation for the other directional accelerations. Use the forward load to choose a tiedown device by finding a tiedown restraint with an ultimate strength greater than or equal the calculated load. This criterion is derived from MIL-HDBK-1791 and MIL-STD-209 and commercial transport standards.

Notes for both load conditions.

*Any safety factors associated with industry such as is used by the National Association Chain Manufacturers guidelines are based on the variance and manufacturing tolerances of the items to guarantee the item can meet the working load. Secondary safety factors are not to be included in the derivation of proper tiedown device sizing.

3.19.4. Ensure reaction forces on aircraft floor, pallet or trailer deck do not exceed the rated capacity for those items. Ensure that all tiedown points (e.g., tiedown rings) do not exceed their rated capacity.

3.19.5. Cargo restraint configurations shall be compatible with weapon design to prevent inadvertent activation of environmental sensing devices.

Chapter 4

EVALUATION CRITERIA FOR NUCLEAR WEAPON SYSTEMS

Section 4A—General Philosophy and Criteria.

4.1. Criteria Applicability. This chapter outlines the minimum evaluation criteria engineering agencies shall apply to combat aircraft, missiles, subsystems, technical order procedures, and facilities to include facility systems and subsystems before AFSC/SEWN shall 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 shall 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 shall 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 shall determine the adequacy of proposed and completed designs, surveys, tests and analyses to meet nuclear safety requirements.

4.1.2. Evaluation Source Data.

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

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. Tests or analyses (or both) may be used to establish that numerical design criteria as defined in AFI 91-107 are met. However, demonstrating by test or analysis that a numerical criterion is satisfied is not sufficient in itself 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, shall 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. System and Subsystem Hazards Analysis. From the conceptual through post design 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.

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

4.1.4.3. Fault Hazard Analysis. This analysis starts during the demonstration and validation phase. It provides component-level information on failure modes, effects, causes and common-cause susceptibilities within a given subsystem. The information is used in fault-tree and common-cause analyses.

4.1.4.4. 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.

4.1.4.5. 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**.

4.1.4.6. 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.

4.1.4.7. Circuit Logic Analysis. Conduct a circuit logic analysis during developmental and post design 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.

4.1.4.8. Bent Pin Analysis. If not covered by any other analysis, perform a bent pin analysis to verify pin assignments and power sources designed according to paragraph **2.16.1**. This analysis shall evaluate the likelihood of critical functions occurring due to bent connector pins.

4.1.4.9. Safety Testing. When required by the system, subsystem, equipment failure modes and effects analysis, perform the following safety validation tests and consider them an integral part of the development and acceptance tests or the demonstration tests:

4.1.4.9.1. Laboratory tests, functional mockups, models or simulations to demonstrate partial verification of safety characteristics or procedures.

4.1.4.9.2. Safety tests on devices and components associated with critical functions to determine the degree of hazard or margin of safety.

4.1.4.9.3. Induced failure tests to demonstrate the failure mode(s) of components associated with critical functions.

4.1.4.9.4. Evaluations of support equipment for nuclear logistics movement and ground mobile combat delivery vehicles according to **Chapter 5**.

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 environmental requirements for each nuclear weapon system from the predicted normal and credible abnormal operational environments. Consider all possible environments with the goal of preventing an adverse response under all conditions.

4.1.7.1. Nuclear Weapon Systems. Use the STS as the basic document to define operational environments, both normal and credible abnormal, for nuclear 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-HDBK-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.

Section 4B—Automata, Software, Firmware and Hardware Generated Using Software.

4.2. Criteria Applicability. All automata, software, firmware and integrated circuits generated using software that receives, stores, processes, or transmits data to monitor, target, prearm, arm, launch, release or authorize the use of a nuclear weapon shall comply with the design and evaluation criteria specified in AFMAN 91-119. An example of an integrated circuit being generated using software is the use of Very-High-Speed Integrated Circuits (VHSIC) Hardware Description Language (VHDL) to design, simulate and synthesize an Application Specific Integrated Circuit (ASIC).

4.2.1. Circuitry Designed with Automated Tools. Critical circuitry designed with automated tools (e.g. synthesized from VHDL) shall be verified IAW AFMAN 91-119.

4.2.2. Reprogrammable Circuitry. Reprogrammable circuitry (e.g. the contents of a Field Programmable Gate Arrays (FPGA) shall be protected IAW AFMAN 91-119.

4.2.3. Circuits with Embedded Software. Critical circuits with embedded software or firmware are subject to AFMAN 91-119.

4.2.4. Electronic Circuits Controlling Critical Signals or Performing Critical Functions. The integrity of critical functions implemented with electronic circuits must be protected as delineated in AFMAN 91-119.

4.2.5. Programmable Logic Devices. Critical circuitry incorporating FPGA's or other logic devices subject to single event upset shall employ redundancy or other discipline to protect the integrity of the critical function for all credible environments of the circuits IAW AFMAN 91-119. Reliability goals specified in AFI 91-107 are sufficient for systems incorporating programmable logic devices.

Section 4C—Electrical Subsystems and Hazards.

4.3. Criteria Applicability. In addition to the weapon system evaluation requirements of paragraph **4.4** and Section 4H accomplish these additional electrical subsystem analyses:

4.3.1. Electromagnetic Radiation (EMR) Evaluation Requirements. DoDD 3222.3-AFPD 33-5, *DoD Electromagnetic Environmental Effects (E3)* and outline 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 shall produce data that cover EMR hazards to electro-explosive, semiconductor and other devices. The evaluation shall include these data as a minimum:

4.3.1.1. Data attesting to system design adequacy to the effects of static electricity, EMC, EMI, external EMR 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 tests and analyses required to ensure compliance with the electrical isolation of the unlock, release, launch and AMAC circuits.

Section 4D—Arming and Fuzing (A&F) Systems.

4.4. Criteria Applicability. These criteria supplement the aircraft or missile system evaluation criteria. The evaluation of the A&F subsystem design shall include:

4.4.1. A&F System Devices and Safety Features. The A&F subsystem evaluation shall 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 shall identify any component failure modes that could contribute to premature prearming or arming. For each 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 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.

4.4.2.5. Consider the use of Sneak Circuit Analysis to determine hidden design faults.

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:

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

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

4.4.3.3. Premature nuclear detonation after the system is armed.

Section 4E—Ground-Launched Missile Systems.

4.5. Criteria Applicability. The design evaluation of ground-launched missile systems shall ensure nuclear safety and security requirements are met. When the implementation of system or equipment specifications shall result in hazards, the system manager shall 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 this analysis.

4.5.1. Analysis of Susceptibility to Unauthorized Launch (UL). Perform an analysis of the nuclear weapon system's UL susceptibility according to AFI 91-106, *Unauthorized Launch and Launch Action Studies*. 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.

Section 4F—Aircraft and Air-Launched Missiles.

4.6. Criteria Applicability. The design evaluation of aircraft and air-launched missile systems shall ensure nuclear safety and security requirements are met. When the implementation of system or equipment specifications shall result in hazards, the system manager shall 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 the following:

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 shall 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 (where applicable) shall integrate the general analyses (refer to paragraph **4.1**); automata and software analyses IAW AFMAN 91-119; electrical subsystem assessment (refer to paragraph **4.3**); A&F subsystem requirements (refer to paragraph **4.4**); test equipment analysis requirements (refer to paragraph **4.7**); and Nuclear Weapon Maintenance, Handling and Storage Facilities analysis requirements (refer to paragraph **4.8**). The integrated system evaluation shall also include these analyses and documentation:

4.6.2.1. Nuclear System Definition. The evaluation shall document a listing of all critical function software and assemblies, wires, connectors and other hardware that, when considered totally, define the 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 Analysis. The integrated assessment shall 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 shall 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 shall 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) shall verify the capability of the AMAC and release systems to meet these design requirements: voltage, current, switching characteristics, signal timing and sequencing, worst load conditions and digital communication 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 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, *General Specification for Testing, Store Suspension and Release Equipment*, or determined by flight conditions, whichever is more stringent.

Section 4G—Test Equipment.

4.7. 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.

4.7.1. 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.

4.7.2. Evaluation Criteria. In addition to the customary industrial standards, the Air Force evaluation agency shall 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.

4.7.2.1. Environmental Tests. Verify the ability of the test equipment to perform its intended function in all environmental conditions identified in paragraph **4.1.7**

4.7.2.2. Required Analyses.

4.7.2.2.1. Circuit analyses of the tester operating with the circuits of the equipment to be tested.

4.7.2.2.2. Failure modes, effects and criticality analysis of the test device to ensure faults within the device shall not degrade the nuclear safety of the equipment to be tested.

4.7.2.2.3. Analysis of the tester interface with the weapon system to verify the test concept.

4.7.2.2.4. Perform a compatibility fit-and-function demonstration to ensure the mechanical and electrical designs are both compatible with the weapon system to be tested.

4.7.2.2.5. Demonstrate operations and procedures at the field level and take appropriate corrective action in problem areas. Verify each applicable section of each procedural document.

4.7.2.2.6. 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.

Section 4H—Nuclear Weapon Maintenance, Handling and Storage Facilities.

4.8. Criteria Applicability. These criteria apply to new and existing facilities that maintain, handle and store nuclear weapons.

4.8.1. Evaluation Criteria. The following systems shall meet customary standards to include the following criteria:

4.8.1.1. LPS. Verify system compliance with NFPA 780, AFMAN 91-201, AFI 32-1065 and UFC 3-520-01.

4.8.1.2. Default Safe Separation Distance (SSD). If the facility (either above ground or underground) is capable of supporting intrusive maintenance operations, implementation plans and procedures for ensuring compliance with the 7-foot rule shall be documented. Verify a default Safe Separation Distance of 7 feet is maintained between a weapon and the walls, ceiling, hoists, structural supports and metallic conductors of the facility in accordance with AFMAN 91-201. This is commonly referred to as the "7-foot rule". Verify that a physical demarcation (e.g., paint or tape) is readily visible and clearly indicates the area in which intrusive maintenance operations can be accomplished. Verify overhead hoists have a designated parking area outside the 7-foot stand-off area, away from where maintenance operations are conducted when hoists are not in use.

4.8.1.3. Alternative to 7-Foot Standoff. Validate the characterization process and its derived SSD by the following measures:

4.8.1.3.1. Verify the Faraday-like Shield boundary of the facility based on facility construction.

4.8.1.3.2. Verify upgraded or additional bonding of all metallic penetrations has been correctly installed at the point of entry to the defined Faraday-like Shield using a methodology approved by the AHJ prior to implementation. Verify bond lengths have been kept as short as practical, ideally less than 4 inches (if possible/practical) and goes downward from the penetration to the Faraday-like Shield. Where bond lengths exceed 4 inches in length, verify that additional calculations of impedance, voltage and side flash have been correctly applied to determine the final SSD.

4.8.1.3.3. Verify appropriate high capacity surge suppression has been installed on all incoming electrical power conductors and on low voltage systems. When it has been determined it is not practical to install high capacity suppression on communications and data circuits, verify adequate alternatives and evaluations approved by the AHJ are in place to assure the possibility of the lightning energy entering the facility through these conductors has been mitigated.

4.8.1.3.4. Verify transfer impedance testing of the facility has been accomplished and the Faraday-like Shield characteristic has been validated. Verify the appropriate SSD has been determined from the bond impedance calculations or the transfer impedance testing.

4.8.1.4. Facility Power Systems. Verify facility power systems; including all auxiliary power systems have the capacity to supply adequate power to subsystems that maintain safety or security of nuclear weapons. Verify the auxiliary power system(s) are available in the event of a primary power system failure and have the capability to supply adequate power.

4.8.1.5. Fire Protection Systems. Conduct a FHA to comprehensively and qualitatively assess compliance with NFPA 13. The FHA shall include an analysis for criticality potential as well as other concerns (refer to T.O. 11N-20-11, *General Firefighting Procedures*). Conduct the FHA in sufficient detail to insure the safety of weapons and to provide baseline documentation to AFSC/SEWN and AFNWC. For existing facilities, completion of the FHA is required within three years of the implementation of this AFMAN.

4.8.1.6. Hoist, Cranes and Similar Devices. Refer to the evaluation criteria in **Section 5C.**

4.8.1.7. Security Systems. Security system designs shall be evaluated from a systems engineering perspective to identify the potential impact to the safety of nuclear weapons and to ensure compatibility (to include EMR) with nuclear weapons. For security systems that control access to nuclear weapons, an unauthorized access analysis shall be conducted to ensure the possibility of unintended or deliberate unauthorized access is adequately mitigated through a combination of design and procedural means.

4.8.1.8. Facility Security System Automata and Software. Evaluate software that is unique and developed specifically to control essential facility systems IAW AFMAN 91-119.

4.8.1.9. Blast Containment/Isolation Features. Evaluate blast containment and isolation features to verify compliance with AFMAN 91-201 *Explosive Safety Standards* and DoDD 6055.9E. Additionally, verify the design mitigates contamination of facilities and weapons by limiting radiation transport mechanisms such as explosions, blasts and fires. Verify blast isolation of the facility incorporates blast zones/areas for the purpose of limiting the spread of contamination and consequential damage to the facility and stored critical assets. Evaluate the blast zones/areas to determine if they are separated from each other by barriers capable of withstanding explosions commensurate with the maximum credible event.

4.8.1.10. Electromagnetic Radiation (EMR) Environment. Verify the EMR survey is current and documents the levels of EMR within each facility. If EMR levels of intentional or unintentional emitters can exceed weapon STS levels, insure mitigation measures reduce the EMR levels to within STS requirements (IAW AFMAN 91-201, chapter 9). Conduct the EMR survey in sufficient detail to insure the safety of weapons and to provide baseline documentation to AFSC/SEWN and 498NSG. Changes to the baseline configuration shall be evaluated either through testing or analysis to determine the EMR impact on the weapon STS levels. Completion of the EMR survey is required within three years of the implementation of this AFMAN. The 85th Engineering Installation Squadron at Keesler AFB, MS is the AF Center of expertise with respect to EMR and EMR surveys.

4.8.1.10.1. The EMR Environment (EMRE) survey shall:

4.8.1.10.1.1. Accomplish discrete tests of all unintentional EMRE emitters utilized in close proximity to critical equipment interior to the facility. These unintentional EMRE emitters include but are not limited to fluorescent lighting; motors; hand tools; computers and monitors; communication equipment such as phones and intercoms; entertainment devices such as TV's, radios, fire alarm control panels, and CD players.

4.8.1.10.1.2. Accomplish discrete tests of all intentional EMRE emitters utilized in close proximity to critical equipment within the facility. These intentional EMRE emitters include but are not limited to computers using wireless devices or networks, radio transmitters, motion sensors, and loss antenna distribution systems.

4.8.1.10.1.3. Accomplish ambient level measurements of representative areas and measurements of specific classes of emitters utilized in close proximity to critical equipment.

4.8.1.10.1.4. Perform an external ambient survey outside of the facility to obtain an overview of the typical EMRE levels encountered in the nearby area.

4.8.1.10.1.5. Accomplish an evaluation and analysis of the results to determine compliance with AFMAN 91-201 or identify compatibility anomalies and recommendations for mitigating these anomalies.

4.8.1.10.2. EMRE Studies for New Facilities:

4.8.1.10.2.1. Conduct an analysis of anticipated EMRE emitters using straw man data to project EMRE levels that could be expected and adjust facility design, equipment selection and/or procedures to reduce EMRE levels if necessary.

4.8.1.10.2.2. Conduct a complete EMRE survey as described above to insure actual levels are below necessary values upon activation.

4.8.1.11. Radiation Monitoring. Verify the radiation monitoring adequately and accurately records the levels of both plutonium and tritium within the environment placed. Verify the design works in conjunction with other facility systems, especially the blast containment/isolation system, HVAC systems, and the fire alarm and suppression systems and minimizes collateral effect to the rest of the facility as well as the local environment.

Chapter 5

EVALUATION CRITERIA FOR NONCOMBAT DELIVERY VEHICLES AND SUPPORT EQUIPMENT

Section 5A—General Philosophy and Criteria.

5.1. Criteria Applicability. 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 shall consist of analysis, examination and testing (as appropriate) by the responsible Air Force agency. Good industrial design practices, standards and features can be used to substantiate nuclear safety design certification of any commercially designed non-specialized equipment as identified in AFI 91-103. Equivalent non-US standards (i.e. European Specifications and Approvals) may be used in lieu of the listed US standards.

5.2. First Article Verification. Use one or more of the following methods to prove the adequacy of the prototype structural design (refer to 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 (refer to paragraph **3.3**):

5.2.2.1. Use the verified rated load multiplied by a factor of 3 for the design load test.

5.2.2.2. Apply the lateral and longitudinal test loads statically with the equipment loaded to its rated capacity and apply the vertical test load statically and independently.

5.2.2.3. 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 to the test article along the appropriate axis until the item exhibits a primary failure mode (refer to paragraph **3.3**). The test loads at this point shall exceed the design load in each appropriate axis.

Section 5B—Ground Transportation Equipment.

5.3. Criteria Applicability. In addition to the criteria in paragraphs **5.1** and **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.

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

5.3.2.2. Perform an analysis to ensure the equipment meets the minimum roadability requirements specified in the STS, CDD, CPD or weapon system specifications.

5.3.2.3. 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.

5.3.2.4. Test brake systems while transporting or towing simulated loads that represent the maximum operational load expected in service, such as maximum weight and extreme center of gravity.

5.3.3. Environmental and General Hazard Evaluations.

5.3.3.1. Analyze the equipment to minimize the potential for fire propagation.

5.3.3.2. Test or analyze the equipment to ensure mechanical shock transmission to the nuclear weapon is within weapon design tolerances.

5.3.3.3. Test tiedown provisions for ground movement of nuclear weapons to verify the equipment's capability to restrain the design load.

5.3.3.4. 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.

5.3.3.5. Perform tests or analyses to determine if the equipment has adequate provisions for static grounding.

5.3.3.6. Inspect the equipment to ensure rated load and gross vehicle 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-HDBK-1784.

5.4.2. Parking Brakes. Test parking brakes to verify the parking brake system capability to hold the vehicle on an 11.5-degree incline when headed either up and down for a minimum of 15 minutes each.

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

5.4.3.1. Distance from the point of tow bar disengagement to final stop.

5.4.3.2. Lateral distance of travel from the point of tow bar disengagement to final stop.

5.4.3.3. Attitude of the trailer at the time of stop.

5.4.3.4. Damage incurred by the trailer or load as a result of disengagement.

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

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

5.5.1. Vehicle and Brake Performance. Accomplish the following tests with the maximum operational load of tow and towed vehicles to verify functional compatibility:

5.5.1.1. Evaluate the towing vehicle performance to ensure it does not have tendencies to tip, tilt, yaw, sway, skid or jackknife under maximum performance maneuvers.

5.5.1.2. Ensure brake performance meets the requirements of the applicable industry standards. 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 safe speed. 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). If deemed necessary, 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 both up and down, for a minimum of 15 minutes each.

5.5.3. Tow Vehicle to Trailer Interconnect Device. Test the vehicle connecting device to ensure compliance with the structural design criteria (refer to 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 shall only operate in neutral, park or with the clutch disengaged (as applicable).

5.5.6. Vehicle structure. Verify that maximum operational loads from the towed trailer or tow bar do not exceed stress levels in paragraph **3.2.3**.

5.6. Self-Propelled Vehicles. In addition to the general test and analysis requirements, subject non-towed vehicles to a 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 (refer to paragraph **5.2**), subject rail-based vehicles to these tests and analyses:

5.7.1. Brake System Verification. Test the brake system 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 shall 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. Lift System. Conduct these demonstrations:

5.8.1.1. 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.

5.8.1.2. Tine and adapter compatibility with the rated load center of gravity in the worst-case environment to which the vehicle shall be subjected.

5.8.2. Movement and Positioning Controls. Conduct these demonstrations:

5.8.2.1. Safe control, consistent with the STS, of the rated load shall be maintained if electrical, hydraulic or pneumatic system failure occurs.

5.8.2.2. Appropriate movement controls are self-centering.

5.8.2.3. Positive control of nuclear weapons is maintained in all operations. If used, test the attachment points and straps.

5.8.2.4. Capability for small increments of movement compatible with required usage.

5.8.2.5. Over travel prevention capability.

5.8.2.6. Capability to uniformly control lifting attitude.

5.8.3. 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.

Section 5C—Hoists, Cranes and Similar Devices

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

5.9.1. Positive Control Features. Test the device at not less than 100 percent or more than 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 over travel 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—Air or Ground Transport Systems, General Use Tiedowns and Restraints.

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

5.15. Cargo Restraint 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 shall 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 at not less than 100 percent or more than 125 percent of the rated capacity.

5.20. Forms Adopted. AF Form 847, *Recommendation for Change of Publication*.

FREDRICK F. ROGGERO, Maj Gen, USAF
Chief of Safety

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD Directive 3150.2, *DoD Nuclear Weapon System Safety Program*, Dec 23, 1996

DoD Directive 3222.3-AFPD33-5, *DoD Electromagnetic Environmental Effects (E3)*, Sep 8, 2004

DoD Directive O-5210.41, *Security Policy for Protecting Nuclear Weapons*, Nov 1, 2004

DoD Directive (S) 5210.81, *United States Nuclear Weapons Command and control, Safety, and Security*, Aug 8, 2005

DoD Directive 6055.9E, *Explosives Safety Management and the DoD Explosives Safety Board*, Aug 19, 2005

NFPA 13, *Standard for the Installation of Sprinkler Systems*, 2007

NFPA 70, *National Electrical Code*, 2008

NFPA 780, *Standard for the Installation of Lightning Protection Systems*, 2008

AFI 32-1063, *Electrical Power Systems*, Jun 10, 2005

AFI 32-1065, *Grounding Systems*, Oct 1, 1998

AFI 63-125, *Nuclear Certification Program*, Mar 15, 2004

AFI 63-1201, *Life Cycle Systems Engineering*, Jul 23, 2007

AFI 91-103, *Air Force Nuclear Safety Design Certification Program*, Sep 16, 2005

AFI 91-106, *Unauthorized Launch and Launch Action Studies*, Nov 23, 1993

AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*, Apr 6, 1994

AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software*, Feb 1, 1999

AFMAN 91-201, *Explosives Safety Standards*, Nov 17, 2008

AFPD 91-1, *Nuclear Weapons and Systems Surety*, Feb 13, 2007

MIL-DTL-6458, *Chain Assemblies, Single Leg, Aircraft Cargo Tie Down*, Apr 18, 2008

MIL-DTL-25959, *Tie Down, Tensioners, Cargo, Aircraft*, Jan 19, 2007

MIL-DTL-38999-XX SERIES, *Connector, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded, and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for*, May 30, 2008

MIL-HDBK-1512, *Electro-explosive Subsystems, Electrically Initiated, Design Requirements and Test Methods*, Sep 30, 1997

MIL-HDBK-1784, *Mobility, Towed and Manually Propelled Support Equipment*, Feb 14, 1997

MIL-HDBK-1791, *Designing for Internal Aerial Delivery in Fixed Wing Aircraft*, Feb 14, 1997

MIL-STD-209, *Lifting and Tiedown Provisions*, Feb 22, 2005

MIL-STD-461, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*, Dec 10, 2007

MIL-STD-464, *Electromagnetic Environmental Effects, Requirements for Systems,* Dec 19, 2002

MIL-STD-648, *Design Criteria for Specialized Shipping Containers,* Apr 10, 2008

MIL-STD-704, *Aircraft Electric Power Characteristics*, Dec 30, 2008

MIL-STD-1366, *Transportability Criteria*, Oct 31, 2006

MIL-STD-1553, *Digital Time-Division Command/Response Multiplex Data Bus*, Jan 15, 1996

MIL-STD-1760, *Aircraft/Store Electrical Interconnection System*, Oct 24, 2007

MIL-T-7743, *Testing, Store Suspension and Release Equipment, General Specification for,* Sep 15, 1999

SAE-AS8090, *Equipment, Towed Aerospace Ground, Mobility*, Sep 17, 1997

SAE-AS8905, *Fittings and Cargo Rings, Tie-Down, Aircraft Floor*, Sep 7, 1999

UFC 3-520-01, *Interior Electrical Systems*, Jun 10, 2002

Abbreviations and Acronyms

A/D—Arm/Disarm

A&F—Arming and Fuzing

AF—Air Force

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFNWC—Air Force Nuclear Weapons Center

AFSC—Air Force Safety Center

AHJ—Authority Having Jurisdiction

AMAC—Aircraft Monitoring and Control

BITE—built-in test equipment

CDD—Capability Development Document

COTS—commercial off-the-shelf

CPD—Capability Production Document

dB—decibels

DoD—Department of Defense

DOE—Department of Energy

EED—electro-explosive devices

EFS—essential facility subsystems

EMC—electromagnetic compatibility

EMI—electromagnetic interference

EMR—electromagnetic radiation

E/TSD—Environmental or Trajectory Sensing Device

FHA—Fire Hazards Analysis

FPGA—field programmable gate arrays

GHz—gigahertz

HDBK—Handbook

HVAC—heating, ventilating, air-conditioning

IAW—in accordance with

kHz—kilohertz

LCP—Launch Control Point

LP—Launch Point

LPS—Lighting Protection System

MAJCOM—Major Command

MIL HDBK—military handbook

MUX—multiplexed

W/m2—milliwatt per square meter

NFPA—National Fire Protection Association

PAL—permissive action link

S&A—safe and arm

SAE—Society of Automotive Engineers

SSD—Safe Separation Distance

SMS—stores management system

STS—Stockpile-to-Target Sequence

TDM—Time-Division Multiplexing

TO—technical order

TPD—Terminal Protective Devices

UFC—United Facilities Criteria

UL—Unauthorized Launch

USG—Unique Signal Generator

VHSIC—Very-High-Speed Integrated Circuits

VHDL—VHSIC Hardware Description Language