NOT MEASUREMENT SENSITIVE

MIL-STD-1822(USAF)
30 SEPTEMBER 1994

MILITARY STANDARD

NUCLEAR CERTIFICATION OF WEAPON SYSTEMS, SUBSYSTEMS, AND ASSOCIATED FACILITIES AND EQUIPMENT

AMSC: F7041

FSC: 11GP

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

FOREWORD

1. This Military Standard is approved for use by the Aeronautical Systems Center, Department of the Air Force and is available for use within the distribution limitations noted on the cover page.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: SA-ALC/NWIL, ATTN: Logistics Management Data Division, Kirtland Air Force Base NM 87117-5617 by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. The purpose of this standard is to provide uniform design requirements to assure weapon system operational capability and compliance with the Department of Defense (DOD) Nuclear Weapon System Safety Standards.

4. This military standard is structured and formatted to facilitate tailoring requirements to the specific system needs. Each system program office is encouraged to selectively apply and tailor these requirements during the acquisition process.

CONTENTS

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

CONTENTS (Contd.)

1. SCOPE

1.1 Scope. This military standard establishes the design requirements for weapon systems, subsystems and associated facilities and equipment nuclear certification. Requirements for evaluation and reporting for nuclear certification are also established.

1.2 Applicability. This military standard applies to Air Force nuclear weapon systems, including their critical functions and components, ground handling and transportation equipment, support equipment, test equipment, and technical orders. Modified portions of nuclear weapon systems, equipment, hardware, and software will also comply with this military standard. This military standard complements proposed Air Force Materiel Command Pamphlet 80-5, Nuclear Certification Plan (NCP), which describes nuclear certification tasks for all weapon systems. The safety analysis requirements, interface specification testing, and technical order development required for nuclear certification by this military standard will be a significant portion of the nuclear certification plan tasks for a given weapon system nuclear certification.

1.3 Application and tailoring guidance.

1.3.1 Applying requirements. Requirements described in this military standard are to be applied in Air Force nuclear weapon system procurements, requests for proposals, statements of work, and Government in-house developments requiring nuclear certification programs for the development, production, and initial deployment of weapon systems and associated facilities and equipment. Although this military standard provides specific nuclear certification requirements, it may be necessary to tailor this military standard to accommodate unique characteristics of a particular weapon system.

1.3.2 Tailoring of requirements. Requirements are to be tailored—by the engineering organization as required by governing documents and as appropriate—to particular systems or equipment depending on the program type, magnitude, and funding. In tailoring the requirements, the detail and depth of the effort is defined by the managing engineering organization and incorporated in the appropriate contractual documents. Also, each program will specify which requirements in this military standard are binding for their specific system design.

Further tailoring guidance is found in the appendix.

1.3.3 Application guidance to the procuring agency. All proposed tailoring and rationale for modifying requirements of this military standard to address unique aspects of the weapon system are recommended to be reviewed by the San Antonio Air Logistics Center, Nuclear Weapons Integration Division (SA-ALC/NWI). Since the proposed tailoring/modifications could have a nuclear safety impact, the procuring agency should formally request a review by the Directorate of Nuclear Surety, Headquarters Air Force Safety Agency (HQ AFSA).

2. APPLICABLE DOCUMENTS

2.1 Government documents

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DoDISS) and supplement thereto, cited in the solicitation (see 6.2).

SPECIFICATIONS

Federal

AA-D-600	Door, Vault, Security

Military

MIL-W-5088	Wiring, Aerospace Vehicle
MIL-T-7743	Testing, Store Suspension and Release Equipment, General Specification for
MIL-C-38999	Connector, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded, and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for

STANDARDS

Military

MIL-STD-209	Slinging and Tiedown Provisions for Lifting and Tying Down Military Equipment
MIL-STD-461	Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference
MIL-STD-462	Electromagnetic Interference Characteristics, Measurement of
MIL-STD-648	Design Criteria for Specialized Shipping Containers
MIL-STD-704	Aircraft Electrical Power Characteristics
MIL-STD-810	Environmental Test Methods and Engineering Guidelines
MIL-STD-882	System Safety Program Requirements
MIL-STD-1366	Transportability Criteria
MIL-STD-1512	Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
MIL-STD-1553	Digital Time Division Command/Response Multiplex Data Bus
MIL-STD-1757	Lightning Qualification Test Techniques for Aerospace Vehicles and Hardware
MIL-STD-1760	Aircraft/Store Electrical Interconnection System

MIL-STD-1773	Fiber Optic Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus
MIL-STD-1784	Mobility, Towed & Manually Propelled Support Equipment
MIL-STD-1791	Designing for Internal Aerial Delivery in Fixed Wing Aircraft
MIL-STD-1795	Lightning Protection of Aerospace Vehicles and Hardware
MIL-STD-1801	User/Computer Interface
MIL-STD-1818	Electromagnetic Effects Requirements for Systems
MIL-STD-2088	Bomb Rack Unit (BRU), Aircraft, General Design Criteria for
DOD-STD-2167	Defense System Software Development
DOD-STD-2169	(C) Electromagnetic Pulse (U)

HANDBOOKS

Military

MIL-HDBK-5	Metallic Materials and Elements for Aerospace Vehicle Structures

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Standardization Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, phone (215) 697-2667.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

Air Force Instructions and Regulations

AFR 8-2	Air Force Technical Order System
AFI 91-101	The Air Force Nuclear Weapon Surety Program
AFI 91-102	Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules
AFI 91-103	The Air Force Nuclear Safety Certification Program
AFI 91-104	Nuclear Surety Tamper Control and Detection Programs
AFI 91-105	Critical Components
AFI 91-106	Unauthorized Launch and Launch Action Studies
AFI 91-107	Safety Design and Evaluation Criteria for Nuclear Weapon Systems
AFR 205-1	Information Security Program Regulation
AFR 207-1	(C) Air Force Physical Security Program (U)

(Copies of Air Force regulations (AFR) are available from the Air Force Publications Distribution Center, 2800 Eastern Boulevard, Baltimore, MD 21220; phone (410) 687-3330/DSN 584-4529.)

Air Force Materiel Command Pamphlets

AFMCP 80-5

Air Force Technical Orders

TO 00-5-1	AF Technical Order System
TO 00-5-2	Technical Order Distribution System
TO 00-5-3	Air Force Technical Manual Acquisition Procedures

(Air Force Technical Orders are available from Oklahoma City Air Logistics Center, OC-ALC/MMEDT, Tinker AFB, OK 73145-5990; phone (405) 736-3771/DSN 336-3771.)

Air Force System Command Design Handbooks

AFSC DH 1-4	Electromagnetic Compatibility
AFSC DH 1-12	Nuclear Weapon Systems Design Handbook

(Copies of AFSC Design Handbooks are available from ASC/ENOSD, Bldg. 126, 2664 Skyline Dr., Wright-Patterson AFB, OH 45433-7800, phone (513) 255-6281/DSN 785-6281.)

AMAC POG Interface Specifications and Standards

Drawing No. 1001-01	System 1 AMAC Systems Specification
Drawing No. 2001-01	System 2 Interface Standard
Drawing No. 2001-02	System 2 AMAC Systems Specification
Drawing No. 173837	Basic Design Specification, Bomber System A (Obsolete for new design)
Drawing No. 173838	Basic Design Specification, Fighter System A (Obsolete for new design)
Drawing No. 185435	PAL Fighter A (Obsolete for new design)
Drawing No. 185475	Basic Interface Requirement, System 1
Drawing No. 186990	Basic Design Specification, PAL Fighter System B (Obsolete for new design)
Drawing No. 306562	Cat D PAL AMAC Requirements

(Copies of AMAC POG Interface Specifications and Standards are available from SA-ALC/NWI, Kirtland AFB, NM 87117.)

Department of Defense Directives, Instructions, and Administrative Publications

DODD 3150.2	Safety Studies and Reviews of Nuclear Weapon Systems
DOD 5200.1-R	Information Security Program Regulation
DODD 5210.41	Security Policy for Protecting Nuclear Weapons
DOD 5210.41-M	(C) Nuclear Weapon Security Manual (U)

(Copies of DOD Directives are available from the National Technical Information Service, 5825 Port Royal Road, Springfield, VA 22161; phone (703) 487-4650.)

Base and Installation Security System Specification

BIS-SYS-10000	General System Specification for the DOD Base and Installation Security System (BISS)

(Copies of this specification are available from ESC/AVJ, 20 Shilling Circle, Hanscom AFB, MA 01731-2816; phone (617) 377-8852, DSN 478-8852.)

Federal Motor Carrier Safety Regulations

393.43	Breakaway and Emergency Breaking
393.52	Brake Performance

(The Federal Motor Carrier Safety Regulations can be obtained by ordering Code of Federal Regulations, Title 49, Parts 200-399 from the Superintendent of Documents, Government Printing Office, North Capitol and H Streets, NW, Washington, DC 20402; phone (202) 783-3238. Copies of individual FMCSR's may be obtained from the Federal Highway Administration, Office of Motor Carrier Standards, phone (202) 366-1790 or from a library that has the Code of Federal Regulations.)

2.2 Non-Government publications. The following document(s) form a part of this standard to the extent specified herein. Unless otherwise specified, the issues of the documents which are DoD adopted are those listed in the issue of the DoDISS specified in the solicitation. Unless otherwize specified, the issues of documents not listed in the DODISS are the issues of the documents cited in the solicitation (see 6.2).

Underwriters Laboratory

UL 768-84	Lock, Combination, Standard for

(Non-Government standards and other publications are normally available from the organizations that prepare or distribute the documents. These documents also may be available in or through libraries or other information services.)

2.3 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 General definitions

3.1.1 Abnormal environment. Those environments in which the weapon or combat delivery vehicle is not expected to retain full operational reliability. Abnormal environments are considered to be synonymous with credible abnormal environments for the purpose of this standard. *See* **Credible abnormal environment.**

3.1.2 Access. Proximity to a nuclear weapon or critical component in a manner such that the opportunity exists to tamper with or damage a nuclear weapon or critical component when such tampering or damage could go undetected upon completion of the task being performed. Normally, a person would not be considered to have access if he or she is part of a Two-Person Concept Team or is properly escorted.

3.1.3 Accidental motor ignition. The accidental initiation or propulsive burning of a missile stage motor, including the post boost vehicle, from causes other than the propagation of a launch sequence. Non-propulsive burning or explosion is not considered accidental ignition.

3.1.4 Aircraft monitor and control. Equipment installed in aircraft to permit monitoring and control of safing, prearming, arming, and fuzing functions of nuclear weapons or nuclear weapon systems.

3.1.5 Air Force nuclear weapons surety program. A program consisting of Air Force policies, procedures, and safeguards used to comply with the Department of Defense Nuclear Weapon System Safety Standards (*see* 3.28). It is made up of elements addressing the safety and security of nuclear weapons and nuclear systems. These elements of nuclear surety enhance the overall reliability of nuclear weapon systems throughout their stockpile-to-target sequence.

3.1.6 Allied-operated nuclear weapon system. A nuclear weapon system used by an allied nation with United States nuclear weapons in Air Force custody.

3.1.7 Arm/disarm device. A mechanical or electromechanical device that provides a positive interruption of the ordnance firing circuit(s) to prevent initiation of an explosive or pyrotechnic train prior to the device's commanded closure.

3.1.8 Armed. The configuration of a nuclear weapon in which a single signal will initiate the action required for obtaining a nuclear detonation.

3.1.9 Armed component. A weapon component is armed when it has responded to a stimulus to change its state to enable a nuclear detonation.

3.1.10 Arming and fuzing system. Those components, devices, and design features which cause weapon/warhead prearming, arming, fuzing, and detonation, including components and design features which protect against unauthorized deliberate or accidental prearming, arming, fuzing, and detonation. The arming and fuzing system is comprised of both Department of Defense and Department of Energy systems.

3.1.11 Authorization. Those functions, procedures, and stimuli which must occur prior to:

a. Prearming and arming a nuclear weapon and

b. Launching or releasing a nuclear weapon system.

3.1.12 Authorization device. A device which prohibits prearming, arming, launching, or releasing until authorization stimuli, provided under the information control concept, are validated.

3.1.13 Automata. A class of sequential machines which, by alteration of their internal state, are capable of performing logical, computational, or repetitive routines. Examples include automatic processors, microprocessors, computers, decoders, controllers and, where specifically designated, their associated peripheral equipment.

3.1.14 Buckling failure. A failure exhibited by excessive rapid deformations (collapse) with a loss of operational capability.

3.1.15 Certified critical component. A critical component that has successfully completed its operational certification/recertification in accordance with approved procedures.

3.1.16 Code component. Any device, assembly, material, software, or information so designated by the National Security Agency.

3.1.17 Combat delivery vehicle. A vehicle, with its installed equipment and components, used to deliver a nuclear weapon to a target. (Installed equipment includes command and control elements and equipment necessary to launch ground-launched missiles.) A combat delivery vehicle operates as part of a nuclear weapon system covered by approved nuclear weapon system safety rules.

3.1.18 Composite failure. Any composite material failure (such as delamination under compressive load) which may result in weapon damage.

3.1.19 Credible abnormal environment. An environment to which a weapon or weapon system may be exposed that would degrade operational reliability or nuclear safety (or both).

3.1.20 Critical. A function, circuit, or activity which applies directly to, or which controls, the authorization, prearming, arming, releasing, or launching of a nuclear weapon, and the targeting functions of a ground-launched nuclear weapon system.

3.1.21 Critical component. Critical components are those components which, if bypassed, activated, or tampered with, could result in, or contribute to, the unauthorized deliberate or inadvertent actuation of one of the critical functions. A component may be designated critical if it does any of the following:

a. Controls, inhibits, or enables critical functions;

b. Contains critical software;

c. Controls access to a no-lone zone, with or without a weapon;

d. Interfaces directly with a nuclear weapon; or

e. Contains secure code components or processes them.

3.1.22 Critical fault. Any nuclear system malfunction which inadvertently applies control signals or power to the bomb, warhead, or missile propulsion system; degrades the integrity of prearm, launch, or release safety or authorization devices; and could cause unintended issuance of critical-function command signals or result in the inability to determine weapon system status.

3.1.23 Critical functions. The functions listed in the DOD Nuclear Weapon System Safety Standards (*see* 3.28) are critical to nuclear weapon system safety. The functions which are explicitly stated are authorization, prearming, arming, nuclear consent, releasing, or launching of a nuclear weapon. Also, targeting as it pertains to protection of friendly territory is a critical function in missile systems with self-contained guidance.

3.1.24 Current limited. Monitor or test currents which are limited so that the most current that can be delivered to a nuclear weapon for monitoring or testing purposes will be less than that required to operate the most sensitive component in the arming and fuzing system.

3.1.25 Custody. The responsibility for the control of, transfer of, movement of, and access to nuclear weapons and components. Custody also includes accountability for nuclear weapons and components.

3.1.26 Decertification. A process accomplished on those items which through analysis, testing, or operational performance have demonstrated inadequate design safety for nuclear weapon protection.

3.1.27 Design load. The minimum load for attaining the design stress levels. Also, the maximum load which will not result in undesirable structural behavior, such as excessive elastic deformation, material yield, buckling, or fracture.

3.1.28 DOD Nuclear Weapon System Safety Standards. These standards are found in DOD Directive 3150.2, Safety Studies and Reviews of Nuclear Weapon Systems (*See* 2.1.2).

3.1.29 Dynamic load. A load imposed by dynamic action (such as acceleration, vibration, shock, or wind gusts) encountered during normal operation (in normal environments) in which equilibrium is not maintained. To determine the dynamic load, the designer will use the rated load and factor-in the loads and accelerations in all directions encountered during ground and air transport as well as the shock and vibration spectra associated with mate, demate, load, and unload operations.

3.1.30 Elastic failure. Failure within material elastic range characterized by excessive structural deflections which may result in weapon damage.

3.1.31 Electrical isolation. The concept of keeping critical electrical loads separated from their sources of energy until their intended use. Separation of electrical circuits, signals, or data to preclude ambiguity, interference, or altered information. Examples of electrical isolation techniques include physical isolation or use of any property (such as time, phase, amplitude, or frequency) which distinguishes one electrical signal from all others.

3.1.32 Electroexplosive device. An explosive or pyrotechnic component that initiates an explosive, burning, electrical, or mechanical train and is activated by the application of electrical energy.

3.1.33 Electromagnetic compatibility. The ability of telecommunications equipment, subsystems, and systems to operate in their intended operational environments without suffering or causing unacceptable degradation because of electromagnetic radiation or response. Design compatibility is achieved by incorporation of engineering characteristics or features in all electromagnetic radiating and receiving equipment to eliminate or reject undesired signals and enhance operating capabilities. Operational compatibility is achieved by the equipment's ability to ensure interference-free operation. It involves the application of frequency management concepts and doctrines to maximize operational effectiveness.

3.1.34 Electromagnetic interference. Any electromagnetic disturbance which interrupts, obstructs, or otherwise degrades or limits the effective performance of electronic/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like, through wire-to-wire, cable-to-cable, or circuit card coupling.

3.1.35 Electromagnetic pulse. The electromagnetic radiation from a nuclear explosion caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges. It may also be caused by nonnuclear means.

3.1.36 Electromagnetic radiation. Radiation made of oscillating electric and magnetic fields and propagated near the speed of light. It includes gamma, X-ray, ultraviolet, visible, and infrared radiation and radar and radio waves and is generated from radar, communications equipment, microwave, and electronic countermeasures equipment, etc.

3.1.37 Emergency. An unexpected occurrence or set of unexpected circumstances in which personnel or equipment unavailability, due to accident, natural event, or combat, may demand immediate action that requires extraordinary measures to protect, handle, service, transport, or employ a nuclear weapon.

3.1.38 **Engineering evaluation.** A technical assessment of the design and operating features of equipment, whether new or modified, which is conducted for the purpose of determining the impact on nuclear safety.

3.1.39 **Engineering organization.** The organization which has program management responsibilities for acquisition and modification.

3.1.40 **Engineering review.** A review of the nuclear safety engineering evaluation and program documentation; accomplished by an Air Force agency which is independent of the engineering organization.

3.1.41 **Environments.** The natural and induced physical conditions—such as climatic, electrical, mechanical, nuclear, biological and chemical—that a system may be exposed to during its operation.

3.1.42 **Exclusion region.** The region within a warhead or weapon which contains the firing set and weapon detonator system. It also has the necessary packaging and safety devices to exclude electrical energy from the firing set and weapon detonator system, except when their use is intended.

3.1.43 **Explosive ordnance disposal procedures.** Those particular courses or modes of action taken by explosive ordnance disposal (EOD) personnel for access to, diagnosis of, rendering safe of, recovery of, and final disposal of explosive ordnance or any hazardous material associated with an EOD incident.

a. Access procedures. Those actions taken to locate exactly and to gain access to unexploded explosive ordnance.

b. Diagnostic procedures. Those actions taken to identify and evaluate unexploded explosive ordnance.

c. Render safe procedures. The portion of EOD procedures involving the application of special EOD methods and tools to provide for the interruption of functions or separation of essential components of explosive ordnance to prevent an unacceptable detonation.

d. Recovery procedures. Those actions taken to recover unexploded explosive ordnance.

e. Final disposal procedures. The final disposal of explosive ordnance, which may include demolition or burning in place, removal to a disposal area, or other appropriate means.

3.1.44 **Facility lifting and suspension systems.** Equipment (such as a hoist, crane, or suspended frame) installed in a facility, used to lift or support nuclear weapons, and which depends upon the facility's structure to support the rated load.

3.1.45 **Factor of safety.** A numerical value that is multiplied times the operational load to obtain the desired structural capability. This capability should account for uncertainties associated with loads, materials, manufacturing processes, and other conditions that could affect the actual structural capability of an item.

3.1.46 **Fail-safe.** Design features of a nuclear weapon system or component which ensure that the system or component will respond to a failure in a predictable, safe manner.

3.1.47 **Fatigue failure.** A failure which is exhibited by fracture incurred by the cyclic application of loads which may be considerably less than the yield strength.

3.1.48 **Firing.** Firing as applied to the Department of Defense (DOD) Nuclear Weapon System Safety Standards in DODD 3150.2, refers to artillery shells, not to ignition of propulsion devices. When used as a term for Air Force weapon systems, firing is used to denote circuits and signals which initiate propulsion systems or ordnance devices.

3.1.49 **Firmware.** A combination of executable computer programs and data (software) which have been stored in any form of read-only memory which is unalterable during program execution. (References to software include firmware.)

3.1.50 Good guidance signal. The signal generated by a missile guidance and control system, including guided missiles launched from aircraft, which must be issued before final warhead arming can occur.

3.1.51 Hardware. The generic term dealing with physical items as distinguished from their capability or function—such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. In data automation, hardware is the physical equipment or devices forming a computer and peripheral components.

3.1.52 Hardwire. A dedicated discrete electrical circuit.

3.1.53 Human errors. Unintentional human actions that result in improper performance of a test. Human errors may be caused by fatigue, haste, stress, distractions, improper controls or tools, improper procedures, failure to follow procedures, hardware features or tasks outside the capability of the person performing the task, etc. Human errors frequently cause or contribute to mishaps. Proper weapon system design and operating procedures will reduce the probability and impact of human errors.

3.1.54 Inadvertent programmed launch. The inadvertent entry into terminal countdown and the resultant launch of a missile to a predetermined target.

3.1.55 Information control concept. The approach to the control of critical functions by using only uniquely encoded information or data words to initiate/command a critical function. The uniqueness of the coded information, combined with the failure modes and reliability of the control devices, will determine the probability of unintended occurrence of the critical function.

3.1.56 Informational storage media. Documents, tapes, disks, cards, plugs, memories, and other devices used to store information.

3.1.57 Intrusion detection system. A system used to detect and report intrusions into areas of security interest. There are three categories of the intrusion detection system (IDS):

a. Exterior IDS detects attempted penetrations of the restricted area boundary;

b. Structure/shelter (entrance and interior) IDS detects attempted penetrations of structures and shelters containing priority resources; and

c. Individual resource IDS detects entry into the area immediately surrounding priority resources.

3.1.58 Jettison. The unarmed release of stores from an aircraft other than in an attack mode.

3.1.59 Launch. The transition from a static state to the dynamic flight of a missile.

3.1.60 Launch action study. An analysis of a specific ground-launched missile weapon system component to determine the actions necessary to cause the component to contribute to an unauthorized launch (UL). Launch action studies provide source data for a UL study, and several of these studies are usually required for each UL study.

3.1.61 Launch action threat. A description of how an individual component of a ground-launched missile can be tampered with to achieve a specific unauthorized result.

3.1.62 Launch activation path. The path by which information and energy flow to effect a ground-launched missile launch. This includes hardware and software components, and the personnel actions necessary to cause a missile to go through the authorization-to-launch sequence.

3.1.63 Launch control point. The facility or vehicle that controls the launch of a ground-launched missile.

3.1.64 **Launch point.** The geographical location (area or facility) of a ground-launched missile when launched.

3.1.65 **Military characteristics for nuclear weapons.** A Department of Defense document submitted to the Department of Energy that specifies performance requirements and physical characteristics for a nuclear warhead, bomb, or basic assembly to be compatible with a specific weapon system or systems.

3.1.66 **Mission equipment.** Equipment designed specifically for use with nuclear weapons.

3.1.67 **Mobility.** Vehicle testing accomplished to determine performance capabilities, stability, and structural integrity and to assess overall safety.

3.1.68 **Monitor current.** A limited current introduced into a nuclear weapon to determine the functional state of selected components or circuits.

3.1.69 **Multiplex system.** A signal transmission system in which two or more signals share one transmission path or bus.

3.1.70 **No-lone zone.** An area where the Two-Person Concept must be enforced because it contains nuclear weapons, nuclear weapon systems, or certified critical components. The terms "close-in security area" in AFR 207-1 and "exclusion area" in DODD 5210.41 are the same as the term "no-lone zone" when nuclear weapons are present.

3.1.71 **Noncombat delivery vehicle.** A vehicle and its installed equipment used to move, load, or ship nuclear weapons. A noncombat delivery vehicle is not operated under specific nuclear weapon system safety rules.

3.1.72 **Nonspecialized equipment.** Equipment used with nuclear weapons but not specifically designed for that purpose.

3.1.73 **Normal environment.** The expected logistical and operational environments in which the weapon or combat delivery vehicle is required to function without degradation in operational reliability or safety.

3.1.74 **Nuclear cargo.** A nuclear weapon or nuclear component (except limited-life components) prepared for nuclear logistics movement.

3.1.75 **Nuclear certification.** The process for determining whether the nuclear weapon system meets the nuclear surety standards and is acceptable for operational deployment, considering system design, compatibility, procedures, safety, security, and unit readiness. Nuclear certification is required prior to a system acquiring operational status.

3.1.76 **Nuclear certified equipment.** Support equipment, combat delivery vehicles, and noncombat delivery vehicles that have received nuclear safety design certification.

3.1.77 **Nuclear certified procedures.** Procedures that have been approved for use with nuclear weapons, nuclear certified equipment, or nuclear weapon systems and have been published in Air Force technical orders or technical publications.

3.1.78 **Nuclear component.** A part of a nuclear weapon which contains fissionable or fusionable material.

3.1.79 **Nuclear consent function.**

a. For aircraft and air-launched missile systems the function is implemented by a deliberate act that provides two-person control over the release system unlock and nuclear weapon prearm functions.

b. For ground-launched missile systems the function is implemented through cooperative actions being required to issue certain critical commands.

3.1.80 Nuclear logistics movement. The transport of nuclear weapons in connection with supply or maintenance operations. Under certain specified conditions, combat aircraft may be used for such movements.

3.1.81 Nuclear safety certification. *See* **Nuclear safety design certification.**

3.1.82 Nuclear safety design certification. A determination by the Directorate of Nuclear Surety, Detachment 1, Air Force Inspection and Safety Center that all applicable nuclear safety design criteria for a given hardware and software design have been met and the design is authorized for use with nuclear weapons. Safety design certification is based upon a satisfactory engineering evaluation which verifies design compliance.

3.1.83 Nuclear safety discrepancy report. A discrepancy report that references the computer hardware/software program materials or outputs in which the discrepancy was detected and provides a detailed description of the problem. A discrepancy report is generated as a result of a violation of one or more nuclear safety requirements.

3.1.84 Nuclear surety. A term used to encompass all activities that ensure Air Force compliance with the DOD Nuclear Weapon System Safety Standards. To comply with these standards, Air Force nuclear weapon systems must be designed, maintained, transported, safeguarded, stored, and employed to incorporate maximum safety and security consistent with operational requirements.

3.1.85 Nuclear weapon. A device in which the explosion results from the energy released by reactions involving atomic nuclei, either by fission, fusion, or both.

3.1.86 Nuclear weapon system. A combat delivery vehicle with its nuclear weapon or weapons and associated support equipment, noncombat delivery vehicles, and facilities.

3.1.87 Nuclear weapon system safety group. The Nuclear Weapon System Safety Group (NWSSG) evaluates nuclear weapon systems to make sure procedural safeguards and design safety and security features are adequate to meet the Department of Defense Nuclear Weapon System Safety Standards. The functions and responsibilities of the NWSSG are described in AFI 91-102.

3.1.88 Nuclear weapon system safety rules. Secretary of Defense-approved procedural safeguards governing all operations with nuclear weapons or nuclear weapon systems. The safety rules establish procedures to ensure compliance with the Department of Defense (DOD) Nuclear Weapon System Safety Standards in DODD 3150.2. Nuclear weapon system safety rules are published in the Air Force 91-series instructions.

3.1.89 Nuclear yield. The energy released through nuclear fission or fusion equivalent to or greater than the energy released by the detonation of four pounds of trinitrotoluene (TNT).

3.1.90 Operational certification/recertification. The process through which tests and approved procedures are used to complete a functional inspection of components (and visual inspection of critical components for ground-launched missile systems) being prepared for use in the nuclear weapon or nuclear weapon system.

3.1.91 Operational command. Those functions of command involving the composition of subordinate forces, the assignment of tasks, the designation of objectives, and the authoritative direction necessary to accomplish the mission. Operational command should be exercised by the use of the assigned normal organizational commanders of subordinate forces established by the commander exercising operational command. It does not include such matters as administration, discipline, internal organization, and unit training, except when a subordinate commander requests assistance.

3.1.92 Operational load. The operational load is the calculated maximum probable load experienced by a part or equipment during its operational life. It includes dynamic effects and engagement forces in each axis over and above the rated load.

3.1.93 **Operational plan data document.** A detailed plan of how the using command intends to operate a nuclear weapon system to assure effective mission accomplishment.

3.1.94 **Opportunity.** Close physical proximity to a nuclear weapon, nuclear weapon system, or certified critical component in such a manner as to allow one or more persons the opportunity to tamper with or damage a nuclear weapon, nuclear weapon system, or certified critical component when such tampering or damage could go undetected at the completion of the activity which afforded access. Normally, a person in close physical proximity to the weapon, weapon system, or component would not be considered to have opportunity if a Two-Person Concept Team of escorts or guards were provided for either the person or the nuclear weapon, nuclear weapon system, or certified critical component. Opportunity must be judged in terms of the nature of the activity being performed and the knowledge of the person suspected of tampering.

3.1.95 **Plastic failure.** Failure caused by material yielding. (Yielding is experienced when stress levels exceed the minimum yield strength of the material as specified in MIL-HDBK-5 or other applicable standards.)

3.1.96 **Prearm command signal.** The signal to the weapon indicating that the personnel controlling the weapon system want it to function and produce a nuclear detonation.

3.1.97 **Prearm device.** The prearm device is a strong link device that will prevent arming of a nuclear bomb or warhead in the absence of a unique signal prearm command which is initiated by the deliberate action of a person.

3.1.98 **Prearmed.**

a. The state of a weapon system in which launch or release of the weapon from the aircraft will start the sequence necessary to produce a nuclear detonation.

b. The state of a ground-launched missile weapon system which indicates the weapon system operators have authorized launch, and arming would be permitted after launch when the weapon has sensed the proper flight environments.

3.1.99 **Present.** As applied to a no-lone zone, this term means that a Two-Person Concept Team member is in a position to observe an incorrect act or unauthorized procedure during a task or operation. Proximity and visual observation of team member actions will depend on the nature of the task to be performed. For example, one team member may be briefly unobserved by the other team member if it is unsafe or physically impossible to maintain constant observation.

3.1.100 **Prime nuclear airlift force.** Those Military Airlift Command aircrews, aircraft, and other functions provided for support of logistical airlift of nuclear weapons and nuclear components.

3.1.101 **Random vibration.** An oscillating motion, the instantaneous amplitude of which can be predicted only on a probability basis. It may be considered as being composed of a continuous spectrum of frequencies whose individual amplitudes are varying in a random manner. Random motion is aperiodic and is described mathematically in terms of statistics rather than trigonometric functions.

3.1.102 **Rated load.** A rated load is that combination of load forces that the basic equipment must support or resist in a static state. This load, consisting of one or more weapons and the associated handling and restraint equipment, is the nuclear certified load.

3.1.103 **Release.**

a. Deliberate or inadvertent separation of a gravity bomb from a carrier aircraft.

b. Deliberate or inadvertent separation of a missile from a carrier aircraft prior to ignition of the missile's propulsive system.

3.1.104 Reversion. The process or event of returning to the original state, phase, or condition.

3.1.105 Roadability. A measure of a vehicle's ability to negotiate the terrain and obstacles expected under normal conditions.

3.1.106 Safe and arm device. A device which physically and electrically interrupts ordnance initiation circuits between the source and the explosive or pyrotechnic train.

3.1.107 Software. A set of computer programs, procedures, rules, data, and associated documentation—including firmware with programs and data—concerned with the operation of a digital processing system; for example, compilers, library routines, manuals, and software design/data flow diagrams.

3.1.108 Specialized equipment. Equipment designed specifically for use with nuclear weapons.

3.1.109 Split-knowledge. A procedure used within the Two-Person Concept. By separating code(s) necessary to implement a function (split so that no lone individual has access to all the required code(s)), weapon unlock, critical component usage, or nuclear weapon access cannot occur by a lone individual.

3.1.110 Static electricity. The buildup of an electrical charge on an object that may be discharged through another object of a different potential that may cause damage to electrical and explosive components.

3.1.111 Stockpile-to-target sequence.

a. The order of events involved in removing a nuclear weapon from storage, and assembling, testing, transporting, and delivering it on the target.

b. A document that defines the logistical and employment concepts and related normal and abnormal environments involved in the delivery of a nuclear weapon from the stockpile to the target. It may also define the logistical flow involved in moving nuclear weapons to and from the stockpile for quality assurance testing, modification and retrofit, and the recycling of limited-life components.

3.1.112 Stores management system. That portion of the aircraft system which provides weapon control, release, and monitoring functions. Specifically, it controls the following nuclear critical functions: authorization, prearming, and releasing or launching. The stores management system typically encompasses the avionics processor(s), weapon control and display panels, and weapon interface units.

3.1.113 Stray voltage. An unintended voltage existing in any part of a weapon system.

3.1.114 Strong link. A device that protects a selected functional unit (such as prearm devices, and environment- or trajectory-sensing devices) by isolating the unit from abnormal environments so that the unit may operate or perform its function only when intended. The strong link must operate in a predictably safe manner to the abnormal environment(s) until after a weak link necessary for system operation becomes irreversibly inoperative when exposed to the same environment(s) as the strong link.

3.1.115 Support equipment. Includes all equipment required to perform the support function, except that which is an integral part of the mission equipment. It does not include any of the equipment required to perform mission operational functions. Support equipment should be interpreted as including tools; test equipment; automatic test equipment; organizational, field, and depot support equipment; and related computer programs and software.

3.1.116 Synchronized operations. Actions involving two or more devices which require simultaneous operations to control yaw, pitch, and roll—for example, two hoists operating simultaneously to lift a weapon.

3.1.117 Tamper. To knowingly perform an incorrect act or unauthorized procedure involving a nuclear weapon, nuclear weapon system, or certified critical component.

3.1.118 Time division multiplexing. The transmission of information from several signal channels through one communication system with different channel samples staggered in time to form a composite pulse train.

3.1.119 Two-person concept. A concept designed to ensure a lone individual never has the opportunity to tamper with or damage, in a way that could go undetected, a nuclear weapon, nuclear weapon system, or certified critical component.

3.1.120 Two-person concept team. A team made up of at least two people, each of whom:

a. is certified under the personnel reliability program;

b. is familiar with the safety and security requirements of the task to be performed;

c. knows the task well enough to promptly detect an incorrect act or unauthorized procedure; and

d. has successfully completed nuclear surety training.

3.1.121 Ultimate failure. Failure exhibited by material fracture.

3.1.122 Unauthorized launch. A deliberate unauthorized act that causes any movement (resulting from the direct impulse of a propulsion subsystem) of a nuclear weapon mated to a missile. The following are launch categories:

a. Type 0 Launch—Ignition of a propulsive stage or engine which results in missile movement but without the missile exiting the launch platform due to physical restraints.

b. Type 1 Launch—Ignition of a propulsive stage or engine which results in missile launch from the launch platform but with an inactive guidance system.

c. Type 2 Launch—Missile launch with an active guidance system which results in powered flight to a preprogrammed target but without a nuclear yield.

d. Type 3 Launch—Missile launch with an active guidance system which results in powered flight to a preprogrammed target with a nuclear yield.

3.1.123 Unauthorized launch scenario. A complete account of how an unauthorized launch can be achieved by using specific launch action threats. The scenario may include one or more launch action threats. It will describe the procedures the agent needs to follow and the tools needed for each step of the procedure. It will also describe normal operating conditions that must be overcome.

3.1.124 Unique signal. A signal format used to allow the receiver to discriminate the unique signal from all other signals in the weapon system and from those which may be accidentally generated or applied from outside the weapon system in abnormal environments. The signal may be digital or analog.

3.1.125 Unique signal device. A device which is designed to react to a unique signal and allow a critical function to occur.

3.1.126 Volatile memory. A storage medium that loses information when power is removed from the system.

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

3.1.128 Weapons safety officer. An individual who manages a base, wing, or equivalent safety program consisting of explosives safety, missile safety, nuclear surety, or any combination of these.

3.1.129 Weapon support load path. All structural components which experience an increase in stress when reacting to the weapon weight or inertial force in any of the three axes.

3.2 Acronyms and abbreviations used in this standard.

ACCD	Aircraft Compatibility Control Drawing
A/D	Arm/Disarm
A&F	Arming & Fuzing
AFI	Air Force Instruction
AFLC	Air Force Logistics Command
AFR	Air Force Regulation
AFMC	Air Force Materiel Command
AFSA	Air Force Safety Agency
AFSC	Air Force Systems Command
AMAC	Aircraft Monitor and Control
ASC	Aeronautical Systems Center
BITE	Built-in-Test Equipment
CPIN	Computer Program Identification Number
DAR	Design Analysis Report
DH	Design Handbook
DID	Data Item Description
DOD	Department of Defense
DODD	Department of Defense Directive
DODISS	Department of Defense Index of Specifications and Standards
DOE	Department of Energy
ECD	Electrical Compatibility Data
EED	Electroexplosive Device
EER	Engineering Evaluation Report
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EMR	Electromagnetic Radiation
EOD	Explosive Ordnance Disposal
E/TSD	Environmental or Trajectory Sensing Device
HOL	Higher Order Language
IDS	Intrusion Detection System
IOC	Initial Operational Capability
ISS	Initial Safety Study

LAP	Launch Activation Path
LCP	Launch Control Point
LP	Launch Point
MAR	Major Assembly Release
MC	Military Characteristic
MCD	Mechanical Compatibility Data
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
NCP	Nuclear Certification Plan
NDI	Non-Destructive Inspection
NSAR	Nuclear Safety or Surety Analysis Report
NSWG	Nuclear Surety Working Group
NWSDD	Nuclear Weapon System Definition Document
NWSSG	Nuclear Weapon System Safety Group
OS/RTE	Operating System/Run-Time-Executive
PAL	Permissive Action Link
POG	Project Officers Group
POSS	Preoperational Safety Study
RF	Radio Frequency
RS	Reentry System
RV	Reentry Vehicle
S&A	Safe & Arm
SA-ALC/NWI	Nuclear Weapons Integration Division
SCP	Software Certification Plan
SDP	Software Development Plan
SMS	Stores Management System
SNL	Sandia National Laboratories
SPO	System Program Office
STS	Stockpile-to-Target Sequence
TNSA	Technical Nuclear Safety Analysis
TO	Technical Order
TOMA	Technical Order Management Agency
TPD	Terminal Protection Device
UL	Unauthorized Launch; Underwriters Laboratories
USD	Unique Signal Device
USG	Unique Signal Generator
WCD	Weapon Capability Date

4. GENERAL REQUIREMENTS

4.1 Nuclear surety certification program

4.1.1 Nuclear surety design goal. The primary goals of the nuclear weapon system surety program are to protect people and property and to conserve nuclear weapons as a national resource by protecting them against all risks and threats inherent in their environment. This includes the design safety of the weapon system in all environments, security measures necessary to retain custody and protect the resource, and appropriate command and control measures to ensure the weapon system is employed only with proper authority. Because of their destructive power and the consequences of an unauthorized or inadvertent detonation of the nuclear or high explosive material, nuclear weapons and weapon systems must be designed to incorporate surety consistent with operational requirements.

4.1.2 Department of Defense nuclear weapon system safety standards. The basis of all nuclear weapons system surety design requirements are the Department of Defense Nuclear Weapon System Safety Standards in DODD 3150.2. Compliance with these standards is mandatory. As a minimum, there shall be positive measures to meet the DOD Nuclear Weapon System Safety Standards which:

a. prevent nuclear weapons involved in accidents, incidents, or jettison from producing a nuclear yield;

b. prevent deliberate prearming, arming, launching, firing, or releasing of nuclear weapons except upon execution of emergency war orders or when directed by competent authority;

c. prevent inadvertent prearming, arming, launching, firing, or releasing of nuclear weapons in all normal and credible abnormal environments; and

d. insure adequate security of nuclear weapons, pursuant to DODD 5210.41.

4.2 Program requirements. A nuclear surety design certification program shall be developed for nuclear weapon systems. This program shall consist of those tasks required to verify the adequacy of the weapon system design from a safety and security standpoint. The nuclear surety certification program shall be folded into the overall weapon system acquisition program.

4.2.1 Applicability. The requirements for this program shall be included in all applicable contracts negotiated by the Air Force procuring activities. These requirements shall also apply to each Air Force organic program and each program developed by any DOD agency for Air Force use.

4.2.2 Purpose. The purpose of this standard is to provide nuclear surety design requirements and guidelines, design verification approaches, and types of analyses and tests to support a nuclear surety design certification program.

4.2.3 Procedures. Surety requirements of this standard shall be met by a basic design that includes safety and security features and devices. The nuclear system design must reduce the dependence of safety and security on procedures or operational restrictions to achieve the required levels of safety specified by this standard.

4.2.4 Equipment nuclear safety design certification. The following equipment shall be nuclear safety design certified:

a. Combat delivery vehicles;

b. Critical components;

c. Noncombat delivery vehicles;

d. Suspension and release equipment—for example, bomb racks, launchers, pylons;

e. Support equipment that moves, supports, stores, handles, loads/unloads, or mates/demates nuclear weapons; and

f. Test equipment used to test and verify the functionality of the authorization, prearm, arm, unlock, release, and launch circuits, or that directly interfaces with nuclear weapons or critical components. Some common tools and test equipment, such as multimeters, do not normally require certification.

4.2.5 Modifications. Any modifications to a design that impact criteria in this standard require an engineering evaluation report (EER) to verify that the modified design meets the nuclear safety design requirements of this standard. The engineering evaluation shall be accomplished and reported in accordance with the appropriate engineering analysis package data item description (DID). Changes to systems/hardware that result in manufacturer's service bulletins are considered modifications.

4.3 Evaluation requirements. The analysis and test requirements must be accomplished to evaluate the nuclear weapon system for nuclear certification. This is required to obtain Air Force certification of critical hardware and software, and to verify that the nuclear weapon system meets the design requirements of this standard and the DOD Nuclear Weapon System Safety Standards. The responsible agency to ensure these requirements are met is the system procurement/development organization that has program management responsibility.

4.3.1 General analyses requirements

4.3.1.1 Basis and documentation. The analyses of the weapon system shall be based on the system, subsystem, and end item specifications and qualified system operating parameters. The supporting analyses are required for, and shall be documented in, the nuclear safety analysis report (NSAR) for new and AFSA designated systems that undergo major modifications. For those systems not requiring an NSAR, analyses shall be documented using an EER.

4.3.1.2 Purposes. The analyses shall address the qualitative and quantitative requirements of this standard for inadvertent prearming; accidental propulsion system ignition and inadvertent programmed launch; inadvertent release or jettison; inadvertent power to the nuclear weapon interface; and circumvention (deliberate or accidental) of two-person control for authorization, launch, prearm, or unlock.

4.3.1.3 Failure rate data. For analysis purposes, failure rates for both warheads and delivery systems shall be expressed in the same units. For these analyses, worst-case generic failure rate data is required as a minimum, but component-specific data can also be used when available.

4.3.1.4 Authorization device for aircraft. Safety studies and calculations conducted for combat delivery aircraft systems shall not take credit for the authorization device to meet the safety requirements. Safety requirements shall be met with the assumption that the authorization device is activated.

4.3.1.5 Authorization device for ground-launched missiles. If the user accepts the restriction that the authorization device shall not be activated until receipt and authentication of the authorization command from higher authority has been given for the ground-launched missile, then safety studies and calculations may take credit for any safety enhancement that the authorization device may provide.

4.3.1.6 Safety and security objectives. A prime objective of the Air Force Nuclear Weapons Surety Program is to achieve safety and security consistent with operational requirements while protecting nuclear weapons as a critical national resource. The plans, reports, and drawings supporting weapon system nuclear certification are specified in the aircraft and missile DID's, such as NCP, NSAR, EER, etc., as defined in 90.1 thru 90.11. Some safety and security areas that shall be analyzed in the nuclear certification program include:

a. Electromagnetic compatibility (EMC)/Electromagnetic interference (EMI)/Electromagnetic pulse (EMP)/Electromagnetic radiation (EMR)/Electrostatic discharge/Lightning

b. Safe-arm fuze and arm/disarm (A/D) devices

c. Guidance and control malfunctions ("Good guidance")

d. Accidental motor ignition

e. Inadvertent programmed launch

f. Protection of friendly territory

g. Credible abnormal environments

h. Critical function processing and execution

i. Testing/Maintenance

j. Radioactivity (generation of, shielding from, and attenuation of)

k. EOD procedures

l. Mission planning

m. Inadvertent prearming/arming

n. Inadvertent application of power to interfaces

o. Alteration to fuzing option

p. Alteration to targeting

q. Launch action study

r. Critical function & command monitoring

s. Status monitoring

t. Physical security

4.3.2 Guidelines for analyses and tests. The data from analyses and tests of systems, subsystems, components, and equipment are necessary to evaluate nuclear safety and security. Qualitative and quantitative analyses and tests provide a basis for the nuclear safety and security evaluations. Analyses and tests must be compatible with the concepts used within the system, such as information control, energy control, etc.

4.3.2.1 Use of specifications and standards. When military specifications or standards exist that satisfy nuclear surety requirements, the analysis and test requirements may be met by showing those specifications or standards have been met.

4.3.2.2 Tailoring of tests. When operational needs differ significantly from the test requirements of a military specification or standard, the test requirements shall be changed to reflect operational requirements.

4.3.2.3 Safety/security analysis. Those features, subsystems, or subassemblies of each item of equipment that affect nuclear safety or security shall be identified and reported according to sections 4 of this standard and section 30 of the appendix.

4.3.2.4 Nonspecialized equipment. Nonspecialized equipment shall be evaluated for nuclear safety adequacy according to the appropriate standards, specifications, and designated tests.

4.3.2.5 Critical component qualification. Critical components shall be qualified to all expected and specified environments—for example, thermal, vibration, shock, electrical or electronic, salt spray, sand, dust, pressure, etc. A summary of qualification test results shall be provided.

4.3.2.6 Nuclear surety analysis. An evaluation of the nuclear weapon system shall be accomplished to determine if the weapon system meets the nuclear surety requirements of this standard. If the implementation of system or equipment specifications shall cause hazards (see MIL-STD-882 as tailored to the specific system), the system manager shall conduct a tradeoff study to achieve nuclear surety consistent with operational requirements. If there are any findings that may have an impact on nuclear surety, these finding(s) shall be reported. If there are no findings which have a nuclear surety impact, this shall also be reported.

4.3.2.7 Nuclear surety verification. When other system, subsystem, and equipment specifications require surety validation tests, test results that impact nuclear surety shall be reported. These shall be considered an integral part of the development and acceptance tests or the demonstration tests. Lab tests, functional mock-ups, models, or simulations may demonstrate partial verification of surety characteristics or procedures.

4.4 Qualitative and quantitative design and evaluation requirements

4.4.1 Prearming

4.4.1.1 Design requirements. Faults and failures in the nuclear weapon system that cause the inadvertent generation and transmission of the prearm command shall not occur with a probability greater than one in 106 per combat delivery vehicle over the system's lifetime in normal environments. Prearm design requirements include the following:

a. All nuclear weapon systems shall have a prearming function.

b. The prearming function shall be separate from the arming, launching, and releasing functions.

c. The prearming function shall prearm nuclear weapons upon command.

d. The prearming function shall prevent nuclear weapon prearming and subsequent arming in the absence of a prearm command.

e. The prearming signal shall be derived from some part of the weapon system under direct operator control.

f. If a weapon is designed to be prearmed prior to launch or release, the process shall be reversible. If the prearm function cannot be made reversible, it shall be designed so that generation and transmission of the prearm command shall occur as late as possible in the launch or release sequence.

g. For nuclear weapons using the information control concept, a uniquely coded prearm command signal shall be used which meets the numerical probability requirements of this standard. The information needed to generate the unique prearm signal shall not be stored in a useable form until its use is required.

h. For nuclear weapons whose design is based on the energy control concept, prearm command discrete signal lines shall be physically and electrically isolated from all other circuits. The prearm command signal line shall avoid the use of a common routing, cabling, or connectors with any wire likely to carry enough power to operate the prearm device. This requirement does not apply to the input side of a unique signal device (USD).

i. Positive safety features shall exist to prevent inadvertent prearming in credible abnormal environments.

4.4.1.2 Evaluation requirements. Analyses or tests shall verify the prearming requirements in 4.4.1.1.

4.4.2 Arming

4.4.2.1 Design requirements. After the nuclear weapon arming and fuzing (A&F) subsystem has been prearmed, but before launch or release, the probability of any system failure in a normal environment that results in arming shall not exceed one in 104 per prearmed weapon. Arming design requirements include the following:

a. Arming shall be prevented until after a positive indication of a launch or release.

b. Arming shall be designed to occur as late as practical in the delivery sequence.

c. Arming shall be prevented until after good guidance is assured in missiles.

d. Arming shall be prevented until after the weapon is prearmed.

4.4.2.2 Evaluation requirements. Analyses or tests shall verify the arming requirements in 4.4.2.1.

4.4.3 Targeting

4.4.3.1 Design requirements. For ground-launched missiles, the probability of faults and failures in the nuclear weapon system which result in the erroneous issuance of the good guidance signal shall not exceed one in 103 per missile perlaunch.

4.4.3.2 Evaluation requirements. Analyses or tests shall verify the requirements in 4.4.3.1.

4.4.4 Non-airbreathing propulsion system operation

4.4.4.1 Design requirements

4.4.4.1.1 Inadvertent programmed launch. Faults and failures in the nuclear weapon system that cause inadvertent programmed launch of a ground-launched missile during a fully assembled weapon system operation shall not occur with a probability greater than one in 1012 per missile over the system's lifetime in normal environments. Positive safety features shall exist to prevent inadvertent programmed launch in an abnormal environment.

4.4.4.1.2 Accidental ignition. Faults and failures in the nuclear weapon system that cause accidental propulsion system, rocket motor, or engine ignition shall not occur with aprobability greater than one in 107 per missile over the system's lifetime in normal environments. Positive safety features shall exist to prevent accidental propulsion system ignition in an abnormal environment. Propulsion system nonpropulsive burning or explosion is not considered to be accidental ignition.

4.4.4.2 Evaluation requirements. Analyses or tests shall verify the propulsion system operation requirements in 4.4.4.1.

4.4.5 Release system operation (aircraft carried weapons)

4.4.5.1 Design requirements

4.4.5.1.1 Inadvertent release or jettison—release system locked. Faults and failures in the nuclear weapon system that cause inadvertent release or jettison of a bomb or missile when the release system is locked shall not occur with a probability greater than one in 106 per weapon station over the system's lifetime in normal environments. Positive safety features shall exist to prevent inadvertent release or jettison of a bomb or missile in an abnormal environment. (Separation of the weapon without operation of the release system, due to aircraft catastrophic structural failure, is not considered to be inadvertent release or jettison.)

4.4.5.1.2 Inadvertent release or jettison—release system unlocked. Faults and failures in the nuclear weapon system that cause inadvertent release or jettison of a bomb or missile when the release system is unlocked shall not occur with a probability greater than one in 103 per unlocking event in normal environments. Positive safety features shall exist to prevent inadvertent release or jettison of a bomb or missile in an abnormal environment.

4.4.5.2 Evaluation requirements. Analyses or tests shall verify the release system operation requirements in 4.4.5.1.

4.4.6 Inadvertent power application

4.4.6.1 Design requirements. Faults and failures in the nuclear weapon system that cause inadvertent application of power or signals (excluding the prearm command) to the DOD/Department of Energy (DOE) warhead/bomb interface shall not occur with a probability greater than one in 104 per combat delivery vehicle over the system's lifetime in normal environments. Positive safety features shall exist to prevent inadvertent application of power or signals in an abnormal environment.

4.4.6.2 Evaluation requirements. Analyses or tests shall verify the power application requirements in 4.4.6.1.

4.5 General design and evaluation requirements

4.5.1 Authorization

4.5.1.1 Design requirements. Authorization design requirements include the following:

a. All nuclear weapon systems shall have an authorization device that mustbe activated for a nuclear weapon to provide a nuclear yield.

b. The authorization device shall prevent prearming, arming, launching, and releasing without authorization. It shall not prevent jettison.

c. The authorization device shall not prevent safing or relocking regardless of the state of the authorization device.

d. The authorization device shall be reversible. The enabled and disabled states shall not be complementary functions; for example, the absence of enabled shall not be construed as disabled, and vice versa.

e. The authorization device shall operate on the information control concept. The information shall be provided by a secure method through command and control channels.

f. The authorization device shall be designed to reveal if unauthorized acts (tampering) have been attempted. Requirements for protection against unauthorized actions shall be provided by the procuring agency.

g. Positive measures shall be taken to prevent inadvertent operation of the data entry device and to protect against an attack on or bypass of the data entry device.

4.5.1.2 Evaluation requirements. Analyses or tests shall verify the authorization requirements in 4.5.1.1.

4.5.2 Nuclear consent

4.5.2.1 Design requirements. Nuclear consent design requirements include the following:

a. Nuclear consent is provided to meet the Two-Person Concept.

b. All aircraft and air-launched missiles shall have a nuclear consent function to enable the following critical functions:

(1) Aircraft: prearm and unlock.

(2) Air-launched missiles: launch.

c. The nuclear consent function shall be independent of the authorization function.

d. The controls for nuclear consent shall be designed and constructed so that a single individual shall not be able to give nuclear consent (not applicable to single-seat combat aircraft).

e. Nuclear consent discrete lines (if used) shall be physically and electrically isolated from all other circuits.

4.5.2.2 Evaluation requirements. Analyses or tests shall verify the nuclear consent requirements in 4.5.2.1.

4.5.3 Single-component malfunction or operation

4.5.3.1 Design requirements. The malfunction or accidental operation of a single component shall not cause any of the following:

a. inadvertent transmission of critical signals;

b. inadvertent prearming, launching or releasing of a nuclear weapon;

c. inadvertent arming of a prearmed nuclear weapon; or

d. enabling of a ground-launched missile system.

These requirements apply before any of the functions are initiated and also when more than one event remains in the function sequence.

4.5.3.2 Evaluation requirements. Analyses or tests shall verify the single-component malfunction or accidental operation requirements in 4.5.3.1.

4.5.4 Human engineering

4.5.4.1 Design requirements

4.5.4.1.1 Human error. Features shall be included to limit the consequences of human error and deliberate unauthorized acts and to meet the requirements of MIL-STD-1801 as tailored to the specific system.

4.5.4.1.2 Dual errors. Nuclear weapon systems shall be designed so no two independent human errors can cause prearming, arming, launching, or releasing of a nuclear weapon, nor authorize the use of a ground-launched missile system. This requirement only applies before initiation of actions designed to accomplish the desired operation.

4.5.4.1.3 Two-man concept. Nuclear weapon system designs shall permit application of the Two- Person Concept to operations involving critical components.

4.5.4.2 Evaluation requirements. Analyses or tests shall verify the human engineering requirements in 4.5.4.1.

4.5.5 Targeting

4.5.5.1 Design requirements. Nuclear weapon systems shall be designed to detect accidental or deliberate unauthorized changes in the targeting function. Changes in the targeting function that occur before launch or release shall be indicated to launch control points (LCPs) for ground-launched missile systems or to the aircraft cockpit for combat delivery aircraft systems.

4.5.5.2 Evaluation requirements. Analyses or tests shall verify the targeting requirements in 4.5.5.1.

4.5.6 Protection of friendly territory

4.5.6.1 Design requirements. Nuclear weapon systems shall be designed to prevent nuclear detonations except within the boundaries of the designated target area. The boundaries of the designated target area shall be specified by the responsible DOD weapon system program manager.

4.5.6.2 Evaluation requirements. Analyses or tests shall verify the protection of friendly territory requirements in 4.5.6.1.

4.5.7 Good guidance signal

4.5.7.1 Design requirements. Missile systems, including 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 that the weapon will impact outside the specified target boundaries.

4.5.7.2 Evaluation requirements. Analyses or tests shall verify the good guidance signal requirements in 4.5.7.1.

4.5.8 System safety devices

4.5.8.1 Design requirements

4.5.8.1.1 General. Safe and arm (S&A) devices shall meet the design requirements in MIL-STD-1512 as tailored to the specific system. They shall arm only in response to an externally generated unique signal. The safing signal shall be dissimilar to the arming signal to reduce the risk of arming during attempted safing. If a monitor signal is used, it shall also be dissimilar to the arming signal.

4.5.8.1.2 Arming signal. USD's shall meet the design requirements in MIL-STD-1512 as tailored to the specific system. The number and sequence of unique bits in the signal shall be specifically selected so that the probability of randomly generating the signal supports the system safety requirements. Related requirements that shall be met are:

a. There shall be no permanent storage within the weapon system of the unique signal in a usable form; and

b. There shall be positive erasure of unique signal data that may have been temporarily stored in the system during system checkout or partial activation. This erasure shall occur as soon as possible after the data is no longer required.

4.5.8.2 Evaluation requirements. Analyses or tests shall verify the system safety device requirements in 4.5.8.1.

4.5.9 Electroexplosive device protection

4.5.9.1 Design requirements. Nuclear bombs, missiles, and their release or ordnance systems shall meet the design requirements of MIL-STD-1512 as tailored to the specific system. The components which control or electrically interface with these systems shall also meet the requirements.

4.5.9.2 Evaluation requirements. Analyses or tests shall verify the requirements in 4.5.9.1.

4.5.10 Monitoring

4.5.10.1 Design requirements

4.5.10.1.1 Monitoring signal. Procuring agency designated nuclear safety devices/functions shall be monitored. Failures of monitored systems shall cause an indication to the system operators.

4.5.10.1.2 Failures. The system shall be designed so failures within the monitoring system do not cause inadvertent actuation or enabling of critical functions. The system shall provide a means for determining if the monitoring system has failed.

4.5.10.1.3 Display. The state of a monitored nuclear safety device or function shall be displayed to the operator.

4.5.10.1.4 Positive display requirement. The monitoring system shall not use the absence of a signal, data, or information to indicate the safe state of a nuclear safety device or function.

4.5.10.2 Evaluation requirements. Analyses or tests shall verify the monitoring requirements in 4.5.10.1.

4.5.11 Nuclear weapon arming and fuzing (A&F) system.

4.5.11.1 Signals and stimuli

4.5.11.1.1 Design requirement. The arming and fuzing system shall only respond to the unique prearming and environment or trajectory stimuli.

4.5.11.1.2 Evaluation requirement. The A&F system signals and stimuli requirement in 4.5.11.1.1 shall be verified at the system and component levels through analyses, tests, and demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.2 Dual-signal arming

4.5.11.2.1 Design requirement. At least two separate and independently derived signals, which cannot be generated by a single source, are required to arm the weapon. These signals shall be interrupted by one or more strong link devices. At least one of these signals shall be continuous after application. This is not meant to be a requirement to have multiple power sources.

4.5.11.2.2 Evaluation requirement. The A&F system dual-signal arming requirement in 4.5.11.2.1 shall be verified at the system and component levels through analyses, tests, and demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.3 Energy discharge

4.5.11.3.1 Design requirement. The A&F system design shall 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.

4.5.11.3.2 Evaluation requirement. The A&F system energy discharge requirement in 4.5.11.3.1 shall be verified at the system and component levels through analyses, tests, and demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.4 Lightning protection

4.5.11.4.1 Design requirement. Lightning protection shall be incorporated to protect critical A&F circuits from the current levels specified in the system, subsystem, or component specifications. The design requirements of MIL-STD-1795 as tailored to the specific system shall be met for lightning strikes.

4.5.11.4.2 Evaluation requirement. The A&F system lightning protection requirement in 4.5.11.4.1 shall be verified at the system and component levels through analyses, tests, and demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.5 Cable and connector design

4.5.11.5.1 Design requirements. Cable and connector design and connector pin assignment shall protect against inadvertent application of power to the prearm or arm circuits in the warhead as a result of damaged cables and connectors. The design shall guard against susceptibility to damage during assembly, maintenance, and test operations. The electrical connector requirements in 4.5.13.5 shall also be met.

4.5.11.5.2 Evaluation requirements. The A&F system cable and connector requirements in 4.5.11.5.1 shall be verified at the system and component levels through analyses, tests, and demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.5.2.1 Connector mismating/misalignment analysis. Connector mismating and connector misalignment analyses shall be conducted for each critical connector.

4.5.11.5.2.2 Cable routing analysis. A cable routing analysis shall be conducted to show protection of identified cables against premature prearming or arming during all system phases.

4.5.11.6 Nondestructive testing compatibility

4.5.11.6.1 Design requirement. Nuclear safety for the A&F system shall not be degraded as a result of exposure to standard Air Force nondestructive testing environments (such as X-ray, ultrasonic, magnetic, etc.) specified for use in the weapon system.

4.5.11.6.2 Evaluation requirement. The A&F system nondestructive testing compatibility requirement in 4.5.11.6.1 shall be verified at the system and component levels through analyses, tests, and/or demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.7 Chemical compatibility and reversion

4.5.11.7.1 Design requirement. All material used in the design shall be chemically compatible in stockpile and storage environments. No materials shall be used that could increase the high explosive sensitivity, generate an explosive gas, cause an electrical short, cause reversion, corrode critical components, generate an unwanted electrochemical potential, or cause similar results.

4.5.11.7.2 Evaluation requirement. The A&F system chemical compatibility and reversion requirement in 4.5.11.7.1 shall be verified at the system and component levels through analyses, tests, and/or demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.8 Monitoring

4.5.11.8.1 Design requirements

a. The capability to monitor the state of at least one strong link in the A&F system shall be provided in all weapon system configurations. This shall be continuous monitoring, periodic monitoring, on-demand, or emergency capability only, depending on the system concept specified in the applicable specification. While the requirement to provide this capability is always placed on the A&F system, the weapon system must be able to use that capability in a way that complements the employment concept.

b. The monitoring function design shall preclude the possibility of introducing energy from any source that might operate an A&F critical function if a system fault or abnormal environment occurs.

4.5.11.8.2 Evaluation requirements. The A&F system monitoring requirements in 4.5.11.8.1 shall be verified at the system and component levels through analyses, tests, and/or demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.9 Input/output isolation

4.5.11.9.1 Design requirement. The electrical inputs to nuclear safety devices shall be isolated from the outputs. Other methods, such as incompatible signals, shall also be used to minimize the possibility of bypassing the safety devices.

4.5.11.9.2 Evaluation requirement. The A&F system input/output isolation requirement in 4.5.11.9.1 shall be verified at the system and component levels through analyses, tests, and/or demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.11.10 Launch or release sensing device

4.5.11.10.1 Design requirements. The A&F system shall contain a device that shall prevent power from being applied inadvertently or accidentally to the A&F system until the launch of a ground-launched missile, or the release of a bomber air-launched missile. This device shall function only upon complete transition to flight, not upon first motion. For aircraft systems, this device shall sense and operate only upon launch or release of the weapon. For ground-launched missile systems, this device shall operate only after sensing an expected launch environment.

4.5.11.10.2 Evaluation requirements. The A&F system launch or release sensing device requirements in 4.5.11.10.1 shall be verified at the system and component levels through analyses, tests, and/or demonstrations to assure nuclear safety during those phases specified in the system, subsystem, or component specification.

4.5.12 Automata and software.

4.5.12.1 General requirements

4.5.12.1.1 Design requirements. These requirements apply to automata and software which receive, store, process, or transmit data to monitor, target, prearm, arm, launch, release, or authorize the use of a nuclear weapon. Equipment and software shall be designed to provide protection against accidental or deliberate unauthorized operation of critical functions.

4.5.12.1.1.1 Software specifications. The tailored requirements of DOD-STD-2167 shall be followed. System requirements shall be translated into program design in a systematic "top down" method. Identified nuclear safety design requirements shall be incorporated into the appropriate software specifications.

4.5.12.1.1.2 Higher order language. Software development or modification shall be principally based on the use of an Air Force-approved higher order language (HOL). Code development in assembly or machine language shall only be utilized when the HOL does not provide adequate capability for time-critical or hardware-interfacing functions.

a. All software verification checks (nuclear critical variables, flags, data, etc.) which can be performed in the HOL shall be accomplished prior to calling assembly or machine language routines.

b. Critical software functions shall not be modified in a language other than the source code for that software unless specifically approved.

4.5.12.1.1.3 Hierarchical design. The software design shall be a hierarchical structure of identifiable programs, subprograms, modules, procedures, and routines.

a. The highest level of control logic shall reside at the top levels, and the computational or algorithmic functions shall reside at the lower levels.

b. Modules performing critical functions shall be single-purpose modules.

4.5.12.1.1.4 Hardware check. The automata design shall provide self-check confidence, or test routines to ensure the integrity and proper state of hardware devices which affect or execute critical functions. Critical failure modes or illegal states shall result in operator notification of the problem and the status of any automated actions taken.

4.5.12.1.1.5 Hardware initialization and shutdown. Critical function hardware which is controlled or monitored by software and automata memory containing nuclear critical information shall be in a known and predictably safe state. Upon system shutdown or program termination, the software shall ensure that all settable nonvolatile devices and relays are set to a known safe state.

4.5.12.1.1.6 Fault tolerance and error handling. The computer system shall revert to a predictably safe state when a critical function system fault is detected.

a. The computer system shall be "fault tolerant" to the effects of power transients and electromagnetic and electrostatic environments.

b. The automated response to critical system errors and faults shall result in a safe weapon command state and shall be displayed to the system operator.

4.5.12.1.1.7 Interrupts. Interrupts which suspend critical program execution or preempt other interrupts shall have specifically defined priorities and responses.

4.5.12.1.1.8 Processor scheduling and operations. Software shall not cause a central processing unit "wait" state. Techniques for deadlock detection and resolution shall be provided.

4.5.12.1.1.9 Instruction alterations. In normal operations, software shall not be capable of modifying its own instruction set or the program instruction set of ancillary programs.

4.5.12.1.2 Evaluation requirements. Analyses or tests shall verify the general automata and software requirements under 4.5.12.1.1.

4.5.12.2 Memory characteristics

4.5.12.2.1 Design requirements

4.5.12.2.1.1 Memory volatility. Automata system design shall ensure that memory contents are not altered or degraded over time during operational use. Storage of critical function program(s) and data in nonvolatile, nondestructive read-only memory is preferred wherever possible. Memory with volatile characteristics shall have provisions to ensure that erroneous data, resulting from power removal or other phenomena, shall not adversely affect any critical function or component.

4.5.12.2.1.2 Hardware faults. A single hardware fault shall not cause a memory change that could cause initiation of a critical function.

4.5.12.2.1.3 Memory integrity verification

a. Memory containing critical function routines and data shall be protected using error-detection techniques.

b. Any detected errors to critical functions or data shall be resolved.

4.5.12.2.1.4 Memory accessibility. Provisions shall exist to protect the accessibility of memory locations containing nuclear critical routines and data. Critical function routines and data base elements shall be protected such that any allowable memory segment address, which is allowed by the system for noncritical functions or data base elements, shall not be able to specifically address critical data base elements or critical function routines.

4.5.12.2.1.5 Memory declassification. A method shall be provided to erase or obliterate any clear-text secure codes from memory.

4.5.12.2.1.6 Memory initialization. All memory not used for initial program and data load, which is available to any processor capable of executing critical function routines, shall be initialized to a known pattern. This pattern, if executed as an instruction, shall not initiate any critical functions or change the state of critical safety features or parameters.

4.5.12.2.2 Evaluation requirements. Analyses or tests shall verify the memory characteristic requirements under 4.5.12.2.1.

4.5.12.2.2.1 Memory volatility. Show by demonstration or analysis that any memory content alteration or degradation shall be detectable and result in compensatory action. Show by demonstration or analysis that any memory change in a volatile memory shall not allow a critical function to be completed. Show that a single hardware fault shall not result in a memory change that could allow a critical function to be completed.

4.5.12.2.2.2 Memory loading and change.

a. Demonstrate or analyze the following features:

(1) Error detection and subsequent operator notification;

(2) Software program execution is stopped until all valid and correct data have been loaded and verified;

(3) Reloading or changing that part of memory involving critical functions is stopped unless the proper means for entry is used. Improper reload or change shall be indicated, rejected, and annunciated; and

(4) Each section of memory is filled by the block of proper program data or instructions to be transferred.

b. Memory declassification. Demonstrate the method used to erase or obliterate clear-text secure codes from memory.

c. Processor deviations. Demonstrate the capability to detect manually initiated commands, message errors, and deviations causing an erroneous entry into a critical routine. Show that, upon detecting errors or deviations, the system shall cease critical command processing, notify the operator, and return the system to a known safe state.

d. Fault detection. Demonstrate the fault detection capability of the system.

e. Test. Demonstrate the self-check, confidence, or test routines.

f. Ancillary equipment. Equipment which provides an interface between an operator and the processors shall be evaluated for the extent of control it exerts on the weapon system and for its susceptibility to unauthorized control.

4.5.12.3 Critical program load verification

4.5.12.3.1 Design requirements

4.5.12.3.1.1 System protection during load. The system shall be designed to prevent program execution or continuation until all program instructions or data (or both) have been loaded and verified. The results of the program load verification shall be displayed to system operators.

4.5.12.3.1.2 Unused memory. Unused memory will be filled with a known verifiable pattern which shall not initiate critical functions if executed.

4.5.12.3.2 Evaluation requirements. Analyses or tests shall verify the critical program load verification requirements under 4.5.12.3.1.

4.5.12.4 Critical command messages

4.5.12.4.1 Design requirements

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

4.5.12.4.1.2 Validity checks. All critical command transmissions must originate with manual operator inputs (see 4.5.12.6.1.1) and the state of all applicable preconditions and inhibits must be verified to be in the correct state prior to transmission.

4.5.12.4.2 Evaluation requirements. Analyses or tests shall verify the critical command message requirements under 4.5.12.4.1.

4.5.12.5 Operating system/Run time executive

4.5.12.5.1 Design requirements. Only the operating system/run time executive (OS/RTE) shall be capable of calling critical function routines and modules. The operating system software, while working on a fixed stack size with accumulated depth in applications use, shall not overflow or overwrite other program instructions or data. An erroneous entry into a critical function routine or sequence (see 4.5.12.6.1.3) shall terminate function execution, provide notification of the error to the operator, if possible, and command the system to a known safe state.

4.5.12.5.2 Evaluation requirements. Analyses or tests shall verify the OS/RTE requirements in 4.5.12.5.1.

4.5.12.6 Critical function routine design

4.5.12.6.1 Design requirements

4.5.12.6.1.1 Operator interface

a. No nuclear critical function shall be initiated without operator intervention nor initiated by a single operator action (two or more actions such as keystrokes are required). Separate and independent crew actions are required in ground-launched missile systems to initiate authorization and launch functions.

b. The software shall provide for detection and notification of improper entries by the operator.

c. Operator cancellation of nuclear critical function processing shall require a minimum number of operator actions and shall be accomplished in a safe manner.

4.5.12.6.1.2 Single-function routines. No routine shall be capable of performing more than one nuclear critical function. Each nuclear function routine shall have both a single unique entry address and a single unique exit address. This shall not preclude critical function execution being performed in parallel in the same processor—for example, launch processing and targeting.

4.5.12.6.1.3 Critical function call/entry checks. Critical function routines shall not be called until all proper conditions exist. All entries into nuclear critical function routines shall have checks to ensure such entries are authorized (operator action is accomplished) and appropriate (all event preconditions are met).

4.5.12.6.1.4 Command/data word format. Decision logic data values shall require a specific binary data pattern of "ones" and "zeros" (such as, not all "ones" or all "zeros"). This reduces the likelihood of hardware or automata malfunctions satisfying the decision logic for critical function initiation or propagation.

4.5.12.6.2 Evaluation requirements. Analyses or tests shall verify the critical function routine design requirements under 4.5.12.6.1.

4.5.13 Electrical systems. The following requirements apply to the electrical characteristics of critical systems of both aircraft and missiles unless specified otherwise. These systems shall be designed to preclude accidental operation or single-component failure from activating or degrading critical functions. Requirements for combat aircraft, and air and ground missiles electrical subsystems are contained under 4.1, 4.2, and 4.3.

4.5.13.1 Electrical isolation

4.5.13.1.1 Design requirements. Critical circuits (both power and control) shall be electrically isolated from other critical and noncritical circuits. The purpose of this requirement is to stop faults or common mode malfunctions from operating critical circuits or explosive components in all environments. The following specific requirements apply to all nuclear weapon systems.

a. Electroexplosive circuitry that affects or is affected by critical functions shall conform to the requirements of MIL-STD-1512 as tailored to the specific system.

b. For hardwired systems and hardwired portions of multiplex systems, electrical functions that are unique to the aircraft monitor and control (AMAC) and release systems shall not share an electrical connector with non-nuclear functions.

c. Critical circuits shall be electrically isolated from potential sources of stray electrical power to ensure critical circuits are not activated.

d. Wire shields shall not be used as current-carrying conductors, and shields shall be covered by an insulation layer.

e. Within aircraft interface control units, critical function circuits shall be isolated from power, noncritical circuits, and other critical circuits using crush-resistant shielded compartments and separate wiring bundles.

4.5.13.1.2 Evaluation requirements. Analyses or tests shall verify the electrical isolation requirements under 4.5.13.1.1.

4.5.13.2 Electrical power

4.5.13.2.1 Design requirements. Electrical power circuits shall conform to the requirements of MIL-STD-704 as tailored to the specific system. Circuits to nuclear subsystems shall have twisted leads with single-point grounding of the return. Structure return shall be avoided to stop common mode problems.

4.5.13.2.2 Evaluation requirements. Analyses or tests shall verify the electrical power requirements in 4.5.13.2.1.

4.5.13.3 Hardwire switching

4.5.13.3.1 Design requirements. The supply side or power side of switchable circuits shall be switched. For critical circuits, both the supply and return sides shall be switched.

4.5.13.3.2 Evaluation requirements. Analyses or tests shall verify the hardwire switching requirements in 4.5.13.3.1.

4.5.13.4 Wiring and cabling

4.5.13.4.1 Design requirements

4.5.13.4.1.1 Shorting. Wiring and cabling shall be designed to prevent short circuits. The cable design shall provide for circumferential bonding of shielded wires.

4.5.13.4.1.2 Power, routing, grounding. Power distribution design and construction, cable routing, and wiring and cabling design shall isolate coupling to at least 20 dB below the operating levels required for critical circuits. Where used, signal returns common to two or more circuits shall use a common ground. Ground wire or shield braid gauge shall be chosen such that the largest current expected during system operation or credible failure shall either not offset the ground plane reference voltage or shall offset it by an order of magnitude less than that level at which system operation or logic state could change or ground-loop symptoms could occur.

4.5.13.4.1.3 Vibration and chafing. Electrical wiring to be installed, insulated, and secured to minimize vibration and chafing shall comply with MIL-W-5088 as tailored to the specific system.

4.5.13.4.1.4 Bonding. Electrical bonding for current return paths and other bonding requirements shall comply with MIL-STD-1818 as tailored to the specific system.

4.5.13.4.1.5 Critical electrical power. Except for weapon and warhead interface connectors, critical electrical power wiring shall end in female connectors at the power source side.

4.5.13.4.1.6 Critical circuits. Critical circuit wiring shall be provided with mechanical support that is an integral part of the connector at the entry point into the electrical connector. Mechanical support shall provide strain relief while the connector is being mated/demated and after mating/demating.

4.5.13.4.1.7 Mating/demating. Cables and connectors shall be designed to protect critical circuit wiring against damage during connector mating and demating procedures and during exposure to operational and maintenance environments.

4.5.13.4.1.8 Design for maintenance. Cable design and routing shall ensure against damage during maintenance operations.

4.5.13.4.2 Evaluation requirements. Analyses or tests shall verify the wiring and cabling requirements under 4.5.13.4.1.

4.5.13.5 Electrical connectors

4.5.13.5.1 Design requirements

4.5.13.5.1.1 Mismating. Electrical connectors shall be designed to prevent mating of wrong connectors.

4.5.13.5.1.2 Misalignment and damage. Electrical connectors shall be designed to prevent misalignment of connector components and bent pins during mating. Only one wire shall be used for each pin.

4.5.13.5.1.3 General. Hardwire electrical connectors associated with aircraft nuclear weapon circuits shall conform to MIL-C-38999 as tailored to the specific system.

4.5.13.5.1.4 Sealing. Connectors shall be environmentally sealed. If used in electrical connectors, potting compounds shall positively preclude reversion.

4.5.13.5.1.5 Single-connector circuits. Circuits within a single connector shall be designed to meet the requirements of 4.5.13.1. If any of these requirements cannot be met, the designer shall show that short circuits cannot be caused by bent pins. Connectors which carry critical circuits shall be designed to limit the coupled current from any bent pin to the critical circuit to at least 20 dB below the level required to operate the critical circuit function.

4.5.13.5.1.6 Shielded wire. Connectors shall be terminated to any carried shielded wire and shall use a backshell that provides for circumferential termination of the shield. Connectors shall use conductive finishes that shall not limit the termination of the shields.

4.5.13.5.1.7 Multipurpose connectors. Connectors shall not contain both discrete critical electrical circuits and lines carrying liquids such as coolants and hydraulic fluids.

4.5.13.5.1.8 Access to connectors. Sufficient access and space shall be provided to allow visible verification of mating and demating.

4.5.13.5.2 Evaluation requirements. Analyses or tests shall verify the electrical connector requirements under 4.5.13.5.1.

4.5.13.6 Voltage and current

4.5.13.6.1 Design requirements

4.5.13.6.1.1 Monitor and test limits. Monitoring and testing current for ordnance circuits shall be limited to a value that is 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.

4.5.13.6.1.2 Lightning. All ordnance devices and firing circuits shall be protected from the effects of direct lightning strikes to the weapon system. Critical circuits within aerospace vehicles (aircraft and missiles) shall meet the requirements of MIL-STD-1795 as tailored to the specific system for lightning strikes.

4.5.13.6.1.3 Static discharge. All critical circuits shall be protected against effects of electrostatic discharge.

4.5.13.6.2 Evaluation requirements

4.5.13.6.2.1 General. Analyses or tests shall verify the voltage and current requirements under 4.5.13.6.1.

4.5.13.6.2.2 Tests. Full scale tests, scale model tests, or analyses are required to demonstrate system invulnerability to static electricity and lightning. Test standards of MIL-STD-1757 as tailored to the specific system shall be used.

4.5.13.7 Panel construction and packaging

4.5.13.7.1 Design requirements. Panels and logic elements for critical electrical functions and weapon monitoring shall be environmentally insulated or hermetically sealed and shall have all external terminals fully insulated. This insulation/sealing shall prevent foreign objects and moisture from causing short circuits.

4.5.13.7.2 Evaluation requirements. Analyses or tests shall verify the panel construction and packaging requirements in 4.5.13.7.1.

4.5.13.8 Electromagnetic interference and compatibility

4.5.13.8.1 Design requirements

4.5.13.8.1.1 Environment. The electromagnetic systems environment shall be controlled in accordance with MIL-STD-1818 as tailored to the specific system.

4.5.13.8.1.2 Compatibility. The emission of and susceptibility to EMI for all subsystems/equipment shall be controlled in accordance with MIL-STD-461 as tailored to the specific system.

4.5.13.8.1.3 Nuclear safety. All electronic and electrical subsystems or equipment in or associated with nuclear weapon systems shall be designed to control undesired responses and emissions which might otherwise interfere with the monitor and control of nuclear weapons. Such equipment shall meet the applicable requirements of MIL-STD-1818, MIL-STD-461, and MIL-STD-462 as tailored to the specific system. AFSC Design Handbooks (DH) 1-4 and 1-12 contain specific nuclear safety design information. (Note: AFSC DH series handbooks shall not be called out in a contract; however, desired language may be tailored into a statement of work.) Wires, switches, cable connectors, junction points, shielding, filters, and other system elements shall be designed to stop undesired radiated and conducted interference or transients when such EMI could cause an initiation of ordnance or critical function.

4.5.13.8.2 Evaluation requirements. Analyses or tests shall verify the EMI/EMC requirements under 4.5.13.8.1. An EMC test shall be conducted on a production-configured aircraft to verify that on-board emitters and switching functions do not initiate critical functions.

4.5.13.9 Electromagnetic radiation

4.5.13.9.1 Design requirements

4.5.13.9.1.1 General. The weapon system shall be designed in accordance with MIL-STD-1818 as tailored to the specific system.

4.5.13.9.1.2 Critical function protection. Critical components, subsystems, and circuits shall not cause initiation of critical functions or inhibit critical status in the following minimum level EMR free-field environment: an average field intensity of 57 dB (mW/m^2) below 10 MHz and at least 194 volts per meter, the equivalent to 50 dB (mW/m^2) above 10 MHz (while operating or performing their intended function). Critical components, subsystems, and circuits shall also be immune to adverse affects from peak-pulsed intensities up to 92 dB (mW/m^2) (from 0.1-40 GHz) at any time that the system could pass within 1000 feet of antennas external to the weapon system.

4.5.13.9.1.3 Openings. Openings which allow access to cables, connectors, and other electrical equipment shall be shielded from radio frequency (RF).

4.5.13.9.1.4 Cables. Protection shall be provided for cables attached to components which could adversely respond to the RF environment and for all external cables attached to nuclear weapons.

4.5.13.9.1.5 Long leads. Circuit isolation devices that are insensitive to or protected from RF energy shall be provided and placed as close as possible to the units to be protected to prevent energy pickup by long leads.

4.5.13.9.1.6 Conductive skin. Where conductive aircraft or missile skin surfaces form part of the shielded enclosure, skin joints shall have low-resistance contacts with fastener spacing designed to minimize gap sizes. Monitor circuits shall be designed to not conduct or couple EMR energy into the shielded volume.

4.5.13.9.1.7 Firing circuits. Electroexplosive device (EED) circuit cabling between the firing unit and the EED that is not interrupted or protected from the transmission of induced current or short circuit shall use two wires which are twisted together and shielded. A single ground point shall be common to all firing circuits.

4.5.13.9.1.8 Electroexplosive devices. When EED's are used, their circuits shall be designed so that the maximum root mean square current in its bridge wire shall be 20 dB below the EED's maximum no-fire threshold when exposed to the tailored system EMR environments specified in the weapon system specifications or 57 dB (mW/m^2) average below 10 MHz and 50 dB (mW/m^2) average above 10 MHz, whichever is greater.

4.5.13.9.1.9 Monitor circuits. Monitor circuits shall not conduct or couple EMR energy into functional or control circuits.

4.5.13.9.1.10 Initiator case. The case of an initiator shall be electrically bonded to the structure. Removable parts of the case (removed during operational and maintenance procedures) shall not degrade the shielding after replacement or reassembly.

4.5.13.9.1.11 Shielded cable. Shields shall not be designed as intentional current carriers. Cable shields shall be terminated at a connector backshell that provides circumferential bonding of the shield.

4.5.13.9.1.12 Shielded connectors. Connectors having shielded critical circuits shall be provided with shielding caps when it is necessary to operate the system with the connector disconnected. When used, shielding caps shall be waterproofed and shall provide electrical continuity from shield to case with no gaps or discontinuities in the shielding configuration.

4.5.13.9.1.13 EED connectors. All EED connectors shall be covered with shielded caps in all configurations where the EED is not directly connected to the ordnance initiation system. This applies primarily during ordnance assembly and mating, but is valid at any time the EED cable is in an open circuit configuration.

4.5.13.9.1.14 Shielded sets within cable bundles. Shields for individual wire sets within cable bundles shall be electrically insulated up to their termination.

4.5.13.9.1.15 Shielded terminators. Shields shall be terminated via backshell, pigtail, or circumferential techniques. Pigtails shall be no longer than six (6) inches.

4.5.13.9.1.16 Terminal protection devices. Terminal protection devices (TPD's) such as filters and surge suppressors shall be used to provide additional circuit protection where shielding alone does not provide sufficient attenuation. TPD's shall also be used on unshielded line penetrations into the shielded volume.

4.5.13.9.2 Evaluation requirements. System analyses or tests shall verify the EMR requirements under 4.5.13.9.1. The analyses/tests shall be conducted to evaluate EMR hazards to electroexplosives, semiconductors and other devices. Also, the analyses/tests shall be conducted over a frequency range of 100 kHz to 40 GHz using field intensities as specified in 4.5.13.9.1.2 or the weapon stockpile-to-target sequence (STS), whichever is applicable.

4.5.13.10 Electromagnetic pulse

4.5.13.10.1 Design requirements. The system shall meet the tailored requirements of DOD-STD-2169.

4.5.13.10.2 Evaluation requirements. Full scale tests, scale model tests or analyses are required to verify the EMP requirements in 4.5.13.10.1 and overall system invulnerability to EMP.

4.5.14 Nonelectrical critical control signals

4.5.14.1 Design requirements

4.5.14.1.1 General. System-level safety devices and features required by this standard may be either electrical or nonelectrical devices. The requirements for data protection and uniqueness which apply to electrical circuits also apply to nonelectrical data transmission media.

4.5.14.1.2 Fiber optics. Fiber optics data buses shall comply with MIL-STD-1773 as tailored to the specific system.

4.5.14.2 Evaluation requirements. Analyses or tests shall verify the nonelectrical critical control signal requirements in 4.5.14.1.

4.5.15 Noncombat delivery vehicles and related equipment. Movement, by noncombat aircraft, of warhead/air vehicle assemblies shall be performed with the warhead separated from the air vehicle for safety purposes. The warhead and air vehicle shall each be transported in separate containers/handling fixtures. The nuclear weapon system STS document will define modes of transportation. Safety shall be incorporated into the design of noncombat delivery vehicles and equipment used to transport, store, support, load, and unload nuclear weapons. The vehicles and equipment shall meet appropriate structural, environmental, stability, and mobility requirements. The intent of these requirements is to prevent reportable damage to the nuclear weapon during handling and transportation, thereby minimizing nuclear weapon system deficiencies and preventing nuclear weapon incidents or accidents. The safety dezine factors shall allow for uncertainties in predicting operational conditions, uncertainties in material strength and manufacturing techniques, and uncertainties introduced by simplified design and test procedures. These requirements supplement good industrial design practices, standards, and features, and are not intended to prohibit the use of any commercial design of nonspecialized equipment (such as trucks, truck tractors, semitrailers, trailers, and cranes) which meet these requirements.

4.5.15.1 Vehicle/equipment structural requirements

4.5.15.1.1 Design requirements. The design load shall be the operational load multiplied by a minimum safety factor of two (2) based on excessive structural deflections or plastic deformation. The design load shall also be the operational load multiplied by a minimum safety factor of three (3) based on structural elastic instability (buckling), fracture, or composite material failure. These factors of safety shall be applied throughout the weapon support load path to prevent structural behavior as defined below:

a. Excessive structural deflections within material elastic range which could result in reportable nuclear weapon damage.

b. Plastic deformation caused by material yielding (0.2% offset or stress levels exceeding the minimum yield strength of the material as specified in MIL-HDBK-5 or applicable national standards).

c. Elastic instability (buckling) characterized by excessive and sudden structural deformation (collapse).

d. Composite material failure which can adversely affect the structural integrity.

e. Fracture characterized by structural failure usually associated with the material ultimate strength.

In addition, the minimum design load shall preclude fatigue failure in two (2) expected service lifetimes of cyclic load application. In determining allowable stresses for equipment, the designer shall select the material and allowable stress specified in Government publications (such as MIL-HDBK-5) and national standards (such as those produced by the Society of Automotive Engineers or the American Society for Testing and Materials). In cases where both an average and a minimum stress are specified, the minimum stress shall be used.

4.5.15.1.2 Evaluation requirements. Using a production-configured article, analyses and/or tests shall verify the requirements under 4.5.15.1.1.

4.5.15.1.2.1 General. The adequacy of the structural design shall be proven using the following methods as appropriate:

a. Analysis. A detailed stress analysis at the design load shall be performed and shall be supplemented by selective structural tests. Test results shall be correlated to the stress analysis results.

b. Nondestructive tests. If nondestructive stress tests are conducted, an abbreviated stress analysis shall be performed to determine all critical stress points. The test design load shall then be applied to the structure with suitable instrumentation at all critical stress points. This test shall not result in structural behavior as defined in 4.5.15.1.1.

(1) Mobility and/or functional test results shall be used to verify the operational load.

(2) The test load shall be the verified operational load multiplied by the appropriate safety factor as defined in 4.5.15.1.1.

(3) The lateral test load shall be applied statically with the equipment simultaneously loaded to its rated capacity. The longitudinal test load shall be applied statically with the equipment simultaneously loaded to its rated capacity. The vertical test load shall be applied statically and independently.

(4) Test results shall be correlated to the abbreviated stress analysis results to determine if the structure meets the design requirements.

c. Destructive tests. If destructive stress tests are conducted, test loads shall be applied simultaneously to the test article along the appropriate axes until the item exhibits a structural behavior as defined in 4.5.15.1.1. The test loads at this point must exceed the design load in each appropriate axis.

4.5.15.1.2.2 Materials analysis. A materials analysis shall be performed and shall include:

a. A materials list.

b. Specific processes which result in material property changes not identified in MIL-HDBK-5.

4.5.15.2 Ground transportation equipment. In addition to the structural requirements of 4.5.15.1, the following requirements also apply to trailers and semitrailers, self-propelled ground vehicles, forklifts, and weapon loaders used to transport nuclear weapons on their basic structure.

4.5.15.2.1 Basic frame support

4.5.15.2.1.1 Design requirement. The nuclear weapon shall be supported during transport by a structural load path which meets the structural design requirements rather than by lift arms, cables, or hydraulic systems. (This requirement does not apply to tires, vehicle suspension, or equipment used only to position or transfer nuclear weapons in a designated area such as a weapon storage area.)

4.5.15.2.1.2 Evaluation requirement. The equipment shall be analyzed and/or tested to ensure the weapon is supported during transport by a structural load path which meets the structural design requirements rather than by lift arms, cables, or hydraulic systems. This requirement does not apply to equipment used solely to position or transfer weapons.

4.5.15.2.2 Static grounding

4.5.15.2.2.1 Design requirements. Static grounding provisions shall be provided for equipment dezined for specific nuclear weapon systems to prevent static electrical discharge through the weapon. A uniform electrical grounding potential shall be maintained on all structural components separated by insulating materials and in direct contact with the weapon. The impedance of the grounding path shall be no greater than 10 ohms.

4.5.15.2.2.2 Evaluation requirements. Analyses and/or tests shall be performed to determine if the system provides a grounding path with an impedance of less than 10 ohms.

4.5.15.2.3 Fire propagation

4.5.15.2.3.1 Design requirement. The equipment shall be designed to protect against exposure of the nuclear weapon to a fire and resultant thermal environment. The equipment shall protect against leaks or failures in vehicle electrical, fuel, hydraulic, or other systems that could initiate a fire.

4.5.15.2.3.2 Evaluation requirement. The equipment shall be analyzed and/or tested to ensure the potential for fire propagation due to failure is minimized.

4.5.15.2.4 Mechanical shock

4.5.15.2.4.1 Design requirement. The equipment shall be designed to attenuate mechanical shock transmission to a nuclear weapon to within the applicable STS environment.

4.5.15.2.4.2 Evaluation requirement. The equipment shall be analyzed and/or tested to ensure that mechanical shock transmission to the nuclear weapon is within the applicable STS requirement range.

4.5.15.2.5 Tiedown/restraint

4.5.15.2.5.1 Design requirement. The tiedown/restraint provisions for ground transport of all nuclear weapons shall be capable of restraining the design load as defined in 4.5.15.1.

4.5.15.2.5.2 Evaluation requirement. The tiedown/restraint provisions for ground transport of nuclear weapons shall be tested to ensure their capability of restraining their design load.

4.5.15.2.6 Braking

4.5.15.2.6.1 Design requirement. All equipment capable of freewheeling shall be designed to restrain itself with its rated load. Parking brakes shall be designed to hold the vehicle with fully loaded equipment, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.2.6.2 Evaluation requirement. Brake systems shall be tested while transporting or towing simulated loads that represent the worst load conditions (such as max weight and extreme center of gravity) expected in service. The parking brake shall be tested to verify the capability to hold the vehicle with fully loaded equipment, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.2.7 Stability

4.5.15.2.7.1 Design requirement. The equipment shall not tip, tilt, yaw, sway, skid, or jackknife in a way that may result in reportable damage to the weapon while loaded in the most adverse load configuration and while undergoing maximum performance maneuvers (such as emergency braking, obstacle avoidance, etc.).

4.5.15.2.7.2 Evaluation requirement. The equipment shall be tested to undergo maximum performance maneuvers to evaluate stability.

4.5.15.2.8 Mobility

4.5.15.2.8.1 Design requirement. Applicable mobility requirements of MIL-STD-1784 as tailored to the specific system shall be met. Equipment which does not have mobility requirements specified in a military standard shall meet mobility requirements based on the operational environment.

4.5.15.2.8.2 Evaluation requirement. Mobility testing requirements of applicable standards and test requirements based on operational conditions shall be met. Mobility testing shall be accomplished to verify structural integrity, stability, and safety.

4.5.15.2.9 Roadability

4.5.15.2.9.1 Design requirement. The equipment must meet the roadability requirements of MIL-STD-1784 as tailored to the specific system.

4.5.15.2.9.2 Evaluation requirement. Analyses and/or tests shall be performed to ensure that the equipment meets the roadability requirements specified in 4.5.15.2.9.1.

4.5.15.2.10 Environment safe operation

4.5.15.2.10.1 Design requirement. The equipment must be capable of safe operation in the most adverse normal environment as specified in the design specifications.

4.5.15.2.10.2 Evaluation requirement. Environmental analyses and/or tests shall be conducted in accordance with MIL-STD-810 as tailored to the specific system, as required, to verify safe operation at extreme normal environments (such as temperature, EMI, etc.) with the equipment loaded at rated capacity.

4.5.15.3 Trailers and semitrailers. In addition to the requirements of 4.5.15.2, trailers and semitrailers shall also meet the following requirements.

4.5.15.3.1 Service brake systems

4.5.15.3.1.1 Design requirement. Service brake systems shall meet the requirements of MIL-STD-1784 as tailored to the specific system.

4.5.15.3.1.2 Evaluation requirement. The service brake system shall be tested in accordance with MIL-STD-1784 as tailored to the specific system.

4.5.15.3.2 Emergency brake systems

4.5.15.3.2.1 Design requirement. Trailers using towbars shall have an emergency braking system which shall automatically activate in case of inadvertent towbar disconnect and bring the trailer to a controlled stop without reportable weapon damage.

4.5.15.3.2.2 Evaluation requirement. The emergency braking system of trailers using towbars shall be tested to verify the trailer performance during accidental towbar disengagement by full-scale testing or by limited analysis and testing. The full-scale testing shall be conducted while towing the fully loaded trailer over a straight, smoothly paved road at the maximum operating speed expected. Disengage the towbar from the tow vehicle and observe the emergency braking action of the trailer. In testing the emergency brake system, record the following:

a. Distance from the point of towbar disengagement to final stop;

b. Lateral distance of travel from the point of towbar disengagement to final stop;

c. Attitude of the trailer at the time of stop; and

d. Reportable weapon damage incurred by the trailer or load as a result of disengagement.

4.5.15.4 Tow vehicles. In addition to the requirements of 4.5.15.2, tow vehicles (such as trucks, tugs, and tractors) shall also meet the following requirements.

4.5.15.4.1 Brake system

4.5.15.4.1.1 Design requirements. The brake system shall be functionally compatible with the towed vehicle brake system. The combination shall not tip, tilt, yaw, sway, skid, or jackknife in a way that may cause reportable damage to the weapon under maximum performance maneuvers. The brake performance shall meet the applicable requirements of Federal Motor Carrier Safety Regulations 393.42 and 393.52.

4.5.15.4.1.2 Evaluation requirements. Testing shall be accomplished with the most adverse operational towing/towed vehicle combination load configuration toverify functional compatibility. The towing vehicle performance shall be evaluated to ensure that it does not tip, tilt, yaw, sway, skid, or jackknife in a way that may cause reportable damage to the weapon under maximum performance maneuvers. The brake performance shall meet the applicable requirements of Federal Motor Carrier Safety Regulations 393.42 and 393.52. In addition, the tow vehicle shall be tested by progressively increasing the speed from which stops are made, in increments of about 5 mph, up to the maximum rated speed of the vehicle. Continue this procedure until failure occurs or until the maximum safe speed has been attained, whichever occurs first. Make the initial tests on a dry, brushed, level concrete surface. Stop the vehicles by operating the brake system to produce maximum braking force ("panic stops"). 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 the following data (as a minimum) on the brake performance: damage or excessive wear, stopping distances, speed range, contact of wheels with the ground.

4.5.15.4.2 Parking brakes

4.5.15.4.2.1 Design requirement. The parking brakes, together with the towed vehicle parking brakes, shall hold a fully loaded towing and towed vehicle combination, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.4.2.2 Evaluation requirement. Testing shall be accomplished to verify the capability of the towing and towed vehicle combination parking brakes to hold the combination, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.4.3 Vehicle connecting device

4.5.15.4.3.1 Design requirement. The vehicle connecting device shall be compatible with that of the towed vehicle and shall meet the structural requirements of 4.5.15.1.1.

4.5.15.4.3.2 Evaluation requirement. The vehicle connecting device structural integrity shall be verified by the methods of 4.5.15.1.2.

4.5.15.4.4 Fifth wheel safety latch

4.5.15.4.4.1 Design requirement. The fifth wheel (if used) shall be equipped with a safety latch to prevent inadvertent disconnect. The safety latch shall allow a visual verification of the locked condition.

4.5.15.4.4.2 Evaluation requirement. Test the fifth wheel safety latch for proper design implementation.

4.5.15.4.5 Movement controls

4.5.15.4.5.1 Design requirements. All movement controls (except for such devices as the parking brake, steering control, transmission selectors, power takeoff, and hydraulic pump) shall be self-centering. The engine start switch shall operate only in the automatic transmission "neutral" or "park" position and only in the standard transmission "clutch-disengaged" position, as applicable.

4.5.15.4.5.2 **Evaluation requirements.** Test to ensure the appropriate movement controls are self-centering. Test to ensure that the engine start switch shall only operate in neutral, park, or with the clutch disengaged, as applicable.

4.5.15.4.6 **Increment of movement**

4.5.15.4.6.1 **Design requirement.** The vehicle design shall include a capability for small increments of movement compatible with required use.

4.5.15.4.6.2 **Evaluation requirement.** Test capability for small increments of movement compatible with required use.

4.5.15.5 *Non-tow self-propelled vehicles*

4.5.15.5.1 **Design requirements.** In addition to the requirements of 4.5.15.2,non-tow self-propelled vehicles (such as trucks, vans, and high-lift trucks) shall comply with the applicable service brake performance requirements of Federal Motor Carrier Safety Regulations 393.43 and 393.52. Structural requirements (3.5.15.1.1.) shall apply to components which directly interface with the weapon and its handling equipment.

4.5.15.5.2 **Evaluation requirements.** In addition to the general analysis and test requirements, non-tow self-propelled vehicles shall undergo brake system testing to ensure compliance with the Federal Motor Carrier Safety Regulations. Structural evaluation shall be accomplished using the methods of 4.5.15.1.2.

4.5.15.6 **Forklifts and weapon loaders.** In addition to the requirements of 4.5.15.2, conventional forklifts, bomb-lift trucks, high-lift trucks, munitions handling trailers with lifting devices, and 463L loading and unloading trucks shall also meet the following requirements.

4.5.15.6.1 **Lift system safe control**

4.5.15.6.1.1 **Design requirements.** The lift system shall be designed to maintain safe control of the rated load if electrical, hydraulic, or pneumatic system failure occurs. Failure of single active components shall not result in uncommanded or uncontrolled payload movement which can result in personnel injury, equipment damage, or reportable weapon damage. If fail-safe design is achieved through the use of redundant components, a means of detecting failure of the redundant system shall be provided.

4.5.15.6.1.2 **Evaluation requirements.** Test to verify that safe control of the rated load shall be maintained if electrical, hydraulic, or pneumatic system failure occurs. Perform a fault-tree and common-cause analysis.

4.5.15.6.2 **Hydraulic and pneumatic systems**

4.5.15.6.2.1 **Design requirements.** The lift system shall be designed with pressure relief valves or regulators in hydraulic and pneumatic systems to prevent overpressure. Internal leakage in lift-system hydraulic components shall be limited so that the maximum drift rate of the lift system does not result in reportable weapon damage. The maximum drift rate for weapon loaders used in weapon assembly and in loading or unloading shall be based on the required use of the loader.

4.5.15.6.2.2 **Evaluation requirements.** Test hydraulic and pneumatic systems to verify that overpressure shall be prevented. Also, test the drift rate at ambient and extreme temperature conditions to verify safe operation based on the required use of the loader.

4.5.15.6.3 **Center of gravity compatibility**

4.5.15.6.3.1 **Design requirement.** The equipment center of gravity and the rated load center of gravity must be compatible under the worst case normal operational environments to which the vehicle will be subjected.

4.5.15.6.3.2 Evaluation requirement. Test, to ensure forklift tine and adapter compatibility with the rated load center of gravity, in the worst case normal operational environments to which the vehicle is subjected.

4.5.15.6.4 Movement controls

4.5.15.6.4.1 Design requirements. All movement controls (except for such devices as the parking brake, steering control, transmission selectors, power takeoff, and hydraulic pump) shall be self-centering. The engine start switch shall operate only when the clutch is disengaged, or the automatic transmission is in the "neutral" or "park" positions.

4.5.15.6.4.2 Evaluation requirements. Test to show appropriate movement controls are self-centering. Test to show the engine start switch operates only when the clutch is disengaged, or the automatic transmission is in the "neutral"or "park" positions.

4.5.15.6.5 Positive restraint

4.5.15.6.5.1 Design requirement. The design shall provide for positive means of maintaining control of the nuclear weapon at all times in the lifting and handling modes. Restraint systems shall meet structural requirements of 4.5.15.1.1.

4.5.15.6.5.2 Evaluation requirement. Analyze and/or test to show how positive restraint of the nuclear weapon shall be maintained. Evaluate attachment points and straps, if used, by the methods of 4.5.15.1.2.

4.5.15.6.6 Increment of movement

4.5.15.6.6.1 Design requirement. Weapon loader design shall include a capability for small increments of movement.

4.5.15.6.6.2 Evaluation requirement. Test capability for small increments of movement compatible with required use.

4.5.15.6.7 Overtravel

4.5.15.6.7.1 Design requirement. Design features shall be included to prevent overtravel in all directions of the lift control.

4.5.15.6.7.2 Evaluation requirement. Test overtravel prevention capability.

4.5.15.6.8 Lifting attitude

4.5.15.6.8.1 Design requirement. The lift system shall be capable of providing a synchronized lifting attitude.

4.5.15.6.8.2 Evaluation requirement. Test to show the equipment can provide a uniformly controlled lifting attitude.

4.5.15.6.9 Brake system

4.5.15.6.9.1 Design requirements. Forklift parking brakes shall be able to 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 independently hold a fully loaded weapon loader, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.6.9.2 Evaluation requirements. Test forklift parking brakes on an 8.5-degree incline while loaded with rated capacity in both forward and reverse directions. Test weapon loader service and parking brakes to verify their capability of holding the vehicle fully loaded, facing both uphill and downhill on an 11.5-degree incline or greater, depending upon expected operation.

4.5.15.7 Hoists, cranes and similar devices. These requirements apply to hoists, cranes, winches, and similar devices. Such equipment, in addition to the structural requirements of 4.5.15.1, shall also meet the following requirements.

4.5.15.7.1 Movement controls

4.5.15.7.1.1 Design requirements. Controls shall ensure the load is under positive operator control. The control design shall have the following features:

a. Automatic stop in the absence of operator control;

b. Automatic stop if the operating mechanism fails;

c. Synchronized operations; and

d. Design features which prevent overtravel of a hoist on rails and stop the chain or wire rope when the hook reaches its upper limit.

4.5.15.7.1.2 Evaluation requirements. Test the device at the rated load to verify:

a. An automatic stop in the absence of operator control;

b. An automatic stop if the operating mechanism fails or power is lost;

c. Synchronized operations; and

d. Design features prevent overtravel of a hoist on rails and stop the chain or wire rope when the hook reaches its travel limit.

4.5.15.7.2 Hook safety devices

4.5.15.7.2.1 Design requirement. Hooks shall be fitted with throat-opening safety devices.

4.5.15.7.2.2 Evaluation requirement. Inspect to ensure that hooks are fitted with throat-opening safety devices.

4.5.15.7.3 Blocks and rope safety factor

4.5.15.7.3.1 Design requirement. A minimum safety factor of ten (10) based on breaking strength for blocks, rope falls, fiber rope, and webbing shall be provided.

4.5.15.7.3.2 Evaluation requirement. Test blocks, rope falls, fiber rope, and webbing to verify a minimum safety factor of ten (10) based on breaking strength.

4.5.15.7.4 Load chains and accessory parts safety factor

4.5.15.7.4.1 Design requirement. A minimum safety factor of five (5) based on the breaking strength for load chains and all accessory parts (such as hooks, rings, shackles, slings, and wire ropes) shall be provided.

4.5.15.7.4.2 Evaluation requirement. Test load chains and all accessory parts (such as hooks, rings, shackles, slings, and wire ropes) to verify a minimum safety factor of five (5) based on the breaking strength.

4.5.15.8 Handling equipment and support fixtures. Handling and support fixtures (such as load frames, hoist trolleys, test/storage stands, handling units, containers, pallets, spreader bars/beams, etc.) shall meet the following requirements.

4.5.15.8.1 Structural integrity

4.5.15.8.1.1 Design requirement. Structural integrity of handling and support fixtures shall be designed using the requirements of 4.5.15.1.1.

4.5.15.8.1.2 Evaluation requirement. Structural integrity of handling and support fixtures shall be verified using the methods of 4.5.15.1.2.

4.5.15.8.2 Mobility

4.5.15.8.2.1 Design requirements. Applicable mobility requirements of MIL-STD-1784 as tailored to the specific system shall be met. Castered equipment which does not have mobility requirements specified in a standard shall meet mobility requirements based on the operational environment.

4.5.15.8.2.2 Evaluation requirements. Mobility testing of castered equipment shall be accomplished in accordance with applicable standards and operational requirements to verify stability and safety.

4.5.15.8.3 Containers

4.5.15.8.3.1 Design requirements. Containers used for storing and transporting weapons shall use the design requirements in MIL-STD-209 and MIL-STD-648 as tailored to the specific system.

4.5.15.8.3.2 Evaluation requirements. Containers shall be analyzed and/or tested as necessary to ensure compliance with the requirements in MIL-STD-209 and MIL-STD-648 as tailored to the specific system.

4.5.15.8.4 Pallets

4.5.15.8.4.1 Design requirements. Pallets shall conform to MIL-STD-1366 as tailored to the specific system.

4.5.15.8.4.2 Evaluation requirements. Pallets shall be analyzed and/or tested as necessary to verify compliance with MIL-STD-1366 as tailored to the specific system.

4.5.15.9 Air cargo restraint systems. Air transportable delivery vehicles and support equipment shall be designed to meet the general specifications of MIL-STD-1791 as tailored to the specific system.

4.5.15.9.1 Design requirements. The structural design (including tiedown rings and attachment points) shall be capable of restraining the nuclear cargo when subjected to the G-loads specified in Table I as follows:

TABLE I. Nuclear weapon tiedown configuration G-load factors for cargo aircraft.

Load Direction	G-Load
Forward	3.0
Aft	1.5
Lateral	1.5
Vertical (Down)	4.5
Vertical (Up)	3.7

4.5.15.9.2 Evaluation requirements. Testing shall be accomplished to show that the restraint configuration is capable of withstanding the G-loads specified in Table I.

4.5.15.10 Production articles

4.5.15.10.1 Design requirements. If fail-safe features are used, they shall be evaluated or tested to demonstrate that they provide safe control of the weapon in any applicable system failure.

4.5.15.10.2 Evaluation requirements

4.5.15.10.2.1 Operational tests. Operational equipment proof tests shall be performed on at least one fully configured production article (and other designated samples as necessary) to demonstrate that the item shall function properly with specified operational loads.

4.5.15.10.2.2 Environmental tests. Selected environmental tests shall be performed on production articles as required after considering the intended use of the vehicle or support equipment.

4.5.15.10.2.3 Hoists. All hoists shall be tested after installation to 125% of the rated capacity.

4.5.15.10.2.4 Composite structures. Composite structures shall have 100% production article testing at the design load. Manufacturing controls combined with non-destructive inspection (NDI) may be substituted for testing if approved by both the procuring MAJCOM engineering agency and the independent engineering evaluation/review agency.

4.5.16 Test and training equipment. The following design requirements apply to test equipment and training devices which interface with nuclear weapons and critical components on combat aircraft and missile systems.

4.5.16.1 Design requirements

4.5.16.1.1 Use of reserve nuclear weapons. A war reserve nuclear weapon or warhead shall not be used as a troubleshooting aid to confirm the existence of a fault, to fault isolate, or to verify a fault has been corrected. The nuclear weapon system and maintenance procedures shall support this requirement.

4.5.16.1.2 Testability. A means shall exist to verify the operation and control of critical nuclear functions on the system or unit under test.

4.5.16.1.3 Release/suspension preload test. Test equipment shall have the capability to perform an aircraft and release and suspension equipment preload test prior to connecting a nuclear weapon, warhead, or release system to a nuclear weapon system.

4.5.16.1.4 Test criteria. Based on weapon system requirements, test equipment shall detect system faults, such as improper wiring, line-to-line shorts, line-to-ground shorts, stray voltage, and improper system operation.

4.5.16.1.5 Safety during test. Test equipment shall have positive measures to prevent activating any portion of any critical function when nuclear weapons are present. Specifically included are the following:

a. Generation of a release, jettison, or launch signal;

b. Negation of the Two-Person Concept requirement for control of nuclear consent for unlocking the release system or prearming the weapon;

c. Unlocking the reversible inflight lock; and

d. Operation of the propulsion system ignition safety device or the A&F system safety device.

4.5.16.1.6 Further safety considerations. Test equipment shall be designed to prevent the following conditions:

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

b. Faults within a tester that could activate ordnance devices of the equipment undergoing test; and

c. Introduction of signals or electrical power of sufficient magnitude to activate ordnance devices or inadvertently actuate any critical function.

4.5.16.1.7 Safe state tests. Test equipment which operates components during a test shall ensure that the components are in a safe state at the completion of the test. The safe condition shall be verified to the operator.

4.5.16.1.8 Electrical fault testing. If separate support equipment is used to test for electrical faults in aircraft, the following pertains:

a. Preloading tests shall show faults in any of the critical functions.

b. Preflight testing, postflight testing, and periodic testing shall be done at the connector(s) interfacing with the weapon to the farthest termination in the combat delivery vehicle (end-to-end check).

c. Isolation resistance tests of all critical circuits external to the weapon shall be done periodically.

d. Isolation resistance tests of the combat delivery vehicle shall be done wherever possible during routine time phase testing.

4.5.16.1.9 Inadvertent operation of item under test. Test equipment shall not cause an item under test to operate or fire unless specifically designed to do so.

4.5.16.1.10 Protection during BITE failure. Failure modes of built-in-test equipment (BITE) shall not be capable of operating critical components or initiating critical functions.

4.5.16.1.11 Built-in test equipment. Critical components which require frequent periodic testing shall have BITE where feasible.

4.5.16.1.12 Minimization of tests. Equipment to test the control, launch, or release systems shall meet the following criteria:

a. Use test equipment only where necessary to set up and verify system operation and safety;

b. Minimize testing after the nuclear weapon is mated to the combat delivery vehicle; and

c. Keep the interval between required tests on nuclear weapon systems to the maximum needed to assure a high confidence level in system operation and safety.

4.5.16.1.13 Maintenance of test equipment. Test equipment shall have periodic maintenance, inspection, and test provisions to ensure it remains in its design certified state.

4.5.16.1.14 Nuclear safety during test equipment failure. A single failure within test equipment shall not cause, initiate, or fail to detect faults in the system under test that could result in any of the following critical events when nuclear weapons are present:

a. Generation of a release or launch signal;

b. Enabling of the consent function;

c. Enabling of the authorization function;

d. Unlocking of the reversible in-flight lock;

e. Operation of the A/D or S&A device; and

f. Initiation of any other critical function or subfunction.

4.5.16.1.15 BITE design. BITE for nuclear weapon systems shall comply with all design and safety requirements that apply to the system/subsystem within which they reside.

4.5.16.1.16 Computer-controlled test equipment. Computer-controlled test equipment shall meet the designated requirements of computer control systems in this standard.

4.5.16.1.17 Electromagnetic emissions. Test equipment shall control emissions to prevent undesired responses in the nuclear weapon system.

4.5.16.1.18 Electromagnetic interference. Electrical system elements of the test equipment shall not cause electrical transients or radiated or conducted interferences with the nuclear weapon system.

4.5.16.1.19 Electromagnetic susceptibility of test equipment. Test equipment shall not have undesired responses or emissions because of EMC/EMI. Refer to MIL-STD-461 for applicable class of test equipment.

4.5.16.1.20 Testing of redundant features. Where redundant features are present in the weapon system (such as parallel circuits), BITE shall indicate the integrity of both the primary and the redundant function.

4.5.16.1.21 Identification of training weapons. Training weapons or missiles and their components shall be explicitly identified as training items.

4.5.16.1.22 Realism of training equipment. Nuclear weapon training equipment and devices shall require controls and responses to ensure that training does not differ from actual weapon system operations.

4.5.16.2 Evaluation requirements. These evaluation requirements apply to BITE, monitor and control test equipment, release or launch test equipment, nuclear bomb or warhead testers, special critical component test equipment, and general test equipment used on critical components.

4.5.16.2.1 General. Equipment shall be evaluated by analysis and/or test to verify the requirements of 4.5.16.1.

4.5.16.2.2 Circuit analysis. An analysis shall be performed of the tester operating with the circuits of the equipment to be tested.

4.5.16.2.3 Test concept. An analysis of the tester interface with the weapon system shall be performed to verify the test concept.

4.5.16.2.4 Fit and function test. Perform a fit and function demonstration showing compatibility of the mechanical and electrical designs with the nuclear weapon system.

4.5.16.2.5 Fault correction demonstration. Demonstrate field level operations and procedures.

4.5.16.2.6 Procedures. Demonstrate maintenance and inspection procedures which verify integrity of the testers prior to use.

4.5.17 Support equipment

4.5.17.1 Design requirements. Support equipment shall be identified which may require nuclear safety certification. The selection criteria for support equipment to require certification includes the vehicles and equipment used during assembly, test, maintenance, storage, transfer, movement, transport, and loading of weapons, weapon components, and subsystems. It also includes special test equipment.

4.5.17.2 Evaluation requirements

4.5.17.2.1 General. Support equipment shall be evaluated within its intended environment, maintenance concept, and operational concept. Fail-safe features designed into equipment shall be evaluated to determine if they provide safe control of the weapon under all normal environments and for system failures which could place the nuclear weapon in an unsafe condition. Applicable analyses conducted on support equipment shall be reported. The information shall include the description, operation, and analysis of all support equipment which must be nuclear safety certified. The analyses shall include the relation of the support equipment to the nuclear weapons or critical components, functional analysis, safety features, and impact on nuclear safety.

4.5.17.2.2 Compatibility. Tests of support equipment shall be conducted to ensure the equipment is compatible with its intended use.

4.5.17.2.3 Nonspecialized equipment. Nonspecialized equipment shall be evaluated for nuclear safety adequacy according to the appropriate standards, specifications, and designated tests.

4.5.18 Facilities

4.5.18.1 Nuclear weapon storage and maintenance. All facilities used to store and maintain nuclear weapons must be Air Force approved, and all installed equipment used to lift, handle, suspend, or test nuclear weapons must be nuclear certified. The design and construction of the facilities is accomplished under the direction of the Corps of Engineers or the Air Force Regional Civil Engineer.

4.5.18.1.1 Design requirements. A facilities requirements plan shall be prepared identifying all facilities and installed equipment required to support a nuclear weapon system. This plan shall be used by the Corps of Engineers (or the using command civil engineering organization, if overseas) to prepare detailed facility drawings. To support the facilities requirements, participation in preliminary design conferences and design reviews, and review of facility drawings prepared by the Corps of Engineers is required. Contracts for constructing the facilities are issued by the Corps of Engineers following final design approval.

4.5.18.1.2 Evaluation requirements. Test requirements shall be developed from the facilities requirements plan and from the requirements for facility installed equipment under 4.5.15.7 and 4.5.15.8. These test requirements shall be integrated into system test plans, detailed test requirements, or any other test planning documents. The required tests for facility installed equipment must be performed prior to their use. An EMI/EMR survey shall be accomplished if applicable.

4.5.18.2 Critical component storage. Certified critical components must be stored by one of the following methods when not under the control of a Two-Person Concept Team. Components in temporary storage, such as Minuteman missile guidance sets remaining overnight at launch control facilities, must be maintained in an area designated as a no-lone zone and protected according to the component's level of security classification. Decertified critical components do not require special storage other than what is needed to meet the security classification of the item.

4.5.18.2.1 *Design requirements*

4.5.18.2.1.1 Facilities and detectors. Certified critical components must be stored either in a vault that meets the construction requirements of a Class A or B vault with an intrusion detection system (IDS) reporting to a remote, continuously manned location; or in a vault or other facility that does not meet the construction requirements of a Class A or B vault but which has entrance and interior detectors, both reporting independently to a remote, continuously manned location. All detectors/sensors utilized must comply with Base and Installation Security System Specification BIS-SYS-10000. See 4.3.7 for vault construction requirements for certified critical component storage.

4.5.18.2.1.2 **No-lone zone/line supervision.** For either of the storage methods in 4.5.18.2.1.1, the components must be stored in an area designated as a no-lone zone that also meets the storage requirements specified in DOD 5200.1-R/AFR 205-1, according to the component's level of security classification. In addition, every entrance to the no-lone zone must be secured by two approved key or combination locks. Only authorized individuals will have control of the keys or know the combinations to the locks, and no single individual will have control of both keys or know the combinations to both locks. Also, the alarm reporting circuits must incorporate a "line supervision" scheme which will detect any tampering with the circuits and report as an alarm to the remote manned location.

4.5.18.2.2 **Evaluation requirements.** Demonstrations or analyses shall verify the storage requirements in 4.5.18.2.1.

4.5.19 **Technical orders.** Technical orders (TO's) will be acquired in accordance with AFR 8-2, TO 00-5-1, and TO 00-5-3. The TO requirements process is described in TO 00-5-1. The developing agency and SA-ALC/NWI shall monitor TO development through review of preliminary TO's and participation in reviews. SA-ALC/NWI shall chair reviews and validation/verifications for its assigned TO's. SA-ALC/NWI is the Technical Order Content Manager for -16, -25, and -30 TO's and category 11-N air-launched-missile/warhead mate/demate TO's, in accordance with TO 00-5-1, and TO 00-5-3; SA-ALC/NW is the TOMA for 11-N series TO's; and OO-ALC is the TOMA for the 21-LG series TO's for ground-launched missiles.

4.5.19.1 **TO process.** The TO acquisition and distribution process shall be followed in accordance with TO 00-5-2 and TO 00-5-3.

4.5.19.2 **TO review and approval.** TO's will be reviewed and approved by appropriate TOMA and responsible approving agency.

5. DETAILED REQUIREMENTS

5.1 Combat delivery aircraft. The following requirements apply to AMAC systems; to required safety devices; and to delivery, launch, suspension, and release systems in aircraft.

5.1.1 General requirements. The weapon system shall meet the requirements of 4.4 for prearm commands, inadvertent release/jettison with system locked, inadvertent release/jettison with system unlocked, and inadvertent power application (to the weapon interface). These requirements apply for each weapon type and release system configuration.

5.1.2 Integrated stores management system. Integrated armament stores management systems (SMS's) that control both nuclear and nonnuclear weapons are authorized provided the nuclear safety requirements of this standard are met. Unless specifically restricted, the safety devices required by this standard for nuclear weapons may also be used for the nonnuclear stores.

5.1.3 Electrical power failure

5.1.3.1 Design requirements

5.1.3.1.1 Effect on safing. Aircraft electrical power failure shall not jeopardize the safe condition of a weapon. Furthermore, the opening of a circuit breaker or other circuit protective device must not cause a critical function to occur.

5.1.3.1.2 Backup power. Prearm, unlocking, S&A, and A/D devices shall have an automatically powered backup or secondary power source. Loss of the primary power source shall not inhibit the safing of these devices.

5.1.3.2 Evaluation requirements. Analyses or tests shall verify the electrical power failure requirements under 5.1.3.1.

5.1.4 Power application

5.1.4.1 Design requirements. For a prearmed release of nuclear bombs, electrical power shall be applied on designated pin(s) of the weapon interface connector before and during electrical separation of the bomb from the aircraft. These pins are identified in the AMAC specifications.

5.1.4.2 Evaluation requirements. Analyses or tests shall verify the power application requirements in 5.1.4.1.

5.1.5 Reversibility

5.1.5.1 Design requirement. Devices for authorization, prearming, propulsion system ignition safing, and aircraft release system locking shall be reversible.

5.1.5.2 Evaluation requirement. Analyses or tests shall verify the reversibility requirement in 5.1.5.1.

5.1.6 Single-component failure

5.1.6.1 Design requirement. The malfunction or accidental operation of a single component shall not result in unintended power application to a nuclear weapon interface or initiation of a critical function.

5.1.6.2 Evaluation requirement. Analyses or tests shall verify the single-component failure requirement in 5.1.6.1.

5.1.7 Aircrew notification

5.1.7.1 Design requirements. The aircrew shall be made aware of the following events:

a. Unlocking of, or an unlock signal to, the reversible in-flight lock when unlocking has not been commanded by normal operation of controls;

b. Prearming of, or a prearm signal to, a weapon when prearming has not been commanded by normal operation of controls;

c. The safe or prearm status of a nuclear weapon (designed to be monitored) which cannot be positively determined. A delay may be designed into the system so that the aircrew shall not receive a caution during weapon change of state from safe to prearm or from prearm to safe; and

d. Nuclear weapon release signals occurring when not commanded by normal operation of controls.

5.1.7.2 Evaluation requirements. Analyses or tests shall verify the aircrew notification requirements in 5.1.7.1.

5.1.8 Interface requirements

5.1.8.1 Design requirements. The aircraft shall meet the applicable AMAC Project Officers Group (POG) interface specifications/standards for each nuclear weapon designated for carriage. Control of power to interface units and weapon interfaces shall require:

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

b. A separate control that removes power from the interface unit (logic and switching assemblies);

c. Positive action to supply power at the weapon interface; and

d. A separate control that removes power from the weapon interface.

5.1.8.2 Evaluation requirements. Analyses or tests shall verify the interface requirements under 5.1.8.1.

5.1.9 Suspension and release systems. Suspension and release systems interface with nuclear stores for the purpose of carriage (during flight and ground operations) and provide for store separation upon authorized command.

5.1.9.1 Design requirements

5.1.9.1.1 Suspension and release

5.1.9.1.1.1 General. The suspension and release system shall meet the criteria of MIL-STD-2088 as tailored to the specific system.

5.1.9.1.1.2 Inadvertent release. The suspension and release system shall prevent weapon separation, release, ejection, launch, or jettison by any means except the proper operation of control devices.

5.1.9.1.1.3 Two independent operations. Operation of the release system shall be controlled by two independent functions: an unlocking function and a release function.

5.1.9.1.1.4 Mechanical cables. All mechanical cables in the suspension and release system shall be protected from accidental operation.

5.1.9.1.1.5 Ground safety lock system. The airborne release system shall be designed to have a manual ground safety lock system which when locked shall prevent the releasing of the weapon even if the proper release sequence is performed. The state of this lock system shall be easily and unmistakably discernible by visual inspection from the ground. As a design goal, visual inspection of the lock system shall be accomplished without the need of mirrors or other extraneous devices.

5.1.9.1.1.6 Electrical safety. The suspension and release system shall be designed such that electrical power shall not be required to be applied to its components until commanded release preparation begins.

5.1.9.1.1.7 Visual inspection. The latched and locked condition of the suspension and release devices (separate from the ground safety lock) shall be easily and unmistakably discernible by visual inspection while the aircraft is on the ground. As a design goal, the latched and locked condition shall be determinable without use of mirrors or other extraneous equipment. The locked condition can be determined electrically while the aircraft is on the ground or in the air in the crew compartment.

5.1.9.1.1.8 Components and squibs. Release system components, including squib cartridges, shall meet the requirements of MIL-STD-1512 as tailored to the specific system.

5.1.9.1.2 In-flight reversible lock. An in-flight reversible lock shall be provided which, when locked, prevents weapon release by both mechanical and electrical means. The in-flight reversible lock shall:

a. Mechanically restrain the releasing device. If hooks are used that can be individually latched or unlatched, the safety lock shall mechanically restrain each hook;

b. Prevent release or launch in the event that the maximum available release force is accidentally applied in the release mechanism;

c. Fail safe (locked) in the event a failure occurs when the lock is locked;

d. Disable all means of release when in the locked position;

e. Permit a visual check of the locked state by ground personnel. As a design goal, visual check shall be accomplished without the use of mirrors or other extraneous devices. For direct visual inspection, the locking device itself shall present an unmistakable indication of the locked state;

f. Be protected from accidental operation;

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

h. Provide a remote indication to the aircrew of the fully locked or unlocked (or both) positions of the in-flight lock. If a single indication for the locked state is used, it shall reflect only the fully locked position of the in-flight reversible lock. If a single indication for the unlocked state is used, it shall reflect every state other than a fully locked state. The remote indication system shall not allow an apparent indication to the aircrews of a locked state when in fact, an unlocked state exists; and

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

5.1.9.1.3 Pylon jettison. Pylons carrying nuclear weapons shall only be jettisonable if the jettison system includes a lock that meets the requirements under 5.1.9.1.2. A single lock may be used for both the weapon and the pylon where such a design is feasible.

5.1.9.1.4 Unlock and release signal isolation. Where discrete (energy control) signals are used, the discrete signals for unlocking the in-flight lock and for releasing the weapon shall remain physically and electrically isolated to the maximum extent possible. No release system fault shall be capable of operating the in-flight reversible lock, nor shall a fault in the in-flight reversible lock be capable of causing a release. In addition, the lock and its control shall be independent of the electrical connection between the aircraft and the stores.

5.1.9.1.5 *Composite structures.* *Composite structures used to form all or part of the suspension and release* system shall have 100% production article testing at the design load. Manufacturing controls combined with NDI may be substituted for testing if approved by the appropriate agency.

5.1.9.2 Evaluation requirements

5.1.9.2.1 General. Analyses or tests shall verify the suspension and release system requirements under 5.1.9.1.

5.1.9.2.2 Tests. The suspension and release system shall be tested in accordance with MIL-T-7743 as tailored to the specific system. If flight testing indicates it is warranted, testing shall be accomplished to more extreme limits.

5.1.9.2.3 Analysis. An analysis shall be performed to define the nuclear system configuration. It shall review and list all assemblies, wires, connectors, and other hardware which define the nuclear suspension and release system.

5.1.9.2.4 Circuit isolation tests. Circuit isolation tests shall be performed to demonstrate that the nuclear system configuration meets the design requirements for electrical isolation of the unlock, release, and launch circuits.

5.1.10 Release system nuclear consent

5.1.10.1 Design requirements

5.1.10.1.1 Controls. The operating controls for the release system shall include a nuclear consent function to inhibit unlocking the release system unless consent is given. Nuclear release consent shall be a hardwired function.

5.1.10.1.2 Relation to in-flight lock. Nuclear consent shall not unlock or inhibit the locking of the reversible in-flight lock. Removal of nuclear consent shall relock the reversible in-flight lock.

5.1.10.1.3 Separation of consent functions. Multi-place aircraft AMAC and release systems shall be designed with separate controls for both prearm and release consent. Each consent function shall require the physically separated and independent action of two crewmembers.

5.1.10.1.4 Single-person operation. A multi-place aircraft used in combat by one person may have a provision for single-person operation of the release system if a bypass is done before flight. This bypass shall be designed so that it cannot be done inflight.

5.1.10.1.5 Application of electrical power. Ejector unlock and EED power shall not be applied to suspension and release components prior to the crew beginning release preparations.

5.1.10.1.6 Safe jettison. The jettison system on a combat delivery aircraft shall permit jettison of a nuclear weapon in a safe configuration. If emergency prearm release is desired, a system override by the operator shall be required.

5.1.10.1.7 Multiple nuclear release. For aircraft designed to release multiple nuclear stores, a crewmember input to the release system controls is required prior to each release of a nuclear weapon on a target or series of releases on a target complex. A one-time activation of nuclear release is not sufficient to satisfy this requirement. The intent is to specifically preclude the automated delivery of numerous weapons without further crew *member input once authorization and nuclear consent* (prearm and unlock) have been accomplished.

5.1.10.2 Evaluation requirements. Analyses or tests shall verify the release system nuclear consent requirements under 5.1.10.1.

5.1.11 Aircraft monitor and control system

5.1.11.1 Design requirements. Except for the safe-off state transition, each nuclear weapon shall be transitioned to a new command state from an adjacent command state. The adjacent states are defined according to the following sequence: off-monitor-safe-arm. These command states shall be defined as follows: off—no power to the weapon interface; monitor—current-limited power to only the nuclear weapon identifier, permissive action link (PAL), safe, and arm monitor lines; safe—only monitor and safe power applied at the weapon interface; and arm—monitor power and prearm power (unique signal generator (USG) and the various option lines) applied to the weapon interface. No change of state shall be made except by the explicit command of a crew member. The Stores Management System (SMS) must ensure these control rules are followed whenever nuclear weapons are selected for a state change.

5.1.11.1.1 Command states. The AMAC system shall be designed to operate each of the electrical states of a nuclear weapon.

5.1.11.1.2 Weapon interface compatibility. The AMAC system shall be compatible with all weapons designated for carriage. It shall provide for the electrical states and transitions in accordance with the applicable AMAC POG interface specifications/standards.

5.1.11.1.3 Prearmed state. The AMAC system shall not allow a commanded transition of a prearmed weapon to off, except in the event of indicated prearm malfunction.

5.1.11.1.4 Interface voltage and current. Voltage and current levels required for operation of weapon/ejector interface units shall be limited in accordance with MIL-STD-704 as tailored to the specific system, in order to minimize the probability of operating critical functions if these voltages and currents are inadvertently applied to the nuclear weapon interface.

5.1.11.1.5 Additional requirements. The AMAC system shall also be designed so that:

a. Sufficient power to operate any critical weapon component cannot be applied at the aircraft-to-weapon interface until control power is deliberately applied to operate the component;

b. Monitor circuits shall be electrically isolated from power and control circuits, and monitor functions shall be performed independently of weapon control functions. The AMAC functions may be combined on a single data bus for MIL-STD-1760 designed weapons; however, there must be positive differentiation between control commands and data;

c. Both the safe and prearm states of the weapon system shall be indicated explicitly through continuous monitoring;

d. Applying a prearm or safing command, or control power to a nuclear weapon(s) shall require a dedicated control or control setting unique to that weapon(s) that requires a deliberate and positive act by the weapon system operator. Initiation or application of the prearm command shall not occur in an accident;

e. There is a positive measure that shall remove power from the weapon interface;

f. The prearm control shall be a USG command signal per the specification for the weapon-to-carrier interface (System 1 or 2). The information needed to define the unique signal events shall not exist totally or in part in a usable form within the SMS and shall be defined through crew member input. The crew input shall be used for both the sequence of unique signal events and the definition of those events (for example, data words); and

g. The function of prearm consent is to inhibit prearming until direct crew action provides the required consent signal. The prearm consent control shall be designed to reveal unauthorized operation or tampering

(see 5.1.10.1.3 and 5.1.10.1.4). The prearm consent function shall be a hardwired control which interrupts power to the prearm circuit controlling the intent strong link. Prearm consent may be implemented through software inhibits/controls, but the consent signal must originate through crew action. Removal of prearm consent shall result in the termination of prearming or releasing functions in process and inhibit prearming and releasing actions until consent has been reestablished. (See MIL-STD-1760 as tailored to the specific system).

5.1.11.1.6 Applications for weapon state. The AMAC system shall base its logical sequencing on the commanded state of the weapon, not on the reported state of the weapon. The reported state of the weapon shall be used for display purposes only. Appropriate fault messages shall be displayed whenever the commanded state disagrees with the reported state.

5.1.11.1.7 PAL capability. The AMAC system shall have a built-in PAL capability compatible with the weapons specified in the system specification.

5.1.11.1.8 Command disable capability. The AMAC system shall have a built-in command disable capability compatible with the weapons specified in the system specification.

5.1.11.2 Evaluation requirements

5.1.11.2.1 General. Analyses or tests shall verify the AMAC system requirements under Section 5.1.11.1.

5.1.11.2.2 AMAC POG standards. The AMAC system capability to meet the applicable AMAC POG interface specifications/standards shall be demonstrated using production aircraft.

5.1.11.2.3 Hardware configuration analysis. An analysis shall be performed to define the nuclear system configuration. It shall review and list all assemblies, wires, connectors, and other hardware which define the AMAC system.

5.1.11.2.4 Circuit isolation tests. Circuit isolation tests shall be performed to demonstrate that the nuclear system configuration meets the design requirements for electrical isolation of the AMAC circuits.

5.1.12 Multiplex systems

5.1.12.1 Design requirements

5.1.12.1.1 Buses. Multiplex data buses used in the AMAC system shall comply with MIL-STD-1553 as tailored to the specific system.

5.1.12.1.2 Store interfaces. Multiplex store interfaces shall comply with MIL-STD-1760 as tailored to the specific system.

5.1.12.1.3 Signals. All hardwired discrete signals in the multiplex system shall meet the requirements of the hardwired AMAC system.

5.1.12.1.4 Inadvertent critical signals. A single component or system fault shall not allow the inadvertent operation of any critical control signal of a nuclear weapon.

5.1.12.1.5 Aircrew control. The multiplex system shall always be under the control of the aircrew.

5.1.12.1.6 Single-bit errors. The alteration of a single bit in a transmission message shall not cause the inadvertent operation of any critical control device.

5.1.12.1.7 Data. For data being transferred:

a. Only the correct stations, as determined by the system programming or control source, shall transmit or receive data on the multiplex bus. Data transfer or change of state of control signals shall not be allowed until the correct stations have been successfully connected;

b. The number of transfers of multiplex signals implementing critical functions shall be minimized; and

c. Unauthorized stations that are transmitting or receiving data shall not affect the nuclear weapon interface.

5.1.12.1.8 Weapons interface unit power. The operator shall be able to command the application or removal of electrical power to any weapons interface unit that interfaces directly with the weapon(s) and directly or indirectly with the SMS computers.

5.1.12.1.9 Weapons interface control unit power. The operator shall be able to command the application or removal of multiplex system power from the weapon interface control unit.

5.1.12.1.10 Positive control of power. The application of multiplex system power to the weapons interface unit shall require a deliberate act by the operator.

5.1.12.1.11 Control of power to System 2. The operator shall be able to command the application or removal of all electrical power to any System 2 weapons interface.

5.1.12.1.12 Startup self-test. Immediately after electrical power is applied to the remote terminal, the unit shall verify correct functional operation with a startup self-test before the unit is capable of outputs to the weapon or release system.

5.1.12.1.13 Uncommanded state protection. The change, application, or removal of power to any part of a multiplex system shall not cause the weapons interface unit (or a System 2 weapon) to transition to an uncommanded state.

5.1.12.1.14 Abnormal environments. For protection in abnormal environments:

a. Subsystems of the multiplex system shall be physically separated within the multiplex transmitting unit as far as possible;

b. Within a remote terminal, opposing critical functions (for example, prearm and safe) shall be electrically isolated; and

c. Voltage and current levels required for operation of weapon/ejector interface units shall minimize the possibility of operating critical functions if these voltages and currents are inadvertently applied to the nuclear weapon interface.

5.1.12.1.15 Positive control of prearm and release. Prearm and release (including jettison) control signals given to the nuclear weapon interface shall be generated only by positive operator control over the multiplex system. Critical functions shall not occur as a result of the automatic action of one multiplex station or the absence of data from the multiplex bus.

5.1.12.1.16 Protection of critical functions. The system design shall prevent the critical functions of authorization, prearm, arm, release, launch, or targeting from occurring in the event of a multiplex system fault.

5.1.12.1.17 Loss of synchronization. If communication or data synchronization is lost, the receiving unit shall not change its output.

5.1.12.1.18 Critical signals change of states. Multiplex units shall provide break-before-make action between changes of state of all critical signals applied to the nuclear weapon interface.

5.1.12.1.19 Self-test. In-flight self-test capability shall not interfere with normal multiplex operation and shall not cause the generation of a nuclear caution or any critical function signal at the nuclear weapon interface.

5.1.12.2 Evaluation requirements

5.1.12.2.1 General. Analyses or tests shall verify the multiplex system requirements under 5.1.12.1.

5.1.12.2.2 Self-test. Self-testing shall not interfere with normal multiplex operation and shall not cause the generation of any consent or critical signal at the nuclear weapon interface. Testing shall not degrade nuclear safety.

5.1.13 Computer-controlled controls and displays

5.1.13.1 Design requirements. The following requirements apply when critical functions can be commanded by selection of options from menus:

a. Critical command signals must be unique to the function being called—for example, the lock and unlock commands cannot be the same command with the signal interpreted differently depending on the state of the reversible in-flight lock;

b. All nuclear function options must be clearly labeled to preclude the inadvertent selection of an undesired nuclear function. AMAC and delivery functions may be combined on the same screen display, but screen formats must clearly differentiate the functions. Software protocols shall preclude the execution of an erroneously selected function;

c. System design shall require a deliberate action on the part of the receiving crew member to transfer system control from one crew member to another. This transference process is typically described as a "take" command;

d. No menu-labeled control on a nuclear display shall have any function that is inconsistent with its label or be displayed unless active (capable of initiating its function);

e. All unlabeled controls on a nuclear menu shall be non-operational;

f. If any nuclear station is powered, the status of the S&A device or the release system lock/unlock device shall be continuously displayed to the crew. In addition, one crew member shall have dedicated control of the nuclear weapon functions; and

g. If there is not a dedicated nuclear caution display separate from the multifunction display, there shall be no menu available in flight that shall display a nuclear caution if a nuclear caution exists.

5.1.13.2 Evaluation requirements

5.1.13.2.1 General. Analyses or tests shall verify the computer-controlled control and display requirements under 5.1.13.1.

5.1.13.2.2 Functional testing. Functional testing of the nuclear system configuration of production aircraft shall be performed to ensure the nuclear system meets the design safety requirements.

5.1.14 Protection of friendly territory

5.1.14.1 Design requirement. Aircraft guidance and bomb release is considered to be under the positive control of the aircrew. If system design or operational procedures allow otherwise, then the aircraft during those circumstances must meet the same requirements for targeting as guided missiles.

5.1.14.2 Evaluation requirement. Analyses or tests shall verify the protection of friendly territory requirement in 5.1.14.1.

5.1.15 Aircraft power control

5.1.15.1 Design requirement. Aircraft designs shall permit the application and removal of power to individual nuclear weapons, to all weapons together, and to groups of nuclear weapons contained on a single pylon or launcher. The operator shall have a means of removing power from nuclear weapons which is not dependent on the successful operation of any automatic or computer-controlled system. This design shall not degrade aircraft safety or operational capability.

5.1.15.2 Evaluation requirement. Analyses or tests shall verify the aircraft power control requirement in 5.1.15.1.

5.2 Air-launched missiles. Air-launched missiles are generally considered extensions of the delivery aircraft and must meet the same requirements for connector design, EMR protection, and electrical subsystems.

5.2.1 Design requirements

5.2.1.1 Ignition. The air-launched missile shall contain a safety device to S&A the propulsion ignition system. The propulsion system safety device shall be separate and independent of other nuclear safety devices for prearm and release system locking. Visual monitoring of the S&A device shall be possible on the ground.

5.2.1.2 Arming. The air-launched missile shall contain a sensing device that shall 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.

5.2.1.3 Safing. Each nuclear safety device shall allow a weapon system operator to apply the safing power. The capability for monitoring the nuclear safety devices for the safe condition, either continuously or on demand, is required.

5.2.1.4 Manual positive locks. Manual positive locks used with the propulsion system safety devices shall be placed so that they can be removed at the last practical point in the missile loading sequence.

5.2.1.5 Connectors. Connectors in the missile motor firing circuits shall not have spare or unused pins.

5.2.2 Evaluation requirements

5.2.2.1 General. Analyses or tests shall verify the air-launched missile requirements under section 5.2.1.

5.2.2.2 Configuration analysis. An analysis shall be made to define the nuclear configuration of the missile. It shall review and list all assemblies, wires, connectors and other hardware which define the nuclear-critical circuits within the missile.

5.2.2.3 Demonstration. The AMAC system capability to meet the applicable AMAC POG interface specifications/standards or interface control document requirements for direct missile warhead control shall be demonstrated using production aircraft.

5.3 Ground-launched missiles

5.3.1 Launch control systems

5.3.1.1 Design requirements

5.3.1.1.1 Operation. Missile launch shall only be possible through intentional operation of the authorization and launch control functions. These functions shall be separate and independent. No other system in its operational or failure mode shall be able to authorize a launch sequence or propulsion system operation.

5.3.1.1.2 **Launching function.** The launching function shall contain two independent functions, one to arm the propulsion system ignition safety device and one to command ignition.

5.3.1.1.3 **Ignition command.** Operation of the propulsion system shall require an ignition command.

5.3.1.1.3.1 **Sequencing.** The launching function shall preclude transmission of the ignition command until the authorization functions have been enabled.

5.3.1.1.3.2 **Accidental transmission.** No single failure shall result in accidental transmission of the ignition command.

5.3.1.1.4 **Propulsion system ignition safety device.** The missile propulsion system shall have an ignition safety device that shall protect against inadvertent propulsion system ignition even if the ignition command is sent, unless the safety device is properly armed. This protection shall be provided when the system is exposed to credible abnormal environments. The propulsion system shall have provisions for both manual and remote safing.

5.3.1.1.4.1 **Sequencing.** Unless the device is properly armed, it shall prevent propulsion system ignition even if the ignition command is sent.

5.3.1.1.4.2 **Accidental command.** No single failure shall result in accidental transmission of the arming command to the device.

5.3.1.1.4.3 **Accidental arming.** No single failure shall result in arming or bypassing the safety device.

5.3.1.1.4.4 **Information control.** The safety device shall be operated by the information control method.

5.3.1.1.4.5 **Authorization.** The launching function shall preclude operation of the propulsion system ignition safety device until the authorization functions have been enabled.

5.3.1.1.5 **Tampering.** The design shall include provisions for detecting and resisting tampering with the launch control system and other systems and devices designated as critical components. There shall be visual and audible indications to the LCP's when there is an attempt to operate the launch control system. These indications shall remain until the system operators acknowledge and reset them.

5.3.1.1.6 **Fail safe.** The launch control system shall remain in, or return to, a safe state when a single-component failure or loss of electrical power occurs.

5.3.1.1.6.1 **Loss of electrical power.** Loss of electrical power shall not initiate or operate any critical function in the launch control system.

5.3.1.1.6.2 **Automatic power shutoff.** The design shall include provisions for automatic and immediate removal of electrical power which could cause prearming, arming, propulsion ignition, or launching of the missile if a critical unsafe condition is indicated and cannot be corrected.

5.3.1.1.7 **Complementary signals.** The arm (or operate) and safe (or off) critical commands shall not be complementary. For example, the absence of arm shall not be construed as safe, and vice versa.

5.3.1.1.8 **Launch prevention.** A positive means, such as mechanical restraints, barriers, or non-erection of the missile, shall be employed to protect against missile launch in the event of inadvertent ignition of the propellant.

5.3.1.1.9 **Multiplex control systems.** If multiplex control systems are used for transmission of critical signals, the following safeguards apply:

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

b. A remote terminal shall only respond to messages addressed to it.

c. The system design shall be compatible with system hazard/fault analyses such that the polling time interval and automation logic shall not mask any critical function activation or fault between successive polls.

5.3.1.2 Evaluation requirements. Analyses or tests shall verify the launch control system requirements under 5.3.1.1.

5.3.2 Arming and fuzing system safety device

5.3.2.1 Design requirements. Each ground-launched missile shall have a safety device(s) or feature in the reentry system (RS), reentry vehicle (RV), or payload section to interrupt power to the warhead interfaces(s) (see 4.5.8.). It shall be possible to safe this device(s) through all phases of weapon system buildup. This device(s) is not required if it can be shown that power cannot be applied to the warhead interface as a result of a single-component failure, the numerical requirements in this standard can be met without the device, and there are provisions for removing power to the missile if a failure occurs that could contribute to power being inadvertently applied to the warhead interface(s).

5.3.2.2 Evaluation requirements. Analyses or tests shall verify the A&F system safety device requirements in 5.3.2.1.

5.3.3 Monitoring

5.3.3.1 Design requirements

5.3.3.1.1 Surety status. Systems shall be provided so that the operator can monitor the surety status of the elements listed below. The weapon control system shall continuously monitor each of the following devices:

a. Missile propulsion system safety devices;

b. Warhead(s) strong link;

c. System safety device(s) in the RS, RV, or payload section; and

d. Surety devices (authorization, launch, and security systems).

5.3.3.1.2 Status change. The monitoring system(s) shall provide a positive indication to the operator of any change in the surety status of the system being monitored or of the loss of status monitoring capability. Notification of change of status shall be as soon as possible. Routine reporting of system status shall be accomplished either periodically or continuously and shall be available on demand. Any delay in reporting change of status shall not cause degradation of nuclear surety.

5.3.3.1.3 Power removal. Electrical power faults and failures that could cause accidental prearming or arming of the nuclear weapon or launching of the missile shall result in power being removed automatically.

5.3.3.1.4 Current. See 4.5.13.6 for limitations to monitoring current.

5.3.3.2 Evaluation requirements. Analyses or tests shall verify the monitoring requirements under 5.3.3.1.

5.3.4 Command and control communications

5.3.4.1 Design requirements

5.3.4.1.1 National command authority to launch control point

5.3.4.1.1.1 Authorization. Ground-launched missile systems shall be designed so the missiles cannot be launched until they are authorized. This authorization shall be contained in a secure code transmitted from the National Command Authority and shall be withheld from the launch crew until a launch is authorized. This code may be used to compute the unique signal input for the propulsion system ignition safety device. If a PAL code is used to authorize warhead use, it shall be different from the code used to authorize the launch of a missile.

5.3.4.1.1.2 Weapon-specific secure authorization. For systems with a selective launch capability, the launch control system shall be secure to allow single missiles to be launched without revealing or compromising any of the codes for the other missiles or military forces.

5.3.4.1.2 Launch control point to launch point communications and code devices.

5.3.4.1.2.1 Communications. Numerical requirements for nuclear command and control communications shall be provided by the Government. The secure code authorization device shall allow only a limited number of attempts at operation using incorrect codes or a device or system to detect and report tampering.

5.3.4.1.2.2 Transmissions. Critical command and status message transmissions shall be made secure against tampering, monitoring, and substituting. If LCP and launch point (LP) locations make physical security measures impractical, the messages shall be encrypted and the status shall be authenticated by cryptographic means. The communications system shall notify the LCP's when tampering with the system has been detected.

5.3.4.1.2.3 Minimum monitor and control requirements. An LP may respond to launch commands from a single LCP. For a tactical nuclear weapon system, one or more LCP's shall monitor and be able to take preventive action if an unauthorized critical command message or status is detected. For strategic nuclear weapon systems, critical LP status shall be monitored at the primary LCP and at least one other LCP. Each location shall be able to take compensatory action if an unauthorized critical command message or status is detected.

5.3.4.1.2.4 Cooperative launch. The consent function in an LCP shall require that at least two people actively cooperate to command launch even after all secure codes for authorization are available. Simple, easily bypassed functions are unacceptable because they do not prevent a single person from issuing a launch command.

5.3.4.1.2.5 Code requirements. LCP and LP secure code storage devices shall be designed to resist bypass or code readout. Access to the storage device's memory, for the purpose of changing the code, shall be secured. Maintenance tools or other devices that may be used to change the memory to a standard unclassified code without gaining access by secure means are prohibited, unless the use of the device or tool stops use of the code storage device for its intended purpose and causes positive indications to be received at the LCP.

5.3.4.1.2.6 Unique signal storage. Signal commands for controlling the critical functions of prearming and launching shall be unique and shall not be stored in the weapons control system in a directly usable form until receipt and authentication of the authorization command from higher authority has been given.

5.3.4.1.2.7 Unique signal protection. The system design shall prevent inadvertent and unauthorized generation or transmission of critical-function-unique signals.

5.3.4.2 Evaluation requirements. Analyses or tests shall verify the command and control communication requirements under 5.3.4.1.

5.3.5 Mobile launch points and launch control points

5.3.5.1 Design requirement. If movement of a fully assembled missile with warhead(s) is necessary, safety devices for the missile propulsion system and the RS's shall be designed to remain in the safe state in all environments until intentionally activated.

5.3.5.2 Evaluation requirement. Analyses or tests shall verify the mobile LP and LCP requirement in 5.3.5.1.

5.3.6 Protection of friendly territory

5.3.6.1 Design requirements. Missile systems, incorporating self-contained guidance, shall require a "good guidance" signal from the guidance and control unit before nuclear warhead arming can occur. This "good guidance" signal shall be withheld if guidance accuracy checks show that the missile will impact outside the specified target boundaries.

5.3.6.2 Evaluation requirements. Analyses or tests shall verify the protection of friendly territory requirements in 5.3.6.1.

5.3.7 Vault construction for certified critical component storage

5.3.7.1 Design requirements. The wall, floor, and roof construction shall follow recognized structural standards. Construction concrete shall be poured in place with a minimum 28-day compressive strength of 2500 psi.

5.3.7.1.1 Class A vaults

5.3.7.1.1.1 Floors and walls. Floors and walls shall be made of 8-inch-thick reinforced concrete. Vault walls which are part of exterior walls, shall be set back from the exterior face of the outside wall to allow 4 inches of the wall facing material to cover the vault wall. Walls shall extend to the underside of the roof slab above.

5.3.7.1.1.2 Roof. The roof shall be a monolithic reinforced concrete slab of thickness determined by structural requirements but not less than the walls and floors.

5.3.7.1.1.3 Ceiling. A normal reinforced concrete slab ceiling shall be placed over the vault area at a height not to exceed 9 feet, if the underside of the roof slab or roof construction exceeds 12 feet in height or the roof construction does not meet 5.3.7.1.1.2.

5.3.7.1.1.4 Door. The door and frame unit shall conform with the requirements of Federal Specification AA-D-600 and the door shall have a General Services Administration approved label for a Class 5 door. Door openings shall be standard 40 inches by 78 inches without a day gate. Doors shall have emergency escape and relocking devices. Door and frame units may not be fire rated.

5.3.7.1.1.5 Locks. Locks shall conform with Underwriters Laboratory Standard UL 768-84, Group 1-R; be manipulation resistant; and meet Federal Specification AA-D-600 for radiological resistance. The underwriters label shall be considered evidence of compliance.

5.3.7.1.1.6 Openings. Openings for air conditioning or ventilation ducts shall have bars to prevent surreptitious entry and to detect attempted forced entry.

5.3.7.1.2 Class B vaults

5.3.7.1.2.1 Floors. Floors shall be made of monolithic reinforced concrete with thickness of the adjacent concrete floor construction, but not less than 4 inches thick.

5.3.7.1.2.2 Walls. Walls shall not be less than 8 inches thick and made of either brick, concrete block, or other masonry units. Hollow masonry units shall be a load-bearing vertical cell type and have cells filled with concrete and steel reinforcement bars. In seismic zones 2, 3, and 4, steel-reinforced monolithic concrete walls shall not be less than 4 inches thick. Vault walls which are part of exterior walls shall be set back from the exterior face of the outside wall to allow 4 inches of the wall facing material to cover the vault wall.

5.3.7.1.2.3 Roof. The roof shall be a monolithic reinforced concrete slab of a thickness determined by structural requirements.

5.3.7.1.2.4 Ceiling. A normal reinforced concrete slab ceiling shall be placed over the vault area at a height not to exceed 9 feet, if the underside of the roof slab or the roof construction does not meet 5.3.7.1.2.3.

5.3.7.1.2.5 Door. Door and frame requirements are the same as 5.3.7.1.1.4.

5.3.7.1.2.6 Locks. Lock requirements are the same as 5.3.7.1.1.5.

5.3.7.1.2.7 Openings. Opening requirements for air conditioning or ventilation ducts are the same as 5.3.7.1.1.6.

5.3.7.2 Evaluation requirements. Analyses or tests shall verify the construction requirements in 5.3.7.1.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use. This document is intended for use in the procurement or modification of Air Force nuclear weapon systems, subsystems, support equipment, and associated facilities.

6.2 Acquisition requirements. Acquisition documents must specify the following:

a. Title, number, and date of the specification.

b. Issue of DODISS to be cited in the solicitation, and if required, the specific issue of individual documents referenced (see 2.1.1).

6.3 Consideration of data requirements. The following data requirements should be considered when this specification is applied on a contract. The applicable Data Item Descriptions (DID's) should be reviewed in conjunction with the specific acquisition to ensure that only essential data are requested/provided and that the DID's are tailored to reflect the requirements of the specific acquisition. To ensure correct contractual application of the data requirements, a Contract Data Requirements List (DD Form 1423) must be prepared to obtain the data, except where DOD FAR Supplement 27.475-1 exempts the requirement for a DD Form 1423.

Reference Paragraph	DID Number	DID Title	Suggested Tailoring
90.1	DI-NUOR-81409	Nuclear Certification Plan	
90.2	DI-NUOR-81408	AMAC Design Analysis Report	
90.3, 90.4	DI-NUOR-81405	Aircraft Nuclear Safety Analysis Report	
90.5	DI-NUOR-81410	Aircraft Electrical Compatibility Data	
90.6	DI-NUOR-81407	Aircraft Mechanical Compatibility Data	
90.7	DI-NUOR-81411	Engineering Evaluation Report	
90.8	DI-NUOR-81413	Aircraft Nuclear Weapon System Definition Document	
90.10	DI-NUOR-81406	Ground Launched Missile Nuclear Surety Analysis Report	
90.11	DI-NUOR-81412	Software Certification Plan	

6.4 Subject term (key word) listing.

Aircraft-weapons compatibility
Missile systems
Nuclear critical components
Nuclear critical functions
Nuclear design
Nuclear evaluation
Nuclear safety
Nuclear security
Nuclear surety

APPENDIX

HANDBOOK FOR USE WITH MIL-STD-1822

10. SCOPE

This section contains general information on surety design and evaluation, and describes reports which may be required under the weapon system contract. This Appendix is not a mandatory part of the standard. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS Documents mentioned in the text of this appendix are listed in section 2 of this standard. Section 100. below is a bibliography of other documents which may be needed during the nuclear design and certification process.

30. OVERALL PERFORMANCE OBJECTIVE

The overall performance objective is set by the Department of Energy.

30.1 Unintentional nuclear yield. For all configurations of the weapon system, the probability of an unintentional nuclear yield should be less than the following:

a. One in 109 per weapon per stockpile lifetime for normal environments, in the absence of bomb- or warhead-unique prearming, or environment or trajectory stimuli;

b. One in 106 per weapon per exposure to abnormal environments, in the absence of bomb- or warhead-unique prearming, or environment or trajectory stimuli; and

c. One in 104 per event after application of the prearm command and deliberate deployment (launch or release), and in the absence of the arming signal.

40. ARMING AND FUZING (A&F) SYSTEM

40.1 Prearm device. The nuclear weapon A&F system should contain a prearm device located in the warhead or bomb.

40.1.1 Operational control. The prearm device should be operated only by a unique prearming signal or unique signal train. The signal should be derived from some part of the weapon system that is under direct human control.

40.1.2 Sequence. Prearming should occur as late in the delivery sequence as possible, preferably after launch or release of the weapon. For weapons that should be prearmed prior to launch or release, the prearm operation should be reversible until as late as operationally feasible in the launch or release sequence.

40.2 Environmental or trajectory sensing device (E/TSD). The A&F system should contain an environmental/trajectory sensing device, preferably in the warhead or bomb.

40.2.1 Operation. The E/TSD should be a strong link device that should prevent arming until the proper environment or trajectory is sensed. The device should only respond to an environment or trajectory unique to intended flight or release of the weapon, and it should not operate until the majority of the unique environment or trajectory has passed.

40.2.2 Functional sequence. The E/TSD should always function before the prearm in ground-launched missile warheads. It may function after prearm only in some bombs or short-time-of-flight weapons.

APPENDIX

40.2.3 Relation to prearm device. Either the E/TSD should be a prerequisite to activating the prearm device, or the prearm function should be a prerequisite to activating the E/TSD.

40.3 Abnormal environment protection. Abnormal environment protective features should prevent prearming, arming, and unintended significant nuclear yield in all abnormal environments specified in the stockpile-to-target sequence (STS) document and in the carrier vehicle specifications.

40.4 Exclusion region strong link/weak link. One of the most important safety concepts used by the DOE in nuclear bombs and warheads is the exclusion region with its associated strong link and weak link. In the nuclear weapon, the exclusion region is an area which contains the firing set and physics package. The exclusion region is isolated from all energy sources by a physical barrier. Access to the exclusion region is controlled by safety devices (normally two devices in series) called strong links. The strong links are dezined to provide electrical isolation in both normal and abnormal environments. Strong link components are normally robust, abnormal environment resistant devices operated by unique signals or a unique environment. Collocated with the strong links are other safety devices called weak links which are designed to respond predictably in abnormal environments. They are designed to fail irreversibly in a safe manner prior to the failure of the strong link. Weak links are components that are essential to the functioning of the weapon, and their failure should prevent the nuclear weapon from functioning. Both the principles of this concept and the strong-link/weak-link devices themselves may be usefully employed in the design of the carrier systems (aircraft or missiles).

40.5 Unique signal concept. The basic concept of unique signal data is that of vital information separation. If a strong link component requires a unique signal to activate it, then it is extremely unlikely that the signal could be generated inadvertently by any credible combination of abnormal environments.

40.6 Two-person concept. The maintenance and operational procedures developed for a nuclear weapon system should consider this requirement.

50. WEAPON/PLATFORM COMPATIBILITY

This section lists requirements for tasks, analyses, and tests which are necessary to show compatibility between an aeronautical system and the nuclear weapons which it carries. The result of these tasks should be a major assembly release (MAR) for bombs and warheads, and an aircraft compatibility control drawing (ACCD) for bombs.

50.1 Aircraft

50.1.1 Aircraft monitor and control (AMAC) system. The AMAC system should be analyzed and tested to ensure it meets the design and nuclear safety requirements. The results of these analyses and tests should be documented in the AMAC Final Design Analysis Report (DAR). The specifics of this report are contained in 90.2.

50.1.1.1 Mechanical compatibility data (MCD). Mechanical compatibility data should be prepared to define the mechanical aspects of the weapons suspension and release system, including electrical connectors as appropriate and clearances during carriage and release. See 90.6.

50.1.1.2 Electrical compatibility data (ECD). Electrical compatibility data should be prepared that identify AMAC system configurations, interfaces, component locations, and other pertinent data. See 90.5.

50.1.1.3 Structural loads analyses and test. Joint analyses/tests should be conducted by the weapon system contractor and Sandia National Laboratories (SNL). The analyses/tests should determine the distribution of forces and pressures on the weapon(s) and aircraft to determine if the aircraft can safely carry the nuclear weapon(s) and if the structural capability of the weapon could be exceeded. The analyses/tests should include ground and flight environments as specified in the STS and the military characteristics (MC's). Limitations should be identified and provided for inclusion in the applicable DOE compatibility document.

50.1.1.4 Environmental flyarounds and data. Support for environmental flyaround tests should be provided. These tests should be conducted by the appropriate Air Force test organization and should provide the basic data to demonstrate the warhead compatibility with the carriage/launch environments (thermal, vibration, and acoustic) for all aircraft weapon carriage locations. Vibration analyses should be conducted to identify the important frequencies and modes for the various arrangements of weapons on the launcher or pylon. Ground vibration tests of selected configurations may be performed to substantiate the vibration analysis results. In-flight measurements of the thermal, vibration, and acoustic environments should be made for selected configurations and flight conditions. Vibration of the weapon bay doors should be measured to demonstrate that the weapon bay door motion is not such that it could cause less than the required weapon-to-door clearance for ejection. Tests should be conducted with a vibrational flyaround assembly to simulate the structure and dynamic response of the actual warhead/bomb. Other environmental data should be gathered by sensors in the weapon bays or external pylons.

50.1.1.5 Ejection characteristics. Ejection characteristic (static drops) tests to assure proper weapon release, ejection velocity, separation, adequate fall-angle clearances, ejection forces, and proper lanyard retention under static-level flight conditions prior to in-flight separation tests should be conducted. Test parameters and instrumentation should be jointly determined by the system program office (SPO), DOE laboratories, SA-ALC/NWI, and contractors. Production or equivalent hardware is required.

50.1.1.6 Separation tests (in-flight). Separation tests to assure compatibility of the aircraft with required nuclear weapons should be conducted. The tests should verify proper separation within the aircraft flight envelope to determine the nuclear weapon launch or delivery envelope. Detailed requirements and instrumentation should be jointly determined by the SPO, DOE laboratories, SA-ALC/NWI, and contractors. The flight parameters of the drop tests should include all of the aircraft flight envelope with conditions tailored to the expected carrier flight and delivery envelopes. The number of tests required should be a function of the completeness of the dynamic analysis and wind tunnel testing. Tests should at least verify the results predicted by wind tunnel tests and analytical modes in the extremes of the flight envelope.

50.1.1.7 Mechanical fit and electrical function tests. The following tests should be performed by SA-ALC/NWI and the DOE laboratories. MCD's and ECD's should be delivered in sufficient time to support these tests.

a. A mechanical fit test should be performed for all configurations of the aircraft and for applicable transportation equipment. The test should include uploading and downloading (mating/demating) of compatibility test unit(s) at all stations using production or production-equivalent hardware and appropriate support equipment.

b. An electrical function test should be performed to verify compliance with the applicable portion of the AMAC POG System 1 or System 2 interface specification/standard and interoperability with other nuclear weapons carried on the aircraft. The test should include a flight test to verify the interface during flight conditions.

50.1.1.8 Aircraft compatibility control drawing. The ACCD is a control drawing prepared and maintained by SNL which establishes the extent of compatibility and restrictions between a nuclear bomb and an aircraft. It is released after the compatibility tasks in 90.2 have been completed. It is published through the Joint Nuclear Weapons Publications System.

50.1.1.9 Major assembly release (MAR). The compatibility analyses and tests between aircraft/missile/warhead/bomb culminate in the issuance by the DOE of a compatibility statement contained in a document called the MAR. The MAR, or an assurance of a MAR, is required prior to mating/uploading nuclear weapons.

APPENDIX

50.2 Air-launched missiles

50.2.1 Aircraft monitor and control (AMAC) system. The AMAC system should be analyzed and tested to ensure it meets the interface requirements. The results of these analyses and tests should be documented in the AMAC Final DAR.

50.2.2 Mechanical compatibility data. MCD should be prepared to define the mechanical aspects of the weapons suspension and release system, including electrical connectors as appropriate and clearances during carriage and release.

50.2.3 Electrical compatibility data. ECD should be prepared to define the electrical and logical interfaces between the warhead and missile and between the warhead and aircraft.

50.2.4 Structural loads analyses and tests. Joint analyses/tests should be conducted by the missile contractor against requirements specified by the Air Force in cooperation with the DOE and their prime contractors. The analyses/tests should determine the distribution of forces and pressures transmitted to the warhead to determine if the warhead environments are within design limits. The analyses/tests should include ground and flight environments as specified in the STS and MC's. Limitations should be identified and provided for inclusion in the MAR.

50.2.5 Environmental flyarounds and data. Support for environmental flyaround tests should be provided. These tests should be conducted by the appropriate Air Force flight test organization and should provide the basic data to demonstrate the warhead compatibility with the carriage/launch environments (thermal, vibration, and acoustic) for aircraft weapon carriage locations. Vibration analyses should be conducted to identify the important frequencies and modes transmitted to the warhead during aircraft carriage and during missile flight. Ground vibration tests of selected configurations may be performed to substantiate the vibration analysis results. In-flight measurements of the thermal, vibration, and acoustic environments should be made for selected carriage locations and flight conditions. Tests should be conducted with special instrumented warheads provided by the DOE through the Air Force.

50.2.6 Ejection characteristics. Ejection characteristic (static drops) tests to assure proper weapon release, ejection velocity, separation, adequate fall-angle clearances, ejection forces and proper lanyard retention under static-level flight conditions prior to in-flight separation tests should be conducted. Test parameters and instrumentation should be jointly determined by the SPO, DOE laboratories, SA-ALC/NWI, and contractors. Production or equivalent hardware is required.

50.2.7 Separation tests (in-flight). Separation tests to assure compatibility of the aircraft with the missile should be conducted. The tests should verify proper separation within the aircraft flight envelope to determine the nuclear weapon launch or delivery envelope. Detailed requirements and instrumentation should be jointly determined by the SPO, DOE laboratories, SA-ALC/NWI, and contractors. The flight parameters of the drop tests should include specified portions of the aircraft flight envelope with conditions tailored to the expected carrier flight and delivery envelopes. The number of tests required should be a function of the completeness of the dynamic analysis and wind tunnel testing. Tests should at least verify the results predicted by wind tunnel tests and analytical modes in the extremes of the flight envelope.

50.2.8 Mechanical fit and electrical function tests. The following tests should be performed by SA-ALC/NWI and the DOE laboratories. MCD's and ECD's should be delivered in sufficient time to support these tests:

a. A mechanical fit test should be performed for all configurations of the aircraft with the missile, for the missile with the warhead, and for applicable transportation equipment. The tests should include uploading and downloading (mating/demating) of compatibility test unit(s) using production or production-equivalent hardware and appropriate support equipment.

APPENDIX

b. An electrical function test should be performed to verify compliance with the applicable ECD(s) AMAC POG interface specification between aircraft, missile, and/or warhead. The interoperability with other nuclear weapons should be verified. A flight test should be included to verify the AMAC system operation during flight conditions.

50.2.9 Time line integration tests. Tests should be conducted to determine if all functions occurring at the missile-to-warhead interface occur in the sequence and time lines as called for in the ECD. This should be a quantitative as well as qualitative test.

50.2.10 Major assembly release (MAR). The compatibility analyses and tests between aircraft/missile/warhead culminate in the issuance by the DOE of a compatibility statement contained in a document called the MAR. The MAR, or the assurance of a MAR, is required prior to mating/uploading nuclear weapons.

50.3 Ground-launched missiles

50.3.1 Major assembly release. The compatibility analyses and tests between missile/warhead/launcher culminate in the issuance by the DOE of a compatibility statement in a document called the MAR. The MAR, or an assurance of a MAR, is required prior to mating nuclear warheads with the RV or missile.

60. OTHER DESIGN CONSIDERATIONS

60.1 Critical components

60.1.1 General. The nuclear weapon system should be designed with a minimum of critical components. Critical components include but are not limited to nuclear weapon components; combat delivery vehicles with nuclear weapons mated or loaded; combat delivery vehicles which have all preload functions completed and are ready for weapon mate or load; and hardware, software, or code components which have been identified by the NWSSG or AFSA. Because of their functions, critical components may require special design safety features, special procedures, and extra security. See 80.13.

60.1.2 Certification. If the critical component is to be part of an assembled weapon system, it should be operationally certified by means of an approved process or be controlled continuously in accordance with AFI 91-104 and AFI 91-105. The Two-Person Concept applies for as long as the item is designated a certified critical component.

60.2 Human error. The system design should contain features which minimize the number of actions and choices which the operator should make during employment, daily operations, and maintenance so that the potential for human error is minimized.

60.3 Environments

60.3.1 Normal. Normal environments for the weapon system include climatic, chemical, electromagnetic, electrical, mechanical, and nuclear effects. Hazards associated with the normal environment include human error, lightning, pressure/temperature, moisture, limited shock and vibration, EMR, etc. Normal environments are referenced in the weapon system stockpile-to-target sequence (STS).

60.3.2 Abnormal. Some examples of abnormal environments include fire, high temperature, impacting, lightning, crushing, immersion, and credible combinations of these. The primary protection against credible abnormal environments is designed into the nuclear bomb or warhead. However, the weapon system will ensure that no nuclear critical signal is transmitted to the weapon, or its release or launch system, as a result of exposure of the weapon system to abnormal environments. Abnormal environments are referenced in the weapon system STS.

APPENDIX

60.3.3 Lightning. Lightning is an infrequent but serious hazard to nuclear weapons and nuclear weapon systems. It contains sufficient energy to detonate high-explosive material or initiate ordnance devices via direct conduction, induced voltages, and arcing between cables and circuits. Lightning may indirectly cause a degradation of nuclear safety by causing other hazards such as fire, mechanical damage, component failure, and power source activation. System antennas, cables, and structures provide entry points for lightning and affect the severity of the effects of the hazard. Lightning is generally classified as both a normal environment and abnormal environment for a weapon system and is referenced in the weapon system STS.

60.4 Facilities. Engineering drawings, building plans, and other designated information required to enable the engineering organization to perform an engineering evaluation for certification of installed facility equipment and facility support structure design should be prepared and delivered. The information should identify positive safety features to gard against fire and explosive hazards caused by fuel spills, sparking of equipment, etc.

70. TECHNICAL WORKING GROUPS SUPPORT

70.1 Project officers group or nuclear surety working group support

70.1.1 Technical support. Agencies participating in weapon system development relative to the monitor and control of the nuclear weapon should participate in either the weapon system POG (for aircraft systems) or the nuclear surety working group (NSWG) (for ground-launched missile systems) to resolve surety, compatibility, support equipment, TO, and facility issues.

70.1.2 Coordination. The weapon system developing organization through the POG or NSWG should establish, encourage, and maintain open communications between all agencies on nuclear certification issues.

70.2 Nuclear weapon system safety group. The system engineering organization should provide technical assistance to the NWSSG for the initial safety study (ISS) (which may be conducted in more than one phase), the preoperational safety study (POSS), or properly identified special safety studies as required.

80. NUCLEAR SAFETY ANALYSES

These analyses support the nuclear certification effort and are reported in the NSAR. The NSAR in turn supports the technical nuclear safety analysis (TNSA) which is prepared by SA-ALC/NWI.

80.1 Fault tree analysis. This analysis is a graphic model and logical representation of various parallel and sequential combinations of events, both fault and normal, which can cause a predetermined undesired event, the "top event". Simply stated, the analysis is an analytical technique whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The purpose of the analysis is to provide, in a formal deductive manner, qualitative and quantitative evaluations of the nuclear weapon system relative to the specified undesired events and to serve as the basis for a common-cause failure search. The analysis should draw on information from other hazard analyses. Any computer software used for the analysis should be referenced and made available, upon request, to evaluating agencies for use and verification.

80.1.1 Combat delivery aircraft. Combat delivery aircraft should have top events for the prearm command, inadvertent release/jettison with system locked, inadvertent release/jettison with the system unlocked, and inadvertent power application (to the weapon interface). Top events for combat delivery aircraft should include each weapon type and each release system configuration unless a worst-case situation can be shown.

80.1.2 Air-launched missiles. Air-launched missiles should have top events for the prearm command, accidental ignition and inadvertent power application (to the weapon interface). Top events for air-launched missiles should include both the carrier vehicle and missile contribution to the event.

APPENDIX

80.1.3 Ground-launched missiles. Ground-launched missiles should have top events for accidental or inadvertent transmission of the prearm command/code, accidental motor ignition, inadvertent programmed launch and inadvertent power/signal application (to the warhead interface).

80.2 Accident risk assessment report. This assessment employs statistical methodologies to provide a probabilistic basis for quantitative comparison of accident risks involved with operation of nuclear weapon systems. For purposes of comparison, risk can be treated as representing the number of consequences of a given accident, per a specified time. Furthermore, accident risk may be broken down into a combination of frequency (events per unit time) and magnitude (consequences/amplitude per event). The process, then, of assessing accident risk is: identify any potential hazards/accidents and determine their likely rates of occurrence; identify undesired effects of those accidents and assign a relative quantity; and combine the latter weighted with the former probability to produce an estimate of overall risk. In determining frequency of an occurrence there are two categories: high and low. High probability events are those events which occur frequently enough that generation of a basis for establishing realistic numbers of failures takes a relatively short observation period. Low probability events are those events which occur so infrequently that they have not been observed and there is no previous experience on which to base quantification of frequency or associated consequences. In all assessments, the role of the engineer's objective judgment is paramount; clear, concise documentation of the specific rationale used to develop the assessment should accompany the assessment.

80.3 Fault hazard analysis. This analysis provides component-level information relative to fault or failure causes, modes, and effects within a given subsystem which may contribute to an undesired event.

80.4 Subsystem hazard analysis. This analysis identifies functional relationships of components and equipment where degradation or failure can result in a safety hazard. It provides an evaluation of the internal level of safety for each component, assembly or system, including identification of hazardous elements or situations within the weapon system. The analysis is primarily, although not exclusively, piece/part failure oriented and is performed on any system containing integrated components or assemblies. It indicates a need for remedial action, including redesign, if the component, assembly, or system does not meet established safety requirements. The analysis is a qualitative, semi-quantitative analysis performed as soon as subsystem designs permit. The analysis should be designed and performed so as to minimize problems in integrating component, assembly, or system hazard analyses into the weapon system hazard analysis.

80.5 System hazard analysis. This analysis is an extension and expansion of the subsystem hazard analysis and specifically addresses component, assembly, or system interface problems. The objective is to verify design compliance with specified safety standards, identify possible combinations of independent or dependent failures as safety deficiencies, identify corrective actions initiated, evaluate adequacy of those corrective actions, and identify top events for a fault tree analysis. The analysis also determines how system operation and failure modes can affect the nuclear safety of the weapon system and its subsystems.

80.6 Failure modes and effects analysis. The purpose of this analysis is to identify failure modes and effects that lead to undesired events in the fault tree analysis. Areas that should be specifically identified are single-point failures, insufficient redundancy in control of critical functions, and operational procedures required to compensate for hardware failures. There are two primary approaches in performing this analysis:

80.6.1 Hardware approach (bottom-up). The hardware approach lists individual hardware items and analyzes their possible failure modes. This technique should be used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. Normally the analysis proceeds in a bottom-up fashion with each identified failure mode being assigned a severity classification used to establish priorities for corrective or compensating actions.

80.6.2 Functional approach (top-down). The functional approach should be performed on more complex systems in a top-down fashion. All identified failure modes are assigned a severity classification which is used in establishing priorities for corrective or compensating actions.

APPENDIX

80.7 Failure modes, effects, and criticality analysis (FMECA). This analysis documents all probable failures in a system to the highest indenture level specified, determines by failure mode analysis the effect of each failure on weapon system operation, identifies single failure points, and ranks each failure according to a severity classification of failure effect. This analysis is essentially similar to a failure modes and effects analysis in which the criticality of the failure is analyzed in greater detail, and assurances and controls are described for limiting the likelihood of such failures.

80.8 Common-cause analysis. This analysis is performed to identify all modes of system failure which have the potential of being triggered by a single, more basic common cause. Thus, failure of a single component, assembly, or system induces distinct failures in two or more separate system elements which subsequently leads to occurrence of an undesired event/hazard.

80.9 Circuit logic analysis. This analysis is performed to verify that critical logic circuits perform only those functions for which they are designed. This analysis should be required since testing may exercise some paths only by chance and may never enter other logic paths which might be used at some random time after system deployment.

80.10 Cable failure matrix analysis. This analysis is a systematic design evaluation that examines, analyzes, and documents the effects of potential shorts or opens for connectors and circuits involved in critical functions.

80.11 Sneak circuit analysis. This analysis is performed to identify latent paths which could either cause undesired or inhibit desired critical functions, assuming all components are operating properly.

80.12 Launch action study. This study is performed to determine any actions necessary to cause the components to contribute to a launch. This study should be performed on all new systems and any weapon system which is significantly modified. Presentation of the launch action threats should be determined by subjective ranking of the importance of the components' contribution to launch. This study provides the source data for the UL study performed in accordance with AFI 91-106. See 80.13.

80.13 Unauthorized launch (UL) analysis. The UL analysis should determine credible UL scenarios and identify system components (see 60.1) which can be compromised or altered to cause, contribute to, or allow a UL. The following should be included:

80.13.1 Parameters. For each identified component, determine:

a. Agent preparations and procedures at each susceptible UL location;

b. Statistics associated with the time required to execute the UL scheme;

c. Tools and equipment needed to carry out the UL scheme;

d. Characteristics of missile support equipment, computer software, and other features and existing procedures which enable the system to detect or stop a UL attempt;

e. Statistics associated with the time required to detect a UL attempt; and

f. Methods to counter the UL attempt.

80.13.2 Evaluation. Based on the above determinations, accomplish the following:

a. Rank UL schemes in the order of what is most likely to occur by considering factors such as time required, technical feasibility, and availability of tools and equipment;

b. Identify the locations most susceptible to a successful UL attempt;

c. Summarize the rationale for the arrangement;

d. Calculate the probability of success without detection for each UL scheme as high, medium, or low;

e. Recommend measures which may be taken to counter each UL threat or scheme;

f. Identify duties requiring assignment limitations after exposure to UL study information; and

g. Identify personnel who require assignment restrictions.

80.13.3 **Threats.** The UL analysis should be based on the following threats:

a. One cognizant agent with characteristics as described in 80.13.5;

b. Any number of third-party agents with characteristics as described in 80.13.5; and

c. A combination of the above.

80.13.4 **Classification of documentation.** Working papers, drafts, and final documents should be classified according to the weapon system classification guide. Access to the analysis should be limited and on a strict need-to-know basis.

80.13.5 **Definition of UL-related terms**

a. **Cognizant agent.** A person who, because of normal duties, has the knowledge and opportunity to tamper with certified critical components, codes, or the nuclear command and control system of a nuclear weapon system. A cognizant agent is normally a member of a Two-Person Concept Team. The term includes persons who control or validate information about the condition of a nuclear weapon or its launch platform. It also includes anyone who could falsely lead others to believe a system is in working order when, in fact, it was being or had been tampered with or stolen.

b. **Third-party agent.** Anyone who does not meet the definition of a cognizant agent. A contractor (non-DOD civilian) is normally a third-party agent. However, when a contractor is performing duties involving a nuclear weapon system at an operational unit, the contractor may be considered to be a cognizant agent.

c. **Credible threat/scenario.** The agency responsible for conducting a UL study should identify all methods that the agent or agents may use to effect such a launch. A major part of this information comes from the launch action studies. The UL study team should not reject threats that are contained in the launch action studies. The team's concern should be that the threat fits the assumptions and ground rules in AFI 91-106. It may be obvious to the study participants that the scenario is too complicated or would take too much time to be successful, but they should not exclude this information from the UL report.

d. **Launch activation path (LAP).** The launch activation path is used to identify weapon system components that could contribute to a UL and to define UL scenarios. LAP's should address all available critical signal paths; that is, if a UL scenario involves bypassing, the report should show how this changes the LAP.

e. **"Contribute to".** This term is subjective, and its application to a component cannot be rigidly applied. A UL study team should weigh the component's importance in the LAP and in the context of its role in any UL scenario. It is generally recognized that no single component, if compromised, would cause a UL by itself. However, some components are more important than others. Those that actually control critical functions are more important than those that only monitor critical functions. If a UL study team feels that the component would play an important part in a UL scenario, then the term "contribute to" would be applied. As a result of such a determination, the NWSSG or AFSA may designate the component as a critical component, but this is not the sole determining factor for critical component status.

80.14 Software hazardous effects analysis. This analysis is performed to ensure system controls are incorporated to prevent the software system from initiating nuclear safety hazards.

80.15 System safety analysis. A nuclear safety analysis of the system in both normal and abnormal environments is performed to determine the probability of the following events:

a. Premature nuclear detonation during storage and logistics operation (system not prearmed);

b. Premature nuclear detonation during each stage of prearming and arming; and

c. Premature nuclear detonation after the system is armed.

90. NUCLEAR SURETY AND COMPATIBILITY REPORTS

90.1 Nuclear certification plan (NCP). The NCP defines the process and identifies what will be used to qualify subsystem and equipment for nuclear certification. It will contain a description of the specific nuclear certification process for the designated weapon system, subsystem, and equipment definition of the nuclear configuration (the items to be nuclear certified) and identifies the tasks required to accomplish nuclear certification and provide operational capability. Authority, responsibility, and schedule constraints will be identified for each task. Schedules will be sufficiently detailed and updated as program requirements dictate to identify nuclear certification impacts to the weapon program. DI-NUOR-81409, Nuclear Certification Plan, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with instructions specified in these DID's.

90.2 Aircraft monitor and control (AMAC) design analysis report (DAR). This report defines and analyzes the aircraft system which controls the interface between the aircraft and the nuclear weapon. It should be submitted in two parts as described below. DI-NUOR-81408, AMAC DAR, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with instructions specified in this DID and prepared to include the following:

90.2.1 Preliminary DAR. This report should describe in as much detail as possible the design details of the proposed AMAC system, which consists of the electrical controls and avionics required to monitor, safe, or prearm a nuclear weapon prior to release. It should be submitted as soon as the design baseline of the AMAC system has been established. Normally, this should be in conjunction with the weapon system preliminary design review.

90.2.2 Final DAR. This report should include a complete design analysis detailing all the circuits and components employed, and an analysis showing compliance with the applicable nuclear weapons requirements. All electrical analyses should be based on worst expected conditions of aircraft direct current loads, power input conditions, and temperature conditions. The complete power distribution analysis should be performed using only the main alternating current generator(s). All constraints used in the analyses shall be substantiated in the report by cross-referencing applicable test reports, specification sheets, and military standard drawings. The design should represent the production design to be deployed, and no changes can be made to the nuclear interface defined in this report unless a revised AMAC report first provides a second review and is approved in writing by the authorized agencies. In order to support the ACCD release [a requirement for weapon capability date (WCD)/initial operational capability(IOC)], the final AMAC report should be completed and submitted at least 270 days prior to WCD or IOC.

90.3 Aircraft nuclear safety analysis report (NSAR). The NSAR is a comprehensive assessment of the surety design features and operational procedures of a nuclear weapon component, assembly, or system. The analyses performed and presented in the NSAR detail the weapon system compliance with the DOD Nuclear Weapon System Safety Standards, nuclear safety design requirements as specified in AFI 91-107, and nuclear security

requirements as specified in DODD 5210.41, DOD 5210.41M, and AFR 207-1. The NSAR is a primary source of input to the nuclear certification process of weapon systems which ensures surety consistent with operational requirements, as specified in AFI 91-101, AFI 91-102, and AFI 91-103. DI-NUOR-81405, Aircraft NSAR, applies to these requirements. Deliverable data should be prepared, to include the following:

90.3.1 Initial NSAR. The initial NSAR should be based on available design data and should be primarily qualitative. It should be structured to show how the nuclear weapon system should meet the DOD Nuclear Weapon System Safety Standards. The initial NSAR should define the nuclear configuration, provide a technical description of the nuclear system and present the maintenance concept for the weapon system nuclear configuration. It should reflect the preliminary hazard analysis and available results of any other system analyses, fault tree analyses, etc., which have been completed. STS normal/abnormal environments should be included in the NSAR assessment. The initial NSAR should summarize the principal nuclear safety features of the nuclear weapon system, summarize nuclear safety analyses performed to date, and assess any deficiencies discovered. Initial NSAR should support the Initial Safety Study (ISS) and should be delivered prior to the ISS as specified in AFI 91-102.

90.3.2 Preoperational NSAR. The preoperational NSAR should be a qualitative and quantitative analysis of the safety of the nuclear weapon system which shows that it meets the DOD Nuclear Weapon System Safety Standards. It should be delivered not later than 180 days prior to the Preoperational Safety Study (POSS). It should be similar to the initial NSAR, but should contain a more detailed, comprehensive, and complete analysis of the weapon system and should include results of all required testing. The following are examples of items and analyses which should be summarized and referenced to the source document:

a. Nuclear configuration definition

b. System description (including stores)

c. Maintenance concept

d. Functional description and analysis of the system and each component (including stores)

e. Failure modes analysis/failure modes and effects analysis/fault hazard analysis

f. Fault tree analysis

g. Hazard analysis

h. System hazard analysis

i. Subsystem hazard analysis

j. Cable failure matrix analysis

k. Failure modes, effects and criticality analysis

l. Analysis of areas of concern documented in the ISS

m. List of deviations of nuclear safety design requirements

n. Summary of design nuclear safety features

o. Analysis showing compliance with safety standards

90.4 System integrated nuclear safety analysis report (NSAR). The system integrated NSAR should be the integrating document that ties together all of the other NSAR's performed by associate or subcontractors for their particular/unique sections of a complex aircraft weapon system. The system integrated NSAR should

combine in one document an integrated comprehensive nuclear safety analysis for the complete aircraft weapon system. The system integrated NSAR is the responsibility of the lead or prime contractor, and should not be delegated to any other source. DI-NUOR-81405, Aircraft NSAR, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with the instructions specified in this DID.

90.5 Aircraft electrical compatibility data (ECD). The ECD's should define the physical, electrical power, and logical signal interfaces between the avionics components at the DOE/Air Force interfaces. They should cover all types of electrical interfaces in the monitor and control circuits of nuclear weapons, whether discrete lines or multiplex data buses. DI-NUOR-81410, Aircraft ECD, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with the instructions specified in this DID.

90.6 Aircraft mechanical compatibility data (MCD). The MCD's should define the physical and mechanical interfaces between the aircraft and nuclear weapons. They should cover dimensions, clearances, forces, installations, etc., associated with the weapons and suspension and release equipment. DI-NUOR-81407, Aircraft MCD, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with the instructions specified in this DID.

90.7 Engineering evaluation report (EER). Development or modifications to existing systems, subsystems, components, support equipment, or test equipment which are not accomplished in conjunction with the development of a nuclear weapon system should require an engineering evaluation by the Air Force. The analyses and tests which are conducted under this standard should be documented in an EER for the specific type of equipment being developed or modified. The EER should define the nuclear weapon system configuration, present a system overview, contain an integrated functional analysis, and present a nuclear safety analysis summary to support the recommendation for nuclear certification. DI-NUOR-81411, Engineering Evaluation Report, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with instructions specified in this DID.

90.8 Aircraft nuclear weapon system definition document (NWSDD). The nuclear weapon system definition document should define the nuclear configuration of the aircraft's avionics and nuclear weapon delivery systems. The nuclear configuration should be defined by the hardware and software components of the aircraft's avionics system and nuclear weapon delivery system. The NWSDD identifies the nuclear weapon system to be detailed in the NCP and also provides the source data for the NCP. DI-NUOR-81413, Aircraft NWSDD, applies to these requirements. Deliverable data identified on the DD Form 1423 should be prepared in accordance with the instructions specified in this DID.

90.9 Technical nuclear safety analysis (TNSA). The TNSA is prepared by ASC/OL-NS/EN and is the supporting documentation for NWSSG safety studies. It is a comprehensive qualitative and quantitative report that describes technical analysis of the total nuclear weapon system design and operational procedures. The TNSA will explain how the total nuclear weapon system does or does not meet the DOD Nuclear Weapon System Safety Standards.

90.10 Ground-launched missile nuclear surety analysis report (NSAR). The ground-launched missile NSAR is a comprehensive assessment of the surety design features and operational procedures of a nuclear weapon component, assembly, or system. The analyses performed and presented in the NSAR detail the weapon system compliance with the DOD Nuclear Weapon System Safety Standards, nuclear safety design requirements as specified in AFI 91-107, and nuclear security requirements as specified in DODD 5210.41, DOD 3150.2, and AFR 207-1. The NSAR is a primary source of input to the nuclear certification process of weapon systems which ensures surety consistent with operational requirements, as specified in AFI 91-101, AFI 91-102, and AFI 91-103. DI-NUOR-81406, Ground Launched Missile NSAR, applies to these requirements. Deliverable data should be prepared to include the following:

APPENDIX

90.10.1 **Initial NSAR.** The initial NSAR should be based on available design data and should be primarily qualitative. It should be structured to show how the nuclear weapon system should meet the DOD Nuclear Weapon System Safety Standards. The initial NSAR should define the nuclear configuration, provide a technical description of the nuclear system, and present the maintenance concept for the weapon system nuclear configuration. It should reflect the preliminary hazard analysis and available results of any other system analyses, fault tree analyses, etc., which have been completed. STS normal/abnormal environments should be included in the NSAR assessment. The initial NSAR should summarize the principal nuclear safety features of the nuclear weapon system, summarize nuclear safety analyses performed to date, and assess any deficiencies discovered. Initial NSAR should support the Initial Safety Study (ISS) and should be delivered prior to the ISS as specified in AFI 91-102.

90.10.2 **Preoperational NSAR.** The preoperational NSAR should be a qualitative and quantitative analysis of the safety of the nuclear weapon system which shows that it meets the DOD Nuclear Weapon System Safety Standards. It should be delivered not later than 180 days prior to the Preoperational Safety Study (POSS). It should be similar to the initial NSAR, but should contain a more detailed, comprehensive, and complete analysis of the weapon system and should include results of all required testing. The following are examples of items and analyses which should be summarized and referenced to the source document:

a. Nuclear configuration definition

b. Nuclear safety theme

c. Maintenance concept

d. Functional description and analysis of the system and each component

e. Failure modes analysis/failure modes and effects analysis/fault hazard analysis

f. Fault tree analysis

g. Hazard analysis

h. System hazard analysis

i. Subsystem hazard analysis

j. Cable failure matrix analysis

k. Failure modes and effects critical analysis

l. Analysis of areas of concern documented in the ISS

m. List of deviations of nuclear safety design requirements

n. Summary of design nuclear surety features

o. Analysis showing compliance with safety standards

p. AFI 91-107, Requirements Allocation Matrix

q. Critical component list

r. Launch action study

90.11 **Software certification plan (SCP).** The SCP is the document that defines the nuclear certification process the software should take toward achieving nuclear certification. DI-NUOR-81412, Software Certification Plan, applies to these requirements. Deliverable data identified on DD Form 1423 should be prepared in accordance with instructions specified in this DID.

APPENDIX

90.12 Computer hardware/software reports. Each nuclear safety discrepancy report should reference the nuclear safety objective that has been violated, using the priority scheme described in AFI 91-103. These discrepancies should be documented on an Air Force Form 261, Discrepancy Report.

100. BIBLIOGRAPHY OF RELATED DESIGN DOCUMENTS

100.1 Government documents

100.1.1 Military specifications, standards, and handbooks

SPECIFICATIONS

MIL-M-5096	Manuals, Technical: Inspection and Maintenance Requirements; Acceptance and Functional Check Flight Procedures and Checklists; Inspection Work Cards; and Checklists; Preparation of
MIL-S-8512	Support Equipment, Aeronautical, Special, General Specification for the Design of
MIL-A-8591	Airborne Stores, Suspension Equipment and Aircraft-Store Interface (Carriage Phase); General Design Criteria for
MIL-M-9977	Manuals, Technical and Checklist: Munitions Loading Procedures, Nonnuclear and Nuclear (Aircraft)
MIL-T-21868	Truck, Lift, Fork, Diesel; Shipboard, General Specification for
MIL-C-25077	Cable Design Requirements
MIL-C-25200	Cable Assembly, Special Weapons, Electrical, General Requirements for
MIL-M-25802	Manual Technical: Loading and Transport of Nuclear Weapon Cargo in Cargo Aircraft, Preparation of
MIL-T-25848	Technical Manual: Aircrew, Special Weapon Air-to-Ground Missile Delivery, Strategic Bomber Aircraft, Preparation of
MIL-T-25959	Tie Downs, Cargo, Aircraft
MIL-M-27026	Manuals, Technical and Checklist: Nuclear Delivery, Level, Strategic Bomber Aircraft, Preparation of
MIL-T-27260	Tie Down, Cargo, Aircraft, CGU-1/B
MIL-M-27579	Manuals, Technical: Aircrew, Nuclear Weapon (Bomb) Delivery, Multimode, Preparation of
MIL-M-27586	Manual, Technical and Checklist: Nuclear Munitions Loading Procedures, Strategic Bomber Aircraft, Preparation of
MIL-T-27594	Technical Manual and Checklist Assembly, Test and Storage Procedures, Missile/Warhead Mating, Preparation of

APPENDIX

MIL-T-28800	Test Equipment for Use with Electrical and Electronic Equipment, General Specification for
MIL-M-38784	Manuals, Technical: General Style and Format Requirements
MIL-S-45152	Semitrailers, Lowbed: Commercial
MIL-T-45333	Trailer, Flat Bed: 10 Ton 4 Wheel, M345
MIL-T-45382	Trailers, Low Bed, 4 Wheel, 2 to 7 Ton
MIL-T-52932	Trucks, Lift, Fork, Internal Combustion Engine, 2000-4000-6000 Pound Capacity, General Specification for
AFGS-87221	Aircraft Structures, General Specification for
MIL-S-87233	Support Equipment Systems

STANDARDS

MIL-STD-12	Abbreviations for Use on Drawings, and in Specifications, Standards and Technical Documents
MIL-STD-100	Engineering Drawing Practices
MIL-STD-275	Printed Wiring for Electronic Equipment
MIL-STD-454	Standard General Requirements for Electronic Equipment
MIL-STD-463	Definition and System of Units, Electromagnetic Interference and Electromagnetic Compatibility Technology
MIL-STD-480	Configuration Control—Engineering Changes, Deviations and Waivers
MIL-STD-785	Reliability Program for Systems and Equipment Development and Production
MIL-STD-962	Military Standards, Handbooks, and Bulletins, Preparation of
DOD-STD-963	Data Item Descriptions (DID's), Preparation of
MIL-STD-1365	General Design Criteria for Handling Equipment Associated with Weapons and Related Items
MIL-STD-1388/2	DOD Requirements for a Logistic Support Analysis Record
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment, and Facilities
MIL-STD-1522	Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems

APPENDIX

MIL-STD-1543	Reliability Program Requirements for Space and Launch Vehicles
MIL-STD-1574	System Safety Program for Space and Missile Systems
MIL-STD-1629	Procedure for Performing a Failure Mode, Effects and Criticality Analysis
MIL-STD-1750	Sixteen-Bit Computer Instruction Set Architecture
MIL-STD-1763	Aircraft/Stores Certification Procedures
MIL-STD-1785	System Security Engineering Program Management Requirements
MIL-STD-2000	Standard Requirements for Soldered Electrical and Electronic Assemblies

HANDBOOKS

MIL-HDBK-244	Guide to Aircraft/Stores Compatibility
MIL-HDBK-255	Nuclear Weapons Systems, Safety, Design, and Evaluation Criteria for
MIL-HDBK-272	Nuclear Weapons Systems, Safety Design and Evaluation Criteria for

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Standardization Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, phone (215) 697-2667.)

100.1.2 Other Government documents, drawings, and publications

US Nuclear Regulatory Commission Publications

NUREG/CR 2300	Probabilistic Risk Assessment Procedures Guide

(This document is available from the US Nuclear Regulatory Commission, Public Documents Room, Washington, DC 20555; phone (202) 634-3273; or NTIS (address below) or the US Government Printing Office (address on page 5).)

Department of Defense Directives

DODD 4540.5	Movement of Nuclear Weapons by Noncombat Delivery Vehicles
DODD S-5200.16	(S) Objectives and Minimum Standards for Communications Security Measures Used in Nuclear Command and Control Communications (U)

(Department of Defense Directives are available from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161-2171; phone (703) 487-4650.)

APPENDIX

Joint Chiefs of Staff Publications

JCS Pub 1	DOD Dictionary of Military and Associated Terms
JCS Pub 13, Vol. I	(S) Policy and Procedures Governing the Authorization and Safeguarding of Nuclear Control Orders (U)
JCS Pub 13, Vol. II	(S-FRD) Policy and Procedures Governing the Permissive Action Link/Coded Switch Cipher System (U)

(Copies of some JCS publications are available from the Air Force Publications Distribution Center, 2800 Eastern Boulevard, Baltimore, MD 21220; phone (410) 687-3330/DSN 584-4529.)

Air Force Regulations

AFR 35-99	Nuclear Weapons Personnel Reliability Program
AFR 40-925	Personnel Reliability Program
AFR 55-30	Operations Security
AFR 56-13	Safeguarding and Control of Communications Security Material
AFR 80-9	Nuclear Weapons Development Procedures
AFR 80-18	Department of Defense Engineering for Transportability
AFR 80-23	The US Air Force Electromagnetic Compatibility Program
AFR 80-54	Aircraft-Stores Certification Program (Seek Eagle)
AFR 88-15	Air Force Design Manual—Criteria and Standards for Air Force Construction
AFR 122-5	Sealing of Nuclear Components
AFR 125-37	The Installation and Resources Protection Program
AFR 127-4	Investigating and Reporting US Air Force Mishaps
AFR 127-100	Explosive Safety Standards
AFR 136-2	The Logistic Movement and Handling of Nuclear Cargo
AFR 136-10	Air Force Explosive Ordnance Disposal Program
AFR 205-4	Industrial Security Program Regulation
AFR 205-25	(S) Safeguarding the Single Integrated Operational Plan (U)
AFR 205-32	USAF Personnel Security Program
AFR 800-16	USAF System Safety Program

APPENDIX

(Copies of Air Force Regulations are available from the Air Force Publications Distribution Center, 2800 Eastern Boulevard, Baltimore, MD 21220; phone (410) 687-3330/DSN 584-4529.)

Technical Orders

TO 11A-1-46	Firefighting Guidance, Transportation and Storage Management Data and Ammunition Complete Round Chart
TO 11N-20-11	(C-RD) General Firefighting Guidance (U)
TO 11N-45-51	Transportation of Nuclear Weapons Material
TO 31Z-10-4	Electromagnetic Radiation Hazards

(Air Force Technical Orders are available from Oklahoma City Air Logistics Center (OC-ALC/MMEDT), Tinker AFB, OK 73145-5990; phone (405) 736-3771/DSN 336-3771.)

Air Force Materiel Command Regulations

AFMCR 80-17	Air Force Engineering Responsibility for Systems and Equipment

(Copies of Air Force Materiel Command regulations are available from the 645th MSSQ/MSIAPD, 4165 Communications Suite 3, Wright-Patterson AFB, OH 45433-5603; phone (513) 257-7191/DSN 787-7191.)

Air Force Systems Command Design Handbooks

AFSC DH 1-6	System Safety
AFSC DH 2-5	Armament
AFSC DH 4-2	Electronic System Test and Evaluation

(Copies of AFSC Design Handbooks are available from ASC/ENOSD, 2664 Skyline Drive, Bldg. 126, Wright-Patterson AFB, OH 45433-7800, phone (513) 255-6281/AV 785-6281.)

100.2 Other publications.

American Society of Mechanical Engineers

ANSI/ASME HST-4M-91	Performance Standard for Overhead Electric Wire Rope Hoists

(Non-Government standards and other publications are normally available from the organizations that prepare or distribute the documents. These documents also may be available in or through libraries or other information services.)

100.2.1 Minimum standards for design. The surety design requirements of this standard were developed to satisfy the DOD Nuclear Weapon System Safety Standards, AMAC POG interface specifications/standards and the Air Force policies on nuclear weapons. Therefore, the surety requirements of this standard are the minimum acceptable. The requirements contained in this standard are not intended to be design solutions, and they are

not intended to restrict the designer in the methods and techniques used to meet operational design requirements. The goal is to design a system that exceeds safety design requirements consistent with operational requirements.

100.2.2 **Minimum standards for verification.** The analysis and test requirements of this standard are the minimum required to verify that the DOD Nuclear Weapon System Safety Standards and the AMAC POG interface specifications/standards have been met for nuclear certification.

100.2.3 **Innovations and deviations.** The design requirements in this standard are not intended to restrict the designer. Innovative designs or advances in the state of the art may result in conflict with specific requirements even though the design solution may meet the intent of the DOD Nuclear Weapon System Safety Standards. In such cases, a deviation to the requirement should be requested. Such requests should be submitted to the applicable engineering organization. The engineering organization should coordinate the request through appropriate Air Force channels. The request should be submitted as early in the program as possible so that an adequate analysis may be conducted and the impact on system development minimized. The request should include supporting engineering data that shows that the alternate design meets the intent of the requirements and cannot meet the actual requirements.

100.3 **Weapon loaders.** For weapon loaders, the design goal is not to exceed a maximum drift rate of 0.5 inch per hour from internal leakage in hydraulic components of lift systems.

INDEX

INDEX (contd.)

INDEX (contd.)

INDEX (contd.)

Custodian:
Air Force – 27

Preparing Activity:
Air Force – 27

(Project 11GP-F003)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, not to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractural requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-STD-1822	2. DOCUMENT DATE *(YYMMDD)* 30 September 1994

3. DOCUMENT TITLE: NUCLEAR CERTIFICATION OF WEAPON SYSTEMS, SUBSYSTEMS, AND ASSOCIATED FACILITIES AND EQUIPMENT

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include Zip Code)*	d. TELEPHONE *(Include Area Code)* (1) Commercial (2) AUTOVON *(If applicable)*	7. DATE SUBMITTED *(YYMMDD)*

8. PREPARING ACTIVITY

A. NAME SA-ALC/NWI	B. TELEPHONE *(Include Area Code)* (1) Commercial: (505) 846-5391 (2) AUTOVON *(If applicable)*: 246-5391
C. ADDRESS *(Include Zip Code)* 1651 FIRST ST SE KIRTLAND AFB NM 87117-5617	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340