NOT MEASUREMENT SENSITIVE

MIL-HDBK-272A(OS)
2 APRIL 1993
SUPERSEDING
MIL-HDBK-272(OS)
15 AUGUST 1984

MILITARY HANDBOOK

NUCLEAR WEAPONS SYSTEMS, SAFETY DESIGN AND EVALUATION CRITERIA FOR

AMSC N/A **AREA NUOR**

FOREWORD

1 This military handbook is approved for use by the Naval Sea Systems Command, Department of the Navy, and is available for use by all Departments and Agencies of the Department of Defense

2 Beneficial comments (recommendations, additions, and/or deletions) and any pertinent data which may be of use in improving this document should be addressed to Commander, Indian Head Division, Naval Surface Warfare Center, (Code 8420), 101 Strauss Avenue, Indian Head, MD 20640-5035, by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document, or by letter

3 This document provides information and guidance on nuclear safety design and evaluation criteria to the project manager, acquisition engineer and others responsible for the design, test, and procurement of nuclear weapons components, equipments, subsystems, and systems The intent is not to provide detailed criteria, but rather to provide guidance and information which should be considered during design and procurement

4 Every effort has been made to reflect the latest information on nuclear weapons systems safety design and evaluation criteria It is the intent to review this handbook periodically to ensure its completeness and currency However, the currency of each reference or associated document should be checked before use

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

PARAGRAPH PAGE

APPENDIX A

SAFETY CRITERIA CHECLKIST

CONTENTS

APPENDIX B

ABBREVIATIONS AND ACRONYMS

APPENDIX C

DOCUMENTS FOR USE IN DESIGN AND PROCUREMENT

TABLES PAGE

THIS PAGE INTENTIONALLY LEFT BLANK

1. SCOPE

1 1. Scope. This handbook provides safety design and evaluation criteria which apply to nuclear weapon systems and their associated equipment for which funding and tasking are the responsibility of NAVSEA or appropriate Program Executive Officer (PEO) and Project Managers (PMs).

1.2. Purpose The purpose of this handbook is to provide safety design and evaluation criteria for nuclear weapon systems and associated equipment This handbook is primarily to provide guidance, and should not be interpreted as a contractual requirement. However, when an existing system is modified, the system should be evaluated to determine the extent to which these criteria should apply. This handbook contains extensive citations of reference documents such as MIL STD and MIL SPEC In order to enhance the usefulness of this handbook, some attempt has been made to paraphrase certain essential and key information from cited reference documents. Additionally, in order to extend the useful lifetime of this handbook, new concepts and technologies which are likely to be used in new or modified nuclear weapon systems are considered Examples include fiberoptics, integrated real-time processors, smart fuzing sensors, high energy lasers, reduction of human role, automatic target recognition and stealth technology Because of the rapidly increasing requirements for software and firmware control associated with these new concepts and technologies, criteria dealing with software and firmware are addressed in considerable detail

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 handbook to the extent specified herein

SPECIFICATIONS

MILITARY

MIL-B-5087	Bonding, Electrical, and Lightning Protection, for Aerospace Systems
MIL-E-6051	Electromagnetic Compatibility Requirements, System
MIL-M-8090	Mobility, Towed Aerospace Ground Equipment, General Requirements for
MIL-C-25200	Cable Assembly, Special Weapons, Electrical; General Requirements for
MIL-T-25959	Tie Downs, Cargo, Aircraft
MIL-T-27260	Tie Down, Cargo, Aircraft, CGU-1/B
MIL-C-28840 (series)	Connectors, Electrical, Circular Threaded, High Density, High Shock, Shipboard, Class D, General Specification for
MIL-C-38999 (series)	Connector, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for

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-463	Definitions and System of Units, Electromagnetic Interference and Electromagnetic Compatibility Technology
MIL-STD-480	Configuration Control - Engineering Changes, Deviations & Waivers
MIL-STD-483	Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs
MIL-STD-490	Specification Practices
MIL-STD-648	Design Criteria for Specialized Shipping Containers
MIL-STD-882	System Safety Program Requirements
MIL-STD-1365	General Design Criteria for Handling Equipment Associated with Weapons and Related Items
MIL-STD-1366	Material Transportation System Dimensional and Weight Constraints, Definition of
MIL-STD-1367	Packaging, Handling, Storage and Transportability Program Requirements for Systems and Equipments
MIL-STD-1385	Preclusion of Ordnance Hazards in Electromagnetic Fields; General Requirements for
DOD-STD-1399 (series)	Interface Standard for Shipboard Systems
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1512	Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
MIL-STD-1574	System Safety Program for Space and Missile Systems
MIL-STD-1660	Design Criteria for Ammunition Unit Loads
MIL-STD-1791	Designing for Internal Aerial Delivery in Fixed Wing Aircraft

MIL-STD-2105	Hazard Assessment Tests for Non-Nuclear Munitions
DOD-STD-2167	Defense System Software Development
DOD-STD-2168	Defense System Software Quality Program

HANDBOOKS

MIL-HDBK-235-1	Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment, Subsystems and Systems
MIL-HDBK-255	Nuclear Weapons Systems, Safety, Design, and Evaluation Criteria for

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

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

ORDNANCE DATA

OD 44942	Weapon System Safety Guidelines Handbook

ORDNANCE PUBLICATIONS

OP 4	Ammunition Afloat
OP 3565 Vol 2	Radio Frequency Hazards to Ordnance, Personnel and Fuel

(Copies of ODs and OPs can be obtained from the Standardization Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.)

SPECIAL WEAPONS ORDNANCE PUBLICATIONS

SWOP 20-20	Navy Safety Certification Procedures for Nuclear Weapons Equipment

(Copies of SWOPs can be obtained from the Officer in Charge, Naval Surface Warfare Center Indian Head Division Detachment, McAlester, Army Ammunition Plant, McAlester, OK 74501-5190)

NATIONAL SECURITY AGENCY PUBLICATIONS

Information System Security Products and Services Catalog

NSAP KAG-30-A/TSEC (S-NOFORN)	Compromising Emanation Standard for Cryptographic Equipment

(Copies of NSAPs can be obtained from the Director, National Security Agency, Attention C-Group, Fort George G Meade, MD 20735-6000)

DIRECTIVES AND INSTRUCTIONS

DODDIR 3150 2	Safety Studies and Reviews of Nuclear Weapon Systems
DODDIR 5030.15	Safety Studies and Reviews of Nuclear Weapons Systems
DODDIR C5200 5	Communications Security (COMSEC)(U)
DODDIR 5200 28	Security Requirements for Automated Information Systems
DODDIR 5200 28-STD	DOD Trusted Security System Evaluation Criteria
DODDIR 5200.29	DOD Technical Surveillance Countermeasures (TSCM) Survey Program
DODDIR 5210 41	Security Criteria and Standards for Protecting Nuclear Weapons
NAVSEAINST 5100.12	System safety program for ships, shipborne systems and subsystems, and equipment; requirements for implementation of
NAVSEAINST 8020.6	Naval Explosives Safety Program; Responsibilities, Policies and Procedures for
NAVSEAINST 8020.7	Hero, Policy for Conduct of a Safety Program to Alleviate
NAVSEAINST 8110.4	Nuclear Weapons System Safety Program Within the Naval Sea Systems Command
OPNAVINST 5239.1	Department of the Navy ADP Security Program
OPNAVINST 8023 19	Safety Criteria and Standards for the Movement of Nuclear Weapons by Non-Combat Delivery Vehicles

OPNAVINST 8110 18	Navy Nuclear Weapons Safety Program
OPNAVINST 8110 20	Safety Studies and Reviews of Nuclear Weapon Systems
OPNAVINST C8126 1	Navy Nuclear Weapons Security Manual

(Copies of DODDIRs, NAVSEAINSTs, and OPNAVINSTs can be obtained from the Navy Avaiation Supply Office, Physical Distribution Division Code 103, 5801 Tabor Avenue, Philadelphia, PA 19120-5099)

MISCELLANEOUS PUBLICATIONS

NAVSEA S9086-1A-STM-000/CH-793	Naval Ships' Technical Manual (Security of Stowed Nuclear Weapons)
NAVSEA S9086-TX-STM-000/CH-583	Naval Ships' Technical Manual (Boats and Small Craft)
NAVSEA S9086-T4-STM-010/CH-589	Naval Ships' Technical Manual (Cranes)
NAVSEA S9AAO-AA-SPN-010/GEN SPEC	General Specifications for Ships in the United States Navy
NWP 14-1	Loading and Underway Replenishment of Nuclear Weapons
NAVFAC P-300	Management of Transportation Equipment
NAVFAC P-307 Volume 1	Management of Weight Handling Equipment (Maintenance and Certification)
AFSC Design HDBK DH 1-11	Air Transportability

(Copies of Government documents, drawings, and publications whose source is not listed above, should be obtained from the procuring activity.)

2 2 Non-Government publications. The following document forms a part of this document to the extent specified herein.

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME)

HST-4M	Performance Standard for Overhead Electric Wire Rope Hoists

(Application for copies should be addressed to the American Society of Mechanical Engineers, 345 East 47th Street, New York, NY 10017)

AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM)

ASTM F1166 Standard Practice for Human Engineering Design for Marine Systems, Equipment and Facilities

(Application for copies should be addressed to American Society for Testing Materials, 1916 Race Street, Philadelphia, PA 19103-1187.)

(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 informational services.)

(For other documents that should be considered for use within the scope of this handbook, see Appendix C, Documents For Use In Design and Procurement)

3 DEFINITIONS

3 1 General. The following definitions are provided to supplement those contained in SWOP 4-1 and OPNAVINSTs 8110 18 and 8110 20 Abbreviations and acronyms are provided in Appendix B

3 2 Access. Close physical proximity to a nuclear weapon or critical component which would allow an opportunity to tamper, damage, or implant unauthorized devices Unauthorized devices are those which could result in or contribute to unauthorized deliberate or inadvertent authorization, prearming, arming, launching, or releasing of a nuclear weapon or cause an unauthorized failure or detonation of the nuclear weapon at other than its planned target Normally, a person would not be considered to have access if an escort or a guard were provided for either the person or the critical component when the person is in close proximity to it

3 3 Activate signals Those signals developed and delivered to the switching assembly where they are combined with electrical power to produce control signals

3 4 Administrative functions Functions within a weapon system which serve solely to provide administrative control (PAL lock, unlock, or re-code) or information (warhead identification or status, system status, etc), vice providing weapon system functional control

3 5 Armed component A weapon component is armed when it has responded to an influence to change its state from Safe, or Disabled (inoperable), to Arm, or Enabled (operable).

3 6 Arm/Disarm (A/D) device A device that provides a positive interruption of the firing circuit

3 7 Automata That class of sequential machines which, by alteration of internal state, are capable of performing logical, computational. or repetitive routines, i.e , automatic processors, computers, decoders, controllers, and their associated equipment.

3 8 Automation Design and implementation of a system which is self-controlling

3 9 Certified equipment Items of support equipment, combat delivery vehicles, and noncombat delivery vehicles which have received a nuclear safety engineering evaluation and have been nuclear safety approved for use with nuclear weapons in accordance with SWOP 20-20

3 10 Combat delivery vehicle Any nuclear capable vehicle and its installed equipment used for the combat delivery of nuclear weapons. Operations of combat delivery vehicles are the subject of specified nuclear safety rules promulgated by the Chief of Naval Operations.

3.11 Computer hardware Devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs

Such devices can perform substantial interpretation, computation, communication, control, or other logical functions

3 12 Computer software (or software) A combination of associated computer instructions and computer data definitions required to enable the computer hardware to perform computational or control functions. Software also includes microcode and firmware Components of nuclear safety critical software are categorized by the degree of involvement in nuclear critical functions:

a. Category I software (direct involvement). That software which is directly involved with the display of data of the control, monitoring, or execution of nuclear critical functions.

b Category II software (indirect involvement). That software which directly or indirectly transfers, stores, or shares data with or controls Category I software. Category II software is divided into subcategories·

(1) Subcategory II A software· system run-time support software.

(2) Subcategory II B software: applications-oriented software. This includes not only tactical software but also application-unique support software

c Category III software (no involvement) That software which is neither Category I nor Category II

3.13 Consent. A function implemented by a deliberate act that provides control over the select, prearm, launch, and fire functions

3 14 Coupling A measure of data connectivity between a module and the program in which it is imbedded.

3.15 Critical The use in this handbook describes functions, circuits, activities, sequences, signals and hardware and software components which apply directly to, or control, the selection, loading, prearming, arming, firing, unlocking, releasing, launching, or targeting functions of a nuclear weapon system.

3 16 Critical component A component which requires special handling during an identifiable portion or all of its life cycle Examples of critical components are as follows.

a. A nuclear weapon, with or without its arming and fuzing system installed.

b. A combat delivery vehicle which has had all preload functions completed and is ready for nuclear weapon mate or load

c. A combat delivery vehicle which has a nuclear weapon mated or loaded

d A component (hardware or software) of a nuclear weapon system which has been identified as critical by the SYSCOM or PEO to the Nuclear Weapon System Safety Group (NWSSG). A component that if bypassed, activated, or tampered with could result in or contribute to unauthorized deliberate or inadvertent authorization, prearming, arming, or launching or releasing of a nuclear weapon, the launching of a combat delivery vehicle carrying a nuclear weapon; or the delivery of a nuclear weapon to other than its planned target

3 17 Electrical isolation Separation of electrical circuits, signals, or data to preclude ambiguity, interference, or information perversion This may be achieved through physical isolation or by any property which distinguishes one electrical signal from all others (for example, time, phase, amplitude or frequency)

3 18 Electrical interfaces All electrical interfaces for the weapon system which are controlled by interface control drawings through joint Department of Defense and Department of Energy and Contractor subcommittees established by the Weapon System Project Officer.

3 19 Electroexplosive device An electrically initiated explosive device having an explosive or pyrotechnic output

3.20 Electromagnetic compatibility. The ability of electronic equipment, subsystems, and systems to operate together in their intended operational environments without suffering or causing unacceptable degradation because of unintentional electromagnetic radiation or response

3 21 Electromagnetic interference (EMI). Any electromagnetic disturbance which interrupts, operates, obstructs, or otherwise degrades or limits the effective performance of electronics/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

3 22 Electromagnetic pulse (EMP) 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 military systems to produce damaging current and voltage surges. EMP may also be caused by non-nuclear means

3 23 Electromagnetic radiation (EMR) Radiation made up of oscillating electric and magnetic fields and propagated at the speed of light Electromagnetic radiation includes x-rays, gamma, ultraviolet, visible, infrared, and radar and radio waves.

3 24 Enhanced (Electrical) nuclear detonation safety (ENDS). A warhead nuclear safety design approach that combines co-located strong link(s), weak link(s), barriers, and unique signals (see 5 5 5).

3.25 Fail-safe A design feature of a nuclear weapon system/component which ensures that, under failure, the item remains in the safe condition such that no critical functions will occur.

3.26 Firmware The combination of a hardware device and computer instructions or computer data (software) that reside as read-only software on the hardware device, and is completely write-protected when functioning in its operational environment.

3 27 First article. The first production-configured item of equipment, which is generally used for evaluation testing

3 28 Hard-wire A dedicated discrete electrical circuit.

3.29 Information security (INFOSEC). The integrated set of computer security (COMPUSEC), communications security (COMSEC) and operations security (OPSEC) measures employed to protect data and information assets during production, use, transmission, storage and processing on all forms of computer and communications-based media. INFOSEC is the protection afforded to telecommunications and automated information systems (AIS) to prevent exploitation through interception, unauthorized electronic access, or related technical threats, to ensure authenticity of data INFOSEC also includes the integrated set of COMPUSEC measures which are taken to protect the confidentiality, integrity, and assured service.

3.30 Intent command signal A control communication used to signify that the nuclear weapon is intended to prearm. The response of the weapon to this signal is to complete the prearming sequence, thus constituting a critical function.

3 31 Jettison. An authorized release of a weapon from the launch platform without initiation of critical functions.

3.32 Limited current. Monitor or test currents limited to less than that required to activate the most sensitive component in the arming sequence. Sometimes referred to as current limited.

3.33 Logic circuits. Interconnected electrical, electronic, and microelectronic circuits that carry and control electrical impulses, for the purpose of providing the "ON-OFF" intelligence for predetermined relationships within a system or subsystem.

3.34 Logistic movement. All movement of nuclear weapons and nuclear components by a noncombat vehicle, from the secure environment of a storage/alert area, not conducted in response to an increased readiness condition or wartime emergency plans.

3 35 Masked weapon A weapon whose trajectory would impact any portion of the shipboard structure, antennas, adjacent launchers and similar equipment

3 36 Microcode A set of sequences of elementary instructions (lower level than machine language) that correspond to computer operations, that are maintained in special storage, and whose execution is initiated by the introduction of a computer instruction into an instruction register of a computer. Microcode is often used in place of hardwired logic, and is usually inaccessible in programming.

3 37 Module An identifiable, self-cor tained, compilable, independent set of computer instructions with one entry point and one exit point that fulfills some well defined function

3 38 Monitor current A limited current introduced into a nuclear weapon to determine the functional status of selected components

3 39 Multiplexed system A signal transmission system in which two or more signals share one transmission path or bus A multiplexer is that portion of the multiplex system which formats, transfers, and processes signals

3 40 Noncombat delivery vehicle Any vehicle used for the movement of nuclear weapons, but not subject to the specific nuclear safety rules approved by the Secretary of Defense in accordance with DOD Directive 5030 15

3.41 Safe/Arm (S/A) device. A device which provides positive interruption of the firing circuits or the explosive or pyrotechnic train until it receives or senses the proper enabling signals or environment(s)

3.42 Selection. The positioning of controls, switches and other devices, or a logic condition that places a nuclear weapon in a position or condition to be further prepared for launch, release, or emplacement As used herein, "selection" is a critical function subject to nuclear safety criteria and evaluation

3 43 Software See Computer software

3 44 Stop attack The act of a single person to render a launched or fired weapon incapable of producing a nuclear yield (see 4 3 13)

3.45 Structured design A software hierarchial design technique with specified rules governing the hierarchy in terms of design order of modules, independence of modules, and specification of data and interfaces

3 46 Structured program. A program whose control logic topology adheres to strict rules of form, being composed of interactions and nestings of a set of basic planar flowchart

constructions. SEQUENCE, IF THEN ELSE, DO WHILE, DO UNTIL, CASE along with, perhaps, paranormal extensions

3.47 Support or ancillary equipment. The equipment ancillary to a nuclear weapon for the purpose of handling and maintaining the weapon as well as that associated test equipment required to verify the functioning of the nuclear system. (General and special purpose hand tools such as pliers, wrenches, screwdriver, and so forth, are specifically excluded).

3 48 Tactical movement That movement of nuclear weapons or nuclear components made to support emergency plans or an alert posture during an increased readiness condition which authorizes a unit to remove nuclear weapons from their storage configuration in preparation for deployment to other locations.

3 49 TEMPEST Compromising emanations that are unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, can disclose the classified information transmitted, received, handled, or otherwise processed by electrical information processing equipment or systems

3.50 Unauthorized access. The capability and opportunity to obtain, alter or substitute a critical component. A person authorized to handle critical components does not have access if the ability to alter or substitute a critical component is prevented through observation by one or more individuals who are also authorized to handle critical components, or by physical controls that prevent access.

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

4 GENERAL GUIDANCE

4.1 Innovative designs The guidance contained in this handbook cannot cover all possible situations. Innovative designs or advances in the state of the art may conflict with specific guidance in this handbook even though the design solution (or an alternative design) may meet or enhance the objectives of the nuclear safety program or provide a significant safety advancement. None of the guidance contained herein is meant to discourage such new or innovative designs

4 2 Nuclear safety

4 2 1 Nuclear weapons safety Because of their political and military importance, their destructive power, their cost, and the consequences of an unauthorized or accidental nuclear or high explosive detonation, nuclear weapons will be protected against the risks and threats inherent in all their environments The conservation of nuclear weapons as a national resource and the safety of the public, operating personnel, and property are of paramount importance. These weapons and weapon systems must be designed to incorporate maximum safety consistent with operational requirements Within DOD, nuclear weapons safety is maximized by prescription and enforcement of the four DOD nuclear weapon system safety standards. The implementation of these standards at the design level is accomplished by requirements for certain critical functions for weapons and/or systems. Certification of the nuclear weapon system is required before operational use is authorized Nuclear weapons safety involving equipment which may be associated with nuclear weapons or warheads during their life cycle (such as storage and handling equipment) is implemented via requirements for nuclear safety certification of such equipment Various DOD departments, commands, and activities which are charged with design, development, procurement, test, storage, handling, maintenance, or operation of nuclear weapons systems and/or components must ensure compliance with the four DOD nuclear weapon system safety standards by developing and enforcing nuclear safety design and evaluation criteria which apply to their respective systems, subsystems, or equipment. OPNAVINST 8110.18 provides overall guidance and policy for the Navy Nuclear Weapons Safety Program. NAVSEAINST 8110.4 provides the same for the Naval Sea Systems Command, and NAVSEAINST 5100 12 provides policy and guidance for ship system safety programs under NAVSEA cognizance.

4 2 2 Minimum criteria Outlined herein are the minimum nuclear safety criteria normally used to evaluate nuclear weapon systems and associated equipment. These criteria are not considered to be design solutions or all-inclusive nuclear safety standards, and are not intended to restrict the designer in the methods and techniques used to meet operational design requirements. Because this guidance is not all-inclusive, the system may still require additional safety features as the specific situation dictates

4.2 3 Nuclear safety standards. The DOD has established four safety standards contained in DOD Directive 3150.2 (which is implemented by OPNAVINST 8110 20) that are the basis for the nuclear safety rules governing nuclear weapon system operations and nuclear

weapon system design and evaluation criteria The system designer should bear in mind that these four nuclear safety standards must be met and that the operational use of a nuclear weapon system may be restricted if design safety criteria are not satisfied These standards require that·

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

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

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

d There shall be positive measures to ensure adequate security of nuclear weapons, pursuant to DOD Directive 5210.41.

4.2.4 Controls At the design level, these safety standards are implemented by control of critical functions in the sequence leading to detonation of the weapon The safety features designed into NAVSEA nuclear weapon systems must provide positive control over the occurrence of these critical functions As a minimum, the four critical functions described below must be included in the design of a nuclear weapon system

a. Authorization or enabling. The first critical function to be controlled is authorization or enabling. The weapon system will use a device (such as a Permissive action Link (PAL)) to control authorization. The function of the device will be to cause an enabled condition (a condition that permits selection, prearming, or arming) of the weapon system when authorization is received, through the command and control system, to prepare to use the system.

b Intent command signal and prearming The intent command signals the weapon that the personnel controlling the weapon want it to ultimately function and produce designed nuclear yield. The weapon's response to this command is to prearm. The prearmed condition is one of the inputs required by the weapon in its sequence of enabling, arming and firing The weapon system design will keep the prearming function totally separate and distinct from the authorization or enabling function. Design features will preclude prearming in the absence of the intent command signal, and will also prevent any bypass of the prearming device(s) that would permit arming without prearming

c. Launching or firing The critical function of launching or firing will be controlled as follows:

1. Self-propelled weapons Operation of the propulsion system (and control of launch) resulting in warhead movement will be controlled through two independent functions. The first function is a Safe/Arm (S/A) command for the ignition or motor start system Without the command to arm, propulsion system ignition or motor start will not occur even if the ignition or motor start command is sent In a rocket motor, a device with such a function is a rocket motor S/A device The second function is an ignition or motor start command Design features will preclude accidental transmission of either the arm command or the ignition/motor start command, and they will prevent any bypass of the ignition/motor start safing device so that ignition/motor start could not occur with the device safed

2 Impulse launched weapons Operation of the firing system will be controlled through two independent functions The first function is an arm command for the firing system Without the command to arm, initiation of the impulse will not occur even if the command to fire is sent A device with such a function is called a firing system S/A device The second function is a command to fire (firing command) Design features will preclude accidental transmission of either the arm command or the firing command, and they will prevent any bypass of the safing device, so that initiation of the impulse charge can not occur with the device safed

d Environmental sensing and final arming Environmental sensing consists of the weapon comparing minimum environmental criteria (preset) with the environment it is actually experiencing. This function occurs after launch or firing of the weapon Often, several environmental measurements are combined to improve the weapon's ability to discriminate against accidental or unauthorized arming and/or detonation If the weapon is prearmed, the response of the weapon to sensing the required operational environment is final arming Design features will include measurements of the environment so that non-operational environments are discriminated against to the maximum degree possible. If the weapon has self-contained guidance, a good guidance signal will be included as an element of the operational environment. The final armed condition is the condition that lets the selected fire signal (for example, radar, contact, or timer) detonate the warhead Design features will preclude final arming unless the required operational environment is sensed, and they will prevent erroneous transmission of the required operational environment signal. Design features will preclude any bypass of the final arming device(s) that would permit nuclear detonation of the warhead without final arming

4.2.5 Nuclear weapons equipment safety certification Safety certification procedures are contained in SWOP 20-20 for nuclear weapons equipment SWOP 20-25 is the Master List of Nuclear Weapons Certified Equipment

4.3 General design guidance

4.3.1 Nuclear safety standards. The DOD nuclear weapon system safety standards must be met.

4.3 2 Single component malfunction The malfunction or accidental operation of any single hardware or software component must not result in the selection, prearming, arming, launching, or firing of a nuclear weapon

4 3.3 Human engineering. Designers must emphasize human engineering to minimize the probabilities of human error (see MIL-STD-1472 and ASTM F1166). Using accepted human engineering methods, weapon system designers should conduct human error analyses and error reduction studies to identify any system mode(s) that may cause a hazardous condition. On the basis of these studies, designers add features which will minimize human error and limit its consequences The design should minimize the number of points within the system where human acts could degrade nuclear safety, and stress positive measures to prevent any accidental operation of controls that could degrade nuclear safety.

4 3.4 Administrative procedures. Adequate nuclear safety should be designed into the system so that dependence on administrative procedures for safety is minimized.

4 3.5 Unauthorized access. The system must be designed such that a single individual with authorized or unauthorized access can not select prearm, arm, launch, or fire a nuclear weapon.

4.3.6 Protection of friendly territory. Weapon systems are normally designed or controlled to prevent nuclear detonations except within specified target boundaries Missile systems utilizing guidance signals must receive a good guidance signal from the guidance and control unit before final arming of the nuclear warhead can occur The guidance signal is withheld if a final guidance accuracy check indicates that the weapon will detonate outside specified target boundaries As a design goal, the nuclear weapon system should be designed to provide means or methods to preclude nuclear detonation in the event that a non-guided round will impact outside specified target boundaries.

4 3.7 Authorized access. Systems must be designed to permit authorized access during all applicable phases of the Stockpile-to-Target Sequence (STS) to those components and circuits as required to carry out command disable, emergency destruct procedures or to operate the permissive action link if applicable

4.3.8 Environmental criteria. Nuclear safety design features must be considered over the full range of credible normal and abnormal environments and credible combinations thereof, to which all configurations of the system could be exposed. Specific normal and abnormal environmental parameters are system dependent and will be specified in the warhead or projectile STS document and in missile and carrier specifications.

4 3 9 Device reversibility Propulsion system ignition/motor start and firing system safing devices, authorization devices, and prearm devices should be reversible in operation prior to launch initiation

4.3 10 Administrative devices Mechanical, electrical, or other types of devices within a nuclear weapon system which are used solely for administrative functions should be isolated from the various circuits and devices which control critical functions. The application of power (controlled energy or uncontrolled energy, e g , lightning and induced currents) to an administrative circuit or device should not cause a nuclear weapon to be selected, prearmed, armed, launched, fired, or jettisoned

4 3 11 System safety precedence The order of precedence for satisfying system safety requirements is as follows

a Design for Minimum Risk From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design selection

b Incorporated Safety Devices If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk should be reduced to a acceptable level through the use of fixed, automatic, or other protective safety design features or devices

c. Incorporate Special Operational or Procedural restrictions. When the required degree of safety cannot be ensured through design or additional safety devices, special operational or administrative procedural restrictions should be developed for the system or appropriate components

4.3 12 Complexity of automated systems The design of complex automated systems, intended to minimize or prevent human errors, should not degrade nuclear safety

4.3.13 Stop attack. If the design includes a "stop attack" feature, it will allow a single person to render a launched, or fired weapon incapable of producing a nuclear yield The "stop attack" features are designed to be operable up to the moment of fuzing.

4 3.14 Explosive ordnance disposal. Nuclear weapons systems must provide for emergency access to those components and circuits required to effect render safe and disposal procedures.

4 3 15 System security Consistent with operational requirements, nuclear weapon systems security design must not inhibit nuclear safety features or requirements. Weapon system design must provide for security control to prevent or deter undetected access to nuclear weapon and nuclear weapon safety critical equipment or secure data. The design must ensure security control and protection of nuclear safety critical cards, software storage media,

keyboards, input controls, components, and devices which are developed to control or command the selection, loading, enabling, prearming, arming, firing, or launching of a nuclear weapon or nuclear weapon system. OPNAVINST C8126 1 is the Navy Nuclear Weapons Security Manual, and applies primarily to shipboard and shore based facilities

4 3.16 Information security (INFOSEC) Information security includes requirements for the development, delivery, control, process security, and integrity necessary to protect the system information from development through use in the Stockpile-to-Target Sequence. Guidance for information security is mandated through DOD Directives 5200.28, 5200 29 and 5200 40, implemented in OPNAVINST 5239.1A, and guided by DOD 5200 28-STD (the DOD Trusted Computer System Evaluation Criteria which is commonly referred to as the "Orange Book").

4 3 17 Hydraulic and pneumatic systems Installed shipboard handling and storage equipment which utilizes hydraulic or pneumatic systems is normally required to be designed in accordance with NAVSEA S9AAO-AA-SPN-010/GEN SPEC or applicable ship specification Sections 556 and 705 to provide positive control of weapons at all times during handling and storage, including both normal and casualty modes of operation In the event of power loss, the equipment should become immobilized until such time as safe, positively controlled operation can be resumed Hydraulic fluids will be selected and utilized to minimize the hazards of fire and toxicity in accordance with NAVSEA S9AAO-AA-SPN-010/GEN SPEC or applicable ship specification Section 556

4 3.18 Nuclear biological chemical decontamination. Use of standard decontamination agents, such as chlorinated compounds, hydrocarbons, chelated compounds, and water-detergent solutions, should not cause a degradation of safety through chemical reaction

4 4 General evaluation criteria

4 4 1 Responsibilities The Navy organization or contractor responsible for each specific system or subsystem will develop the specific plans, tests, and analyses necessary to demonstrate the operation of nuclear safety features and the compliance with nuclear safety standards and requirements. Navy organizations that have responsibility for providing engineering and compatibility guidance for a system or subsystem developed by an allied country for use with U S. nuclear weapons will be responsible for providing nuclear safety evaluation for such systems or subsystems. The responsible organization and the appropriate nuclear safety evaluation agency will determine the adequacy of test plans and completed tests and analyses as an integral part of the design and development process. The baseline for applying evaluation criteria is drawn from user requirements which are specified in formal documents such as the Justification for Major System New Starts, Operational Plan Data Document, Program Management Directive, the STS document, and the military characteristics document. Evaluation will be performed continuously by the responsible Navy agency as developmental modifications occur. General guidelines for evaluation requirements and responsibilities are provided by MIL-STD-882 and OD 44942. The DOD and Department of

the Navy developed non-nuclear components which contain energetic materials, as defined in MIL-STD-2105, and which are a part of the total nuclear weapon (exclusive of the DOE nuclear warhead), are required to have a PEO/PM sponsored systems safety program implemented by NAVSEAINST 8020 6 The details of such a program are described in OD 44942. The propulsion system must be tested in accordance with MIL-STD-2105. This system safety program must be reviewed periodically by the OPNAV Weapon System Explosives Safety Review Board prior to initial operational capability

4.4.2 Use of existing specifications When military specifications or standards which specify nuclear safety requirements exist, test and analysis requirements may be satisfied by demonstrating accomplishment of those specifications or standards When operational requirements are found to deviate from the test requirements indicated in the military specifications or standards, the test requirements should be supplemented accordingly

4 4.3 Identification of safety features Those safety features of subsystems and/or subassemblies of each item of equipment that provides nuclear safety should be identified as a part of the evaluation process

4 4.4 Control of targeting. Weapon systems will be evaluated to determine if the design is adequate to prevent accidental or unauthorized changes in targeting. They will also be evaluated to determine if adequate control is present to prevent nuclear detonations except within the boundaries of the designated target area

4 4 5 Emergency access Nuclear weapon systems are evaluated to make sure adequate emergency access is permitted to those components and circuits as required to carry out explosive ordnance disposal procedures These systems are analyzed to ensure that render safe and disposal procedures can be performed when necessary so as to positively preclude the possibility of a nuclear yield

4 4.6 Arm/Disarm and Safe/Arm devices A/D and S/A devices are tested and evaluated in accordance with MIL-STD-1512.

4 4 7 Environmental criteria The environmental requirements for each nuclear weapon systems are contained in the STS The testing requirements for support or ancillary equipment will generally be derived from the STS, the operational history of previous, similar equipment, and other equipment military standards

4 4 8 Safety analyses, demonstrations, tests and reviews. Detailed criteria, design reviews, analyses, testing, demonstrations, documentation, and reporting recommended by this document will ensure optimum incorporation of nuclear safety at the design level Test, analysis, and evaluation require the application of sound engineering judgement by personnel responsible for nuclear safety in all phases of system development, acquisition, modification, and operation. The data derived from tests and analyses are essential to accomplishing nuclear

safety evaluations. Both qualitative and quantitative analyses provide a basis for the nuclear safety evaluation

4.4.9 Objective of safety analysis. The objective of the safety analysis is to identify potential weakness in the design of nuclear weapon procedures and nuclear weapon system critical components that may lead to an undesired event through design errors, storage and handling deficiencies, transportation hazards, or improper administrative or operational procedures, and to make recommendations for hazard elimination or control. The safety analysis should identify all the potential causes of nuclear safety hazards, examples of which are.

a. Accidental nuclear detonation

b. An inadvertent or unauthorized event(s) such that any of the following may occur·

1. Emergency destruct
2. Loss or theft
3 Selection
4. Loading
5 Prearming
6. Arming
7 Launching or firing
8. Sneak circuit
9. Jettison
10 Loss of power
11. Command Disable

c. Any inadvertent or unauthorized event or sequence of events that may apply power to the nuclear weapon interface.

4.4.10 Examples of tests, reviews and analyses The following types of tests, reviews, and analyses are examples of those normally required to support weapon system development and DOD safety study efforts For more information on hazard analyses, see MIL-STD-882 and OD 44942

a Fault hazard analysis (FHA) Fault hazard analysis provides component level information on failure modes, effects, causes, and common modes susceptibilities within a given subsystem. The information is used in fault tree and common cause analyses

b. Operating and support hazard analysis (O&SHA). The operating and support hazard analysis is used to identify and control maintenance and operations, personnel errors and procedures which can contribute to potential hazards. The resulting information is used in fault tree and common cause analysis.

c. Fault tree analysis (FTA). A fault tree analysis is a technique for analyzing systems to identify all the faults and combinations thereof that will result in an undesired event (a specified system failure or event, such as a nuclear detonation) The objective of the FTA is to identify and analyze critical fault paths for which additional safety controls may be necessary The faults can be hardware failures, program errors in software or firmware, human errors, or any other pertinent events that could lead to the undesired event- the top event of the fault tree The fault tree itself is a graphic model of the parallel and sequential combinations of faults that will result in the undesired event.

d. Common modes analysis. Common modes analysis, conducted after the fault tree is constructed, uses the fault tree to identify similar or identical components that could fail simultaneously from the same cause or input, resulting in a system failure.

e Configuration definition A review and list of all assemblies, wires, transmission lines, (including microwave and fiberoptics), connectors, and other hardware, which, when considered totally, contribute to potential hazards relative to the nuclear weapon and launching systems.

f System interfaces A safety analysis of the inter-relationships between the nuclear system and other systems

g. Bent pin analysis Analysis of connectors which transmit critical nuclear functions to determine the result of shorts caused by bent pins

h Electromagnetic radiation compatibility Analysis of electromagnetic radiation compatibility to include all applicable spectral regimes (e g , optical if fiberoptics are employed in critical components or functions).

i Failure mode and hazardous effects analysis (FMHEA). Failure mode and hazardous effects analysis of nuclear configuration components and subsystems whose operation or failure could cause critical nuclear functions to occur.

j. Preliminary hazard analysis (PHA) The PHA is the initial analysis conducted during a system safety assessment of a weapon system at the beginning of a system safety program. A PHA is a gross assessment or appraisal of the potential hazard sources applicable to the weapon system design. This analysis can provide the basis for determining other required analyses. See MIL-STD-1574 for areas to be considered

k. Subsystem hazard analysis (SSHA). For a weapon system, the SSHA is a hazard analysis of a subsystem such as a fuzed, rocket motor, guidance section, missile fire control radar, launcher, computer, etc , and has two objectives. (1) identifying hazards as the design of each subsystem becomes available, and (2) providing initial

of critical components.

s. Software analysis Provides assurance that the software or other program controls as designed, coded, and implemented, cannot contribute to accidental, unauthorized, or fault activation of critical nuclear weapon system functions.

4.4.11 Susceptibility to inadvertent actuation. The objective of inadvertent actuation analyses (or inadvertent launch analysis (ILA)) is to reveal facts about nuclear weapon systems design which will establish the basis upon which an overall determination can be made concerning the likelihood of such actuation These facts may reveal design deficiencies in the system whereby either human actions, component failures, or combinations may negate the

nuclear safety design safeguards In reviewing these analyses, the NWSSG must determine to what extent a nuclear weapon system is susceptible to inadvertent actuation.

a Analysis of inadvertent actuation (equipment malfunction)

1 Assessment of potential events Determine the malfunctions required for occurrence of significant undesired events using techniques such as fault tree analysis The analyses will determine the critical paths and identify equipment and components which could, by malfunction, result in the occurrence of such events.

2 Identification of safety features Interlocks and other fail safe features to reduce or limit the likelihood of an undesired event caused by a malfunction are identified, described, and analyzed to determine level of effectiveness.

b. Analysis of inadvertent actuation (human error)

1 Critical areas of maintenance Referring to those points of susceptibility previously identified, describe the general type, frequency, and degree of maintenance performed on the equipment Designate those points as critical areas of maintenance

2 Critical maintenance and operational procedures. Describe each maintenance or operational procedure that involves replacement, repair, or checkout of any component, module, drawer, or black box which can be identified as critical with respect to inadvertent actuation of the nuclear weapon system

3. Identification of tools Identify and describe the general types, quantity and complexity of tools and equipment used to perform maintenance on these components

4. Fail-safe design features. Identify and describe each design feature or condition of the equipment which will cause the system to fail-safe if incorrect procedures are used by maintenance or operational personnel Determine if the failsafe feature(s) are adequate

5 Human engineering design features Identify and describe each design feature which, from a human engineering standpoint, is specifically designed to minimize human error

6. Assessment of potential undesired events. From the information described above, arrange all maintenance activities in the order of their likelihood (highest to lowest) of causing an undesired event

4 4.12. Analysis of unauthorized actuation (or unauthorized launch analysis (ULA)). An analysis of the weapon system to determine its susceptibility to unauthorized actions leading to events such as selection, loading, prearming, arming, launching or firing, jettison, command disablement, application of power to the nuclear weapon, and access, is normally required Each specific threat must be treated uniquely and in combination, to establish a complete threat assumption

a Potential threats This analysis should, as a minimum, be based on the following threats

1 One person in the command's Personnel Reliability Program (PRP).

2. Any number of third party agents.

3 One PRP member plus any number of third party agents but not two PRP members in collusion.

b Assumptions

1 Ordnance Data (ODs), Ordnance Pamphlets (OPs) and Special Weapons Ordnance Pamphlets (SWOPs) are accurate and complete

2 Nuclear weapon system hardware, software and firmware are free of manufacturing defects and have been delivered undamaged

3 Nuclear weapon system hardware, software and firmware may have been subjected to tampering which can remain undetected unless tests or inspections designed specifically to detect this tampering are imposed.

4. ODs, OPs, SWOPs, schematics and miscellaneous nuclear weapon system documentation are available for agents use

5. Agents are skilled in tasks necessary to perform the unauthorized launch.

6. Agents have access to, or knowledge of, codes, mass data storage devices, nuclear surety links, secure plugs, security alarm systems, permission-to-fire keys, or other sensitive system components only to the extent required by their assigned billet.

7. Besides the tools normally present at the site, an agent can use as many tools or devices as can be carried without creating suspicion. Planned support or previously placed tools may be available to the agent for use after penetration of the security system.

[redacted]

permit a determination of the degree to which the intrinsic weapon system design features inhibit an unauthorized launch. Based on this initial assessment, procedural security features will be reintroduced to develop realistic time lines.

4 Probability of the actual occurrence of a scenario will not be considered The probability that an agent might attempt a particular scenario or their methods of attack involve predicting the intent of an unknown individual which is considered an insupportable speculation

5. Scenarios which are not deemed credible based upon a predictably low degree of technical success, their probability of detection, or low overall probability of success shall not be considered for further analysis These scenarios however will be included in the report as a non-credible scenario.

6 Scenarios will be ranked in the order of probability of overall success. The scenarios most likely to result in a successful unauthorized launch shall be ranked first.

7. To ensure the adequacy of the analysis, each scenario and its variations will be developed thorough a comprehensive logic tree which is used to verify that all credible paths related to the top level event have been identified and addressed in the scenario analysis

8 The basic assumptions are meant to be conservative in that they envision the worst case of agent capability and knowledge. Additional conservatism will therefore not be added to the analysis Each step of the analysis will be accomplished in a realistic manner so that the analysis results will be credible and not overstated

jettisoning Nuclear weapon systems are evaluated to ensure that the design precludes generation of a nuclear yield in all credible abnormal environments associated with accidents, incidents, or jettison events in which the weapon system may be involved. The DOD portion of the system must provide part of the protection against accidental yields to meet the MC requirements for performance in normal and abnormal environments. The allocation of the DOE and DOD responsibilities is normally made by the Project Officers Group.

4.5 Responsibilities

4.5 1 NAVSEA project office The appropriate NAVSEA PEO/PM office responsible for the development or modification of a specified nuclear weapon system may utilize this document in the design and acquisition phase as an aid in ensuring nuclear safety

4.5 2 Nuclear weapon safety office The NAVSEA nuclear safety office will assist and advise the NAVSEA PEO/PM office in the implementation of nuclear safety analysis activities

5 SAFETY DESIGN CRITERIA

5.1 Shipboard systems

5.1 1 General. The design criteria set forth in this section apply to shipboard weapon systems as well as shipboard equipment and spaces used to stow, handle, transfer, assemble, load, and launch or fire nuclear weapons In general, these weapon systems are (but not limited to) missile systems, gun fired systems, torpedo systems, and atomic demolition munitions. In addition, these design criteria apply to those shipboard systems that are used to monitor weapons and systems used for weapon control Nuclear weapon systems that are ship-based but dependent upon an intermediate carriage mode by manned flight vehicle to the final launch point fall under the guidelines of MIL-HDBK-255(AS).

5.1.2 Shipboard fire control systems. The design of shipboard fire control systems for nuclear weapon systems must include positive means to prevent the unauthorized selection, prearming, arming, launching, jettisoning, or detonation of a nuclear weapon Consideration should be given to isolating switches, devices, controls, and circuitry controlling the safe condition of a nuclear weapon from those controlling conventional weapons. When possible, nuclear weapon designated switches and controls should (1) be of a different design (shape and mode of operation) from any other immediately adjacent controls and switches, (2) require two or more distinct movements before they are activated, and (3) prevent any device which singularly controls or selects nuclear weapons from being placed accidently in the nuclear weapon position

a Other equipment Controls, switches, circuits, circuit breakers, and other devices, when used solely for a conventional weapon system, must not cause the selection, prearming, arming, launching or firing of any nuclear weapon when operated in their intended mode The failure of any conventional weapon system control or device must not permit selection, prearming, arming, launching, or firing of a nuclear weapon

b Fire control system power failure The failure of power to the nuclear weapon system, fire control apparatus, switch, or circuit should cause any prearmed nuclear weapon Safe/Arm (S/A) device (such as the unique signal switch and the weapon propulsion unit's S/A device) to return to the SAFE condition. In addition, any nuclear weapon select switch or control that is in the "select" position should go to a "deselect" position Restoration of power must not automatically select, prearm, arm, launch or fire a nuclear weapon system

5.1 3 Launcher and launching devices The launcher or launching device for a shipboard nuclear weapon should be designed according to the following

a Single component failure. The failure of any single component in a launching system must not cause the weapon to select, prearm, arm, launch, or fire the weapon

b. Separate functions. The function within the launcher or launching device that controls the safe and arm system for the propulsion unit and the function that controls ejection or propulsion ignition should be separate and distinct functions. The propulsion system should not respond to an ignition or launch signal without having previously received a valid arm signal.

c. Accidental transmission. Launcher design features must preclude accidental transmission to the propulsion system of either the arm command or ignition command as a result of a component failure, stray voltage, electrical short, etc..

d. Launcher power failure. The loss of power to a launcher with a nuclear weapon present must cause the Unique Signal Switch (USS) and the propulsion system S/A device to return to SAFE. Return of power to the launcher should not cause the S/A device to return to ARM

e Launcher motion Motion of the launcher or launching device that is transmitted to an attached nuclear weapon must not exceed the design limits of any single component, or group of components within the weapon The motion induced into a nuclear weapon by a launcher must not cause the propulsion system or weapon's warhead to prematurely prearm, arm, launch, fire, or release the weapon. When evaluating a new weapon for use on existing launchers, the weapon should be designed to existing launcher motions

f. Physical limits. The total envelope of all possible positions that a launcher-weapon combination can occupy must not permit physical interference between the weapon and shipboard structure

g. Launcher-weapon separation trajectory. The launcher design must include interlocks within the launch command (firing circuits) to prevent interference between the weapon's projected separation trajectory and shipboard structures. Consideration must also be given to ensure that such interference will is precluded for movable structures such as rotating antenna, adjacent launcher, and similar equipment.

h Masked weapon indicator. The design of the shipboard weapon system should include provisions for a visual indication at the fire control center when a weapon is obstructed by shipboard structure.

5.1.4 Assembly areas and magazines. Shipboard nuclear weapon assembly areas must be designed to provide for the safety and security of nuclear weapons and nuclear weapon

components. These spaces must be designed to permit at least two persons to be present during authorized entry, to prevent unauthorized entry and to minimize the exposure of nuclear weapons and nuclear weapon components to abnormal environments. Shipboard nuclear weapon assembly areas and magazines are designed in accordance with SWOP 20-7, NAVSEA S9AAO-AA-SPN-101/GEN SPEC or applicable ship specification (Sections 703, 720, 730, 750, 770, 780, and 792), NAVSEA S9086-1A-STM-000 (Chapter 793), OP 4, and the following·

a Sprinkler systems Fire protection of the contents of magazines must be designed to maximize coverage.

b Personnel safety. Although magazines are designed to resist intrusion, these areas must provide means for personnel to exit the magazine rapidly in the event of an emergency

5 1 5 Administrative devices Mechanical, electronic, or other types of devices that may be within a nuclear weapon or within a nuclear weapon tactical container that are for administrative functions (such as PAL, warhead identification, indication of system status) must be separate and distinct from the various circuits and devices which control critical functions. The application of power (controlled energy or uncontrolled energy, e.g , lightning strikes) to an administrative circuit or device must not cause a nuclear weapon system to select, prearm, arm, launch, or fire.

5.2 Ground delivered systems

5.2.1 General. The design guidance described in this section applies to ground delivered nuclear weapon systems (artillery fired atomic projectiles (AFAPs), and atomic demolition munitions as examples)

5 2 2 Command and control systems. The design of command and control systems for ground delivery of nuclear weapons must include positive means to prevent the unauthorized launching, prearming, arming, firing, or detonation of a nuclear weapon

5 2 3 Delivery systems Howitzers, cannons, launchers, and other devices used to launch or fire nuclear weapons should be designed according to the following:

a Single component failure The failure of any single component must not cause the delivery system to prearm, arm, launch, or fire the weapon

b. Separate functions Those functions and devices within a delivery system that control the S/A system for the firing mechanism and those functions within the device that control the firing system should be separate and distinct functions. The firing system must not respond to a command to fire without having previously received a valid arm signal, or a deliberate manual operation

c Accidental transmission Delivery device design features must preclude accidental transmission of either the arm command or the fire command as a result of a component failure, stray voltage, electrical short, etc.

d Delivery device power failure If applicable, the loss of power to a nuclear weapon delivery device must cause the firing system S/A device to return to SAFE. Return of power to the delivery device must not cause the S/A device to ARM.

5.2 4 Nuclear projectiles Nuclear projectiles and associated equipment (hoist, loading trays, rams, etc.) must be designed so that the motion and forces induced into a nuclear weapon by this equipment does not cause the weapon to prearm, arm, or detonate prematurely.

5 2 5 Atomic demolition munitions Delivery techniques and handling equipment (if applicable) must be designed so that the environmental conditions (motion and forces due to parachuting, ground impact, hydrostatic and barometric pressure variations, and other effects) will not cause the munitions to prearm, arm, or detonate prematurely

5 3 Transportation and related support equipment

5.3 1 General. Safety must be incorporated into the design of vehicles and support or ancillary equipment used to transport, store, support, load and unload nuclear weapons. The vehicles and equipment must meet appropriate structural, environmental, and mobility requirements as defined in the applicable documents referenced in 2 1 and 2.2 The Stockpile-to-Target Sequence (STS) document defines transportation modes and environments the weapon system will encounter. The intent of the criteria in this section is to prevent damage to the nuclear weapon during handling and transportation. The safety design factors allow for the uncertainties in predicting operational conditions such as overloads, fatigue, wear, corrosion, residual stress, temperature influence on metal properties, and impact loads. The safety design factors also allow for the uncertainties or variations in material strength and manufacturing techniques and the uncertainties introduced by simplified design and test procedures. These criteria supplement good industrial design practices, standards, and features. They are not intended to prevent the use of any commercial design of equipment (such as trucks, truck tractors, semitrailers, trailers, and cranes) which meets these criteria

5 3 2 Ground transportation and support or ancillary equipment design criteria. NAVFAC P-300, Management of Transportation Equipment, and NAVFAC P-307 Volume 1, Management of Weight Handling Equipment, provide guidance and criteria for Navy transportation and support equipment. The following criteria apply to ground transportation equipment used to transport nuclear weapons on their basic structure, including trailers, semitrailers, self-propelled ground vehicles, forklifts and weapon loaders:

a Weapons support. This equipment should be designed so that the nuclear weapon is supported by the basic frame of the equipment rather than by lift arms, cables, or

hydraulic systems This does not apply to equipment used only to position or transfer nuclear weapons in a designated area such as a weapons storage area

b Grounding provisions Static grounding provisions must be provided for equipment designed for specific nuclear systems in order to prevent static electricity discharge through the weapons, if the design agency requires it

c Fire retardant/containment The equipment should be designed to reduce the propagation of fire due to electrical or fuel system failure

d Thermal buildup Enclosed transportation equipment should be designed so that the combination of inherent heat from weapon(s), solar heating, and ambient temperatures will not result in dangerous thermal buildup.

e. Tiedown configurations. The tiedown configuration for ground transport of all nuclear weapons must have and consider the following:

1 Tiedown points Provide the number of cargo tiedown points sufficient to restrain design loads

2 Tiedown terminals Ensure that the end of each tiedown device terminates at a separate attachment point without passing through any other attachment point.

3. Road conditions Consider worst case road conditions as identified in the STS

5 3 3 Structural design criteria The following structural design criteria will be determined by

a Rated load The rated load is that combination of forces that the basic equipment must support or resist in a static state This static load consists of the weapon(s) and the associated handling and tiedown equipment.

b Dynamic load To determine the dynamic load, the designer must consider lateral, horizontal, and vertical dynamic loads, accelerations encountered in ground transport environments, and shock loads associated with mate, demate, load, and unload operations

c Design load. The design load will, where practical, be based on the rated load multiplied by a factor of three, or on the dynamic load multiplied by a factor of two, whichever is greater This design load will be considered the minimum load for attaining the design stress levels.

d Allowable stress. In determining allowable stresses for equipment, the designer will select the material and type of 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 will be used.

5.3 4 Design criteria for trailers and semitrailers. All trailers and semitrailers used to transport nuclear weapons should meet the specific criteria in 5.3.1-5.3.3 and the following

a. Free-wheeling support equipment. All free-wheeling support equipment should be designed to restrain itself, e g , dead-man-brake, with its rated load.

b. Trailer allowable dynamics In a fully loaded configuration, trailer and semitrailer design should be designed to minimize

1. Tendency to yaw, sway, or skid under operating and braking conditions and minimum stopping distances

2. Tendency to tip, tilt, or jackknife.

c. Parking brakes Parking brakes should be designed to hold a fully loaded trailer on an 11 5 degree incline with the trailer headed up or down

d. Other braking requirements. Trailers and semitrailers must be equipped with an emergency braking feature to bring the trailer or semitrailer to a controlled stop if breakaway from the tow vehicle occurs The design should allow for a manual override of the breakaway device when the trailer is being moved by hand.

e. Mobility. Mobility requirements of MIL-M-8090 must be met if invoked.

5.3 5 Self-propelled vehicles. This subsection covers self-propelled ground vehicles such as trucks, vans, tugs, and tractors used to transport nuclear weapons, and vehicles used to tow (as a prime mover) other vehicles carrying nuclear weapons (excluding self-propelled howitzers or launchers). This subsection does not include loading/unloading trucks

a Tow vehicles

1. Braking system. Braking system must be functionally compatible with the towed vehicle braking system The towing vehicle should not add to yaw, sway, skid, tip, tilt, or jackknife of the towed vehicle under maximum braking conditions and minimum stopping distances.

2 Controls. Controls must be designed to ensure towed vehicles are under positive control

3 Parking brakes. The parking brakes, together with the towed vehicle parking brakes, should hold a fully loaded towing and towed vehicle combination on an 11 5 degree incline with the tow vehicle headed up or down

4. Vehicle connecting device The vehicle connecting device must be compatible with that of the towed vehicle.

5 Fifth wheel The fifth wheel (if used) must be equipped with a safety latch The safety latch should be designed to allow a visual check of the locked condition

6 Self-centering controls All movement controls (except for such devices as the parking brake, steering control, transmission selectors, power takeoff, and hydraulic pump) will be self-centering The engine start switch must operate only in the automatic transmission "neutral" or "park" position.

7 Creep movement A capability for small increments of forward and reverse movement is normally required

b. Transport vehicles A vehicle used to transport nuclear weapons on its basic structure should satisfy the criteria in 5 3 2 through 5.3 3 and have parking brakes that will hold the vehicle with rated load on an 11 5 degree incline with the vehicle headed up or down.

5 3.6 Material handling equipment (MHE) This section applies to equipment used to lift and load nuclear weapons (such as forklifts, missile lift trucks, high-lift trucks, munition handling trailers with lifting devices, and loading/unloading trucks). The criteria in 5 3.2 and 5 3 3 apply, as well as the following:

a. Fail-safe. The equipment must be designed to maintain safe control of the rated load if electrical, hydraulic, or pneumatic system failure occurs.

b. Parallel systems. If more than one power operating component in a mechanically parallel system is used to lift the weapon, the components may be individually controlled to provide weapon attitude adjustments However, the components must be capable of synchronization to provide a uniformly controlled lifting attitude.

c. Self-centering controls All movement controls (except for such devices as the parking brake, steering control, transmission selectors, power takeoff, and hydraulic pump) should be self-centering. The engine start switch must operate only when the automatic transmission is in the "neutral" or "park" position.

d Positive control Design must provide for positive control of the nuclear weapon at all times in the lifting and handling modes. One control method is to use load attachment points and straps.

e Motion limiting devices Mechanical stops or electrical switches must be added to prevent overtravel in all directions of the lift control Failure of a single motion limiting device should not result in damage to the weapon

f. Parking brakes Forklift parking brakes should 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 should independently hold a fully loaded weapon loader on an 11.5 degree incline with the loader headed up or down.

g. Tines and adapters. The forklift tines and adapters must be designed to safely meet all nuclear weapon operational requirements for the forklift. The forklift center of gravity must be compatible with this requirement

h. Creep motion capability. Weapon loader design will include a capability for small increments of movement in both reverse and forward directions

5 3 7 Hoists, cranes, and similar devices. The following criteria apply to hoists, cranes, winches, and similar equipment NAVSEA S9086-T4-STM-010/CH-589 is the Naval Ships' Technical Manual on cranes This equipment should be designed, as a minimum, to have:

a Positive control. Controls to ensure that the load is under positive operator control.

b Fail-safe stops. Features to make sure prompt, automatic stops are possible if the operating mechanism fails.

c. Automatic stops. Features to automatically stop the device in the absence of operator control.

d. Load and rate limits Identified limits and rates for maximum lift capacity and positioning.

e. Adequate safety factor. All hoists should be tested to a minimum of 125 percent and a maximum of 150 percent with a 200 percent static test for 10 minutes at the rated capacity.

f. Hooks. Hooks fitted with throat-opening safety devices.

g. Stops. Stops or limit switches to prevent overtravel of the hoist on rails and to stop the chain or wire rope when the hook reaches its upper limit. Failure of a single motion limiting device must not result in damage to the weapon.

5 3.8 Containers. Containers used for storage and transportation of nuclear weapons must meet the applicable portions of the weapon system STS and MCs, and should incorporate design criteria specified in MIL-STD-209 and MIL-STD-648 Tiedown points must be adequate to enable tieing down the container to meet ground, shipboard and aircraft cargo restraint criteria

5 3 9 Pallets Pallets designed for transportation and storage of nuclear weapons should meet the following criteria

a. Pallet design Pallet design should conform to MIL-STD-1366, and MIL-STD-1367. MIL-STD-1660 covers the design criteria for assemblage of items on a pallet

b. Tiedown Palletized weapons should be tied down directly to the vehicle Pallets must have provisions for attachment to the weapon for hoisting or handling without interfering with the tiedown points used to secure the weapon to the vehicle

5 3.10 Shipboard transportation systems Transportation and support equipment (including pallets) designed for use onboard ships and small craft should meet the applicable criteria of 5 3 1 through 5.3 9 NAVSEA S9086-TX-STM-000-/CH583 is the Naval Ships' Technical Manual on boats and small craft Additionally, the equipment should meet the following criteria

a Load criteria. The number and design of equipment tiedown points must be sufficient to restrain design loads based on maximum expected sea state conditions

b Separate terminator Each tiedown device should terminate at a separate attachment point without passing through any other attachment point.

5 3 11 Underway replenishment systems Shipboard equipment used for the Underway Replenishment (UNREP) of nuclear weapons or nuclear weapons components in accordance with NWP 14-1 should be designed and tested to preclude damage to nuclear components

a Pallets. Pallets used for UNREP of nuclear weapons must meet performance criteria of MIL-STD-1660

b. Containers. The containers must meet the shock isolation criteria in MIL-STD-648

c Floatation. Sufficient buoyancy should be considered as part of nuclear weapon UNREP equipment to provide floatation for the nuclear weapon and other equipment that may be lost overboard in the event of an underway replenishment accident or mishap

d. Load capacity. Pads, cables, winches, pulleys and other components of underway replenishment equipment should be designed to withstand the maximum expected load with a static safety factor of 5, 4 for a tension system and a dynamic load of 3.

5 3.12 Air transportation systems Air transportation and support equipment (including containers and pallets) should be designed to meet the general specifications of MIL-STD-1791 and applicable criteria of 5.3.1 through 5.3.9.

a Tiedown configurations Additional, nuclear cargo tiedown configurations should:

1. Not impose a reaction load that exceeds the strength of aircraft tiedown rings identified in the applicable cargo aircraft specifications.

2 Limit one tiedown device to one aircraft tiedown ring

3. Consist of tiedown patterns symmetrical about the longitudinal axis of the aircraft.

4. Require at least four tiedown devices for each item. Only tiedown devices that meet MIL-T-25959 for chains and MIL-T-27260 for straps will be used with nuclear cargo

5 Require each end of each tiedown device to terminate at a separate attachment point without going through any other attachment point.

b. Pallet configuration. Nuclear cargo tiedown configurations on pallets should.

1. Meet restrictions defined in the specifications for the pallet

2. Not exceed allowable deck roller loads identified in the applicable cargo aircraft specifications The pallets should bridge the rollers satisfactorily

c. Cargo restraint criteria. The design loads for the tiedown patterns are determined by applying the minimum acceleration due to gravity (G) restraint criteria approved by NAVAIRSYSCOM for the applicable aircraft (as specified in the STS). Depending upon the aircraft, these criteria may be in the NAVAIR cargo loading manual or the NATOPS manual for the aircraft. Tables I and II are provided as typical examples only The actually criteria may vary from aircraft to aircraft. Tiedown patterns must be structurally analyzed or proof-tested (or both) to make sure they meet the proper G load factors before these patterns are published in the aircraft cargo loading manuals and check lists. Off-pallet tiedowns which meet the criteria in 5.3.12 may be used to secure pallet loads in cargo aircraft

TABLE 1 Typical Nuclear Weapons Tiedown Configuration G Load Factors for Other than COD Aircraft (Example Only).

Load Direction	G Load
Forward	10.0
Aft	7 5
Lateral	3.0
Vertical (Down)	4 5
Vertical (Up)	3 7

TABLE 2. Typical Nuclear Weapons Tiedown Configuration G Load Factors for COD Aircraft (Example Only)

Load Direction	G Load
Forward	20 0
Aft	7.5
Lateral	3 0
Vertical (Down)	4.5
Vertical (Up)	10.0

5.3.13 Vertical replenishment criteria Equipment intended for use in vertical replenishment operations involving nuclear weapons must be designed in accordance with the requirements of NWP 14-1.

5.4 Electrical and fiberoptic systems

5.4.1 General A major portion of any nuclear weapon system is composed of subsystems designed to monitor, select, load, prearm, arm, launch, fire, and release nuclear weapons. These subsystems may depend upon electrical energy, light energy (for fiberoptics), or a combination of these. The design of these subsystems must preclude accidental operation, a single component failure, or an optical or electrical disturbance from performing or degrading critical functions.

5 4.2 Electromagnetic interference. All electronic and electrical subsystems/equipment in or associated with nuclear weapon systems must be designed so that undesired responses and emissions are minimized. Appropriate portions of MIL-B-5087, MIL-E-6051, MIL-C-25200, MIL-STD-461, MIL-STD-462, MIL-STD-463, MIL-STD-1385, DOD-STD-1399, MIL-HDBK-235, and OP 3565 Vol 2 apply. In addition, the design must ensure that the requirements of the National Security Agency TEMPEST program are met for the electrical, electronic, and fiberoptical equipment which process secure codes (NSAP KAG-30-A/TSEC).

a General Wires, switches, cable connectors, junction points, and other system elements must be designed to prevent undesired radiated and conducted interference or transients

b. Circuit protection The nuclear weapon monitor and control circuits, as well as launching and firing circuits, must be protected from Electromagnetic Interference (EMI) Protection from EMI must be carried through all applicable connectors, junction boxes, and other discontinuities, such as access doors and missile module joints.

5 4.3 Optical interference energy. All fiberoptic subsystems in or associated with nuclear weapon systems must be designed so that undesired responses and emissions are minimized. Fiberoptic cables, connectors, junctions and other system elements must be designed to prevent undesired radiated interference, transients, or degradation of subsystem performance when such interference or transients could result in a nuclear hazard, undesired release, launch of a weapon, or undesired firing of the weapon propellant Nuclear weapon monitor circuits, weapon control circuits, release circuits, and nuclear weapon firing circuits must also be protected from Optical Interference Energy (OIE). Protection from OIE must be carried through all applicable fiberoptic cable connectors, junction boxes, and other discontinuities.

5 4 4 Isolation. Isolation must be provided to prevent select, prearm, arm, launch, or fire functions from occurring during catastrophic events or abnormal environments. The following specific requirements apply

a Wire shields Wire shields must not be used as current carrying connectors. Shields should be covered by an insulation layer.

b. Electroexplosive circuits. MIL-STD-1512 applies to electroexplosive circuitry affecting critical functions

c Command and control, consent functions. Circuits for nuclear functions must be physically and electrically isolated from all other circuits and from each other.

d. Prearming and safing circuits. Prearming control circuits and safing circuits must be electrically isolated from all other circuits

e. Power circuits. Prearming power circuits must be physically and electrically isolated from all other circuits; however, the power and control circuits may coincide at the final switching assembly prior to the nuclear weapon interface Physical isolation within the final switching assembly must be maintained to the maximum extent possible.

f. Monitor circuits. Monitor circuits must be electrically isolated from power and control circuits. Monitor functions should be capable of being performed independent of weapon control functions

g. Logic circuits All logic circuit signal leads must be located away from power leads and must be routed to prevent short circuits and minimize inductive and capacitive coupling.

h Nuclear/non-nuclear functions For hard-wired systems, electrical functions which are peculiar to the nuclear weapon monitor, control, and release systems must not share an electrical connector with non-nuclear functions

i. Functional operation-warhead circuitry isolation Electrical wiring, circuits, components, etc , employed for functional operation of nuclear weapon guidance, must be electrically and physically isolated from the critical warhead circuitry.

j. Stray power sources Critical circuits must be isolated from potential sources of stray electrical power.

k Monitoring-functional circuit isolation. Hard-wired monitoring circuits should be separated from functional circuits Monitoring may be accomplished through separate circuits leading to back contacts or separate contacts of explosive switches, S/A devices, barometric switches, relays, etc. The above design practices that logically apply to fiberoptic circuitry and performance characteristics should apply to the design of fiberoptics used in or with nuclear weapon systems

l. EMP protection Critical weapon control system circuits and data must be protected from the effects of nuclear event related electromagnetic pulses specified in the STS

5 4 5 Alternating current power Power circuits must have twisted leads with single point grounding of the return Structure return should be avoided to eliminate common mode problems.

5.4 6 Thermal batteries. When thermal batteries are utilized, provisions should be incorporated to discharge the energy if the mission is aborted.

5.4 7 Switching. Normally, the ground side of power circuits will not be switched. To meet two-fault safety criteria, ground switching may be used in addition to hot-side switching

5.4 8 Design criteria for wiring and cabling The following criteria apply to electrical wiring and cabling These criteria that logically apply to fiberoptic links should be utilized in the design of nuclear weapon systems utilizing fiberoptics.

a. Electrical coupling and wiring separation. Wiring and cabling design to minimize coupling and provide for optimum separation within the available wiring space. Cable design should provide for adequate termination of shielded wires.

b. Cable construction. Cable construction should provide for twisting of each signal wire and the individual return wire. Equipment design and cable routing should minimize circulation currents Where employed, a signal return common to two or more circuits should use a common ground reference connection

c. Vibration Electrical wiring installed and secured to minimize vibration, minimize the effects of vibration, and prevent chafing.

d. Connector selection Except for weapon and warhead interface connectors, electrical power wiring should terminate in female connectors at the source outlet

e. Wiring support Wiring for critical circuits provided with mechanical support which is an integral part of the connector at the entry point into the electrical connector

f Fiberoptic links. Fiberoptic designed to preclude entry of stray optical radiation. Cable routing, securing methods, and bundling techniques designed to minimize the probability of damage to the links which could allow entry of stray optical radiation.

5.4.9 Design criteria for electrical connectors The following criteria shall apply to electrical connectors and to fiberoptic connectors where applicable:

a. Alignment. Electrical connectors designed to prevent misalignment of connectors, minimize bent pins during mating/demating, and prevent mating of adjacent connectors. Only one wire per pin should be used Connector pins not used as a terminal or tie-point for multiple connectors Spare pins not used for mechanical support of in-line components. (Such practices result in an inherent multi-fault condition.)

b. Connectors All hard-wired electrical connectors associated with nuclear weapon circuits must conform to MIL-C-38999 or MIL-C-28840 (for submarine applications). Electrical connectors isolated from non-electrical connectors. Potting compounds, if used in electrical connectors, must positively preclude reversion.

c. Pin assignment. The assignment of functions to pins within a connector must ensure that a short circuit occurring as a result of a bent or misaligned pin must not result in delivery of excessive/unintended current to the nuclear weapon or to critical function circuits.

d Back shell requirements. Connectors used to carry shielded wire should use a back shell that provides for peripheral bonding of the shield. Nonconductive finishes which would limit the bonding of the shields should not be used on these connectors.

5 4.10 Electrical current considerations Monitoring and testing current should be limited to levels below that required to actuate the most sensitive component in the nuclear weapon system

5 4.11 Design criteria for panel construction. Panel construction for critical electrical functions, if not hermetically sealed, should have all terminals fully insulated (or the panel fully enclosed) so that foreign objects cannot enter to cause terminal-to-terminal or terminal-to-ground short circuits. If a control panel applies power to the nuclear weapon, and is not hermetically sealed, it should be fully enclosed and all electrical contacts insulated. (Drain holes may be required by applicable military specifications) Logic elements used for the control, monitor, and release of nuclear weapons should be fully insulated if not hermetically sealed, to prevent terminal-to-terminal or terminal-to-ground short circuits caused by moisture or foreign objects

5 4.12 Electromagnetic radiation hazards to nuclear weapon systems. Nuclear weapon systems must be designed to protect Electroexplosive Devices (EEDs), semiconductor devices, fiberoptic devices, and other devices from Electromagnetic Radiation (EMR). The systems shall be designed and tested to assure their safety and reliability. EMR shields specified in MIL-STD-1385 must be certified as per NAVSEAINST 8020 7, HERO, Policy for Conduct of a Safety Program to Alleviate.

5 4.13 Design to eliminate or minimize electromagnetic radiation effects. Maximum practicable protection must be maintained against the hazards of EMR, including lightning and electro-magnetic pulse (EMP). The shielding design philosophy employed should recognize that the entry of electromagnetic energy into a system can occur through cable and wire couplings, windows and deliberate antennas, and the weapon system (acting as an antenna).

5.4.14 Shielding design. The following guidance is provided for achieving satisfactory shielding design:

a Place all susceptible components, subsystems, and systems in metallic enclosures (for example, storage and transport containers for missiles, shells, and reentry vehicles provide considerable protection against electromagnetic energy).

b. Provide Radio Frequency (RF) shielding for openings which provide access to cables, connectors, and other electrical equipment.

c Provide RF shielding for cables attached to susceptible components and for all cables attached externally to the nuclear weapon

d Provide attenuators, filter networks, lightning arrestor connectors, or electrical surge arrestors where practicable.

e. Use circuit-isolation relays or switches which are insensitive to RF energy and position them as close as possible to the elements to be protected to prevent energy pickup by long leads.

f. Ensure all section joints of the weapon are low-resistance contacts so that the weapon skin serves as an RF shield.

g. Firing circuits for EED should consist of two wires, twisted together and shielded A single ground point shall be common to all firing circuits.

h The system should be designed such that, regardless of the no-fire threshold of the EED, the maximum root mean square current experienced in the bridgewire is 20 db below the maximum no-fire current when exposed to the stray electrical energy environment specified in the STS, or 100 w/m^2 average, whichever is greater. However, maximum no-fire current is not the only design criteria of shielding. MIL-STD-1385 has other EMR field requirements that must be met.

i. Monitor circuits designed so that they will not conduct or couple EMR energy into functional or control circuits A 100 milliampere limitation applies for nuclear weapon/warhead monitoring.

j. The case of an initiator electrically bonded to the structure. All removable parts of the case, which are removed and replaced during operational and maintenance procedures, should not degrade the shielding after replacement or reassembly.

k. Maintain electrical continuity and isolation of circuitry shielding. Shields must not be used as intentional current carrying conductors. Metallic (water-proofed) shielding caps should be provided to ensure electrical continuity from shield to case with no gaps or discontinuities in the shielding configuration. When EED male connectors are open, shielding caps should be installed.

5.4.15 Electromagnetic radiation environment throughout the stockpile-to-target sequence. A comprehensive survey of the EMR environment which weapons will encounter is not available to date However, a general conclusion drawn from available measurements is that the ground-based, shipboard, and airborne radio transmitters now in the Navy inventory

generate average field intensities ranging from a few microvolts/meter to about 300 v/m, and that radars can generate peak power densities of about 75 dbm/m^2 in the near vicinity of the antenna The above mentioned power densities are presented here as an indication of the order of magnitude of the EMR environments anticipated The environments actually experienced by a particular weapon throughout the STS may be determined once the location and characteristic of all RF emitters in the vicinity of the weapon have been determined

5 5 Arming and fuzing systems.

5 5.1 General. The Arming and Fuzing (A&F) system is the sum of component devices and design features which cause weapon prearming, arming, fuzing, or firing, as well as those components and features which protect against deliberate unauthorized or accidental prearming, arming, fuzing, or firing The guidance set forth in this section is intended to be used by the NAVSEA PEO/PM and their contracted designers and evaluators Both DOD and DOE subsystems are normally a part of the total weapon system A&F design Effective design should incorporate the components and design concepts described herein to satisfy the criteria in 4 2

5.5.2 Design standards. Weapon system design must ensure against unauthorized or accidental selection, prearming, and arming signals being provided to the nuclear warhead in normal or abnormal environments The design must also ensure against premature launch, or firing The normal and abnormal environment nuclear safety protective features in the warhead can provide maximum protection only if these signals and events are controlled

5 5 3 Input for arming and fuzing The A&F system controls the energy required to cause prearming of propulsion units and warheads Some systems require a unique authorization stimulus. Missiles, projectiles, and warheads require unique prearming and unique environment or trajectory stimuli for operation In addition, weapons launched from ships, aircraft, and other vehicles, sense launch or firing from the delivery platform

5 5.4 Premature DOD input The A&F system provides the capability to respond to unique prearming and environment or trajectory input to the DOE warhead NAVSEA is responsible for protecting against premature transmission of the authorization, prearming, launch or release, and environment or trajectory inputs to the warhead in both normal and abnormal environments

5.5.5 Safety design concept Safety devices and features utilized in achieving nuclear safety should be designed to be a part of an integrated safety design concept for the weapon system. This is done by the DOE with their contractors for the bomb/warhead, which is designed to meet enhanced nuclear detonation safety (ENDS) criteria, and the various safety criteria in the MCs, in the absence of specific safety critical inputs One example of a DOE nuclear weapon safety design concept is the weak link/strong link, exclusion region concept, described below.

a Exclusion region. A region of the warhead containing the safety-critical arming and firing elements The region is protected, or isolated, from sources of electrical power by a barriers composed of accident resistant materials. Access to an exclusion region is normally controlled by a strong link.

b. Strong link. A warhead component that precludes energy transfer to an exclusion region under normal and abnormal environmental conditions unless it receives a unique signal indicating intent to arm As a safety device, it is capable of a predictable safe response at specified levels of abnormal environments

c. Weak link. An element of the warhead, critical to the arming and firing sequence, that becomes predictably and irreversibly inoperable at threshold environmental levels lower than those at which the associated strong links will remain operable, and barriers will maintain integrity.

d Unique signal (unique prearming signal). A unique signal is a specific, non-changeable sequence of bits of a pseudo-random nature specified by the DOE laboratory which contains sufficient information to assure that inadvertent or accidental generation, (e.g., as a result of circuit faults in abnormal environments), is precluded (see 5 5.6 c). This signal is required to authorize (or enable) detonation.

5 5 6 Devices and systems criteria for arming and fuzing The following guidance applies to shipboard arming and fuzing systems devices and to systems design features

a Warhead identification. When nuclear weapons of one type are mixed with nuclear weapons of a different type, or with conventional weapons, the launch platform weapon system should have the capability to query each nuclear warhead section and receive a fail-safe, unambiguous identification signal, as a result of the query, from the nuclear warhead section. A secondary means of identification should be provided (such as visual, radiographic sensor, etc.). In the event of an incorrect warhead identification, interlocks must prevent any additional movement, or selection, prearming, arming, launching or firing of the weapon, until positive identification is confirmed through secondary means.

b. Prearm device. The A&F system should contain a prearm device located in the warhead, missile, torpedo, projectile, or mine It may be a strong link safety device that is operated by a Unique Prearming Signal (UPS). This signal is generally derived from some part of the weapon system that is under direct human control If operational considerations permit, the function provided by human action should be reversible up to the actual launch, firing, or release of the weapon.

c. UPS signal

1. General. Inadvertent or accidental application of the prearming signal to the weapon system in normal and abnormal environments must be precluded by proper system design The design may incorporate the use of a UPS entered by a human, demonstrating intent (whether authorized or not) to use the nuclear weapon. An intent strong link unique signal may be derived from the UPS entered into the weapon system upon intent to use. A basic safety premise is that entry of the UPS into the weapon system results in a potential loss of the assured safety which is provided by the weapon system in abnormal environments

2. UPS implementation concept The basic implementation concept for UPS entry into the weapon system is that. (l) all of the necessary information be physically separated from the weapon system and retained in such a manner that it is readily apparent if the data has been entered, and (2) that the data cannot be accidently inserted, entered, or generated as a result of situations arising from a credible combination of abnormal environments.

3. UPS safety design criteria The following UPS data entry safety design criteria should be met within the weapon system. The fundamental intent of these criteria is to isolate key safety critical components from significant electrical energy in the absence of initiating human action. In the absence of human intent, the UPS must be precluded from the weapon system

   (a) Prevention of accidental UPS entry All of the information necessary to generate the UPS should be isolated from the weapon system, (e.g , physically separated), until entry is intended There should be no prior storage of the UPS data, or representation of the data such that it could be accidently entered into or generated by the weapon system. Word lengths and information content for UPS will be predicated on an analysis which assumes a single try implementation Algorithms which detect errors in the UPS data and automatically retry if not correct, should not be incorporated into design if they may create the possibility of multi-try capability in abnormal environments

   (b) Prevention of inadvertent UPS entry The data entry method should provide positive design features to prevent inadvertent human actions which could result in an insertion of the UPS data. These include mechanical features to assure that inadvertent operation or normal operation for non-nuclear functions will not cause UPS data insertion.

   (c) Positive erasure. The design of the UPS data entry system should assure positive and verifiable erasure of the UPS data after use in the system during system tests involving training or test rounds, or after use authorization of the nuclear weapon has been withdrawn.

4. Data entry methods Two general classes of UPS data entry methods are compatible with these considerations. The first is one in which the human operator physically inserts the UPS data into the weapon system with a device such as a read only memory plug, "credit card", magnetic tape, or other physical means. This type of UPS data entry system offers the most straight forward implementation of the stated considerations. The second method uses an input device such as a keyboard for the operator to enter the UPS data If this design approach is used, abnormal environment safety considerations may dictate that more keyboard strokes be used to enter the UPS data than would be needed to satisfy data requirements, since significant fragments of the UPS may be generated with a single keystroke

d. Environment sensor. In appropriate nuclear weapon systems, the A&F system will contain an Environment or Trajectory Sensing Device (E/TSD), preferably in the warhead or projectile. The E/TSD is a strong link device that will prevent arming until the proper environment or desired trajectory is sensed Since the weapon will respond properly to the specified environment or trajectory, it is essential to prevent premature launching or firing of the weapon

e. Launch or release sensing device The A&F system will normally contain a device that will prevent power from being applied to the arming and fuzing system. For ground or ship launched weapons, this device (such as a pressure actuated valve or an impulse sensing switch), will sense the proper environment unique to launch. Other types of weapons, such as mines, may utilize other sensors which would have a unique response to environments characteristic to the employment of that type of weapon. These devices are designed to ensure against accidental or inadvertent operations.

f Abnormal environment protection. Abnormal environment protection features will prevent prearming and arming in all abnormal environments specified in the STS document and in the applicable carrier vehicle specification.

g. Dual signal arming. At least two separate and independently derived signals, which cannot be generated by a single signal at any point, are normally required to arm the weapon. These signals are normally interrupted by one or more strong link devices. At least one of these signals must be continuous after application. This does not require multiple power sources After the A&F system has been prearmed, but before the weapon senses the final arming environment or trajectory, an A&F system failure should not result in arming the weapon.

h Energy discharge When applicable, the A&F system design will 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. The A&F system must not automatically return to an armed status upon the unintentional restoration

of interrupted power, without the proper re-sequencing of the weapon prearm and arming procedures

i. Lightning protection Lightning protection is normally required to protect critical A&F circuits Reference must be made to the STS document.

j Cable and connector design Cable and connector design and connector pin assignment must protect against premature transmission of prearm and arming power to the warhead or the weapon as the result of damaged cables and connectors. The design should guard against cable or connector selection and cable routing that is susceptible to damage during assembly, maintenance and test operations.

k. Nondestructive testing compatibility. Nuclear safety for the A&F system must not be degraded as a result of exposure to standard Navy nondestructive testing environments specified in use for the weapon systems These tests include, but are not limited to, X-ray, ultrasonic, magnetic, and similar tests

l System monitoring requirements for A&F The capacity to monitor the state of at least one strong link may be provided in all weapon system configurations The extent to which this capacity will be used is system dependent. In some systems this monitoring capability may only be used in emergency situations to determine the safe status of the weapon In others, monitoring may be required periodically during alert operations While the requirements to provide this capability are always placed on the A&F systems, the requirements placed on the weapon system to use the capability will be developed to complement the employment concept The monitoring function design should prevent the introduction of energy from any source that might operate an A&F critical function if a system fault or abnormal environment occurs Non-electrical monitor systems should be considered

m Chemical compatibility. All material used in the design must be chemically compatible in stockpile and storage environments No materials should be used that could increase the high explosive sensitivity, generate an explosive or toxic gas, cause an electrical short, reversion, or similar results

n. Input and output isolation Signal inputs, such as electrical current, fiberoptic light energy, or other similar energy to nuclear safety devices must be isolated from the outputs Other methods, (such as incompatible signals), may also be used to minimize the possibility of bypassing the safety devices

o. Dual enable system Systems which contain integrated real-time processors to determine fuzing parameters should be designed to have two independent systems to enable fuzing The interplay of the two systems should be controlled in the same manner as dual signal arming requirements discussed in paragraph 5.5.6.g.

5.6 Nuclear weapon system data processing hardware and software.

5.6 1 Data processing requirements These design criteria apply to hardware and software which receive, store, process, or transmit data to select, load, prearm, arm, enable, unlock, fire, or launch a nuclear weapon Such equipment should be designed to provide the highest degree of protection against accidental or unauthorized activation of critical command and control functions General guidelines for weapon system software development are provided in DOD-STD-2167. Guidelines for information security design criteria are contained in DOD Directives 5200 28, 5200 29 and 5200.40, implemented in OPNAVINST 5239.1A, and guided by DOD 5200.28-STD (the DOD Trusted Computer System Evaluation Criteria, commonly referred to as the "Orange Book")

5 6 2 General software nuclear safety criteria. The software developed for a nuclear weapon system must be designed to implement positive measures that satisfy the DOD nuclear safety standards These positive measures must ensure that the software is highly reliable and predictably safe. Components of nuclear safety critical software are categorized by the degree of involvement in nuclear critical functions

a. Category I software (direct involvement) That software which is directly involved with the display of data of the control, monitoring, or execution of nuclear critical functions.

b. Category II software (indirect involvement). That software which directly or indirectly transfers, stores, or shares data with or controls Category I software Category II software is divided into subcategories·

    1. Subcategory II A software: system run-time support software.

    2 Subcategory II B software: applications-oriented software. This includes not only tactical software but also application-unique support software.

c. Category III software (no involvement). That software which is neither Category I nor Category II.

5.6.3 Software development safety criteria. Software development should ensure that all software that could be directly or indirectly involved with critical functions contains no requirement, design, or code that causes or contributes to:

a Unauthorized or accidental prearming, arming, unlocking, enabling, launching, firing, releasing, or detonation of a nuclear weapon.

b Unsafe or premature operation of a nuclear weapon system.

c Alteration, modification, or unauthorized disclosure of validated targeting data.

d Unauthorized, improper, or erroneous display of status or classified information which could degrade nuclear safety

e Improper handling, invalid verification, or unauthorized retrieval of cryptographic codes which could compromise the control of the National Command Authority

f Alteration or modification of weapon system control software

5 6 4 Software design

5 6.4.1 General

a. The software design should be a structure of identifiable programs, sub-programs, modules, procedures, and routines developed in accordance with DOD-STD-2167A (Navy). Software configuration control should be conducted in accordance with DOD-STD-480A and MIL-STD-483, and software quality assurance conducted in accordance with MIL-S-52779A, which is tailored to meet system requirements.

b The implemented software (code) should be traceable directly to the design specifications (program design specification, interface design specification, data base design document, etc) The design specifications should be traceable directly to the software functional and performance specifications (program performance specification, interface design specification, etc) The software functional and performance specifications should be traceable directly to the system design requirements allocated to software from system level specifications (MIL-STD-490 Type A or B specification, system operational design, etc) The software should not include any code which cannot be traced directly through the software specifications.

5 6 4 2 Top-level design requirements The Software Design Organization (SDO) should ensure that the software top-level design incorporate nuclear safety features to.

a Prevent any unauthorized intra- or inter-system interactions from initiating or sustaining any nuclear critical functions

b. Prevent the initiation or sustaining of a nuclear critical function in the event of a malfunction or accidental operations

c. Prevent the initiation or continuation of a nuclear critical function in the event of two independent human errors

d Provide validity checks for program load or data load

e Prevent execution or use of transferred programs and data until all programs and data have been loaded and verified

f Immediately notify an operator if an error is detected during program or data loading

g Halt program or data loading and prevent the data or program from being used or executed if an error occurs

h. Detect unauthorized or inadvertent program or data transfers and prevent the execution or usage of unauthorized or inadvertently altered program or data.

i Provide a mechanism to ensure memory integrity of fixed program of data associated with nuclear critical functions.

j Ensure that the system enters a known, predictable, and safe state when a hardware malfunction is detected If the software has an operator interface, detected hardware malfunctions should automatically result in immediate operator notification

k. Ensure that memory (used or unused) is protected from unauthorized or inadvertent change

l. Provide positive measures to prevent unauthorized or inadvertent recovery of classified information This should include providing a method to overwrite any clear text nuclear critical secure codes from memory, per OPNAVINST 5239.1

m. Incorporate positive measures to preclude a single individual, with access, from accomplishing all nuclear critical functions.

n. Provide a uniquely controlled entry into each nuclear critical routine

o Ensure that changes to the nuclear critical state (e g., prearm, arm) of the weapon system cannot occur without independent invocation of the corresponding nuclear critical function

p. Ensure that reporting of nuclear critical state is based on positive indications (e.g., absence of an "arm" indication does not imply a "safe" state).

q. Provide an error classification scheme that distinguishes nuclear critical function errors from all others. Operator notification of nuclear critical functions errors must have priority over all other error notification.

r. Provide positive measures to prevent unauthorized or inadvertent access to the software system

s. Identify all data associated with nuclear critical functions

t Provide well-defined, predictable prioritization schemes

u Hardware and software used to implement critical functions should be designed to provide the capability to detect manually initiated commands, message errors, and deviations causing an erroneous entry to a critical routine.

v Provide maximum assurance against significant nuclear yield except within the boundaries of the authorized, designated target area

5.6 4.3 System execution/control structures System execution/control structures must incorporate nuclear safety to the maximum extent possible To achieve this objective, the following criteria are recommended as a minimum·

a The system contain only features or capabilities required by the system

b The system be initialized to a known and predictable state

c The system provide orderly shut-down

d The system provide for a nuclear-safe reduced system capability.

e The system provide fault detection and isolation capability

f The system provide weapon system and/data security.

g. The system provide positive control of nuclear critical functions at all times (e g., no deadlock, no infinite loop.)

h. The system provide the operator/user with nuclear safety critical notification consistent with human engineering practices

i The system provide for safe error recovery

5.6 4.4 Data transfer integrity The system should verify the integrity of program and data during remote data transfer. System operation should not begin until program and data verification has been assured Some examples of techniques to achieve these objectives are:

a. Verify transfer integrity for field, record, and file data (e g., by use of nonlinear checksums, bit-for-bit comparison data in Read Only Memory (ROM)).

b. Provide synchronization to shared equipment and distributed data bases.

c. Use of sending and receiving communication protocols

d Use of locking and time-stamping mechanisms for distributed data base updates.

e. Each block of data or program instructions being transferred in a local or remote mode to memory will exactly fill all memory available for the transfer If this requirement cannot be met, the memory available for the transfer will be overwritten with a fixed non-executable data pattern before writing the transferred data or program instructions

5.6.4 5 Coding and checkout The software design organizer should incorporate the following software nuclear safety recommendations into the translation of detailed design code

a Category I and II software should contain no extraneous code.

b. Patches to object code should be prohibited. Errors or discrepancies should be corrected in the source code format and re-compiled or reassembled.

c. The end-item program should not contain any non-operational code (e g., developmental, diagnostic, test and debug software).

d. Each flag should have a unique purpose.

e. Program self-modified by instructions during execution should be prevented.

5.6.5 Memory characteristics. Memory characteristics should ensure that contents of memory are not altered nor degraded over time during operational use. Memories with volatile characteristics should have provisions to ensure that erroneous or unexpected information from them due to power removal or other phenomena that change their state will not affect any critical function or component The system should inhibit any memory changes due to hardware failure. A single hardware fault should not cause a memory change that could initiate a critical function.

5.6 6 Memory integrity. Memory allocated program or data storage should be protected from accidental or unauthorized change. Unused memory, if any, should be filled with a known bit pattern which will ensure the maintenance of a positive system control in the event the system attempts to use the unused locations. A periodic test of the unused memory, all executable code, and fixed data should be performed and the operator notified if any change of state is detected.

5.6 7 Configuration management The organization for software development should establish configuration control procedures for all project materials These procedures must

ensure that developers use current authorized materials. The nature of nuclear software modules requires that special safeguard procedures be followed for critical nuclear software, in addition to the standard DOD security measures These procedures must prevent any single individual from accessing materials (program documentation, source and object code, software tools used for test or demonstration, etc) All developed code should be baselined and placed under configuration control.

5 6.8 Firmware integrity. The development, delivery and maintenance system utilized for nuclear critical firmware shall provide a system that allows the Fleet to verify nuclear critical firmware, specifically, hardware and/or software shall be provided that can be used to validate the state of nuclear critical hardware and firmware elements when required

5 7 Test and training equipment.

5 7 1 General The design criteria guidelines in this section apply to test equipment and training devices for nuclear weapon systems These guidelines are not necessarily all inclusive and should not limit the designer from introducing new, innovative ideas to further improve nuclear safety. War reserve weapons cannot be used as test or training devices. Where several agencies provide components of a system, coordination of the design must assure establishment and maintenance of a safe interface. In the event of conflicting requirements, the procuring activity shall determine the guiding requirement

5.7 2 Test equipment Equipment used to test nuclear weapon systems should meet the following design criteria

a Utilization Test equipment should be used only where necessary to establish and verify system operation, reliability, and safety The majority of any required testing should be done before the nuclear weapon is mated to the combat delivery vehicle. Testing should be minimized after a nuclear weapon is mated to its delivery system and/or delivered to its organizational level unit.

b. Test intervals. Intervals between required tests on nuclear weapons or weapon systems should be the maximum permissible to maintain a high confidence level in the system operation and safety.

c. Malfunction isolation The design should ensure that no malfunction or fault in the test equipment or test circuits can occur which could operate nuclear weapon critical functions or which could degrade the nuclear safety of the equipment being tested

d. Electrical isolation. The design should ensure that the introduction of stray voltages, unlimited current, or Electromagnetic Radiation (EMR) energy into the weapon system is minimized Interference and susceptibility within test equipment should be controlled by adequate provisions to eliminate undesired responses and

emissions from all electronic and electrical equipment in, or associated with, nuclear weapon systems

e Safing. Test equipment must ensure that any weapon system component which has been operated during testing is in the safe or inactivated condition at the completion of the test The safe condition of such components should be verified by a positive indication.

f. Fault identification. Based on system requirements, test equipment should reveal improper wiring, line-to-line shorts, line-to-ground shorts, stray or improper voltages, and improper system operation.

g Test equipment stability When nuclear weapons are present, electrical test equipment, including built-in test equipment, must be incapable of

1. Generating firing or launch signals

2 Causing any critical nuclear function to occur

3 Negating two-man control functions

4. Unlocking any safety interlock on the launch vehicle.

5. Activating an Arm/Disarm or Safe/Arm device

h. Data processing hardware and software Automata and software used for testing or checkout must meet the provisions of 5 6 of this handbook.

i. Power limitations Testers should not be capable of applying sufficient power to cause the operation or firing of any item being tested except when specifically designed to do so Electric currents for monitoring must be limited to values below the level capable of functioning the most sensitive component of the warhead section.

j Junctions, switches, and connectors Wires, switches, cable connectors, junction points, and other electrical system elements, as appropriate, should be designed to prevent undesired radiated and conducted interferences or transients

k. Monitoring currents. Monitoring currents should be placed on non-functional circuits through separate circuits leading to separate contacts of relays, electroexplosive devices, safe/arm devices, and barometric switches.

l. State of the art methods Wherever possible, the use of blocking schemes, fiberoptics, and any other state of the art system(s) to further isolate and protect critical circuits from those under test are encouraged.

5 7.3 Devices and simulators Training devices or nuclear weapons simulators cannot be used with war reserve nuclear weapons Further, training devices and simulators must not be capable of arming or launching a nuclear warhead Those items used to duplicate a nuclear weapon or weapon system function must have an explicit means of identification as a training item.

6 SAFETY EVALUATION CRITERIA

6 1 Nuclear weapon systems.

6.1 1 Shipboard Evaluation requirements and procedures for obtaining nuclear safety approval of a shipboard nuclear weapon consist of an evaluation of the design by analysis and test (where applicable) and a study and physical examination of the weapon system in accordance with OPNAVINST 8110 20 The primary requirements for nuclear safety for shipboard systems are described in the applicable design criteria sections.

6.1 2 Ground delivered When the implementation of system or equipment specifications will result in hazards, (see MIL-STD-1574), the system manager will conduct a trade-off study to achieve maximum nuclear safety consistent with operational requirements. The primary requirements for nuclear safety for ground delivered systems are described in the applicable design criteria sections

6 2 Transportation and related support equipment

6 2 1 General. Evaluation requirements for certification consists of analysis, examination, or testing by the responsible Navy agency. OPNAVINST 8023.19 provides the safety Criteria and Standards for the Movement of Nuclear Weapons by Non-Combat Delivery Vehicles. Weapons involved in logistic movement will not be in the completely assembled for launch configuration unless specifically authorized

a Fail-safe features. If fail-safe features are incorporated, they must be evaluated or tested to determine that they provide safe control of the weapon in any system failure. The weapon should not be supported by lift arms, cables, or hydraulic system, but by the basic frame of the equipment during both air and ground transport. This does not apply to equipment used solely to position or transfer weapons

b Fire or shock. The equipment must prevent or reduce the transmission of fire or shock to nuclear weapons This requirement can be demonstrated by analysis, testing, or a combination of both

c. Roadability The equipment must meet minimum roadability requirements as specified in the Stockpile-to-Target Sequence (STS)

d. First article analyses and structural tests. These analyses or tests determine that the design criteria of 5.3.3 have been met. (For wheeled vehicle testing, the article should be supported only by the structural members since it is not intended that tires withstand required test load) Adequacy of the designated structural safety design factor, (three times the static rated load, or two times the dynamic load, whichever

is larger in each axis, is recommended), should be demonstrated by one or more of the following ways

1 Performance of a detailed stress analysis This analysis may be supplemented by selective structural test

2. Nondestructive tests to conditions which approach the yield strength of the structure with suitable instrumentation at all critical stress points as determined by stress analysis These tests should not cause yielding of any component. (Yield has occurred when strain instrumentation reveals a permanent set, as defined by material properties) Results of these tests should be combined with an abbreviated stress analysis to determine whether the design meets the required design criteria The test design load must be determined by analysis, and must include the static design load or appropriate dynamic design load (whichever is greater in each axis) Mobility test results will be used to determine the total dynamic load These test loads must be applied simultaneously to the test vehicle along the appropriate axis.

3 Destructive test loads applied simultaneously to the test vehicle along the appropriate axis until the item fails The test loads at this point must be related to a load at the material yield point greater than the static design load or the dynamic design load

e Operational proof tests Tests should be performed on at least one fully configured article and other designated samples as necessary to determine that the item will withstand specified rated loads Example methods are

1 Testing the first fully configured article to 110 percent of rated load and all other articles to 100 percent of rated load

2 Testing the first fully configured article and selected samples to 110 percent of rated load

f Rated load and gross weight Rated load and gross weight must be clearly identified on all equipment

6 2 2 Forklifts and weapon loaders.

a First article and proof load test The tests recommended in 6.2.1 d. and 6.2.1.e. should performed.

b. Temperatures Lifting devices should be tested at test site ambient temperatures and then again at the extreme operating temperatures using rated load capacity.

c. Drift rate tests Drift rate tests should be conducted with the lifting device positioned at extreme and mid-heights Internal leakage in hydraulic components of lift systems must be limited so that the maximum drift rate is consistent with the precision required to prevent damage to a weapon

d. Parallel systems If more than one power actuating component in a mechanically parallel system is used in lifting the weapon, the component may be individually controlled to provide for weapon attitude adjustments and must be capable of synchronization for a uniformly controlled lifting attitude.

e Over-pressure Determine if hydraulic and pneumatic systems are designed to prevent over-pressure.

f. Attachments or lifting devices. Any attachment or lifting device fitted to a vehicle should be analyzed or tested to ensure compatibility in the worst case environment to which the vehicle will be subjected.

g Parking brakes Parking brakes should be tested to ensure that a fully loaded vehicle does not roll on slopes as specified in 5 3

6 2 3 Commercial vehicles Commercial vehicles should be evaluated for nuclear safety adequacy in accordance with appropriate standards, specifications, designated tests, etc. Equipment should meet the guidance contained in this document to the extent of its use with nuclear weapons The responsible evaluation agency must ensure that nuclear safety is not compromised for the intended use

6 2.4 Trailers, tow vehicles and self-propelled vehicles The service brakes of all vehicles, including tow vehicles and towed vehicle combination brake systems, should be tested as applicable

a Service brakes Test the service brakes of all vehicles by progressively increasing the speed from which stops are made, in increments of approximately 5 mph, up to the maximum rated speed of the vehicle, 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 (that is, "panic stop" conditions). Repeat the procedure on surfaces similar to those expected during the operational life of the vehicle. In each test, determine the maximum safe towing speed and record the following data on the brake performance as a minimum·

1. Tendency to yaw, sway or skid.

2. Tendency to tilt, turn over or jackknife

3 Damage or excessive wear

4. Stopping distances.

5 Towing speed

6 Contact of wheels with ground

b. Accidental trailer towbar disengagement Test the emergency braking system of trailers using towbars Accidental trailer towbar disengagement may be verified by full scale testing or by analysis and limited testing. Limited testing may be specified by the procurement/development agency and safety evaluation agency For full scale testing, the following will be accomplished. While towing the fully loaded trailer at maximum expected operating speeds over a straight, smoothly paved road, disengage the towbar from the tow vehicle, and watch the emergency braking action of the trailer The following items must be considered to determine whether the emergency brake system is adequate.

1 Distance from point of towbar disengagement to final stop.

2 Lateral distance of travel from point of towbar disengagement to final stop

3 Attitude of trailer at time of stop.

4 Damage incurred by trailer and/or load as a result of disengagement

c Parking brakes Test or analyze the parking brakes to ensure that the fully loaded vehicle does not roll when parked on an 11 5 degree slope. Conduct the test with both the forward and aft end of the trailer pointed up the slope The procurement/development agency and safety evaluation agency will specify if analysis is to be used in lieu of testing.

d Associated equipment Test all equipment used to load nuclear weapons on vehicle basic structure against the criteria of 6 2 1 d. and 6 2 1 e

e Mobility requirements The procurement/development agency and the nuclear safety evaluation agency will determine the applicability of mobility requirements of MIL-M-8090

f Ground transport tiedowns Ensure that nuclear weapon ground transportation equipment is compatible with tiedown techniques specified in 5 3.2 d.

6 2 5 Combat ships and shipboard transportation systems Shipboard equipment, devices, subsystems, systems, magazines, nuclear weapon support equipment, elevators, loading

devices, launchers, etc , will be evaluated to the extent of their intended use with respect to nuclear weapon and nuclear weapon systems safety

a Structural evaluation. Shipboard compartment and magazine structure, tiedown points, and other integrally constructed hardware should be evaluated by structural test, structural analysis, or a combination of both to demonstrate the adequacy to withstand the design loads required to achieve nuclear safety.

b Electrical and electronics hazards. Electrical and electronic computers and controls, circuits, circuit breakers, switches, transformers, etc , that are integral to the ship's equipment, should be evaluated for proper grounding, Electromagnetic Radiation (EMR) and Electromagnetic Interference (EMI) hazards, and other electrical or electronic hazards with respect to nuclear safety to the extent of their intended use.

c. Shipboard safety devices Shipboard sprinklers, fire and smoke detection devices and other shipboard fire fighting equipment, should be evaluated with respect to the guidance provided by this document in so far as nuclear safety is required

d. Safety interlocks test. The system must be evaluated to ensure proper functioning of safety interlocks intended to preclude weapon or platform damage while the weapon is being loaded, aimed, launched, or fired

e Underway replenishment Shipboard equipment that is utilized in the underway replenishment of nuclear weapons should be evaluated with respect to 5 3 12. Tackle, winches, booms, padeyes, etc , should be evaluated by use of structural analyses or properly designed proof testing. NWP-14 should be reviewed to ensure compatibility.

6 2.6 Cargo aircraft compatibility All equipment used for the transport of nuclear weapons in cargo aircraft must be evaluated with respect to nuclear safety.

a Tiedown strength Tiedowns must satisfy the restraint criteria contained in the NAVAIR nuclear cargo loading manuals for applicable aircraft specified in the STS, and should be consistent with the guidance in 5 3.2.

b. Tiedown configuration. Tiedown patterns should be structurally tested or verified by analysis according to the restraint criteria contained in the NAVAIR nuclear cargo loading manuals for applicable aircraft specified in the STS, and should be consistent with the guidance in 5.3.2 d Palletized loads, if tested, should be secured to a simulated aircraft section

c Tiedown test or analyses A tiedown pattern is considered acceptable if the rated strengths of the aircraft floor and pallet fittings are not exceeded, the rated strengths of the restraint devices are not exceeded, and the total load on any tiedown devices

attached to the test item does not exceed its rated strength. During the development of loading and tiedown procedures, a determination must be made on required use of additional aids (such as under the axle or under the frame shoring) for equipment with flexible suspension systems and pneumatic tires, or shoring to protect the aircraft deck from excessive floor loadings

6 2 7 Reusable containers. The acceptance criteria contained in MIL-STD-648 and MIL-STD-209 normally apply to reusable containers Tiedown points must be adequate to enable tieing down the container to meet ground, shipboard, and aircraft cargo restraint criteria.

6.2 8 Hoists, cranes and similar devices The procurement/development agency and the safety evaluation agency will normally evaluate such devices in accordance with the following·

a Determine if the design factors have been met.

b. Determine if additional tests are necessary

c All hoists should be tested to a minimum of 125 percent and a maximum of 150 percent with a 200 percent static test for 10 minutes at their rated capacity, depending on the design specifications

d Test results at rated load should be used to determine effectiveness of the fail-safe and synchronization features

e Electrical, hydraulic and pneumatic systems should be analyzed for safe operation at rated capacity.

f Safety devices (for example, braking devices, locking pawls, safety catches, rail stops, limit switches and valves) should be tested at rated load

g The procurement/development agency and safety evaluation agency will determine the required environmental tests, this is normally done based on the STS for the weapon system

6.3 Electrical and fiberoptical systems.

6 3.1 General evaluation of electromagnetic pulse and electromagnetic radiation requirements Evaluation of electromagnetic pulse (EMP) and electromagnetic radiation (EMR) effects is performed to ensure Electromagnetic Compatibility (EMC) of all military communications-electronics equipment, subsystems, and systems during conceptual, design, acquisition, and operational phases. In evaluating the system's vulnerability to credible EMR environments throughout the STS, consider these documents from the DOD EMC program: EMC Program Plan, EMC Control Plan, EMC and EMI Measurement Program Plan, and the EMC/EMI Measurement Test Report. Before the system is certified, the evaluation agency

must have the evaluation data that covers EMR hazards to electroexplosive devices, semi-conductors, fiberoptical, and other devices.

6 3.2 Isolation requirements Tests and analyses are conducted as necessary to make sure electrical (and optical, if appropriate) isolation requirements have been met in the system design.

6.3 3 Abnormal environments Positive measures provided to protect nuclear critical functions are tested and analyzed for proper performance in credible abnormal environments as well as in normal environments.

6 4 Arming and fuzing systems

6 4 1 General All Arming and Fuzing (A&F) systems are evaluated at the system and component levels (through analysis, tests, and demonstrations) to assure nuclear safety during those phases specified in the STS.

6.4.2 Specific data requirements. Specific data will normally include:

a. Critical components Identification of each critical component (and its failure modes) whose fault or failure could contribute to premature operation of the A&F system

b Failure mode information and information source Qualitative information on the likelihood of each identified failure mode and the source of such information

c Fault tree analysis A fault tree analysis of all critical component failure modes that could contribute to premature operation of the A&F system

d. Normal and abnormal environments. A nuclear safety analysis of the system in both normal and abnormal environments which, as a minimum, evaluates compliance with the requirements for precluding:

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

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

3. Premature nuclear detonation after the system is armed.

e. Thermal analyses. Thermal analyses with a graphic "temperature-time" presentation showing relative component temperature as a function of exposure time. These analyses should cover every component that can be thermally operated, every thermal-protective component and design feature, and all explosive components

f Response characteristics Graphic presentations of all operate and non-operate response characteristics for components in both normal and abnormal environments.

g Bent pin and connector misalignment analyses Bent pin and connector mismating and misalignment analyses for each connector to protect against premature operation of the A&F system

h. Cable routing analysis A cable routing analysis to ensure protection against cable damage throughout the STS which could contribute to premature operation of the A&F system

6.4 3 Other requirements. Design criteria in 5 5 that are not included in at least one of the above requirements, should be demonstrated or analyzed individually.

6.5 Nuclear weapon system data processing hardware and software.

6 5 1 General. Software Nuclear Safety Analysis (SNSA) should be performed on all nuclear weapon system software that is identified as having a direct or indirect effect on nuclear critical functions. The use of safety devices in the design of nuclear critical functions does not negate the need for SNSA The SNSA organization should be managerially, financially, and technically independent of the software development organization(s).

6 5 1 1 Software Software associated with nuclear critical functions should be designed to:

a Minimize reliance on administrative procedures.

b Minimize the number and complexity of nuclear critical interfaces.

c Employ sound human engineering principles to minimize the probability of human error.

d. Meet the trust requirements of the information security (INFOSEC) requirements of DOD Directives 5200 28, 5200 29 and 5200 40, per OPNAVINST 5239 1A and DOD 5200.28-STD

6 5.1.2. SNSA process SNSA is an interactive process which begins in the early stages of system definition and is carried on in parallel with system development SNSA augments traditional forms of software and safety analyses. It is not meant as a substitute for Independent Validation & Verification (IV&V) of software or other analyses directed by DOD Directive 3150.2 Any SNSA tools and facilities used to support these analyses and tests should themselves be qualified during the SNSA to verify their correctness. This qualification will ensure that results obtained from the application of these tools can be used to draw valid conclusions about nuclear safety.

6 5.1.3 SNSA objective The objective of SNSA is to demonstrate that software associated with nuclear critical functions is in compliance with the four DOD nuclear safety standards throughout the life cycle of the nuclear weapon system. The SNSA demonstrates compliance in the areas of general software design, resistance to inadvertent operation, resistance to deliberate unauthorized operation, program loading, targeting accuracy as well as controlling execution of critical factors and the implementation of detection, display, correction and abnormal processing.

6 5.2 Specific analysis guidelines

6.5.2 1 Memory characteristics Memory characteristics should be evaluated by demonstration or analyses to ensure that critical contents are not altered or degraded over time. Demonstrate (or show by analysis) that memory changes in a volatile memory, or a single hardware fault, will not result in a memory change that could initiate a critical function.

6 5 2.2 Memory stability. Evaluate the following features regarding memory loading and change·

a. Errors are detected and the operators notified.

b. Reset, halt, or synchronization functions are operable

c. Automatic operation is stopped until all valid and correct data have been loaded and verified.

d Unauthorized or incorrect loading, reloading or changing of memory involving critical functions is stopped unless the proper means for entry is used. Also, that improper load, reload, or change will be indicated and rejected

e. Each section of memory utilized is correctly filled by the block of proper program data or instructions to be transferred.

6 5 2.3 Processor deviations. Processor deviations must be properly evaluated. Evaluate the capability to detect manually started commands, message errors, and deviations causing an erroneous entry to a critical routine. Show that, upon detecting errors and/or deviations, the data processing equipment will stop transmitting critical commands and will either recycle, self-test, or perform automatic shutdown while providing an indication to the operator.

6.5.2.4 Hardware evaluation. The following hardware evaluation should be performed:

a. Self-check, confidence or test routines.

b. Evaluation of the hardware to make sure it meets current National Security Agency TEMPEST requirements (see MIL-STD-461) (This requirement does not apply to functional areas that do not process secure codes)

6 5.3 Critical function analysis. The SNSA organization should perform a criticality analysis to assess the nuclear safety impact of system functions allocated to software and determine the SNSA effort that should be applied to each software function. Each associated requirement should be assigned a criticality factor which will determine the methods and resources to be used for analysis. The critical function analysis will:

a. Establish a set of nuclear criticality classes meaningful to the system.

b. Assign a criticality class to each system requirement based on its nuclear safety impact.

c. Determine what analysis and test methods are to be used to evaluate the nuclear safety of each function

d. Estimate the resources required to perform SNSA on each software function.

6 5 4 Configuration management The SNSA organization must develop configuration control procedures for all project materials. These procedures shall ensure that analysts use current authorized materials and that reported results are accurate and up-to-date. The critical nature of SNSA requires that special safeguard procedures in addition to the standard DOD security measures be followed for SNSA material. These procedures must prevent any single individual from accessing formal SNSA materials (program documentation, source and object code, software tools used for formal SNSA test or demonstration, etc.). A configuration Management Plan (MP) should be developed that contains the following control procedures.

a. Security. To ensure the protection of materials used for SNSA, control procedures must include the facility personnel access requirements, methods of verifying the current version, and special handling requirements for critical software tools.

b. SNSA software tools. As SNSA software tools are developed, acquired, or modified, the tools should be baselined and placed under configuration control so that analysis and testing results are valid and repeatable. These control procedures should use methods for identification, documentation and change control and working copy distribution

c. Discrepancy reporting. Control procedures for Discrepancy Reports (DRs) should describe the identification and log scheme to track DRs from generation to resolution, the internal review cycle, and the status reporting scheme

d Documentation The originals of all documents received from external sources should be maintained under configuration control Procedures for document control should include the identification and log scheme, change page handling methods, document distribution, formal SNSA master handling methods, and working copy authorization plan.

e Code delivery Each code delivery and associated documentation should be placed under configuration control upon receipt. Control procedures should include the identification and log scheme, comparison techniques to identify changes from previous delivery, formal SNSA master handling methods, and working copy distribution

6.5.5 System design review (SDR) support The SNSA organization should provide·

a. A summary of the nuclear safety system requirements analysis at the SDR.

b. Technical support to the program manager.

6 5.6 Discrepancy reporting The SNSA organization should generate DRs for all identified discrepancies. The DRs should be prioritized as follows:

6.5 6.1 Discrepancy priorities.

PRIORITY #1: Critical Design, procedural or coding error(s) which could lead to a violation of one of the four DOD nuclear weapon system safety standards.

PRIORITY #2. Serious Design, procedural or coding error(s) which could lead to a violation of one of the four DOD nuclear weapon system safety standards with a small probability. Such errors may be controlled temporarily by an administrative work-around which must be incorporated prior to software certification. These errors must be corrected in the next release.

PRIORITY #3: Degraded Design, procedural or coding error(s) which could lead to a degradation of one or more nuclear critical functions without resulting in a priority 1 or 2 discrepancy.

PRIORITY #4· Noncritical. Design or error which a technical violation of one or more nuclear safety objective and has been determined by analysis and/or testing not to degrade a critical function nor lead to a violation of one of the four DOD nuclear weapon system safety standards.

PRIORITY #5: Minor. A documentation error which could become a nuclear safety problem if implemented in the code.

6 5.6 2 Resolution priorities.

Priority #1· All priority one discrepancies must be fixed prior to program certification

Priority #2. All priority two discrepancies must be resolved prior to program certification either by fixing the deficiency or by identifying a work-around which eliminates the effect of the deficiency and implemented prior to deployment All work-arounds are considered temporary and will be fixed at the next program revision.

Priority #3· Priority three discrepancies are strong candidates for resolution, however, they may be tolerated in the certified design Priority three discrepancies may be deferred but not ignored and are to be considered for correction in the next program revision All targeting discrepancies will be classified as priority three discrepancies

Priority #4 Priority four discrepancies are recommended for correction but may be deferred

Priority #5· Priority five discrepancies are recommended for correction but may be deferred

6.5.7 Software nuclear safety analysis requirements Software nuclear safety analysis (SNSA) should be conducted in accordance with the following requirements

6 5 7.1 Baseline configuration The documentation, equipment, and software to be analyzed should reflect the approved configuration and be identical to the engineering master The hardware configuration in which software is tested or analyzed in conjunction with SNSA should be the baseline configuration corresponding to the software baselines Proposed changes to baseline documentation, equipment, and software should be examined to determine their impact on completed, in process, and planned tests and analyses New or repeated testing or analyses is then be performed as required to ensure that SNSA requirements are satisfied for the final as-built software.

6 5 7.2 Critical factors, automata, and software examination. Examination of the system performance requirements, specifications, design specifications, interface control documents, and engineering drawings are conducted to identify those general critical factors which apply to the system under analysis. The factors that apply are those affecting the hardware and software which receive, store, process, or transmit data to select, load, prearm, arm, enable, unlock, or launch a nuclear weapon Those hardware and software which control critical functions, circuitry, activities, sequences, signals, hardware components, and software, will be identified and categorized by the degree of involvement in critical functions Finally, positive measures are examined to determine their sufficiency and adequacy to protect the specific critical functions identified. The results of these analyses are forwarded to the responsible design agent for appropriate action

6.5 7.3 Document verification This is done to verify that the documentation for nuclear safety critical hardware and software complies with the nuclear safety design requirements contained in Section 5.6.4 Documentation deficiencies are identified per the following requirements.

a System documentation (both hardware and software) are analyzed to ensure that the general software design requirements of Section 5.6.4 are satisfied.

b. For each instance in which the design does not comply with the requirements in Section 5.6.4, an assessment is made to determine the impact, if any, to weapon system nuclear safety with respect to weapon system design. Where critical or serious deficiencies are identified that impact nuclear safety, these deficiencies are identified for correction The software will not be recommended for certification until corrective action is taken Critical deficiencies are errors which could lead to violation of one of the four DOD nuclear weapon system safety standards

6.5.7.4 Design integrity. The procedures in this subparagraph can be used to verify the design integrity of nuclear safety critical software by ensuring that the software code complies with the software documentation. These procedures are designed to ensure that nuclear safety requirements flow down through documentation to the code This approach takes the form of an audit which, at a minimum, includes line-by-line code inspection. While this inspection may not require a re-derivation of equations or line-by-line verification, any software component that violates or has a potential of violating software documentation should undergo additional analysis This may include re-derivation of equations, algorithm test case validation, or line-by-line verification to ensure proper function. This verification is described below:

a Verify that the functional specification contained in the program performance specification or its equivalent is directly traceable to the lowest level applicable system specification and the top-level requirements document.

b. Verify that the detailed design specification contained in the program design specification or its equivalent is directly traceable to the functional specifications. During this analysis, it should be verified that only those functions necessary to meet the functional specification are included in the design. The data base design contained in the data base definition document or equivalent will be verified. All control data items are verified to ensure that they exercise an active designed control throughout the design, i.e., only required decision paths are present. Examinations, analyses, tests, and audits are applied to all nuclear safety critical software.

c. Verify that the code is directly traceable to the control structure and logic defined in the performance design specification or its equivalent All coded modules are examined to ensure that they execute the function defined in the performance design specification and only that function The software should not include any code

which cannot be traced directly to the performance design specification. Patches which create unused or nonfunctional code are examined to determine any potential impact of this "dead code" on nuclear safety. As a general guideline, dead code should be removed The following code areas, as a minimum, should be examined:

1. Analyze data bases to ensure that they are consistent with the data base design document or its equivalent This analysis includes an inspection of the data base to ensure that no executable sequence or code is present that can cause inadvertent execution of a critical function

2. Analyze data structures for each software module to ensure consistency from module to module, e g., common data storage areas and subroutine argument lists.

3 Analyze argument lists to verify that only those data items required by a software module are passed to that module.

4. Analyze conditional statements to verify that controlling parameters can allow all possible design conditions, and no others, to execute

5 Verify that the bounds on the data structures and control parameters are not exceeded, e g., array limits or undefined mathematical operations.

6 Analyze design interfaces to verify the proper design for each software component's interface with other software components and external hardware and software

d. Noncompliance. When requirements are not met, an assessment is made to determine the effect on nuclear safety Where deficiencies are identified which affect nuclear safety, these deficiencies are identified for correction to ensure compliance with safety standards prior to issuance of software for operational use.

6.5 7.5 Criticality analysis. The criticality analysis categorizes the components of nuclear safety critical software by the degree of involvement in critical function performance. This analysis is based on the System Functional Flow Diagram (SFFD) and the defined critical functions, and produces functional flow diagrams which are used to categorize the system software. Functional flow diagrams which clearly identify all hardware and software components (down to at least the module level) should be prepared for each critical function in the nuclear weapon system for each possible weapon load, including one or more nuclear weapons or nuclear system program loads, and for all normal and casualty operational modes of the system. The functional flow diagrams are analyzed to determine possible nuclear safety hazard paths and associated potential nuclear safety impacts

6.5.8 Testing.

6.5.8.1 SNSA test requirements. Testing is used to validate the results of analyses and provide additional data on the performance of the software which cannot be obtained through analyses Test used includes the following.

a For Category I software, tests should be performed to provide data for analysis of hazard paths. In addition to nominal testing using nominal conditions and parameters, performance spectrum testing (testing across the specified range of inputs) and stress testing (testing using erroneous signal inputs outside of specified ranges, timing, sequence, faults, etc) is conducted to uncover potential hazard paths and to more fully evaluate performance. The results of this testing are examined to ensure that the software performance meets the nuclear automata and software safety requirements Adequate replication with varying system loads and operator actions is included to ensure confidence in results of the analytic examination. Hazard situations identified in testing are analyzed to determine possible nuclear safety effects

b For Category I and II A software, load testing should be performed to ensure that any resultant performance degradation does not degrade nuclear safety, e.g., maximum central processor unit load, maximum memory utilization, maximum input/output load.

c. For all categories of software:

1 Where nuclear safety critical software interfaces with noncritical software, performance tests and those which include injecting erroneous signals (inputs outside specified ranges, timing, sequence, etc.) are utilized to assess the possible nuclear safety effects of interfaces with noncritical software. Critical software is responsible for the safety associated with its interactions with noncritical software.

2. All nuclear hardware and software safety requirements related to notifying an operator that a failure has occurred is thoroughly tested, and test results analyzed for proper performance.

3. System level testing, including hardware or software operation outside specified performance ranges, is performed to ensure that software responses do not degrade nuclear safety. The purpose of this requirements is to ensure that the nuclear hardware and software safety requirements are satisfied through DOD-STD-2167A

4. System level testing including hardware, software and operator action is performed for all normal and casualty operational modes of the system.

6 5 8 2 Integration and test The SNSA organization should conduct test and analysis on the executable code as specified in the approved test procedures. Activities performed are as follows.

a. Verify that the software used in testing corresponds to the program listing.

b. Conduct a Test Readiness Review.

c. Establish and maintain a hardware configuration baseline throughout each test session.

d. Conduct testing to demonstrate that the system, when operated beyond the extremes of the envelope, responds in a predictable safe manner

e. Conduct testing to demonstrate the system response in the normal operating environments to the extremes of the envelope

f Conduct stress and overload testing to demonstrate the system's capability to respond in a predictable safe manner

g. Perform regression tests to account for all code changes

h Correlate all tests to the System Requirements Specification (SRS)

i Verify that object code contains no extraneous code or patches.

j. Generate DRs for all identified discrepancies

6 5 9 Operational test and evaluation The Software Nuclear Safety Analysis (SNSA) organization should support Operational Test and Evaluation by performing the following activities

6 5.9.1 Control of master end item software. The SNSA organization must protect the masters of the software end items and documentation that was subjected to SNSA from single individual access After the successful completion of the certification demonstration, the program manager or his representative should maintain the certified masters of the software end items and documentation in accordance with operational security requirements.

6.5 9.2 Certification demonstration The SNSA organization should conduct a certification demonstration of the Verification Design Document (VDD) and Software Design Organization (SDO) DD250 version of the operational program code The demonstration should.

a Verify that the SDO product delivered to the Government is identical to the product subjected to the SNSA.

b. Be conducted in a controlled environment

c Be conducted using the operational medium unless otherwise directed by the program manager.

d. Be witnessed by representatives of the program manager.

Following the successful completion of the certification demonstration and proper resolution of all discrepancies, the SNSA organization should determine whether to recommend certification of the product(s) for operational use.

6.6 Test and training equipment.

The criteria in this section apply to nuclear weapon system built-in test equipment, launch or fire control test equipment, nuclear weapon or warhead testers, component testers and general test equipment. The Navy development agency will establish specific criteria for tests, analyses, and demonstrations in the following areas.

6 6.1 Environmental tests Conduct environmental tests according to 4 4.7

6.6 2 Analyses

a. Circuit analyses. Circuit analyses of test equipment operating with the circuits of the equipment to be tested.

b Failure modes and effects analysis. Failure modes and effects analysis of test devices to ensure that faults within the devices will not degrade the nuclear safety of the equipment to be tested

c. Tester interface analysis Analysis of the tester interface with the weapon system to verify the test concept.

d. Analysis of maintenance procedures. Provide analysis of procedures for the maintenance and inspection of testers to make sure the integrity of the testers can be verified before they are used

6.6.3 Demonstrations

a. Fit and function demonstration. Perform a fit and function demonstration to make sure both the mechanical and electrical designs are compatible with the weapon system to be tested.

b Demonstration of procedures Demonstrate operations and procedures. Verify each application section of each procedural document.

THIS PAGE INTENTIONALLY LEFT BLANK

7 NOTES

7.1 Intended use. Documents used within the scope of this handbook are intended to be used to obtain safe and secure nuclear weapons, components, equipments, subsystems, and systems This handbook is for information and guidance for acquisition engineers, contractors, program managers, and others responsible for nuclear safety and security as related to the DoD. This handbook is intended to provide the guidance needed to ensure that the nuclear weapons systems meet the DoD safety standards

7 2 Subject term (key word) listing

Analysis
Automata
Component, critical
Critical
Electromagnetic compatibility
Electromagnetic interference
EMR
ENDS
Equipment, certified
Fiberoptic
Guidance, new personnel
Ordnance, naval
Responsibilities
Safety
Security, information
Susceptibility, yield generation
Tests, operational proof
Vehicles

7 3 Changes from previous issue Marginal notations are not used in this revision to identify changes with respect to the previous issue due to the extensiveness of the changes.

APPENDIX A

SAFETY CRITERIA CHECKLIST

10 PURPOSE AND SCOPE

10.1 Purpose. The following checklist is a general guide for nuclear weapons and nuclear weapon systems safety design and may not be all encompassing. The designer is responsible for ensuring that all criteria are adequately and properly applied.

10.2 Scope. This checklist summarizes the safety criteria to be considered by contractors, program managers and others involved in the design, construction, manufacture and operation of nuclear weapons systems. In all areas, the safety considerations are based on the following four safety standards set by the DOD as minimum requirements:

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

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

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

d. There shall be positive measures to ensure adequate security of nuclear weapons, pursuant to DOD Directive 5210.41.

These four criteria should represent the essence of all safety considerations when involved with any aspect of the nuclear weapon.

20 WEAPON SYSTEM

20.1 Type. The type of weapon system being analyzed, (missile, gun fired, torpedo, etc.).

20.2 Areas. Areas of the weapon system being reviewed for safety:

a. Warhead
b. Launcher
c. Handling and transportation
d. Administrative procedures
e Magazines

k. Are the switches, controls, etc , that control the critical functions of the nuclear weapon, distinct in both shape and mode of operation from any conventional weapon switches, controls, etc , located in the proximity?

l. Is there any switch, device, etc , in the weapon system that is common to both nuclear weapons and conventional weapons? If so, can any nuclear weapon critical function be activated accidentally or in an unauthorized manner through such a common element?

m Can the operation or activation of any element in a conventional weapon system control, switch, device, etc , cause the activation of any nuclear critical function?

n Are the switches, controls, or devices used to control a nuclear weapon propulsion system distinct and separate from those switches, controls, or devices used to control nuclear weapon warhead critical functions?

50. POWER FAILURE

a. Will a power failure result in a nuclear weapon response of the following type.

1 Selection
2. Prearming
3. Arming
4 Launching, firing or jettison
5. Detonation
6 Command disable

b If a nuclear weapon has been selected, prearmed, or armed, and a power failure occurs, does the weapon and weapon status revert to a "deselected" condition?

c Upon restoration of power, for any reason, will a previously selected, prearmed, or armed event become automatically reestablished?

d. Upon bringing power up, without any previous power outage, can a nuclear weapon control result in.

1 Selection
2. Prearming
3 Arming
4 Launching, firing or jettison
5 Detonation
6 Command disable

e In the event of a power failure to the nuclear weapon system command and control apparatus, does a prearmed nuclear weapon or nuclear weapon propulsion system return to the safe condition?

f Will a power failure to the launcher or launching device cause the Safe/Arm device on the propulsion unit to return to SAFE?

g With the restoration of power, does the Safe/Arm device ARM?

h Are the performance characteristics of volatile memory elements such that power fluctuations, surges, or outages will cause erroneous or unexpected data or information to be generated? Can these variations from expected data or information cause an undesired nuclear critical function to result?

i Upon restoration of power, does the weapon or weapon system automatically return to the previously selected critical function position (i.e , does a previously prearmed weapon return automatically to the prearmed condition)?

j. Is the power level used in the administrative device significantly less than that required for critical functions?

k. Can the firing system in a propulsion unit respond to a fire command without a previous arm command?

60 LAUNCHER

a. Can the failure of any single component in a howitzer, gun, cannon or launcher cause a nuclear critical function to occur?

b. For a weapon on a launcher or in a tactical launching container, can any function such as select, prearm, arm, launch or fire occur out of sequence? (e.g., can a weapon be prearmed prior to selection command?)

c. Will a failure of any device in the launcher cause any nuclear weapon function to result in:

1. Selection
2. Prearm
3. Arm
4. Launch, fire or jettison
5. Detonation
6. Command disable

d. Can the motion of the launcher, in its most critical mode, transmit forces, accelerations or velocities, to a nuclear weapon or nuclear weapon component in excess of the weapon or component design limits?

e Can the motion induced into a nuclear weapon or propulsion system by a launcher cause

1 Selection
2. Prearming
3. Arming
4. Launching, firing or jettison
5. Detonation
6 Command disable

f. Does the weapon, when in its most critical position on the launcher, interfere with any adjacent structure?

g On the launcher, what is the clo..st point of approach of any part of the weapon (nose, control surfaces, etc ,) to any of the adjacent structures?

h. Upon launch, what is the closest point of approach of any part of the weapon to any of the adjacent or movable structures?

70. MASKED WEAPON CONDITION

a Under "masked weapon" conditions, are interlocks activated that would prevent launching or firing of a "masked weapon"?

b. Is there a "masked weapon" indicator?

80. MAGAZINES

a. Are assembly areas and magazines for nuclear weapons free of harmful electromagnetic radiation generated by equipment and machinery in close proximity?

b. Are assembly areas, magazines and stowage areas of sufficient size and shape to allow at least two men to be present within the area at the same time? Is the layout, arrangement and physical characteristics of the space such that each person has an unobstructed view of the other?

c Are the various locations, racks, containers, canisters or stations marked to assist in strikedown, inventory, selection or performing any individual missile operations?

d. Is the spray pattern of the fire protection sprinkler system within the assembly area, magazines and stowage areas arranged to preclude an umbrella effect?

e. What are the rapid evacuation characteristics of assembly areas and magazines?

90. SUPPORT EQUIPMENT, TRANSPORTATION AND TIEDOWN

a Are the various components of support equipment, stowage racks, etc., designed to discriminate between conventional weapons and nuclear weapons?

b Can support or ancillary equipment that is an integral part of a launcher, cannon or other type of delivery system induce velocities, accelerations or forces into a nuclear warhead or propulsion unit that would result in·

1. Degradation?
2. Activation of a critical warhead function?
3. Activation of a critical propulsion function?

c. With respect to nuclear demolition munitions, can the motion and forces imposed upon the munition by various non-target environments such as handling, transportation, parachuting, ground impact, hydrostatic and barometric pressure variations, etc , cause any nuclear critical function to activate?

d Based upon the stockpile-to-target sequence for the nuclear weapon under review, list the various modes of transportation specified.

e Except for special warfare applications, for each mode of transportation noted, is the nuclear weapon or nuclear critical component supported by the basic frame of the transportation device as opposed to being suspended or supported by slings, straps, lift arms or hydraulics?

f. Is the nuclear weapon or nuclear weapon component under positive restraints during transportation?

g. If required by the system, is there a means to provide adequate protection from static electricity throughout the transportation evolution?

h What is the degree of protection from fire that is provided to the nuclear weapon during transportation? Is this in keeping with the various criteria for the weapon in question?

i Does the magnitude and duration of shock imposed by the transportation onto the nuclear component exceed the allowable levels as defined for these critical components?

j. Are there sufficient tiedown points of adequate strength provided in each element of the transportation scheme? Are the tiedown straps or chains of adequate strength?

k Are worst case transportation mode/environments used in the transportation analysis?

l For a particular transportation element which was procured under military specification where there are areas of non-compliance, are these areas of non-compliance detrimental to nuclear safety? (e g , braking, structural strength, trailer dynamics, etc.)

m For other transportation elements which were procured under military specifications, are these transportation elements compatible with nuclear safety?

n. In the event that a particular support equipment element experiences a failure, (such as electrical, hydraulic or pneumatic), does the device maintain control of the load (up to a rated load)?

o For support equipment with hydraulic systems, are provisions made for preventing over-pressure?

p Is the drift rate for hydraulic systems within the specified limits?

q Are the following characteristics of support equipment within the acceptable range insofar as nuclear safety is concerned?

1 Parallel lifting systems
2 Self-centering controls
3. Positive controls
4. Motion limiting devices
5 Parking brakes
6 Tines and adapters
7. Creep motion
8 Fail-safe stops
9 Synchronized operations
10. Automatic stops
11 Load and rate limits
12 Maximum allowable safety factor
13. Power up and down control
14 Hooks

r. Does the operational concept or STS document identify or suggest any commercial vehicles to be used? Are these commercial vehicles suitable from a safety standpoint and compatible with the various principles of nuclear safety?

s Are the various containers used for storage and transportation in compliance with MIL-STD-209 and MIL-STD-648?

t. For shipboard transportation of nuclear weapons and nuclear weapon components, are the assigned stowage compartments and magazines equipped with adequate fire protection

equipment? Are sprinkler heads located such that all areas of the compartment/magazine are covered?

u. Are all tiedown points designed to the proper load levels?

v. Are there a sufficient number of tiedown points to accommodate the design capacity of the space?

w. Are hatches, elevators and doorways of sufficient size to allow safe and unhindered passage of nuclear weapons, containers, pallets and other portable support equipment?

x Are hoists, booms, cranes, etc , of sufficient strength to safely lift the nuclear weapons?

y. Do these hoists, booms and cranes have the proper safety devices installed?

z. Is the underway replenishment floatation gear for nuclear weapons of sufficient capacity to provide floatation for the nuclear weapons and support equipment, tackle, etc., that could be lost overboard with the nuclear weapon in the event of an underway replenishment accident?

aa Do the pallets or other gear that may be used in underway replenishment have sufficient shock absorbing capacity to prevent shock transmission to a nuclear weapon that would exceed the weapon design values?

bb. Do air transport delivery vehicles meet the specific nuclear safety requirements with regard to:

1. Tiedown characteristics?
2. Magnitude of forces on tiedown rings?
3. Number and location of tiedown points?
4. Symmetry of tiedown pattern?

cc. Are all structural devices essential to air transportation and nuclear safety properly designed to the required acceleration levels and directions? Is there sufficient capacity to adequately withstand these accelerations and forces?

dd. Is the character of the environment transmitted into the nuclear weapons (vibration, shock, temperature, etc.) such that degradation of the nuclear weapon is caused?

ee. Do the forces and motion induced into a nuclear projectile by the various components of the cannon or loading equipment exceed the allowable design levels of the projectile?

ff Are there adequate means to safely and positively extract a nuclear projectile from the breach end of a cannon?

100 ADMINISTRATIVE DEVICES

a. Are there administrative devices internal to the weapon structure or to the tactical container?

b. Are these devices of such a nature that data (serial number, etc.) can be determined by applying or connecting an electronic or fiberoptic interrogation device to the weapon or tactical container?

c. Does this administrative device introduce any electrical, mechanical or light energy into the weapon such that any critical function could be actuated?

d What nuclear safety criteria are being satisfied through the use of administrative procedures?

110. OPTICS

a. For those components that are sensitive to visible light, has the design been arranged so as to preclude the entry of stray unwanted light?

b. Can stray or undesirable light enter optic fiber links or circuits and produce a nuclear hazard, such as activation of a nuclear critical function?

120. ELECTRICAL CIRCUITS

a. Are the following components designed to minimize the influence of electromagnetic interference?

1. Wires and wiring
2. Switches
3. Cables and connectors
4 Junction points
5 Nuclear weapon monitor circuits
6 Nuclear weapon control circuits
7 Nuclear weapon release circuits

8 Nuclear weapon firing circuits

b. Are optical and electrical circuits properly isolated to prevent activation of a critical event due to short, improper interference, stray or residual signals?

c. Are wire shields used to carry current?

d Is the structure used as a ground plane?

e. Have the criteria of MIL-STD-1512 been applied to all electroexplosive circuits?

f. Are nuclear consent function circuits physically and electrically isolated from all other circuits?

g Are prearming control circuits and safing circuits electrically isolated from other circuits?

h Are prearming power circuits physically and electrically isolated from other circuits?

i. Are monitor circuits so constructed and isolated that monitoring functions are independent of weapon control functions?

j. Are logic circuits suitably isolated and routed to prevent short circuits?

k Are critical circuits isolated from potential sources of stray electrical power?

l. Has any switching been placed in the ground side of power circuits?

m Has the following criteria been followed in the design of wiring and cables to the maximum extent possible?

1. Minimizing coupling
2. Optimizing separation
3. Wiring secured to prevent vibration and chafing
4 Proper power wiring terminals
5 Wiring for critical circuits mechanically supported

n. Are the electrical connectors, pin details, connector supports, etc., designed in accordance with the rules of good design practice?

o Are spare pins used for mechanical support of in-line components?

p Can a short circuit due to a bent pin deliver more than 100 milliamperes current to the nuclear weapon or to critical function circuits?

q. Are the current levels used in monitoring and testing applications limited to a functional value below the level required to actuate the most sensitive component in the nuclear weapons system?

r. Are nuclear weapon/warhead electrical monitoring signals current limited to required levels? For continuity, are electroexplosive devices and pressure testing circuits also designed to this limitation?

s. Are the criteria and constraints of panel construction and packaging followed in the design?

t. Have the effects of electromagnetic radiation on electroexplosive devices been properly taken into account?

u List the design features within the arming and fuzing systems and associated control and monitor circuits that preclude deliberate unauthorized or accidental activation of nuclear critical functions

130 ABNORMAL ENVIRONMENT

a Evaluate the effectiveness of the weapon system's safety design features in various abnormal environments.

b. In the exposure of a nuclear weapon to a specific abnormal environment, to what extent will the various safety features survive beyond the survivability of the critical arming devices or of the nuclear device?

140 ADDITIONAL SAFETY CHECKLIST ITEMS

a Describe the dual signal system used in arming the warhead and how these signals are independent of each other.

b. Have the design criteria for the arming and fuzing device been met? Are there any deviations from the required criteria? Do these deviations diminish the overall nuclear safety?

c Does the automatic data processing equipment design have the necessary protective elements that will prevent automatic control until all valid and correct program data have been loaded and verified?

d. In the event a program error has been generated due to incorrect loading, does the system have the capability to prevent the use of the data?

e. Is the program and system hardware designed to comply with the constraints on unauthorized changes due to hardware faults or attempts to change without proper entry procedures?

f. Can programs transmitted from remote sites to the weapon control sites be verified as correct prior to utilization of the transmitted data?

g. In the event that automata control procedures deviate from expected or proper sequencing, will the system automatically shut down?

h. Denote the program or software elements of the automata system that have a first level interface with nuclear weapons and those that have a second level interface

i. Can diagnostic software or residual elements of such material remain in memory after completion of maintenance or diagnostic testing?

j. Has the software nuclear safety analysis determined any discrepancies in the controlling software? What are the discrepancies and how do they effect nuclear safety?

k What tests and training devices or elements are there for the nuclear weapon system in question?

l Does any of this test and training equipment deviate from the required design criteria? Do any such deviations degrade nuclear safety?

m. Can any training device in this nuclear weapon system be used on a nuclear weapon?

n Based upon the application of accepted human engineering concepts to the various elements of the nuclear weapon system, what are the hazardous human error features?

o. Can any single human error result in the activation of a nuclear critical function? Can two independent human errors result in the activation of a nuclear critical function?

p. Describe how the guidance signal, for guided nuclear weapons, interacts with the final arming sequence. Once the weapon is armed, will the removal of a valid guidance signal, indicating improper impact with respect to target boundaries, cause the weapon to disarm?

q. Are there access means in the nuclear weapon that allow for emergency render safe procedures?

APPENDIX A

r. Are there any criteria specified within this document or any referenced document that result in the degradation of nuclear safety? What particular requirements have a degradation effect and what element or to what degree is nuclear safety compromised?

s Identify any advanced technology concepts used in the weapon system that are not provided for in these criteria What elements of this new technology are there that can lead to nuclear safety degradation and to the violation of the four basic nuclear safety standards.

APPENDIX B

ABBREVIATIONS AND ACRONYMS

10. SCOPE

10.1 Abbreviations and acronyms. The abbreviations and acronyms used in this handbook are defined as follows

A/D	-	Arm/Disarm
A&F	-	Arming and Fuzing
ADM	-	Atomic Demolition Munition
AFAP	-	Artillery Fired Atomic Projectile
AFSC	-	Air Force Systems Command
AS	-	Air System
ASTM	-	American Society for Testing and Materials
BITE	-	Built In Test Equipment
CAL	-	Completely Assembled for Launch
CD	-	Command Disable
COD	-	Carrier Onboard Delivery
CONREP	-	Connected Replenishment
DOD	-	Department of Defense
DOE	-	Department of Energy
DR	-	Discrepancy Reports
ED	-	Emergency Destruct
EED	-	Electroexplosive Device
EMC	-	Electromagnetic Compatibility

APPENDIX B

EMI	-	Electromagnetic Interference
EMP	-	Electromagnetic Pulse
EMR	-	Electromagnetic Radiation
ENDS	-	Enhanced (Electrical) Nuclear Detonation Safety
EOD	-	Explosive Ordnance Disposal
E/TSD	-	Environment or Trajectory Sensing Device
FED STD	-	Federal Standard
G	-	Acceleration due to gravity
GVW	-	Gross Vehicle Weight
HE	-	High Explosive
HERO	-	Hazards of Electromagnetic Radiation to Ordnance
ILA	-	Inadvertent Launch Analysis
ILSP	-	Integrated Logistics Support Plan
IOC	-	Initial Operational Capability
JMSNS	-	Justification for Major System New Starts
LLC	-	Limited Life Component
MCs	-	Military Characteristics
MIL HDBK	-	Military Handbook
MIL SPEC	-	Military Specification
MIL STD	-	Military Standard
NAVSEA	-	Naval Sea Systems Command

APPENDIX B

NBC	-	Nuclear, Biological, and Chemical
NSA	-	National Security Agency
NSAP	-	National Security Agency Publication
NWEF	-	Naval Weapons Evaluation Facility
NWP	-	Nuclear Weapon Publication
NWSSG	-	Nuclear Weapon System Safety Group
OIE	-	Optical Interference Energy
OP	-	Ordnance Publications
OPDD	-	Operational Plan Data Document
OPNAV	-	Office of the Chief of Naval Operations
OS	-	Ordnance System
PAL	-	Permissive Action Link
PEO	-	Program Executive Officer
PM	-	Project Manager
PMD	-	Program Management Directive
RF	-	Radio Frequency
RMS	-	Root Mean Square
ROM	-	Read Only Memory
S/A	-	Safe/Arm
SAE	-	Society of Automotive Engineers
SDO	-	Software Design Organization

APPENDIX B

SDR	-	System Design Review
SNSA	-	Software Nuclear Safety Analysis
SRS	-	System Requirements Specification
STS	-	Stockpile-to-Target Sequence
SWOP	-	Special Weapons Ordnance Publication
TNT	-	Trinitrotoluene
ULA	-	Unauthorized Launch Analysis
UNREP	-	Underway Replenishment
UPS	-	Unique Prearming Signal
USS	-	Unique Signal Switch
WR	-	War Reserve
WSESRB	-	Weapon System Explosive Safety Review Board

APPENDIX C

DOCUMENTS FOR USE IN DESIGN AND PROCUREMENT

10. SCOPE

10 1 Scope of appendix The scope of this appendix is to identify documents known to be useful for information and guidance on nuclear safety design and evaluation criteria pertaining to the design, test, and procurement of nuclear weapons components, equipments, subsystems, and systems for NAVSEASYSCOM.

20. ASSOCIATED DOCUMENTS

20.1 Use of documents. The following documents shall be used to incorporate requirements for nuclear weapons, components, equipments, systems and associated systems as appropriate

20 2 Movement equipment

a Cranes:

MIL-C-28546	Cranes, Overhead Traveling, Underhung, Electric Powered

b Hoists·

MIL-H-904	Hoists, Chain, Hand Operated, Hook and Trolley Suspension
MIL-H-19925	Hoists, Wire Rope, Electric Power

c. Fork lifts:

MIL-T-21868 (series)	Trucks, Lift, Fork, Diesel; Shipboard, General Specifications for
MIL-T-21869 (series)	Trucks, Lift, Fork, Electric, Sit-Down, Front Wheel Drive, Rear Steering; General Specifications for
MIL-T-52932 (series)	Trucks, Lift, Fork, Internal Combustion Engine 4,000 - 6,000 Pound Capacity, General Specification for

20.3 Commercial transportation

a. Trucks and truck tractors:

KKK-T-2107	Trucks and Truck Tractors· Commercial, Diesel or Gasoline Engine Driven, 14,000 to 21,000 Pounds GVW, 4 X 2
KKK-T-2108	Trucks and Truck Tractors. Commercial, Diesel or Gasoline Engine Driven, 24,000 to 32,000 Pounds GVW, 4 X 2
KKK-T-2109	Trucks and Truck Tractors: Commercial, Diesel Engine Driven, 34,500 to 66,000 Pounds GVW, 6 X 4
KKK-T-2110	Trucks and Truck Tractors Commercial, Diesel or Gasoline Engine Driven, 24,000 to 35,000 Pounds GVW, 4 X 4
MIL-T-62318	Truck, Multistop Delivery Forward Control and Chassis, Truck Forward Control, Diesel and Gasoline Engine Driven, 13,000 to 21,000 Pounds GVW, 4 X 2, Commercial
MIL-T-62319	Trucks, Cargo Diesel or Gasoline Engine Driven, 9,000 to 24,000 Pounds GVW, 4 X 2 and 4 X 4, Commercial
FED-STD-292	Trucks, Light Commercial, Gasoline/Diesel Fueled, Four Wheel Driven (4 x 4, 3,000 to 11,000 Pounds GVW)
FED-STD-307	Trucks, Light Commercial, Gasoline/Diesel Fueled, Two Wheel Driven (4 x 2, 3,000 to 14,500 Pounds GVW)

b Trailers and semitrailers

MIL-S-45152	Semitrailer, Lowbed, Commercial
MIL-T-45333	Trailer, Flatbed 10 Ton, 4 Wheel M345

20 4 Security systems.

a Program management·

MIL-STD-1785	System Security Engineering Program Management Requirements

b. Certified equipment·

SWOP 20-25	Master List of Nuclear Weapons Certified Equipment

c. Computer system evaluation:

NSCS-TG-005	Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria
NSCS-TG-009	Computer Security Interpretation of the Trusted Computer System Evaluation Criteria

d. Computer resource management·

DODDIR 5000.29	Management of Computer Resources in Major Defense Programs

e DOD operations:

DODDIR 5205.2	DOD Operations Security Program

f Information system (products and services)

Catalog	Information System Security Products and Services

20.5 Reliability and maintainability.

DODDIR 5000 40	Reliability and Maintainability

20 6 Weapons movement.

a Instructions·

SWOP 45-51 (series)	Instructions for Logistic Movement of Nuclear Weapons
SWOP 45-56 (series)	Instructions for Navy Movement of Nuclear Weapons

b. Preparation and use procedures.

SWOP 50-20	Procedures for Preparation and Use of Military Characteristics (MC's) and Stockpile-to-Target Sequences (STS) for Nuclear Weapons

20 7 Ammunition and explosives

OP 5	Ammunition and Explosives Ashore
OP 4098	Handling Ammunition and Hazardous Materials with Industrial Trucks
MIL-I-23659	Initiators, Electric, General Design Specification for

20.8 Safety.

a. Nuclear:

SWOP 20-7	Nuclear Safety

b General fire fighting·

SWOP 20-11	General Firefighting Guidance

20 9 Aerospace vehicle structures

MIL-HDBK-5 (vol 1 and 2)	Metallic Materials and Elements for Aerospace Vehicle Structures

30 Document sources Copies of documents listed in this appendix can be obtained from sources as follows·

a. SWOPs

Officer in Charge
Naval Surface Warfare Center
Indian Head Division McAlester
Army Ammunition Plant
McAlester, OK 74501-5190

b. NSCS-TGs

Director
National Security Agency
Attention: Infosec Awareness Operations Center (IAOC)
Fort George G Meade, MD 20755-6000

c Catalogs

Superintendent of Documents
U.S. Government Printing Office
Washington, DC 20402-0001

d. Specifications, standards, handbooks, DODDIRs

Standardization Documents Order Desk
Building 4D, 700 Robbins Avenue
Philadelphia, PA 19111-5094

CONCLUDING MATERIAL

Custodian:
Navy - OS
Review Activity:
Navy - SH

Preparing Activity:
Navy - OS
Project NUOR-NOO1

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, nor 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 contractual requirements

I RECOMMEND A CHANGE:	1 DOCUMENT NUMBER	2 DOCUMENT DATE (YYMMDD)
	MIL-HDBK-272A(OS)	920402

3 DOCUMENT TITLE

"NUCLEAR WEAPONS SYSTEMS SAFETY DESIGN AND EVALUATION CRITERIA FOR

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	b TELEPHONE (Include Area Code)	
Commander, Indian Head Division Naval Surface Warfare Center	(1) Commercial (301) 743-4358/4510	(2) AUTOVON 354-4358/4510
c ADDRESS (Include Zip Code) (Code 8420) 101 Strauss Avenue Indian Head, MD 20640-5035	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	