BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 91-103

26 JUNE 2001

Safety

AIR FORCE NUCLEAR SAFETY CERTIFICATION PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ AFSC/SEWE
(Major William J. Kralik)
Supersedes AFI 91-103, 11 February 1994

Certified by: HQ USAF/SE
(Maj Gen Timothy A. Peppe)
Pages: 23
Distribution: F

This instruction implements AFPD 91-1, *Nuclear Weapons and Systems Surety*. It defines the process for certifying hardware, software, and procedures used with nuclear weapon systems. It applies to organizations that design, develop, modify, evaluate, or operate nuclear weapon systems. It does not apply to the Air Force Reserve and Air National Guard. Send proposed supplements to this instruction to HQ AFSC/SEP, 9700 G Avenue, Kirtland AFB NM 87117-5670, for coordination and approval before publication. **Attachment 1** lists abbreviations and acronyms used in this instruction. Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule*.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision includes substatiative changes. It gives the Air Foce Chief of Safety the authority to approve weapon maintenance programs performed in Air Force facilities. It separates Engineering MAJCOM responsibilities between the MAJCOM and the program's single manager. It establishes timelines for submittal of Nuclear Surety Evaluations in the event an AFI 91-102 safety study is required. It requires procedures that involve nuclear safety processes to be appropriately marked. It requires nuclear certification plans (NCP) to include requirements, schedules, and responsibilities for certifying procedures involving new weapon systems or significant modification to existing weapon systems. It defines AF/XON's responsibility to ensure a statement of intent is submitted to HQ AFSC/SEW for any nuclear weapon maintenance program to be performed in Air Force facilities. It expands on the information provided for nuclear certified software certification to include the requirement for an Independent Validation and Verification (IV&V) of the software and outlines a generic IV&V program plan. In addition, organization names were changed to reflect changes since the last publication of this instruction.

Section A—Scope and Responsibilities

1. Definitions. See AFI 91-101, *Air Force Nuclear Weapons Surety Program*.

2. Program Goal. The Air Force Nuclear Safety Certification Program evaluates hardware, software, and procedures against specific nuclear safety criteria before use with nuclear weapons. The program's goal is to prevent nuclear weapon accidents and incidents.

3. Responsibilities:

3.1. Chief of Safety (HQ USAF/SE). HQ USAF/SE oversees the Air Force Nuclear Safety Certification Program. As manager of the program, HQ AFSC/SEW will:

3.1.1. Implement an effective program.

3.1.2. Publish design and evaluation criteria according to AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*.

3.1.3. Approve nuclear surety impact statements (NSIS) and nuclear certification plans (NCP).

3.1.4. Approve test and maintenance programs for operational facilities.

3.1.5. Approve weapon maintenance programs performed in Air Force facilities.

3.1.6. Certify hardware, software, and procedures to be used with nuclear weapons.

3.1.7. Designate and certify critical components according to AFI 91-105, *Critical Components*.

3.1.8. Certify Tamper Detection Indicators (TDI).

3.1.9. List certified hardware and software items and restrictions on usage in Technical Order (TO) 00-110N-16, *USAF Nuclear-Certified Equipment and Software*.

3.1.10. Approve operational certification (OPCERT) and decertification (DECERT) procedures.

3.1.11. Decertify the designs of hardware and software.

3.2. MAJCOM Responsibilities. The MAJCOM operating the system will:

3.2.1. Establish a nuclear safety certification program.

3.2.2. Designate a person to manage the certification program.

3.2.3. Provide guidance to units on the nuclear safety certification program (send copy to HQ AFSC/SEW for review).

3.2.4. Identify uncertified equipment for use with nuclear weapon systems and request a nuclear surety evaluation from the organization with program management responsibility.

3.2.5. Identify new uses for TDIs and request approval from HQ AFSC/SEW.

3.2.6. Coordinate the certifying of facility lifting and suspension systems.

3.2.7. Ensure hardware, software, and procedures used with nuclear weapons are design certified before use.

3.2.8. Ensure critical components are operationally certified before use.

3.2.9. Ensure nuclear units report deficiencies on certified items according to procedures in AFI 91-204, *Safety Investigations and Reports*.

3.3. Air Force Materiel Command (AFMC).

3.3.1. In addition to the responsibilities outlined in paragraph **3.2.**, AFMC will:

3.3.1.1. Establish and manage a nuclear surety program for AFMC. Ensure a nuclear safety certification is institutionalized throughout AFMC. Advocate and apply the appropriate focus and emphasis on nuclear surety to obtain an operational capability.

3.3.1.2. Designate a person to manage the nuclear surety/safety certification program.

3.3.1.3. Provide membership to the Nuclear Weapon System Safety Group (NWSSG).

3.3.1.4. Participate, as requested, in weapon project officer's groups, surety and certification working groups, safety analyses, plans, evaluations, and reviews for nuclear weapon systems according to **Attachment 2**.

3.3.1.5. Ensure processes, policy, and guidance are in place for AFPEO/DAC programs, SPOs, single managers, etc., to maintain configuration control of design certified hardware, software, and procedures. Ensure Single Manager's Bluebook is available to HQ AFSC/SEW and all AFMC weapons safety managers.

3.3.1.6. Ensure hardware, software, and procedures used for nuclear weapons, critical components, etc., are design certified before use.

3.3.1.7. Ensure independent technical support (analyses, assessments, evaluations, reviews, etc.) is provided by (AAC/WN), Nuclear Weapons Product Support Center (NWPSC) to HQ AFSC/SEW. NWPSC will coordinate with HQ AFMC/SEW on nuclear safety and surety matters.

3.3.1.8. NWPSC will maintain corporate expertise for the nuclear safety certification process.

3.3.2. Single Manager(s) acquiring and sustaining the system:

3.3.2.1. Has ultimate, program management responsibilities for execution of the nuclear certification program reflected in **Attachment 5**.

3.3.2.2. Is accountable to the Assistant Secretary for Acquisition (SAF/AQ) through the AFPEO/DAC for nuclear weapons systems or other items requiring nuclear certification.

3.3.2.3. Establishes a nuclear safety certification program within the SPOs.

3.3.2.4. Designates a person to manage the nuclear safety certification program.

3.3.2.5. Establishes surety and certification working groups for nuclear weapon systems according to **Attachment 2**.

3.3.2.6. Prepares a NSIS for hardware, software, test or maintenance programs.

3.3.2.7. Develops a NCP for each weapon system or subsystem to be nuclear certified.

3.3.2.8. Performs unauthorized launch (UL) studies according to AFI 91-106, *Unauthorized Launch and Launch Action Studies.*

3.3.2.9. Supports the TDI development and evaluation process.

3.3.2.10. Conducts NSE of the hardware, software, and procedures used with a nuclear weapon or weapon system.

3.3.2.11. Evaluates support equipment provided by other DoD agencies for use with Air Force procedures.

3.3.2.12. Evaluates Air Force use of Department of Energy (DOE)-certified equipment with nuclear weapons to determine whether operating environments are identical and if any differences impact nuclear surety.

3.3.2.13. Ensures all certified items are marked (when possible) with labels (e.g. data plates) to enable positive identification in TO 00-110N-16.

3.3.2.14. Reviews deficiencies (materiel deficiency reports, service bulletins, and nuclear safety deficiency reports) for possible impact on nuclear surety or certification status and implements required corrective action.

3.3.2.15. Ensures all procedures involving nuclear safety processes are marked with the "Nuclear Surety Procedures" (NSP) symbol to enable positive identification. Special emphasis must be applied to the NSPs to protect against degrading or rendering ineffective the critical nuclear safety features of the weapon system.

3.3.2.16. Develop OPCERT and DECERT procedures.

3.3.2.17. Evaluate nuclear surety for hardware, software, and procedures used with a nuclear weapon or nuclear weapon system.

3.4. Assistant Secretary of the Air Force (Acquisition), (SAF/AQ). SAF/AQ will ensure a nuclear safety certification program is established and that Air Force Program Executive Officers (AFPEOs), Designated Acquisition Commanders (DACs), and Single Managers for nuclear weapon systems or other items requiring nuclear safety certification comply with the requirements of this AFI.

3.5. Headquarters United States Air Force Directorate Nuclear and Counter Proliferation (AF/XON). AF/XON will ensure a statement of intent is submitted to AFSC about certain nuclear programs that will be accomplished in Air Force facilities. The qualifying programs are:

3.5.1. Programs to accomplish warhead ALTs and MODs that require bypassing or disabling any weapon safety features.

3.5.2. Other programs that require bypassing or disabling any weapon safety features.

3.5.3. New or revised programs for continuing maintenance of warheads.

Section B—Certification Criteria

4. Items That Require Design Certification:

4.1. Hardware and Software:

4.1.1. Combat and noncombat delivery vehicles.

4.1.2. Operational and support equipment used to move, support, store, handle, load and unload, or mate and demate nuclear weapons.

4.1.3. All hardware and software components that directly interface (electrically or physically) with a nuclear weapon, critical component, certified software, or are identified in a current launch activation path.

4.1.4. Items that could degrade the command, control, and status reporting capability.

4.1.5. All new and currently certified critical components and software.

4.1.6. All hardware or software used to directly control critical functions such as targeting, enable, or launch commands or data generation.

4.1.7. TDIs used in an operational system, as well as TDIs used in a nonoperational environment for storage and transportation.

4.1.8. Operational and maintenance hardware and software used to command and control critical functions and perform status reporting.

4.1.9. Facility lifting and suspension systems (such as cranes, hoists, and suspended frames) used to lift, support, or move nuclear weapons.

4.1.10. Modifications to nonspecialized equipment that could impact the item's primary structure, electrical and hydraulic power systems, load-bearing capacity, steering and braking capability, or positive control features as well as any changes resulting in noncompliance with specific AFI 91-107-directed design criteria.

4.1.11. Test equipment that:

4.1.11.1. Verifies the proper operation of the critical function circuits of a combat delivery vehicle or directly interfaces with nuclear weapons or operationally certified critical components.

4.1.11.2. Is used to operationally certify, decertify, or verify proper operation of applicable items identified in this paragraph.

4.1.11.3. Is used in special test or maintenance programs to identify system anomalies or failures.

4.2. Procedures. Nuclear weapon or weapon system technical order procedures involving operations, maintenance, troubleshooting, OPCERT, DECERT, handling, movement, restraint configurations, loading, unloading, testing, and delivery. Technical order procedures which are to be nuclear safety-certified, contain the explicit instructions that must be followed to conduct operations with nuclear weapons.

5. Items That Do Not Require Design Certification:

5.1. Common items :

5.1.1. General purpose handtools (such as pliers, wrenches, and screwdrivers).

5.1.2. Tiedown chains.

5.1.3. Cables, straps, and adjusters used for ground transportation.

5.1.4. Depot and intermediate-level test equipment if the critical circuits of the tested items are verified at the organizational level before use with nuclear weapons.

5.1.5. Common, multipurpose, and nonspecialized test equipment such as multimeters, decade resistance boxes, and impedance bridges unless the equipment directly interfaces with nuclear weapons.

5.2. Nonspecialized Equipment. Certain modifications to nonspecialized equipment (see paragraph **13.**) do not require formal safety design certification. These modifications include:

5.2.1. Common add-on equipment such as fire extinguishers, radios, lights, bedliners, camper shells, sirens, foreign object damage (FOD) magnets or containers.

5.2.2. Minor field-level modifications to vehicles that clearly do not impact the braking, steering, lifting, powertrain, or load carrying/restraint systems.

5.3. Other Agency Items:

5.3.1. Support equipment and procedures for nuclear logistics movements that other DoD agencies have certified for nuclear weapons handling, if used within established operating criteria.

5.3.2. DOE-certified equipment for use with nuclear weapons providing the operating environments are identical.

NOTE: When items do not clearly fall into any of the categories identified, HQ AFSC/SEW determines if nuclear safety design certification is required.

6. Additional Requirements. The following requirements apply to critical components, TDIs, special test and maintenance programs, and ally-operated weapon systems and procedures:

6.1. Critical components also require OPCERT before use in operational systems to verify the component is functioning as design certified and to mitigate all credible UL threats and scenarios. (Refer to AFI 91-105 and AFI 91-106.) Certain critical components also require specific procedures for DECERT.

6.2. TDIs may be used to protect the certification status of critical components if sufficient justification exists for their use. However, TDIs may not be used to substitute for Two-Person Concept control of codes, coded devices, or critical components exposed to operational codes that cannot be decertified. TDIs used in an operational system are identified in the safety rules for the affected nuclear weapon system according to AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs.*

6.3. Special test or maintenance programs conducted in operational facilities that are not covered by certified procedures must be approved by HQ AFSC/SEW.

6.4. When used with nuclear weapons in Air Force custody, ally-operated nuclear weapon systems and procedures must satisfy the same nuclear safety criteria required for Air Force systems and procedures.

Section C—Certification Process

7. Certification Process for New or Modified Weapon System Hardware and Software. Use the following paragraphs in conjunction with **Attachment 5**, **Figure A5.1.** to determine the steps and timelines for the nuclear safety certification process. All items to be certified must be marked (when possible) with labels to enable positive identification in TO 00-110N-16. For hardware, include the national stock num-

ber, part number, and manufacturer or other pertinent data, as applicable. For software, include the computer program identification number or equivalent identifier approved by HQ AFSC/SEWE.

7.1. The operational MAJCOM or Single Manager identifies items that may require safety design certification according to paragraph **4.**

7.1.1. Single managers must coordinate with the wing or center safety office on all nuclear surety/safety matters. The safety office will serve as the interface between the single manager and HQ AFSC/SEW and NWPSC on all nuclear safety certification processes and issues.

7.1.2. The single manager (e.g. SPO, ALC, etc,) must maintain configuration control of identified hardware and software items to be nuclear safety certified throughout their life-cycle. Configuration control may be maintained via a Change Configuration Board.

7.2. For new weapon systems, the Single Manager prepares an NCP. The NCP must address system-level and individual hardware and software certification requirements according to **Attachment 2**, paragraph **A2.2.** The Single Manager should develop the initial NCP before the system design review or equivalent program milestone to minimize any program impact resulting from nuclear surety requirements. Since the NCP outlines all analyses and testing required for certification, HQ AFSC/SEW must review and approve the plan.

7.3. For weapon system modifications, the Single Manager prepares an NSIS which provides the functional description of the modification and an assessment of its impact on nuclear surety. The Single Manager should develop the NSIS before preparing the statement of work and technical requirements document to minimize any program impact resulting from nuclear surety requirements. Submit the NSIS through the wing or center safety office to HQ AFSC/SEW and NWPSC. The NSIS must be submitted to HQ AFSC/SEW 45 calendar days before the release of a request for proposal or an equivalent program milestone. ***NOTE:*** Modifications to a weapon system include all physical and functional configuration changes to existing certified hardware and software; addition of new operational or support equipment; and new uses for existing equipment.

7.3.1. The NSIS must address those hardware or software items that require certification and recommend a certification approach for verifying compliance with AFI 91-107-directed criteria according to **Attachment 2**, paragraph **A2.3.** NSIS findings and proposed certification approaches fall into one of the following categories:

7.3.1.1. The modification has no potential for adverse nuclear surety impact. Therefore, a Nuclear Surety Evaluation (NSE) is not required. However, if the modification involves currently certified items, HQ AFSC/SEW must update TO 00-110N-16, to reflect any change in item markings (e.g., new part numbers, manufacturers).

7.3.1.2. The modification involves a limited number of hardware or software items and may adversely impact nuclear surety. These items must have clearly defined AFI 91-107-directed design and evaluation criteria, and the certification approach must be well established (based on precedence or directly specified according to AFI 91-107).

7.3.1.3. The modification involves items with significant nuclear surety impact or involves numerous items to be certified. In either case, the modification will be treated as a new system development and an NCP is needed (see paragraph **7.2.**).

7.3.2. When a modification effort is initiated by an operational unit, the unit must coordinate the modification with their operational MAJCOM before proceeding.

7.4. HQ AFSC/SEW reviews the NSIS and either approves or disapproves the proposed certification approach within 30 calendar days. If the proposed certification approach is disapproved, HQ AFSC/SEW informs the MAJCOM with program management responsibility that more information is required or the approach is insufficient to prove compliance with AFI 91-107-directed criteria. Once the NSIS has been approved, the Single Manager imposes design requirements and ensures compliance with AFI 91-107-directed criteria during development or modification.

7.5. As the development or modification effort nears completion (determined by the required operational capability or certification need date), the Single Manager prepares an NSE according to **Attachment 2**, paragraph **A2.4.** and a certification recommendation as specified in **Attachment 4**. Submit the evaluation and certification recommendation through the wing or center safety office to HQ AFSC/SEW. Provide a copy to the Nuclear Weapons Product Support Center (NWPSC). If required, HQ AFSC/SEW will task NWPSC to perform an independent nuclear surety review.

7.5.1. If an AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules* safety study is required, submit the evaluation 120 calendar days prior to the study. ***NOTE:*** For new (and some modified) weapon systems, a Nuclear Safety Analysis Report (NSAR) typically serves as the evaluation.

7.5.2. If a safety study is not required, submit the evaluation 60 calendar days prior to the required operational capability or certification need date.

7.6. When tasked by HQ AFSC/SEW, NWPSC reviews the design, evaluation, and certification recommendation according to **Attachment 2**, paragraph **A2.5.** and sends its assessment to HQ AFSC/SEW.

7.6.1. When a safety study is required, this assessment is submitted as required by AFI 91-102. ***NOTE:*** For the AFI 91-102 process, this assessment is referred to as the Technical Nuclear Safety Analysis (TNSA).

7.6.2. If a safety study is not required, submit the assessment 20 calendar days prior to the required operational capability or certification need date.

7.7. HQ AFSC/SEW will provide a safety design certification statement and list certified items (with any applicable restrictions on usage) in TO 00-110N-16. ***NOTE:*** Restrictions on the use of items in a nuclear role may be imposed to compensate for design deficiencies or significant operational hazards.

8. Certification Process for Nuclear Safety-Certified Technical Order Procedures. The certification process involves the following actions:

8.1. A thorough review of the procedures by the technical order management agency (TOMA) to ensure that these procedures are validated, verified, complete, accurate, and safe. The technical content manager for these procedures must ensure consistency with nuclear weapon system safety rules (if available), requirements in current 91-100 series Air Force publications, nuclear safety restrictions, and proper use of design safety features. All procedures involving nuclear safety processes must be marked with the NSP symbol to enable positive identification.

8.2. For OPCERT/DECERT procedures, NWPSC reviews these procedures for new weapon systems or critical components, and HQ AFSC/SEW approves the procedures. HQ AFSC/SEW must approve major changes to OPCERT procedures, but NWPSC may approve minor changes. The review of the

procedures must adequately verify that the system or component functions as design certified and mitigates all credible threats and scenarios.

8.3. For new weapon system developments or significant weapon system/subsystem modifications, the NCP will include requirements, schedules, and responsibilities for certifying these procedures.

8.4. The certification process is complete when the TOMA publishes the procedures.

9. Critical Components. For certification of critical components, the organization with program management responsibility:

9.1. Initiates the design certification process for hardware and software.

9.2. Provides for a nuclear safety cross-check analysis (NSCCA) or independent validation and verification (IV&V) of software critical components according to **Attachment 2**, paragraph **A2.6.**

9.3. Develops OPCERT and DECERT procedures for hardware critical components and sends the procedures to HQ AFSC/SEW for approval.

10. Tamper Detection Indicators (TDIs):

10.1. For certification of TDIs, the operational MAJCOM or Single Manager determines the need for TDI application and sends a request to HQ AFSC/SEW that:

10.1.1. Identifies the critical component requiring a TDI.

10.1.2. Justifies why a TDI is needed because Two-Person Concept control cannot be used.

10.1.3. States whether the TDI will be used in an operational system or a nonoperational environment for storage and transportation.

10.2. HQ AFSC/SEW evaluates the TDI application request and sends the approved application to the National Security Agency (NSA) for development of a suitable TDI.

10.3. By agreement, the NSA:

10.3.1. Develops the appropriate TDI based on the parameters and intended-use data provided by the operational MAJCOM.

10.3.2. Coordinates TDI development with the organization having program management responsibility.

10.3.3. Sends the TDI data required for application, control, storage, and inspection procedures to HQ AFSC/SEW for certification.

10.4. The requesting MAJCOM maintains responsibility for all procurement actions and costs associated with TDI development and integration.

10.5. Upon approval of the application, the Single Manager provides the technical requirements to the NSA and develops the nuclear surety evaluation required to obtain certification.

11. Special Test and Maintenance Programs:

11.1. The Single Manager must evaluate all aspects of the proposed programs for potential nuclear surety degradation. This evaluation includes conditions that could violate AFI 91-107-directed criteria, degrade existing safety and security features, or contribute to UL scenarios.

11.2. The Single Manager generates a certification request according to paragraph **7.5.**

11.3. HQ AFSC/SEW bases the approval decision on the findings of the evaluation and the independent review (if required by paragraph **7.6.**). A special safety study may also be required according to AFI 91-102.

12. Nuclear Weapon Maintenance Programs:

12.1. AF/XON must ensure a statement of intent is submitted for any nuclear weapon maintenance program to be performed in Air Force facilities. This requirement applies to maintenance programs as outlined in paragraph **3.5.** The statement of intent will:

12.1.1. Provide a background and description of the maintenance action to be performed.

12.1.2. Identify temporary removal, bypass, or disablement of the surety features of the weapon itself.

12.1.3. Specify the Air Force facility where the maintenance program will be performed.

12.2. Submit the statement of intent to HQ AFSC/SEW no later than 180 days prior to scheduled maintenance. If required, HQ AFSC/SEW will task NWPSC to evaluate the maintenance program in relation to the facility where the program is to be performed.

12.3. HQ AFSC/SEW bases the approval decision upon review of the statement of intent and NWPSC's evaluation (if required).

13. Nonspecialized Equipment. Any equipment used with nuclear weapons but not specifically designed for that purpose is considered nonspecialized equipment. Certain modifications of nonspecialized equipment may not require formal certification if the equipment is still used for its original purpose and the changes do not adversely impact nuclear safety. Use the following process to determine the appropriate course of action.

13.1. Identify item(s) to be modified and provide a complete description of the proposed changes to the item Maintenance Supervisor/Superintendent (or equivalent) and the Unit Safety Office.

13.2. These offices will jointly review the proposed modification to determine if approval can be granted at the unit level or if further evaluation of the nuclear safety impact is necessary (see paragraph **5.2.**).

13.2.1. If there is clearly no impact to nuclear surety, approve the modification locally.

13.2.2. If further evaluation is required, submit a request for evaluation/approval from the operational MAJCOM's safety office.

13.2.3. If formal safety design certification is not required, the operational MAJCOM will:

13.2.3.1. Provide formal approval to the field unit.

13.2.3.2. Inform the item manager and HQ AFSC/SEW of the approved modification.

13.3. If the modification requires formal nuclear safety design certification, the operational MAJCOM will:

13.3.1. Notify the submitter that further evaluation is necessary.

13.3.2. Follow the process specified in paragraph **7.3.**

14. Facility Lifting and Suspension Systems:

14.1. The Single Manager performs a nuclear surety evaluation and sends certification request to HQ AFSC/SEW according to paragraph **7.5.**

14.2. A design or civil engineering agency evaluates the facility that will support the lifting or suspension system to determine if the structure meets the design requirements in AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems*. The evaluation agency provides HQ AFSC/SEW with a certification request and an appropriate analysis that the structure is safe for the rated load and meets the required margins of safety according to AFMAN 91-118

14.3. An inspection and maintenance cycle for each certified facility lifting system will be established according to AFOSH Standard 91-46, *Materials Handling and Support Equipment*.

14.4. The owning MAJCOM is authorized to use suspended load-frame assemblies at 100 percent of their rated load. These assemblies do not require periodic load testing but must be periodically inspected.

14.5. The Single Manager evaluates item or facility support structure modifications to determine their impact on the certification status.

14.6. HQ AFSC/SEW certifies and lists the facility lifting system in TO 00-110N-16.

Section D—Decertification Process

15. Design Decertification:

15.1. HQ AFSC/SEW may decertify items that have demonstrated inadequate design safety through analysis, testing, or operational performance.

15.2. Any Air Force agency may send a recommendation for design decertification to HQ AFSC/SEW. The recommendation must identify the item as listed in TO 00-110N-16 and include documentation that supports the recommendation to decertify.

15.3. As the final authority on decertification action, HQ AFSC/SEW reviews the decertification recommendation and takes action to remove the item from TO 00-110N-16.

15.4. A certified item may be restricted from use with nuclear weapons at any time and for any reason (e.g., damage, modifications, or changes to intended usage, etc.). Such restrictions do not constitute decertification. Appropriate documentation in historical or permanent records is required to preclude inadvertent use. If desired, submit an Air Force Technical Order (AFTO) Form 22 for TO 00-110N-16 to restrict specific item(s) from use.

16. Operational Decertification:

16.1. Critical components or systems that have been improperly stored or not maintained according to AFI 91-105 require decertification if the resulting mishap investigation does not positively rule out tampering. Decertification is also required if a critical component is connected to an uncertified interface.

16.2. Operational MAJCOMs may decertify critical components if they use approved decertification procedures (when applicable) and the intended life cycle for the critical component does not specifically prohibit decertification.

TIMOTHY A. PEPPE., Major General, USAF
Chief of Safety

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

GOVERNMENT REFERENCES

DoD 3150.2-M, *DoD Nuclear Weapon System Safety Standards, Policy, and Criteria*

DoD Guidelines for Software Development

USAF REFERENCES

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

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

AFI 91-104, *Nuclear Surety Tamper Controland Detection Programs*

AFI 91-105, *Critical Components*

AFI 91-106, *Unauthorised Launch and Launch Actio n Studies*

AFI 91-107, *Design, Evaluation, Troubleshooting and Maintenance Criteria for Nuclear Weapon System*

AFI 91-204, *Safety Investigations and Reports*

AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon System Hardware*

Technical Order 00-110N-16, *USAF Nuclear Certified Equipment and Software*

Abbreviations and Acronyms

AAC/WN—Air Armament Center/Weapons Nuclear

AFI—Air Force Instruction

AFSC—Air Force Safety Center

AFSC/SEW—AFSC, Weapons, Space, and Nuclear Surety Division

AFSC/SEWE—AFSC/SEW, Space and Engineering Branch

AFTO—Air Force Technical Order

DECERT—Operational Decertification

DoD—Department of Defense

FOD—Foreign Object Damage

HQ AFSC—Headquarters, AFSC

IV&V—Independent Validation and Verification

MAJCOM—Major Command

NCP—Nuclear Certification Plan

NSA—National Security Agency

NSAR—Nuclear Safety Analysis Report

NSCCA—Nuclear Safety Cross-Check Analysis

NSE—Nuclear Surety Evaluation

NSIS—Nuclear Surety Impact Statement

NSP—Nuclear Surety Procedures

NWPSC—Nuclear Weapons Product Support Center (Office Symbol: AAC/WN)

OPCERT—Operational Certification

TDI—Tamper Detection Indicator

TNSA—Technical Nuclear Safety Analysis

TO—Technical Order

TOMA—Technical Order Management Agency

UL—Unauthorized Launch

Attachment 2

GROUPS, SAFETY ANALYSES, PLANS, EVALUATIONS, AND REVIEWS

A2.1. Surety and Certification Working Groups:

A2.1.1. For ground-launched missile systems, a nuclear surety working group is used to coordinate nuclear surety requirements among the various agencies involved in nuclear safety certification. This group is chaired by the Single Manager and membership includes:

A2.1.1.1. Operational MAJCOM.

A2.1.1.2. Nuclear Weapons Product Support Center.

A2.1.1.3. Air Force Security Forces Center .

A2.1.1.4. National Security Agency.

A2.1.1.5. Air Force Safety Center; Weapons, Space , and Nuclear Safety Division.

A2.1.2. For aircraft and air-launched missile systems, a nuclear certification working group or an air vehicle project officers group is used to coordinate nuclear safety certification issues and any other nuclear certification issues. The Single Manager designates a nuclear certification manager to chair this group and membership includes:

A2.1.2.1. Operational MAJCOM.

A2.1.2.2. Nuclear Weapons Product Support Center.

A2.1.2.3. National warhead design laboratories (when appropriate).

A2.1.2.4. Air Force Safety Center; Weapons, Space, and Nuclear Safety Division.

A2.1.2.5. Sandia National Laboratories, Albuquerque

A2.2. Nuclear Certification Plan (NCP). The purpose of the NCP is to ensure proper planning and define the approach for obtaining nuclear safety design certification of hardware and software items and procedures used within a weapon system and associated support equipment. The NCP must include:

A2.2.1. Equipment or system description that explains the nuclear safety implications of all items addressed in the NCP. As a minimum, the description must address how the equipment interacts to perform nuclear critical functions.

A2.2.2. Allocation matrix that maps all applicable AFI 91-107-directed requirements to the equipment or system components.

A2.2.3. Specific methods to be used for compliance verification (proposed certification approach).

A2.2.4. Approaches for operationally certifying and decertifying potential critical components addressed by the NCP and for addressing system-level certification issues (such as compatibility requirements for aircraft systems, OPCERT requirements for ground-launched missile systems, and technical data development and approval).

A2.2.5. Schedule that includes major certification and program milestones.

A2.2.6. Responsibilities of each agency identified in the NCP.

A2.2.7. Signature page that indicates approval by all responsible agencies.

A2.3. Nuclear Surety Impact Statement (NSIS). Includes a functional description of the proposed modification or test program and an evaluation of its potential for nuclear surety impact. The evaluation must address the modification in enough detail to substantiate a recommended certification approach. As a minimum, the evaluation must address any potential impact to AFI 91-107-directed criteria and degradations to existing nuclear weapon system safety features. When preparing an NSIS, the Single Manager should review existing UL analyses to determine whether the modification includes items that are likely candidates to be designated critical components. If it does, use an NCP to further develop the certification approach associated with design certifying the item and to develop the OPCERT and DECERT concepts. The only exception to this requirement is when the modification involves critical components that already have a design certification approach approved by HQ AFSC/SEW and OPCERT and DECERT concepts.

A2.4. Nuclear Surety Evaluation (NSE). Evaluates items to be certified using the approved certification approach (as identified in the NSIS or NCP). The NSE focuses on all AFI 91-107-directed design and evaluation criteria applicable to the item. It includes a recommendation for certification or certification with restrictions (to meet AFI 91-107-directed criteria).

A2.5. Independent Nuclear Surety Review:

A2.5.1. The independent nuclear surety review:

A2.5.1.1. Is of sufficient depth to ensure the nuclear surety evaluation is technically correct and complete.

A2.5.1.2. Specifically addresses the design requirements.

A2.5.1.3. Indicates if the design meets AFI 91-107-directed criteria.

A2.5.2. When requirements are not met, the review must include comments and documentation on the adequacy of compensatory measures and specify if the reviewing agency concurs with the evaluating agency's recommendation for nuclear safety design certification.

A2.6. Software Evaluations. Nuclear critical software evaluation can be accomplished by Nuclear Safety Cross-Check Evaluation (NSCCA) or Independent Validation and Verification (IV&V). AFM 91-119 provides guidelines for determining the method of and criteria for evaluation. Requirements for software evaluation can range from full NSCCA to qualification testing depending on the relationship to critical functions (authorization, prearming, launching, releasing, arming, and targeting). Additional factors include the potential for unauthorized launch threats and scenarios. Although these evaluations use many similar techniques, they are typically performed by different organizations, have different objectives, and produce different results. NSCCA and IV&V are performed by an organization technically, managerially, and financially independent of the developer. HQ AFSC/SEW will make the final determination regarding independency requirements.

A2.6.1. Nuclear Safety Cross-Check Analysis (NSCCA). An NSCCA has the single objective of ensuring that the program cannot perform in any way that could contribute to a nuclear safety violation. Analysis and testing focus on ensuring that nuclear safety-critical functions are performed correctly and that the program does not perform any unintended functions that could violate nuclear safety. The NSCCA is also unique in its concern for sabotage. While the other forms of software eval-

uation assume that any program deficiencies will be unintentional, the NSCCA also looks for intentionally caused problems and employs special security and control measures to prevent sabotage of the NSCCA effort itself. An NSCCA begins with the development of nuclear safety objectives (NSOs) and nuclear safety requirements (NSRs). NSOs represent the overall objectives a nuclear weapon system must satisfy in order to obtain nuclear safety certification. NSRs form the basis for all subsequent NSCCA activities. A traceability analysis is performed to demonstrate that all NSOs are represented in the NSRs and that all NSRs are derived from one or more NSOs. The NSCCA is completed by conducting a bit-for-bit comparison (under the Two-Person Concept) between the software delivered to the operational MAJCOM and the software analyzed by the NSCCA organization.

A2.6.2. Independent Validation and Verification (IV&V). IV&V is a software evaluation process that includes both analysis and testing and extends throughout program development. “Verification” analyzes software requirements, design, and code to detect program deficiencies before they can propagate into later development phases. “Validation” analyzes and tests the final program to determine its compliance with requirements. IV&V is distinguished from qualification testing by its emphasis on detecting program weaknesses and unforeseen circumstances that the program will be unable to handle. **Attachment 3** provides a generic IV&V program plan to define the approach used by the IV&V contractor/evaluation team in support of software nuclear safety design certification.

Attachment 3

GENERIC INDEPENDENT VALIDATION AND VERIFICATION (IV&V) PROGRAM PLAN

A3.1. Purpose. The purpose of this program plan is to define the approach to be used by the IV&V contractor/evaluation team in support of nuclear safety design certification of the software/firmware in question. The overall nuclear safety design certification effort is defined in another program plan. Nuclear certification of software/firmware is one of the positive measures the Air Force uses to assure that the software/firmware, as designed, coded, and implemented, complies with the DOD Nuclear Weapon System Safety Standards (DOD Directive 3150.2) and meets the safety design and evaluation criteria for nuclear weapon systems in AFI 91-107.

A3.2. Equipment/system Description. This section provides a brief description of the weapon system that will allow the reader to understand the functional and nuclear safety implications of the weapon system. Where individual software/firmware pieces are involved, provide a brief description of each item at the block diagram level. A brief description includes performance requirements and software/firmware design showing correlation to requirements and stressing features that provide nuclear surety.

A3.3. IV&V Concepts:

A3.3.1. Validation is defined as the test and evaluation process that ensures the software/firmware meets all system and software performance requirements; verification is the repetitive process for ensuring that, during each development phase, the software/firmware satisfies and implements only those requirements approved at the end of the previous phase. For the purpose of nuclear safety, the conduct of this validation and verification effort has primary emphasis placed on the nuclear safety issues identified below. Using an independent contractor to perform this task adds an additional layer of confidence and security to the process.

A3.3.2. The IV&V effort will concentrate on the software/firmware functions that must be verified to obtain nuclear safety design certification in accordance with AFI 91-103. The key step in this effort is identifying the nuclear safety contributions and how the software/firmware could possibly impact or affect the weapon system nuclear critical functions as defined in AFMAM 91-118. These critical functions are: authorization, launching/releasing, warhead prearming/arming, and targeting. All of the software/firmware functions and capabilities will be evaluated to determine the level and extent of their contributions, resulting in nuclear safety impacts to the above critical functions. Contributions which cause a possible degradation of nuclear safety or performance will be reported as discrepancies for program office evaluation.

A3.3.3. The nuclear safety design certification effort is led by AFSC/SEWE. A Software Advisory Group meets as required to resolve difficult issues. The Software Advisory Group is composed of members from the Program Office, Safety Center, Nuclear Weapons Integration Division, Space Command, Strategic Command, the developing contractor, and the IV&V contractor.

A3.3.4. All nuclear safety discrepancies will be identified, evaluated, and prioritized according to their potential impact on nuclear safety. A priority scheme is used to evaluate nuclear safety discrepancies and determine their impact on nuclear safety (Critical, Urgent, Degraded, Noncritical, Minor).

A3.3.5. The results obtained from the IV&V effort will be included in the final IV&V report and will also be used in the preparation of the demonstration test plan and Nuclear Surety Evaluation (NSE)

report. Inputs will also be made to the qualification demonstration and data will be examined from those tests with regard to verification of the software/firmware. Finally, the data from these efforts will be maintained in a data base at the program office to support future modifications and technical order updates.

A3.4. IV&V Approach. This section describes the specific approach that will be taken to conduct the IV&V effort.

A3.4.1. Test Plan. The IV&V contractor designs and conducts tests to verify the software/firmware design complies with AFI 91-107. This test approach is detailed in the IV&V Test Plan.

A3.4.2. Configuration Control. The program office will maintain configuration control. This task may be contracted out, but the ultimate responsibility for configuration control remains with the single manager. Discrepancy reports will address performance as well as nuclear safety aspects of the software/firmware functions and capabilities. These reports will provide all pertinent information (such as problem areas, descriptions, impacts, and recommendations) required to pursue appropriate action.

A3.4.3. Analysis Tools. In order to implement the IV&V approach effectively, specific analysis tools may be developed to perform both the tracing studies and the software/firmware checkout. The analysis tools themselves will be validated to the degree required to ensure accuracy and completeness.

A3.4.4. AFI Compliance. AFI 91-107/AFMAN 91-119 will be used to guide and direct the IV&V efforts. Particular attention will be given to memory organization, fault detection/handling capabilities, and the adequacy of self-test circuitry. A summary table should show compliance and the specific analysis or demonstration efforts.

A3.4.5. Source Code Testing. The source code is checked for implementation, using the Computer Program Development Specification and the Computer Program Product Specification. Items that will be checked are the code structure, decision/branch points, input/output handling, and module coupling. The test plan outlines the steps to check the source code at both the modular and/or functional level for those areas impacting nuclear safety. A “test requirements" checklist versus a "test approach" checklist will be generated to determine how functions will be verified. A "master procedures" checklist will be constructed to identify which tests are exercised for each module (or logical group of modules). The tests will be a combination of manual analysis and development site testing.

A3.4.6. Test Results Report. A test results report will discuss the software/firmware code checkout effort. Summary result tables will be provided. All discrepancy reports and their resolution will be included.

A3.4.7. Object Code Testing. Once the source code is checked, it will be compiled into an executable object code. For ground-launched missile systems, a bit-by-bit compare against the object code delivered by the development contractor will be accomplished. Differences will be identified and explained. Discrepancies will be documented and resolution recommended.

A3.4.8. Final Report. A final report will include IV&V results. The report will evaluate whether the software/firmware satisfies AFI 91-107 design standards and, via the discrepancy reports, will identify any known nuclear safety concerns. Each discrepancy report will have an evaluation and recommendation. The report will conclude with a recommendation on nuclear safety design certification. The report will be included as part of the Nuclear Surety Evaluation (NSE).

A3.5. Schedules. Significant milestones are submittal/approval of IV&V Program Plan, IV&V Test Plan, Final IV&V Report, and the NSE report. The first two items are especially critical to the success of IV&V.

Attachment 4

RECOMMENDATION FOR NUCLEAR SAFETY DESIGN CERTIFICATION AND SUMMARY OF ENGINEERING EVALUATION

A4.1. Certification Action. Recommend certification or certification with restrictions (to meet AFI 91-107-directed criteria).

A4.2. Item Identification. For hardware or software (as applicable) provide:

A4.2.1. Nomenclature or common name.

A4.2.2. National stock number (the number in use rather than the master number).

A4.2.3. Manufacturer and code.

A4.2.4. Model and part number.

A4.2.5. Computer program identification number.

A4.2.6. Item manager (include the functional address symbol and telephone number).

A4.3. Uses and Description. Provide information on:

A4.3.1. Equipment uses.

A4.3.2. Weapons.

A4.3.3. Weapon types (as considered in the analysis).

A4.3.4. Top-level description.

A4.4. Summary of Engineering Analysis (Evaluation and Test):

A4.4.1. Identify the specific AFI 91-107-directed criteria used in the design and evaluation process for the item.

A4.4.2. Discuss the certification approach used (compliance verification methods).

A4.4.3. Identify or reference the specific test and analysis procedures used.

A4.4.4. Summarize the results of the certification analysis, and discuss any discrepancies identified during the evaluation and their disposition.

A4.5. Recommended Restrictions. Recommend any restrictions needed to compensate for uncorrected design deficiencies or discrepancies.

Attachment 5

NUCLEAR SAFETY CERTIFICATION PROCESS FLOWCHART

Figure A5.1. Nuclear Safety Certification Process Flowchart.