

11 FEBRUARY 1994



Safety

**AIR FORCE NUCLEAR SAFETY
CERTIFICATION PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFSA/SENA
(Lt Col John D. Waskiewicz)
Supersedes AFR 122-3, 5 December 1988, and
AFR 122-9, 24 August 1987.

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

Pages: 13
Distribution: F

This instruction implements AFR 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 AFSA/SENA, 9700 Avenue G, Kirtland AFB NM 87117-5670, for coordination and HQ USAF/SE, 1400 Air Force Pentagon, Washington DC 20330-1400, for approval before publication. **Attachment 1** lists abbreviations and acronyms used in this instruction.

SUMMARY OF REVISIONS

This is the initial publication of AFI 91-103 revising AFRs 122-3 and 122-9. It directs unauthorized launch studies and discusses certification and decertification procedures; defines responsibilities for preparing the Nuclear Surety Impact Statement and Nuclear Certification Plan; and tells how to certify Tamper Detection Indicators and get approval for test or maintenance programs.

Section A—Scope and Responsibilities

- 1. Definitions.** See AFI 91-101, *Air Force Nuclear Weapons Surety Program* (formerly AFR 122-1).
- 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. The Commander, Air Force Safety Agency, manages the program. HQ AFSA/SEN:

- Implements an effective program.
- Publishes design and evaluation criteria according to AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems* (formerly AFR 122-10).
- Certifies hardware, software, and procedures to be used with nuclear weapons.
- Designates and certifies critical components according to AFI 91-105, *Critical Components* (formerly AFR 122-17).
- Certifies Tamper Detection Indicators (TDI).
- Lists certified items and restrictions on usage in Technical Order (TO) 00-110N-16, *Equipment Authorized for Use With Nuclear Weapons*.
- Approves operational certification (OPCERT) and decertification (DECERT) procedures.
- Approves major command (MAJCOM)-prepared nuclear surety impact statements (NSIS) and nuclear certification plans (NCP).
- Approves test and maintenance programs for operational facilities.
- Decertifies the designs of hardware and software.

3.2. MAJCOM Responsibilities. The MAJCOM operating the system:

- Establishes a nuclear safety certification program.
- Designates a person to manage the certification program.
- Provides guidance to their units (send a copy to HQ AFSA/SEN for review).
- Ensures hardware and software used with nuclear weapons are design certified before use.
- Ensures critical components are operationally certified before use.
- Ensures nuclear units report deficiencies on certified items according to procedures in AFI 91-204, *Investigating and Reporting US Air Force Mishaps* (formerly AFR 127-4).
- Identifies uncertified equipment for use with nuclear weapon systems and requests a nuclear surety evaluation from the engineering MAJCOM.
- Identifies new uses for TDIs and requests approval from HQ AFSA/SEN.
- Coordinates the certifying of facility lifting and suspension systems.

3.3. Engineering MAJCOM Responsibilities. The engineering MAJCOM:

- Establishes a nuclear safety certification program.
- Designates a person to manage the certification program.
- Provides guidance to their units (send a copy to HQ AFSA/SEN for review).
- Evaluates nuclear surety for hardware, software, and procedures used with a nuclear weapon or nuclear weapon system.
- Prepares an NSIS for hardware, software, and test or maintenance programs.
- Develops an NCP for each weapon system or subsystem.
- Performs unauthorized launch (UL) studies according to AFI 91-106, *Unauthorized Launch and Launch Action Studies* (formerly AFR 122-6).
- Supports the TDI development and evaluation process.

- Develops OPCERT and DECERT procedures.
- Designates a MAJCOM agency, with HQ AFSA/SEN approval, to perform independent nuclear surety reviews.
- Ensures certified items are uniquely marked.
- Reviews deficiencies (materiel deficiency reports, service bulletins, and Dull Sword reports) for possible impact on nuclear surety or certification status and implements required corrective action.
- Evaluates support equipment provided by other DoD agencies for use with Air Force procedures.
- 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.
- Establishes surety and certification working groups for nuclear weapon systems according to **Attachment 2**, paragraph **A2.1**.

Section B—Certification Criteria

4. Items That Require Design Certification:

4.1. Hardware and Software:

- Combat and noncombat delivery vehicles.
- Operational and support equipment used to move, support, store, handle, load and unload, or mate and demate nuclear weapons.
- 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.
- Items that could degrade the command, control, and status reporting capability.
- All new and currently certified critical components and software.
- All hardware or software used to directly control critical functions such as targeting, enable, or launch commands or data generation.
- TDIs used in an operational system, as well as TDIs used in a nonoperational environment for storage and transportation.
- Operational and maintenance hardware and software used to command and control critical functions and perform status reporting.
- Facility lifting and suspension systems (such as cranes, hoists, and suspended frames) used to lift, support, or move nuclear weapons.
- 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.

4.2. Test Equipment:

- That 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.
- Used to operationally certify, decertify, or verify proper operation of applicable items identified in paragraph 4.1.
- Used in special test or maintenance programs to identify system anomalies or failures.

4.3. Procedures. Nuclear weapon or weapon system technical order procedures involving operations, maintenance, troubleshooting, OPCERT, handling, movement, restraint configuration, loading, testing, and delivery.

5. Items That Do Not Require Design Certification:

5.1. Common items:

- General purpose handtools (such as pliers, wrenches, and screwdrivers).
- Tiedown chains, cables, straps, and adjusters used for ground transportation.
- 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.
- 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. Certain modifications to nonspecialized equipment identified at field level including the addition of special equipment to a vehicle (such as camper shells, radios, sirens, foreign object damage magnets, and lights) where the nuclear safety design of the item is clearly not impacted by the change.

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

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

5.5. When hardware or software items do not clearly fall into any of the categories identified, HQ AFSA/SEN 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* (formerly AFR 122-4).

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

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 Hardware and Software. The process includes the following actions:

7.1. The operational or engineering MAJCOM identifies items that may require hardware or software certification according to paragraph 4.

7.2. For new weapon systems, the engineering MAJCOM prepares an NCP. The NCP must address system-level and individual hardware and software certification requirements according to **Attachment 2**, paragraph **A2.2**. The engineering MAJCOM 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 AFSA/SEN must approve the plan.

7.3. 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.
- New uses for existing equipment.

7.3.1. For weapon system modifications, the engineering MAJCOM prepares an NSIS. The NSIS provides the functional description of the modification and an evaluation of nuclear surety impact. The engineering MAJCOM should develop the NSIS before preparing the statement of work and technical requirements document to minimize any program impact resulting from nuclear surety requirements. HQ AFSA/SEN must receive the NSIS at least 45 calendar days before the release of a request for proposal or an equivalent program milestone.

7.3.2. 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**. The NSIS findings and proposed certification approaches fall into one of the following categories:

7.3.2.1. The modification has no potential for adverse nuclear surety impact. Therefore, certification is not required. However, if the modification involves currently certified items, HQ AFSA/SEN must update TO 00-110N-16, to reflect any change in item markings (e.g., new part numbers, manufacturers, etc.).

7.3.2.2. 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).

7.3.2.3. The modification involves items with significant nuclear surety impact or involves numerous items to be certified. In either case, the modification must be treated as a new sys-

tem development and an NCP is needed.

7.3.3. HQ AFSA/SEN evaluates the NSIS or NCP and either approves or disapproves the proposed certification approach within 30 calendar days. If the proposed certification approach is disapproved, HQ AFSA/SEN informs the engineering MAJCOM that more information is required or the approach is insufficient to prove compliance with AFI 91-107-directed criteria.

7.4. Once the NCP or NSIS has been approved, the engineering MAJCOM:

- Imposes design requirements and ensures compliance with AFI 91-107-directed criteria during development or modification.
- Ensures the items are marked with unique identifiers (preferably the national stock number for hardware and the computer program identification number for software) to enable positive identification in TO 00-110N-16.
- Prepares a nuclear surety evaluation (NSE) and certification recommendation according to **Attachment 2**, paragraph **A2.4**. and documented as specified in **Attachment 3**.

7.5. Certification Request. The engineering MAJCOM sends the NSE and certification recommendation to HQ AFSA/SEN and a copy to the MAJCOM-designated independent review agency 60 calendar days before the certification need date. If required, HQ AFSA/SEN will task the MAJCOM-designated review agency to perform an independent review.

7.6. When tasked by HQ AFSA/SEN, the MAJCOM-designated review agency assesses the design, NSE, and certification recommendation according **Attachment 2**, paragraph **A2.5**. and sends its assessment to HQ AFSA/SEN.

7.7. If all design requirements are met, HQ AFSA/SEN completes the process by listing the requested 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 Procedures. The certification process involves the following actions:

8.1. The engineering MAJCOM reviews the procedures to ensure consistency with:

- Nuclear weapon system safety rules (if available).
- Requirements in 91-100 series Air Force directives.
- Nuclear safety restrictions.
- Proper use of design safety features.

8.2. The independent review organization reviews OPCERT procedures for new weapon systems or critical components, and HQ AFSA/SEN approves the procedures. HQ AFSA/SEN must approve major changes to OPCERT procedures, but the independent review agency may approve minor changes. Approval is given only if the procedures adequately verify the system or component functions as design certified and mitigates all credible threats and scenarios.

8.3. The certification process is complete when the technical order management agency publishes the procedures after validation and verification are completed.

9. Critical Components. For certification of critical components, the engineering MAJCOM:

- Initiates the design certification process for hardware and software.
- Provides for a nuclear safety cross-check analysis (NSCCA) of software critical components according to **Attachment 2**, paragraph **A2.6**.
- Develops OPCERT and DECERT procedures for hardware critical components and sends the procedures to HQ AFSA/SEN for approval.

10. Tamper Detection Indicators (TDI):

10.1. For certification of TDIs, the engineering or operational MAJCOM determines the need for TDI application and sends a request to HQ AFSA/SEN that:

- Identifies the critical component requiring a TDI.
- Justifies why a TDI is needed and Two-Person Concept control cannot be used.
- States whether the TDI will be used in an operational system or a nonoperational environment for storage and transportation.

10.2. HQ AFSA/SEN 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:

- Develops the appropriate TDI based on the parameters and intended-use data provided by the operational MAJCOM.
- Coordinates TDI development with the engineering MAJCOM.
- Sends the TDI data required for application, control, storage, and inspection procedures to HQ AFSA/SEN 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 engineering MAJCOM 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 engineering MAJCOM 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.
- Contribute to UL scenarios.

11.2. The engineering MAJCOM generates a certification request according to paragraph **7.5**.

11.3. HQ AFSA/SEN 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, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules* (formerly AFR 122-2).

12. Nonspecialized Equipment. Any equipment used with nuclear weapons but not specifically designed for that purpose is considered nonspecialized equipment. Nonspecialized equipment may not require formal certification of certain modifications identified at field level if the equipment is still used for its original purpose and the changes are approved by the operational MAJCOM.

12.1. Field units wanting to make changes to certified nonspecialized equipment must:

- Identify items to be modified.
- Provide a complete description of the proposed modifications.
- Submit a request for approval of the modification to the operational MAJCOM's safety office.

12.2. The operational MAJCOM reviews field unit requests for modifications to nonspecialized equipment and determines if formal nuclear safety design certification is required.

12.2.1. If the proposed modification does not require formal nuclear safety design certification, the operational MAJCOM:

- Provides formal approval to the field unit.
- Informs the engineering MAJCOM item manager and HQ AFSA/SEN of the approved modification.

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

- Disapproves the modification pending further action.
- Follows the process specified in paragraph **7.3.1**.

13. Facility Lifting and Suspension Systems:

13.1. The engineering MAJCOM performs a nuclear surety evaluation and sends certification request to HQ AFSA/SEN according to paragraph **7.5**.

13.2. A design or civil engineering agency evaluates the facility that will support the lifting or suspension system to determine if the structure meets civil engineering design standards and provides proper interface for installing the system. The evaluation agency notifies HQ AFSA/SEN (by letter) that the structure is safe for the rated load and meets the required margin of safety according to civil engineering design standards.

13.3. The base or owning MAJCOM civil engineering organization establishes a periodic inspection and maintenance cycle for each certified facility lifting system. This cycle must include load tests at 125 percent of the rated load for each lifting system. The system may then be used only within the periodic inspection cycle and up to its rated load.

13.4. 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.

13.5. The engineering MAJCOM evaluates item or facility support structure modifications to determine their impact on the certification status.

13.6. HQ AFSA/SEN certifies and lists the facility lifting system in TO 00-110N-16.

Section D—Decertification Process

14. Design Decertification:

14.1. HQ AFSA/SEN may decertify items that have demonstrated inadequate design safety through analysis, testing, or operational performance.

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

14.3. As the final authority on decertification action, HQ AFSA/SEN reviews the decertification recommendation and takes action to change TO 00-110N-16.

14.4. Any unit commander or responsible engineering agency may restrict the use of a certified item based on inadequate safety performance, but such restrictions do not constitute decertification. The commander or agency must immediately notify HQ AFSA/SEN of any restrictions placed on nuclear safety design-certified equipment.

15. Operational Decertification:

15.1. 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.

15.2. 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.

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

Attachment 1

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

AFI—Air Force Instruction
AFR—Air Force Regulation
AFSA—Air Force Safety Agency
AFSA/SEN—AFSA, Directorate of Nuclear Surety
AFSA/SENA—AFSA/SEN, Nuclear Systems Engineering Division
DECERT—Operational Decertification
DoD—Department of Defense
HQ AFSA—Headquarters, AFSA
MAJCOM—Major Command
NCP—Nuclear Certification Plan
NSA—National Security Agency
NSCCA—Nuclear Safety Cross-Check Analysis
NSE—Nuclear Surety Evaluation
NSIS—Nuclear Surety Impact Statement
OPCERT—Operational Certification
TDI—Tamper Detection Indicator
UL—Unauthorized Launch

Attachment 2

WORKING 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 responsible engineering agency and membership includes:

- Operational MAJCOM.
- Engineering MAJCOM-designated independent review agency.
- Air Force Security Police Agency.
- National Security Agency.
- HQ AFSA/SEN.

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 engineering MAJCOM designates a nuclear certification manager to chair this group and membership includes:

- Operational MAJCOM.
- Engineering MAJCOM-designated independent review agency.
- National warhead design laboratories (when appropriate).
- HQ AFSA/SEN.

A2.2. Nuclear Certification Plan. 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 used within a weapon system and associated support equipment. The NCP must include:

- 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.
- Allocation matrix that maps all applicable AFI 91-107-directed requirements to the equipment or system components.
- Specific methods to be used for compliance verification (proposed certification approach).
- 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).
- Schedule that includes major certification and program milestones.
- Responsibilities of each agency identified in the NCP.
- 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 engineering MAJCOM 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 AFSA/SEN and OPCERT and DECERT concepts.

A2.4. Nuclear Surety Evaluation. Evaluates items to be certified using the approved certification approach (as identified in the NSIS or NCP). The evaluation 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:

- Is of sufficient depth to ensure the nuclear surety evaluation is technically correct and complete.
- Specifically addresses the design requirements.
- 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. Nuclear Safety Cross-Check Analysis (NSCCA). An NSCCA supports the design certification process by identifying applicable AFI 91-107-directed criteria and verifying compliance. It also supports the OPCERT process by using an organization that is financially and managerially independent from the developing contractor to mitigate, through analysis and testing, the potential for UL threats and scenarios associated with the software. An 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.

Attachment 3

RECOMMENDATION FOR NUCLEAR SAFETY DESIGN CERTIFICATION AND SUMMARY OF ENGINEERING EVALUATION

A3.1. Certification Action. Recommend certification or certification with restrictions (to meet AFI 91-107-directed criteria).

A3.2. Item Identification. For hardware or software (as applicable) provide:

- Nomenclature or common name.
- National stock number (the number in use rather than the master number).
- Manufacturer and code.
- Model and part number.
- Computer program identification number.
- Item manager (include the functional address symbol and telephone number).

A3.3. Uses and Description. Provide information on:

- Equipment uses.
- Weapons.
- Weapon types (as considered in the analysis).
- Top-level description.

A3.4. Summary of Engineering Analysis (Evaluation and Test):

- Identify the specific AFI 91-107-directed criteria used in the design and evaluation process for the item.
- Discuss the certification approach used (compliance verification methods).
- Identify or reference the specific test and analysis procedures used.
- Summarize the results of the certification analysis, and discuss any discrepancies identified during the evaluation and their disposition.

A3.5. Recommended Restrictions. Recommend any restrictions needed to compensate for uncorrected design deficiencies or discrepancies.