ure from allowing bypass of the ignition safing device that would permit ignition when the device is safed.

2.2.2.4. Releasing. Operation of the release system for aircraft-carried weapons is controlled through two independent functions: the release system unlock command and the release command. Without the unlock command, separation of the weapon from the combat delivery aircraft will not occur even if the release command is sent. Design features must preclude accidental transmission of the unlock and release commands and must also prevent any failure from allowing bypass of the lock device that would permit release of the weapon when the device is locked. For air-launched missiles, the ignition system arm and the release system unlock must be separate and independent functions.

2.2.2.5. Arming. If the weapon is prearmed, arming will be the design response of the weapon to sensing that the environment is within the limits defined for operational use (after launch or release). Design features must include measurements of the environment so environments other than "intended use" are discriminated against to the greatest extent possible. If a missile has self-contained guidance, include a good guidance signal (paragraph **2.9.1.**) as a measurement of the proper operational environment. The armed condition allows the selected fuze signal (such as radar, contact, or timer) to detonate the warhead. Design features must preclude arming unless the proper operational environment is sensed; prevent erroneous transmission of the good guidance signal; and preclude bypass of the arming system that would permit nuclear detonation of the warhead without arming.

2.2.2.6. Targeting. Targeting is a critical function for ground-launched missiles. It includes the preparation, weapon system processing, and transmission of targeting data to missile guidance and arming and fuzing systems. Targeting data consists of the flight control and fuzing constants needed to deliver and detonate the weapons within the designated target area. The weapon system design must prevent erroneous targeting functions and accidental or unauthorized changes to targeting data.

2.2.3. Reversible Operations. Ensure the operation of devices for authorization, prearming, propulsion system ignition arming, and aircraft release system unlocking is reversible.

2.3. Critical Function Numerical Requirements. The numerical requirements specified in AFM 91-107 apply to ground-launched missile and combat delivery aircraft systems to show that, in normal environments, the calculated probability of occurrence of inadvertent prearming, launching, releasing or jettisoning, arming, or erroneous targeting of nuclear weapons is unlikely to occur during the system lifetime. Although numerical specifications for credible abnormal environments are only defined for DOE bombs and warheads, Air Force nuclear weapon system designers will incorporate positive safety features for these environments into the design of combat delivery vehicles to protect against inadvertent critical function activation.

2.4. Safety Features and Procedures. Ensure the nuclear safety features eliminate or minimize the dependence of safety and security on administrative procedures.

2.5. Explosive Ordnance Disposal. Design aircraft and missile systems to permit emergency access to those components and circuits required to carry out render-safe procedures. Develop render-safe procedures with the intent of meeting the numerical requirements of AFI 91-107.

2.6. Physical and Internal Security. According to the fourth DoD Nuclear Weapon System Safety Standard, a physical security system must prevent access to nuclear weapons and protect critical equipment and secure data. In support of the second DoD standard, nuclear weapon systems and nuclear weapons must incorporate internal security features to prevent unauthorized use.

2.7. Environmental Parameters. Consider nuclear safety design features over the full range of normal and credible abnormal environments to which the system could be subjected. Since specific normal and abnormal environmental parameters are system dependent, use the parameters specified in appropriate bomb and warhead STS and MC documents and in the weapon system specifications.

2.8. Safe and Arm (S&A) and Arm/Disarm (A/D) Devices. Ensure these devices meet the design criteria in MIL-STD-1512. If the devices are electrically actuated, they must arm only in response to an externally generated unique signal. The safing signal must differ from the arming signal to reduce the risk of arming during attempted safing. If a monitor signal is used, it must also be different from the arming signal.

2.9. Protection of Friendly Territory. Design weapon systems to prevent nuclear detonations, except within specified target boundaries.

2.9.1. Good Guidance Signal. Missile systems, including guided missiles launched from aircraft, must receive a good guidance signal from the guidance and control unit before nuclear warhead arming can occur. The good guidance signal must be withheld if a final guidance accuracy check shows the weapon will impact outside the specified target boundaries.

2.9.2. Target Boundaries. The boundaries for airborne release and delivery systems vary with the number of weapons, weapon yield and type, methods of use, geographical location, and operational needs. Consequently, the DoD weapon system program managers, with coordination from the operating command and the appropriate nuclear safety evaluation agency, must specify target boundaries.

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

2.11. Human Engineering. Design the system so no two independent human errors or acts will cause prearming, arming, launching, or releasing of a nuclear weapon in an operational weapon system or will authorize the use of a ground-launched missile system. This criterion applies only before initiation of actions required to complete the desired operation. The design must minimize the number of points within the system where human actions could degrade nuclear safety or security. The design must also stress positive measures to prevent deliberate unauthorized or accidental operation of controls that could degrade nuclear safety or security.

Section 2B—Automata and Software

2.12. General Design Requirements. These design safety criteria apply to automata and software that receive, store, process, or transmit data to monitor, target, prearm, arm, launch, release, or authorize the