SANDIA REPORT

SAND86–2955 • RS3151/87/004
~~Nuclear Weapon Data • Sigma 2~~
Specified External Distribution Only*
Printed February 1987

~~Secret~~

REDACTED COPY

~~Extracted pages~~
~~S-11, 11-22~~

A Review of the US Nuclear Weapon Safety Program – 1945 to 1986 (U)

RS 3151 87 004
THIS DOCUMENT CONTAINS
28 PAGES, COPY NO. 237
OF 240 COPIES, SERIES A
FOR ORG 3141

R. N. Brodie

REDACTED COPY

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

~~Classified by [illegible] July 7, 1982~~

~~CRITICAL NUCLEAR WEAPON [illegible] INFORMATION~~
~~DOD DIRECTIVE [illegible] APPLIES~~

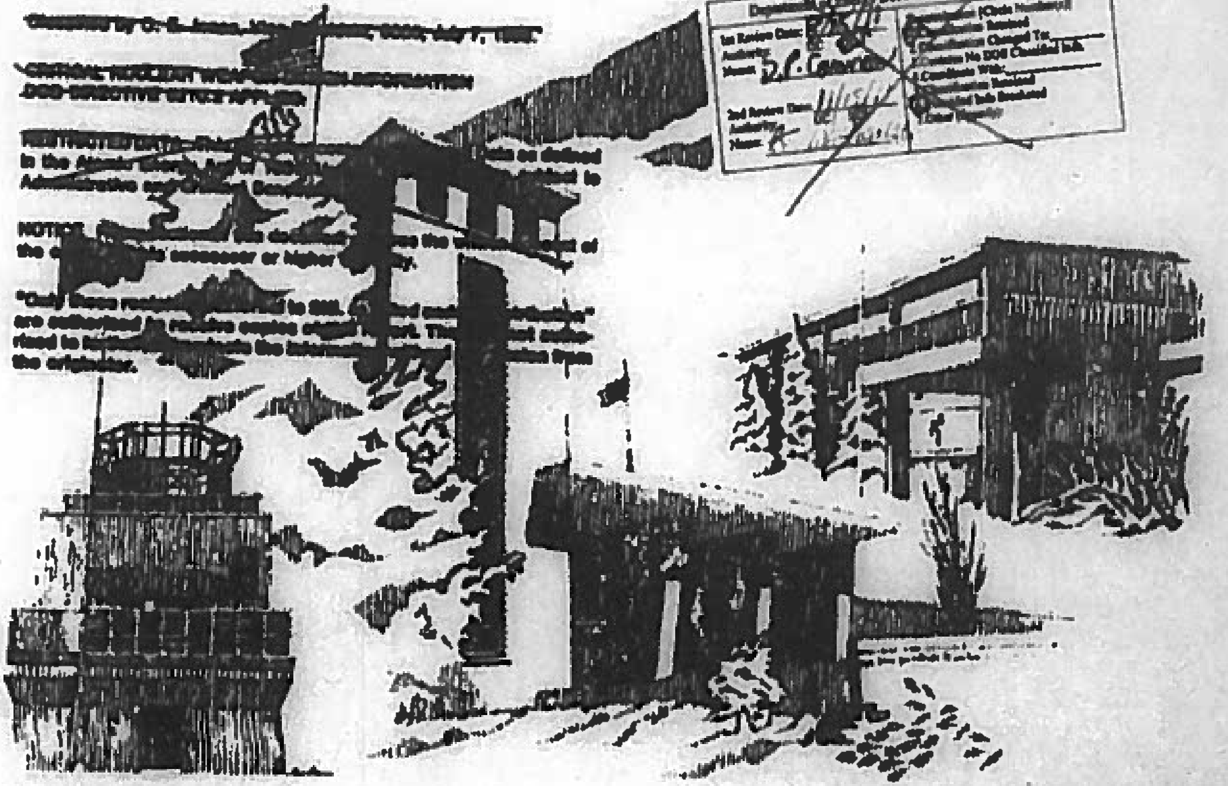
~~RESTRICTED DATA~~ [illegible] as defined in the Atomic [illegible] Administrative and [illegible]

NOTICE: [illegible] the [illegible] successor or higher [illegible]

*Only those [illegible] to SNL [illegible] are authorized [illegible] copies [illegible] rized to [illegible] the information [illegible] upon the originator.

~~2ND REVIEW DATE~~
~~AUTHORITY~~
~~NAME~~
~~D.P. Carson~~
~~CONTAINS NO DOE CLASSIFIED INFO~~
~~COORDINATE WITH~~
~~CLASSIFICATION CANCELLED~~
~~CLASSIFIED INFO BRACKETED~~
~~OTHER (SPECIFY)~~
~~DOS~~

~~Department of Energy Declassification Review~~
~~1st Review Date:~~
~~Authority:~~
~~Name: D.P. Carson~~
~~2nd Review Date:~~
~~Authority:~~
~~Name:~~
~~Determination (Circle Number(s))~~
~~Classification Retained~~
~~Classification Changed To:~~
~~Contains No DOE Classified Info~~
~~Coordinate With:~~
~~Classification Cancelled~~
~~Classified Info Bracketed~~
~~Other (Specify):~~



[redacted]

[redacted]

[redacted]

[redacted]/RD

SAND86–2956 • Nuclear Weapon Data • Sigma 2
RS3151/87/004
Specified External Distribution Only
Printed February 1987

Distribution
Category C–72

A Review of the US Nuclear Weapon Safety Program – 1945 to 1986 (U)

R. N. Brodie
Sandia National Laboratories
Albuquerque, NM 87185

Classified by O. E. Jones, Vice-President, 5000, July 7, 1986.

CRITICAL NUCLEAR WEAPON DESIGN INFORMATION
DOD DIRECTIVE 5210.2 APPLIES.

RESTRICTED DATA This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

NOTICE Reproduction of this document requires the written consent of the originator, his successor or higher authority.

SEC[redacted]

Intentionally Left Blank

Contents

Intentionally Left Blank

Introduction

The development of the nuclear weapon during World War II introduced a radically new instrument of national and international policy. Although to say that nuclear weapons are unique (immensely destructive, viewed with strong emotions, politically sensitive, etc.) is passe', not to acknowledge their special nature is nonsense. The continued existence and general deployment of nuclear weapons implies that decision makers and the general populace presume that they are exceptionally safe and secure. The intent of this paper is to present the essence of the US nuclear weapon safety program.

The term "nuclear safety" has historically been associated with prevention of an unintended nuclear detonation, which is often spoken of as "the blinding white flash" to emphasize the enormity of the consequences. Nuclear detonation safety will be the major focus of this paper; however, because of increased concern for radiation contamination, attention will also be given to fissile-material-scattering safety as well.

Since 1968, the nuclear detonation criteria that we have worked toward achieving through weapon design are that the probability of an unintended nuclear detonation* prior to launch (prior to receipt of the prearm signal in the case of bombs) shall not exceed:

> 1 in 10^9 per weapon lifetime for normal environments,
> 1 in 10^6 per weapon exposure for abnormal environments.
> (To give some sense of such probabilities, 1 in 10^4 is an estimate of the order of the probability of one or more Americans being struck by a meteor in a year.)
>
> There are no corresponding criteria for the scatter of fissile material.

"Normal environments" are defined to be those environments listed in the Stockpile to Target Sequence (STS) document wherein the weapon is required to function with full operational capability. Correspondingly, "abnormal environments" are defined to be those environments in the STS where the weapon is not expected to retain full operational capability, e.g., an accident.

In addressing the above two quantitative safety requirements for an implosion weapon, there are two distinctly different design considerations: keeping the warhead electrical system (WES) from supplying energy to the detonators when not intended, and preventing a high explosive (HE) detonation that was not initiated by the WES from giving a nuclear yield. For a gun type device, the concern is to prevent the two fissile components from assembling unintentionally, regardless of the energy source.

Partitioning the Safety Burden

Both the design of the nuclear weapon and the manner in which it is deployed can contribute to or detract from meeting the nuclear safety criteria. Active-alert deployments require weapons and weapon systems to be in a high readiness state. This requirement puts those weapons at greater risk of being involved in a significant accident environment and hence, from a national perspective, should require those weapons to "somehow be safer" than if they were not subjected to the active-alert deployments. Conversely, if a weapon were known to be unusually susceptible to detonation when exposed to a particular environment, then deployments having a significant risk of subjecting that weapon to the unfavorable environment would likely be denied.

In principle, the burden of meeting the nuclear safety criteria could be placed solely on the design of the weapon (i.e., any deployment mode would be allowed). The Fat Man implosion bomb of WW II might be considered such a design since it was not to be assembled until after an authenticated strike order had been received. In its unassembled state it was absolutely safe from a nuclear detonation

---

* Nuclear detonation is undefined in this usage. A nuclear yield equivalent to 4 pounds of TNT is used as a standard in one-point safety, to be discussed later.

viewpoint since in that form the fissile material was physically separate from the chemical high explosive. If the fissile material was stored a reasonable distance from the HE, its scatter was also improbable. In fact though, when assembled, Fat Man would be considered unsafe by any reasonable safety standards so that deployment restrictions (i.e., that it remain unassembled) were indeed a key factor in its nuclear safety theme.

Conversely, one could consider placing the burden of meeting the nuclear safety criteria for a nuclear weapon solely on the way it is deployed, without regard to weapon design. However, even permanent storage in vaults isolated from shock, electrical, and other environments would not be sufficient to meet the criteria if the weapon designer allowed a design that could experience either spontaneous initiation of the HE or activation of the firing system. Even in the most benign environments, attention must still be given in the design to nuclear safety considerations. The evolving relationships between weapon design and weapon deployments will be a continuing theme of this report.

Nuclear Safety - 1945 to 1968

Nuclear Design

Fat Man—With the 1946 Atomic Energy Act, the development and production of nuclear weapons rested with the Atomic Energy Commission (AEC), a government agency separate from the user, the Department of Defense. Until the mid-1950s, the custody of all fissile material was also vested with the AEC. Hence, in that time frame the design agency of the Fat Man in reality had full assurance that the user would not assemble the weapon prior to an authorized strike mission and thereby inadvertently subvert the nuclear safety design intent. The other type of WW II nuclear weapon, the Little Boy, was a gun type weapon (one of the two subcritical pieces of enriched uranium would be inserted along with a propellant charge while the aircraft was en route to the target).

Manually Inserted Capsules—From 1946 through 1948, we had a few tens of weapons, all bombs of the Fat Man or Little Boy design. The nuclear testing conducted in 1948 brought about a new concept: a removable capsule design where the fissile material would be DELETED DELETED could be inserted or removed manually from an otherwise fully assembled weapon. This design offered several advantages: (1) The assembled weapon without the capsule installed (called the weapon assembly) was absolutely nuclear safe, and the capsule could be inserted while on the way to the target and removed before landing if the mission was cancelled or aborted; (2) the reliability of the weapon assembly could be examined on a continuous basis; and (3) the time required to respond to a strike order was shortened considerably. The Little Boy, since it was a gun type weapon, had safety and operational deployment characteristics similar to the removable capsule implosion design.

DOE 6.2(a)

DOE 6.2(a)

Mechanically Inserted Capsules—With the advent of the Mk 5 DELETED nuclear weapons began being incorporated in DoD weapon systems as entities other than bombs. Beginning in 1952, the Mk 5 was fielded in the Matador and Regulus cruise missiles, and the Mk 7 DELETED. was incorporated into seven other-than-bomb weapon system applications. Since these were not manned systems, the capsules had to be placed in the weapon (which was within the missile or other weapon system) prior to launch. Since the Mk 7 bomb was small enough to be carried externally on a fighter aircraft, the same problem now existed for some bomb applications. The solution chosen was a weapon component named the In-Flight Insertion (IFI) device, which could hold the capsule in a position external to the HE sphere but would cause it to be physically inserted by an electrically operated screw jack. The IFI device could be operated while the weapon was en route to the target (and could be reversed prior to landing for the bombs), which seemed to preserve both the safety advantages gained by the Mk 4 and Mk 6 designs and the desired increased operational capability. However, the designer had intended that the capsules would be installed in the IFI device shortly before launch. He had not intended that they remain in the IFI device for long periods of time within an alert-ready missile or bomb because actual capsule insertion into the HE sphere was accomplished by operation of an electric

DOE 6.2(a)

DOE 6.2(a)

motor; thus inadvertent or accident-caused operation of the motor would bypass the major safety feature of the weapon.

Sealed Pits—In 1957, the first so called sealed-pit nuclear weapons entered the stockpile. These weapons did not use a removable capsule of fissile material but rather had the active material in a relatively thin spherical shell permanently sealed inside the HE assembly. The sealed-pit design offered several advantages over the capsule type design: (1) it required less fissile material, thereby allowing a larger stockpile with the existing quantity of fissile material; (2) it had less weight and volume for a given yield, or more yield for a given weight and volume; and (3) it required less maintenance and had higher system reliability. There were obvious disadvantages from a safety viewpoint: operation of the WES with the HE still intact would likely result in a nuclear yield, and most HE detonations (nonnuclear) would result in a scattering incident.

One-Point Safety and Mechanical Safing—Some of the first sealed-pit weapons were not inherently one-point safe.

[i.e., given that the high explosive is initiated at a single point, the inherent design of the pit and HE system is such that no significant nuclear yield will result. The modern one-point safety criterion (post-1968) is that there should be no greater than a one-in-a-million probability that, given a single initiation point in the HE, no greater than 4 pounds of TNT equivalent nuclear yield will result. The possibility that an accident would produce more than a single initiation point—not the result of fireset operation—with sufficient simultaneity and location to interact constructively or enforce the other is thought to be of the order of one in a million or less.]

DOE 6.2(a)

Several of these weapons were modified so that the last of their production run would be DELETED DELETED by the modern standard. Others—some of which were developed during the 1958–1961 nuclear testing moratorium—had sufficient foreign material placed in the pit to "dud" the device and provide mechanical safing. This material, DELETED , would be withdrawn from the pit during the arming process. The retracting mechanism was called an ANA (Actuator Nuclear Arming).

DOE 6.2(a)

DOE 6.2(a)

Nuclear Deployments

1946 to 1951—Nuclear weapons were not deployed in today's sense during this period. From 1945 to 1948, weapons of the Fat Man design, by then called the Mk 3, were kept unassembled, first at Los Alamos, DELETED and later in the National Storage Sites (NSSs). With their introduction in 1949 and 1951, respectively, the Mk 4 and Mk 6 bombs were eventually stored in the NSSs as weapon assemblies, but without the fissile material capsules. The capsules were stored in compartments that were physically separate from the weapon assemblies and also were in the custody of the resident AEC representative. In the 1950 time frame, heightened tensions between the West and the Communist countries, coupled with the desire on the part of the military to train with real weapons, resulted in transfer of many of the weapon assemblies to DoD control.

DOE 6.2(a)

1952 to 1956—International tensions continued to mount during this period, and nuclear weapons were developed and deployed for tactical use. Nuclear weapons with capsule designs having IFIs entered the stockpile in 1952. Nuclear weapons were incorporated into DoD missiles for the first time in 1952 with the Air Force Matador cruise missile application of the warhead version of the Mk 5. Smaller NSSs were constructed at each Strategic Air Command (SAC) main operating base, and custody of fissile material was gradually transferred to the DoD (this was by Presidential decision over the objections of the AEC). In mid-1956, SAC, in part due to heightened international tensions, began standing ground alert with some capsules installed in the IFIs.

1957 to 1968—SAC ground alert continued through this period. The introduction of land- and sea-based strategic missiles had reduced the several-hour strategic warning time (and hence strike preparation time) that existed with the all-aircraft-delivered threat to an hour or less (flight time of the missile). Thus, around-the-clock airborne-alert operations began in 1958. Large deployments of nuclear weapons were made to Europe, and Programs of Cooperation (POCs) which had been authorized under the Atomic Energy Act of 1954 and negotiated with our Allies were implemented. This arrangement ensured that the US retained legal custody of the weapon, but the weapon system (excluding the bomb or warhead/warhead section) was owned and manned by the Ally. Many of these POC weapons were placed on ready-alert status. Several accidents involving both capsule type and sealed-pit weapons occurred during this time (the majority were associated with airborne operations). The accidents at Palomares, Spain (1966) and Thule, Greenland (1968) received the most media attention because both involved the scattering of plutonium on foreign soil.

Firing Set Design

In this section we review the evolution, from the Fat Man era through 1968, of nuclear weapon electrical system safety components which predate the "modern nuclear detonation safety" philosophy of today's weapons. These features were incorporated to inhibit the warhead electrical system in an accident from delivering sufficient electrical energy to the detonators to cause their initiation. Since many weapons which were designed and produced prior to 1968 are still in active use, all of the features discussed below can be found within the stockpile.

Removable Components—Even though the prime nuclear safety theme of the Fat Man was to keep it unassembled (and thereby keep separate the fissile material from the HE) prior to receipt of a strike order, Fat Man also had what were called "red" and "green" plugs. The green plug interrupted the arming circuit until it was physically replaced with the red plug, which completed the arming circuit. Eventually, bombs had a removable component called a "strike enable plug" which served the same function as the "red" plug when installed and the "green" plug when removed. Several weapons, e.g., W30, B28, used the high voltage, thermally activated batteries as a removable component.

No Power Supply in the Warhead—Beginning with the W49 (first used on Atlas, Thor, and Jupiter), power was obtained for warhead applications from the weapon system, which meant there was no power supply capable of arming and firing the detonators within the warhead itself. When the warhead was separate from the weapon system, e.g., during most warhead logistic operations, the absence of internal power in the warhead provided a positive safety measure. Since the "requirements" (until about 1974) in the Military Characteristics (MCs) stated that the quantitative safety criteria, stated in the Introduction, were to be met in the absence of normal arming, firing, and test signals from the weapon system, lack of power in the warhead would serve, from a strictly legalistic viewpoint, as a similar positive measure in meeting the safety criteria when the warhead was mated to the weapon system.

Low and High Voltage Safing Switches—The motor-driven safing switches incorporated into bombs, called "ready-safe" switches, were operated by the pilot moving a control knob in the cockpit. Switches capable of holding off in excess of 2500 volts were required for those systems (e.g., W25, B28, W31), which had incorporated high voltage, thermally activated batteries. Systems which used low voltage power sources and some type of voltage step-up technique could use low voltage switches for the safing switch. Both high and low voltage safing switches had motor-driven contacts that would close when a 28-volt signal was applied.

Thermal Fuses—In the late 1950s, with the introduction of sealed-pit weapons, concern for the WES response during accidents, with their prevalent thermal environment, resulted in application of thermal fuses. Thermal fuses were components that were designed to provide an open circuit when exposed to temperatures exceeding some threshold level, say 320°F. The immediate application was to provide additional isolation of the high voltage, thermally activated batteries from the capacitor bank in a severe thermal environment (which could activate the batteries).

Environmental Sensing Devices—Concern developed over the realization that several existing weapons could be caused to detonate (giving a nuclear yield) by incidentally, accidentally, or intentionally supplying certain signals at the warhead connector. The W25 warhead associated with the Air Defense Genie rocket was such a weapon (later retrofitted). The same concern existed for other weapons when they were partially disassembled during maintenance operations. The design feature to counter this condition was a device which would detect some unique environment associated with the weapon having been irrevocably committed to use (e.g., acceleration force over a time during a missile launch, or deceleration over a time during parachute deployment of a bomb), which would then cause a motor to run, closing a set of contact points in the arming circuit. The feature was questioned by the Services on the grounds that if it was a safing device, it was not an AEC responsibility vis-a-vis existing agreements. The devices were eventually called Environmental Sensing Devices (ESDs) and incorporated by the AEC initially with a ground-handling safety rationale. In some systems, ESDs have also been incorporated by the DoD within their hardware.

Nuclear Safety Review Process

1946 to 1959—Until the introduction of sealed-pit weapons in 1957, there was essentially no institutionalized nuclear safety process or structure. This was simply the result of the perception that there was no need—nuclear safety during peacetime was demonstrably obtained through the separation of the fissile material from the HE in the case of implosion weapons and from separate storage of the two pieces of fissile material in the case of gun type weapons. Recall also that until the mid-1950s, fissile material was controlled by AEC custodians with the military delivery units having possession of only the weapon assemblies (the assembled weapon less the fissile material). The decision made by President Eisenhower in the mid-1950s to transfer custody of the fissile material to the DoD gave the Services operational control of the complete nuclear weapon. Thus, for the first time, it would be possible to mate the fissile material with the weapon assembly prior to receipt of a strike order without the involvement of the AEC, whose field representatives had been recalled following the Presidential decision. However, the impending introduction of sealed-pit weapons would make this issue irrelevant.

Beginning in 1957, the need gradually became evident for an institutionalized process in which an appropriate balance must be determined between nuclear weapon safety features designed into a weapon on the one hand, and the safety procedures associated with actual weapon deployment on the other, *and then* for this balance to be reviewed at appropriate times or events to ensure that the desired level of safety is still being achieved. This need was realized by both the AEC and elements of the DoD. Motivation on the AEC side grew from the realization that nuclear weapon deployments (such as loading the capsule in the IFI assembly, in 1956, in bombs on alert-ready aircraft) were being made without AEC involvement. Motivation from the DoD side came from the realization that they knew very little about the new sealed-pit designs soon to be introduced into the stockpile in large quantities (the absolute visual assurance of nuclear safety afforded by the capsule designs was missing).

In the 1957 – 1959 interval, the stockpile began to grow very rapidly and a nuclear weapon safety process gradually evolved. The DoD convened an Atomic Weapon Safety Board in 1957 with a Navy Captain (W. M. Klee) as the Chairman; several broad recommendations relative to weapon design were made. In the same year, the Air Force Special Weapons Center held three formal nuclear weapon safety studies for three new systems entering the stockpile. The AEC, in particular Sandia, participated in these three studies but was not an actual member per instructions of the Director of Military Application (AEC). In 1958, the Air Force established a permanent Nuclear Weapon System Safety Group (NWSSG). The Joint Chiefs of Staff (JCS) then determined that each Military Department would have the nuclear safety responsibility for each of its systems that employed sealed-pit weapons, but further recognized that some DoD-wide guidance was desirable. A mutually acceptable Joint Nuclear Weapon System Safety Group process was derived by an AEC/DoD Ad Hoc Steering Committee and subsequently documented in a 1960 DoD Directive (5030.15, now 3150.2).

Post-1959—DoD directive 5030.15 institutionalized what will be called the *nuclear weapon system safety* (qualitative) process. The deployment/design interface is examined from a safety perspective through this system safety process. The detailed *nuclear weapon design safety* (quantitative), on the other hand, is examined through the formal weapon development review process.

Nuclear Weapon System Safety (Qualitative)—The process detailed in 1960 remains essentially intact today and reviews the nuclear safety of a system from a broad perspective. It does not examine compliance with the quantitative nuclear safety criteria presented earlier; rather, the complete man-hardware-procedure system is evaluated against the following subjective standards (source DoD Directive 3150.2):

> There shall be positive measures to:
>
> 1. Prevent nuclear weapons involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield.
> 2. Prevent DELIBERATE prearming, arming, launching, firing or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority.
> 3. Prevent INADVERTENT prearming, arming, launching, firing, or releasing of nuclear weapons in all normal and credible abnormal environments.
> 4. Ensure adequate security of nuclear weapons, pursuant to DoD Directive 5210.41.
>
> There is no corresponding standard for the scatter of radioactive material.
>
> (NOTE: The term "prearming" refers to prearming the system for subsequent "arming, launching, firing or releasing of nuclear weapons," which were understood to be the commitment of the system to use.)

The term "positive measure" refers to a tangible design feature or procedural action whose existence is relied upon to ensure that the goal is met. As an aside, observe that from a broad system level perspective, security and control are included in the safety study process review, as may be noted by the second (control) and the fourth (physical security) standards.

Each of the Military Departments has a permanent Nuclear Weapon System Safety Study Group. There is one DOE member (Albuquerque Operations Office), and Sandia provides a technical advisor to that member. These groups conduct safety studies and reviews which provide (1) a judgment as to the adequacy of the positive measure to be in effect and (2) a draft set of proposed Nuclear Safety Rules. Safety rules outline the operational concept for the system, describe the system hardware, and prescribe procedures to be used. Safety rules are approved at the Cabinet level, and the President is notified of their issuance.

Nuclear Weapon Design Safety (Quantitative)—The nuclear safety design of a weapon is reviewed by several different groups prior to its entry into the stockpile. The design is evaluated against the quantitative nuclear detonation criteria previously presented. However, the most stringent review comes from within the DOE, in particular from the technical safety group within each laboratory. This group typically is independent from the project design group (at Sandia, the first common supervisor is the President). The DoD has its first direct involvement in monitoring the progress of design safety for the weapon through the chairing of the mandatory safety subgroup of the Project Officers Group (POG). The formal review by the DoD comes through the Design Review and Acceptance Group's (DRAAG's) effort to measure all design parameters against the stated MCs.

Accident Experience

The definition of a nuclear accident as contained in TM 4-1, *Glossary of Nuclear Weapon Materiel and Related Terms*, is "Any unplanned occurrence involving loss or destruction of, or serious damage to, nuclear weapons or their components which results in an actual or potential hazard to life or property."

This definition was expanded in the nuclear weapon reporting system to include:

> Accidental or unauthorized launching, firing, or use, by US forces or supported allied forces, of a nuclear-capable weapon system which could create the risk of an outbreak of war.
>
> Nuclear detonation.
>
> Nonnuclear detonation or burning of a nuclear weapon or radioactive weapon component, including a fully assembled nuclear weapon, an unassembled nuclear weapon, or a radioactive nuclear weapon component.
>
> Radioactive contamination.
>
> Seizure, theft or loss of a nuclear weapon or radioactive nuclear weapon component, including jettisoning.
>
> Public hazard, actual or implied.

Through May 1986, the US has had 32 such accidents, all now acknowledged to the public. Thirty-one of these accidents occurred either in 1968 or before.

The first official nuclear accident involved a Mk 4 weapon assembly (with a dummy capsule) which was jettisoned in Puget Sound from a B-36 bomber experiencing an in-flight emergency. None of the 32 accidents produced any measurable nuclear yield and only 5 resulted in radioactive contamination beyond the immediate accident site.

Because the definition of what would constitute a nuclear weapon accident was formulated at a time when any part of a nuclear weapon was highly classified and literally regarded with awe, events where no fissile material was present (or where only fissile material capsules were involved) were included. If we exclude accidents involving weapon components only and non-sealed pit weapons (unless the capsule was inserted in the pit or stored within the IFI) then the US would have counted only 19 nuclear weapon accidents.

Since accidents usually occur during human operation of equipment, most of the accidents have taken place during ground- and airborne-alert operations. Of the 32 accidents, 29 have been with weapons which were in Air Force custody. This does not imply a cavalier attitude on the part of the Air Force, but rather that the preponderance of alert-ready weapons have been associated with Air Force systems. In fact, because of the number of accidents handled by the Air Force, their reporting chain for safety matters is exemplary in that it is within the Inspector General's office and the Inspector General (a Lieutenant General) has direct access to the Air Force Chief of Staff, independent of the major operating commands.

Considerable insight may be gained by a review of a few of the more troubling accidents without attempting to detail each individual one.

Bunker Hill AFB, 1964—A B-58 bomber on active alert with two B43 bombs externally carried under each wing and a B53 bomb in the centerline pod skidded on ice while taxiing onto the runway for a simulated takeoff during an exercise. The aircraft left the runway, collapsing the landing gear, and began to burn. Two of the B43s were crushed by the aircraft wing box while being subjected to a fuel fire at the same time that the lower halves of the bombs were immersed in melted-snow water. Aircraft power was available and potentially present at any external connector. The HE of these two B43s, although directly exposed to the fire, did not detonate even though the weapon's electrical system was badly charred. The other two B43s and the B53 were shielded from direct effects of the fire and were relatively undamaged. The aircraft was a total loss.

Goldsboro, NC, 1961—A B-52 flying alert with two B39 bombs experienced a ruptured wing-fuel-tank and broke up over Goldsboro, NC. Before the accident, the manual arming pin in each of the bombs was in place. Although the pins required a horizontal movement for extraction, they were both on a lanyard to allow the crew to pull them from the cockpit. During the breakup, the aircraft experienced structural distortion and torsion in the weapons bay area sufficient to pull the pin from one of the bombs, thus arming the Bisch generator. The Bisch generator then provided internal power to the bomb when the pullout cable was extracted by the bomb falling from the weapons bay. The operation of the baroswitch arming system, parachute deployment, timer operation, low and high voltage thermal batteries activation, and delivery of the fire signal at impact by the crush switch all followed as a natural consequence of the bomb falling free with an armed Bisch generator. The nonoperation of the cockpit-controlled ready-safe switch prevented nuclear detonation of this bomb. The other bomb, which free-fell, experienced HE detonation upon impact. One of the secondary subassemblies was not recovered.

Ellsworth AFB, 1964—A maintenance team was dispatched to check the security system at a remote Minuteman launch site. The procedure involved pulling a fuse to reset the system after each check. The team found that they had failed to bring a fuse-puller with them, and since it was a considerable distance back to the base, they elected to use a screwdriver to remove the fuse. While they were attempting to remove the fuse after two successful tests, there was a violent explosion. The Mk 11 RV containing a W56 warhead fell approximately 75 feet to the floor of the silo. The RV sustained significant damage, but the warhead high explosive did not detonate and no nuclear yield or radiation contamination resulted.

Palomares, Spain, 1966; Thule, Greenland, 1968—Both these accidents involved an airborne-alert B-52 DELETED At Palomares, the B-52 collided with its KC-135 tanker and both aircraft crashed. The bombs separated from the aircraft; two of them free fell and the other two descended with partially deployed chutes. The two free-falling bombs detonated low order upon impact. There was no nuclear yield, but radioactive contamination over a fairly large agricultural area resulted. The two partially retarded bombs landed without significant damage: one on land and the other in fairly deep water. At Thule, the B-52 experienced a fire. The crew successfully bailed out over Thule AFB and the aircraft eventually crashed on the icecap; all four bombs detonated. While there was no nuclear yield, significant radioactive contamination did occur.

DOE
(b)(1)(a)

Summary—1945 to 1968

Until the mid-1960s, there really were no unresolved nuclear safety issues. Nuclear safety was achieved in a visible and almost absolute manner by ensuring that the fissile material was kept physically separate from the HE and that gun type devices remained unassembled.

The decision to go to an all sealed-pit stockpile and alert deployments was made for the overriding reasons mentioned earlier, but the full impact on nuclear safety was not duly considered or immediately recognized. The late 1950s and early 1960s saw considerable remedial activity in trying to address adequately nuclear detonation safety for sealed-pit weapons and their widespread alert deployments. These activities included application of those firing set features previously discussed and both mechanical safing and inherently one-point safety designs of the nuclear subsystem. It was also in this period that the need for a nuclear weapon system safety process was realized and slowly formulated. While continued weapon system incidents and accidents indicated some problem areas of concern, concerted hardware reviews uncovered others. For example, recognition that power levels of search radars and communications transmitters were increasing (e.g., on aircraft carriers) was cause to review the stockpile for susceptibility to electro-magnetic radiation (EMR), with one nuclear weapon type being retrofitted by the AEC on an urgent basis to replace the electroexplosively operated, ready-safe switch with one not susceptible to EMR.

Beginning in 1961, essentially all of the stockpile was retrofitted to include environmental sensing devices as a measure to prevent intentional or accidental detonation of a warhead in other than the intended-use mode.

After this rather frantic period, the mid-1960s were rather static with respect to nuclear safety. This was due in part to the relative inactivity in new weapon development work during that time and a perception that the existing safety features and review process were sufficient.

1968 may be viewed as the beginning of a transition between what might be called "old" safety and "new," or "enhanced" nuclear safety. We will see that some of the features which were incorporated as safety measures and which were based on then current design practices would not have provided the level of protection in certain accident environments for which they were given credit.

SECRET

Nuclear Safety - 1968 to 1986

A Time for Reflection

New Criteria—While strategic airborne alert was discontinued shortly after the Thule accident, the prime motivation for termination was the cost of the operations and the competition for those asset, from the rising commitment in Vietnam. However, the Palomares and Thule accidents did cause a number of individuals within the weapons program to begin reexamining the weapon design safety and deployments issue.

The first significant step taken was to look at the existing nuclear detonation safety criteria. While the majority of the stockpiled weapons had been designed to meet a quantitative "premature" nuclear detonation criteria of from 1×10^{-5} to 1×10^{-4}, there was general misunderstanding or uncertainty as to what the dimensional units were—and hence what the numbers represented. For example, if the units were the probability of having a nuclear detonation per weapon per year, then the fact that we had over ten thousand weapons would mean that the probability of having a nuclear detonation over a period of a year would be somewhere between one in ten to one in a hundred—obviously not acceptable. The key to the *dilemma* was in *finally* recognizing that a weapon could exist in only one of two types of environments, one bounded and the other unbounded:

(1) Those environments anticipated by the user and the designer and for which the weapon is expected to retain its full reliability. These are called "normal" environments.

or

(2) Those environments in which a weapon is no longer expected (required) to retain its full operational reliability. These are called "abnormal" environments.

Criteria were jointly formulated during late 1967 and early 1968 within the AEC and DoD and documented in letters from the Chairman, Military Liaison Committee, to the Assistant General Manager for Military Application, AEC.

These criteria, given earlier in the Introduction, are called the "modern" nuclear detonation safety criteria. The probability of an unintended nuclear detonation for a weapon exposed to normal environments is to be no greater than 1×10^{-9} per weapon over its lifetime. If all weapons met this criteria for normal environments, the risk of nuclear detonation per year for a ten thousand plus stockpile would be no greater than of the order of one in a million, assuming the lifetime for a weapon is of order of ten years.

For a weapon exposed to environments that are abnormal, i.e., given that an accident has occurred, the probability of an unintended nuclear detonation is to be no greater than 1×10^{-6} per accident. Note that for abnormal environments, the number of weapons affects only the accident rate, not the probability of a nuclear detonation given that the accident has occurred. We have seen that the annual accident rate averaged over the life of the weapons program is a little less than one per year. Using this historical accident rate (but realizing that the rate over the last two decades is only about one per ten years), we see then that the annual risk of a nuclear detonation from abnormal environments is also no greater than of the order of one in a million. In this sense, the two criteria "numbers" are consistent, but we will see they can require quite different means for achievement.

Search for New Understanding—In 1968, Sandia Laboratories established a safety assurance program to study and understand the implications of designing nuclear weapons for safety in abnormal environments. A detailed retrospective examination of nuclear weapon accidents and incidents, concurrent with hardware and technology analysis and testing, indicated that then extant design practices could not be shown to predictably meet the new abnormal environments criterion. For instance, the low and high voltage safing switches mentioned earlier were open contact points which would be closed by running a motor. The motor and its controlling switch were typically operated by the presence of 28 volts DC on a wire from the weapon system. There were documented cases of these safing switches being operated to the closed, or "arm," position by faults within the weapon system (when not exposed to accident

~~SECRET~~

environments). Since any 28-volt DC source could cause the motor to run, how could one argue that in severe environments 28 volts DC would never be applied to that wire, which might be tens of feet long?

If the retarded bomb in the Goldsboro accident had experienced inadvertent operation of its ready-safe switch prior to breakup of the aircraft, a nuclear detonation would have resulted.

The value of not including in the warhead a power source sufficient to fire the warhead detonators is small if the warhead is mated to an alert ready weapon system which does include such a power source. Likewise, a thermal fuse was designed to open at relatively low temperature, but testing showed that when the temperature was increased substantially above that level, the fuse material could flow back together and form a current-carrying bridge. ESDs are designed to detect a particular environment which the weapon would (presumably) experience only after being irreversibly committed to use. If the warhead were to "see" this environment during the accident, then there is a good likelihood that the ESD would function (as designed, but in this case not as desired). Whenever 28 volts DC was present on the correct wire, the fissile capsule stored within an IFI device would be inserted into the pit, or the foreign material would be extracted by the ANA mechanism in mechanically safed systems. Obviously, an electrical fault could supply the requisite power.

A great deal of testing and analysis was done to increase the understanding of how materials, components, etc., react in a wide range of abnormal environments. Simple questions such as "how far apart do two wires have to be in order to ensure that they could never be interconnected?" or "can one use standard fault tree analysis to determine predictability of a system as then currently designed?" had disconcerting answers. In the first case it is not possible to specify a "safe" distance. In the second, recall the Ellsworth accident; a typical missile system safety fault tree would not have included the silo's physical security circuits.

The continued accumulation of knowledge of how materials and systems react in severe environments led Sandia to the realization that it is simply not feasible to prevent electrical faults from occurring in a weapon system when it is exposed to abnormal environment conditions, and that simple electrical faults could operate then existing safety subsystems. In addition, it was observed that with then existing hardware, current methods of analyzing weapon systems exposed to abnormal environments were inadequate to predict probability thresholds for a nuclear detonation. In fact, the hardware response itself was not predictable in abnormal environment exposures.

Concurrent with the concerted WES safety efforts, Sandia, with Los Alamos participation, looked at changing bomb case designs as an approach to reducing the likelihood of radioactive contamination due to an aircraft accident (such as Palomares and Thule). While there was considerable weight penalty associated with such an approach, it showed that it was possible to mitigate the susceptibility of air-delivered sealed-pit weapons to scattering radioactive material when involved in accidents.

With these realizations, in 1970–71, the need for fresh safety design approaches was clear, both in nuclear detonation safety and radioactive contamination safety.

A New Nuclear Detonation Safety Design—A WES design that would make the response of nuclear weapons more predictable when exposed to abnormal environments had to address several then known response deficiencies. Some of these major deficiencies were that (1) safing subsystems were designed to operate when 28 volts DC was present on a line; (2) safing subsystems were in effect an interrupt in an arming line, and hence the function could be bypassed by faults completing the arming circuit independent of the safety subsystem; (3) single faults could bypass, or cause to operate, more than one safety subsystem (negating the independent subsystems concept).

The following design considerations began to crystallize:

- Since it would be very difficult in abnormal environment conditions to prevent faults from occurring throughout a weapon/weapon system, then to prevent bypass of the function itself the safety subsystems should be located as close as possible to the firing system with their input-output lines protected in some fashion against interconnection.
- Operation of a safety subsystem should require more than a 28-volt DC presence on a line; rather some uniquely human action if possible.
- Independence of safing systems and their initiation stimuli must be zealously preserved.

- There should be at least one component whose operation is essential for the WES to fire the weapon detonators and which can be shown to predictably fail in very severe environments before the safing subsystems fail.

The safety design concept which evolved from the above attributes involves an "exclusion region," "unique signals," "strong links," and "weak links."

- The exclusion region is a closed volume, formed by a barrier material having special properties (good fire and crush resistance, etc.) and containing a few detonation-essential components (including the weapon detonators). The purpose of the exclusion region is to isolate nuclear detonation-essential components from abnormal environments.
- The unique signals are constructed to contain information of sufficient complexity so that the probability of their being duplicated (generated) in an accident environment is less than one in a million.
- The strong links are components which control (deny prior to receipt of the proper unique signal) entry into the exclusion region of energy to arm or fire the firing set.
- The weak link is a component whose operation is essential for a nuclear detonation to occur but which can be shown to fail predictably and irreversibly for environmental levels which are less severe than those for which the barrier and strong links can be shown to retain their full integrity (for a firing system with a capacitor discharge unit, the capacitor can be an excellent thermal environment weak link).

The design intent for what we will call the "modern" nuclear detonation safety theme follows:

> Since false signals and potential bypass conditions may be present throughout a system in abnormal environments, attention should be focused on a relatively small portion (volume and number of components) of the system. Protect a few detonation-essential components from false signals and potential bypass conditions by placing them in an *exclusion region*. Allow direct electrical communication with the components within the exclusion region only through *strong links* which can be operated only by *unique signals* generated outside the system. And finally, protect the concept from catastrophically severe environments which would eventually breach the exclusion region barrier or strong links by colocating *weak link* components which can be shown to predictably fail prior to the barrier or the strong links losing their integrity.

A New Radioactive Contamination Safety Design—The Los Alamos and Lawrence Livermore laboratories investigated nuclear system designs which could reduce the likelihood of radioactive contamination in accidents such as Palomares and Thule. Rarely is it possible to make a step-function improvement in some area without causing a commensurate decrement in another. The decrement associated with the introduction of sealed-pit weapons was the immediate increased burden placed on nuclear detonation safety, and the complete loss of radioactive contamination safety in accidents where the weapon's HE detonates.

Similarly, steps taken to reduce the likelihood of scattering fissile material from that of then existing sealed-pit designs were expected to have a negative impact on some other attribute.

Several exploratory development programs were pursued. Included were:

- New concepts for an insertable nuclear component (a modern capsule design).
- "Paste" HE (pit suspended within a void with the paste HE stored elsewhere in the weapon—on command, the paste HE would be transferred to the void surrounding the pit).

DELETED

DOE
6.2(a)

- "Insensitive high explosive" (IHE), (a high explosive much less sensitive to impact and temperature insults than then current weapon explosives—used to replace the "normal" HE in sealed pit designs).

All of the above design alternatives had weight and volume penalties and most would require somewhat more fissile material and introduce additional reliability considerations. IHE involved the least perturbation to sealed-pit weapon designs and had the least impact on the DoD weapon system, even though it is only about two-thirds as energetic as existing conventional nuclear weapon explosives. IHE has been included in six of the last nine weapons to enter the stockpile.

A New One-Point Safety Understanding—Since the mid-1960s, the DoD had included in the MCs the statement that one-point safety should be achieved inherently in the nuclear design itself rather than through the use of mechanical safing. The entry of the B61-0 tactical bomb into the stockpile in 1967 was almost coincident with the revised definition of nuclear detonation criteria.' When the DoD reviewed the bomb to determine whether to accept it as a standard stockpile item, they noted that in meeting the desired one-point safety probability, the probability of the weapon being detonated at a particular point (the one giving the highest yield) had been included (used in the calculation). The DoD asked that the weapon be redesigned so that it would meet the 4-pound TNT equivalent/one in a million criteria for initiation at any point in the HE. Adjustments were made in the B61-0 nuclear design, and it entered the stockpile in 1968 having been certified as one-point safe under this new understanding. Meeting the "new one-point safe criteria" did not require new technology development, but rather was a clarification that accident-related probabilities would not be included.

A Stockpile Initiative

Review of the Stockpile—By the 1972-73 time frame, the new safety designs were ready to commit to new weapon programs as they entered into Phase 3, Engineering Development.' An internal review of stockpiled weapons and their deployments led Sandia, in 1974, to question the continued usage of certain weapons which had demonstrable abnormal environment susceptibilities on continuous alert. Deployments of particular concern were the older strategic air-delivered bombs, and warheads on ground alert. Eventually, a joint DoD/DOE safety study of the stockpile was undertaken. This review was co-chaired by the Director of Military Application and the Deputy Assistant to the Secretary of Defense for Atomic Energy. The study began in May 1975 and was completed in mid-1977. As might be expected since no weapon then in the stockpile had either IHE or the modern nuclear detonation safety features, the study concluded that for every weapon there were some abnormal environments in which the probability threshold for a nuclear detonation was simply not predictable.

Herein was a complex dilemma. On the one hand, it could be argued that there was cause to replace the complete stockpile, or at least all alert weapons, on an expedited basis. In the 1950s this would have been relatively easy to accomplish since rapid changes in technology and the perceived external threat resulted in regular weapon replacements (the average age of the stockpile did not exceed 2.7 years until 1963). By the 1970s, yield-to-weight and yield-to-volume ratios had been almost constant for a decade and the perceived need for either additional, or replacement nuclear weapons was low. In fact, since 1967, considerably more weapons and weapon systems have been retired than were produced. In the mid-1970s, for the first time, the nuclear weapon program had to compete for funding with conventional weapons and increasing social spending commitments.

On the other hand, one could take an historic viewpoint. Even though there had been numerous accidents and incidents involving nuclear weapons and the weapons of concern had been in the stockpile for many years, there had never been an unintended nuclear yield. Hence, as long as the weapons of greatest concern were programmed for eventual replacement (which could include desired safety improvements), there was no need for immediate action.

However abnormal-environment safety probabilities are not expected values. They are thresholds of risk which should not be exceeded. The technology investigations leading to the new safety designs had found that then existing hardware in the stockpile could not be shown to predictably meet the desired safety thresholds for all environments. The fact that the hardware could not be shown to meet the desired criteria also implied that it could not be analytically shown how "unsafe" it was. This is a very different situation from that which exists for reliability. When a weapon's reliability estimate falls below its desired threshold, that same estimate would be used to evaluate whether the weapon system should continue to be deployed as is or corrective actions should be undertaken.

The unpredictable nature of existing designs, when exposed to abnormal environments, unfortunately do not lend themselves to the cost-benefit analyses that decision makers desire before committing dollars to corrective actions. Hence the prevalent response to the DoD/DOE stockpile safety study was either "let the situation improve gradually as new weapons enter the stockpile" or "do more studies."

Stockpile Improvement Program—{There were a few within Sandia, those closest to the hardware and its implications, that were not comfortable with the laissez faire handling of the safety study conclusions. Intimate knowledge of the hardware which could be affected in abnormal-environment conditions, and full understanding of the national implications if it should be so affected, lent a certain urgency to their motivation. In the fall of 1977, a study to identify and prioritize the stockpile concerns—and to develop a time-phased corrective program—was begun. The study recommended that four nuclear weapons/weapon systems be addressed on a time-urgent basis because of nuclear detonation safety concerns. A second set of systems was recommended for corrective action over a ten-year period.

The Sandia study was modified slightly within DOE and transmitted to the DoD in September 1978. The DoD accepted the study in principle in March 1979. However, only two of the weapon systems were approved for immediate implementation; the remaining ones were delegated to further study and consideration. The most far-reaching proviso of the DoD concurrence was that all modifications or retrofits suggested by the study should be accomplished on a "no competition with new weapons in production" basis. In an era of increasing competition for scarce resources, this proviso delayed, and constrained severely, the hardware modified through the program.

{Three weapon systems are being retrofitted with modern nuclear detonation safety features. The B28 strategic bomb and the W31/Nike Hercules (both priority one systems in the study) are being modified in the field by the DoD with retrofit kits provided by the DOE. The B61-1 strategic bomb is being factory retrofitted for both modern nuclear detonation safety and radioactive contamination safety (IHE). All three of these systems are also receiving a modern use control device.}

{Additionally, concerns expressed in the original DOE study for several other systems have been met by early retirements and redeployments. It is reasonable to conclude that the concerns raised in the stockpile improvement study influenced the following stockpile deployment changes:

W25/Genie	Early retirement
W31/Honest John	Early retirement
B43/Strategic & Tactical bomb	Modern B83 and B61-3,4 bombs substituted, as they became available, for alert deployments
W44/ASROC	No above-deck storage allowed except in increased states of readiness
B53/Strategic bomb	Withdrawn from normal peacetime alert prior to placement in strategic reserve
W53/Titan	Alert status discontinued, placed in strategic reserve
W54/SADM	Withdrawn from Europe
B57, B61-0,2,5/ Tactical bombs	Modern B61-3,4 bombs substituted, as they became available, for alert deployments

Thus the other two priority one systems of concern (W25/Genie and B53) were accommodated by adjustments in their deployments rather than through hardware modifications. Of the total of 17 priority two systems in the Stockpile Improvement Study, the concerns raised have been addressed for 11: one through a factory retrofit, four through redeployment/retirement actions, and six through the introduction of new war reserve weapons. The major concerns for two of the remaining six systems were in the area of use control and security, and are being alleviated to a large extent through security upgrades. The remaining four systems of concern remain in essentially their 1978 state. No retrofit actions had been recommended for these six systems because each had been scheduled to be replaced by new weapon systems, which for various reasons has not occurred. However, without question the stockpile is in an improved position relative to nuclear safety vis-a-vis 1974.

What Is the National Risk?

Discussion—Even though one would prefer it to be otherwise, once a nuclear weapon is assembled, there exists a nonzero probability that it could be unintentionally detonated—particularly if it should be exposed to severe abnormal environments which might be present in a weapon system accident. An unintentional nuclear detonation would be such a catastrophic event that one would presume that every possible measure to prevent its occurrence would be taken. Before pursuing this thought further, we should review the reasons for having nuclear weapons in the first place.

From 1945 into 1948, the US retained a relatively modest number of nuclear weapons, and in view of its monopoly of nuclear weapons, a small number was deemed to be conservatively sufficient to deter gross misbehavior on the part of our potential adversaries. However, beginning in 1948 with the Berlin Blockade, the Communist overrun of mainland China and the Soviet test of their first atomic device in 1949, and then the invasion of Korea in 1950, the US felt threatened from both actual Communist excursions and their declared intentions for world domination. Communist potential for fielding very large conventional land armies increased our concern. The US had little desire to maintain a sufficient conventional force structure (from either an economic or sociological perspective) to match the Communists' conventional forces and hence chose to try to deter the Communist threat by intimidation with a superior force of nuclear weapons, which could be produced and maintained with a smaller cost in dollars and manpower. With the advent of the Soviet thermonuclear test in 1953 and Sputnik in 1957, US technological superiority began to be in doubt, or at least questioned. The United States sought to maintain its superiority by building a larger stockpile and maintaining a percentage of its weapons on immediate alert (to prevent a "strike out of the blue" from disarming us). Here lies the tie with nuclear detonation safety discussed earlier in this report. It is the perceived need to keep weapons fully assembled and deployed on combat-ready systems that prevents us from claiming, in an absolute sense, that we take every action, short of not building nuclear weapons, to ensure their safety. However, nuclear weapons are not built just to be kept safe. They are built to support national policy and national security objectives, specifically nuclear deterrence—which since the mid-1950s have been interpreted to require that nuclear weapons be deployed on alert-ready systems. Consequently, design safety must bear a large portion of the safety burden.

We have seen that the quantitative safety criteria (previously discussed under New Criteria) for weapons operating in normal environments and for weapons exposed to abnormal environments produce about equal annual risk of a nuclear detonation with threshold values of about one in a million. Again, these are not expected value numbers, but threshold values not to be exceeded. These criteria were determined in 1968 after the Palomares and Thule accidents. The logical question today might be: *Are these still the correct values or should we be trying to design nuclear weapons to a no greater than 1 in* 10^7 *or 1 in* 10^8 *probability of a nuclear yield for abnormal environments instead of the current 1 in* 10^6*?* and, *Could weapons be designed that would meet more stringent criteria?*

Conversely, one might suggest that since only one nuclear weapon accident has occurred since 1968, the abnormal-environment nuclear detonation criterion could be reduced by an order of magnitude to refelect the order of magnitude reduction of the accident rate for this period relative to the historical rate. This course is probably ill advised, particularly in light of the Challenger space shuttle accident. Although nuclear weapon *accidents* have been considered in this report, nuclear weapon *incidents* have not been discussed. As should be expected, there have been many more incidents than there have been accidents, and the actual consequences of these incidents have been relatively minor (at least with respect to the nuclear weapon itself). However, many of the incidents have had the potential for significant national impact. One such *incident* occurred on September 15, 1980, at Grand Forks AFB,

North Dakota. During a cartridge start for an alert exercise, an alert-configured B-52G (four B28FI
bombs in the forward weapons bay and eight W69/SRAM missiles in the aft weapons bay) experienced a
fire in the number 5 engine. The fire was fought for three hours before the fuel flow to the engine pod wa
shut off and the flames extinguished. A 30-knot wind was fortuitously blowing in the direction which
kept the flames from enveloping the wing and damage was restricted to the engine pod and leading edge
of the wing, with only minor damage to the fuselage skin. The weapons were not damaged. Three day
later, the Titan II/W53 accident at Damascus, Arkansas occurred.*

What Should the Criteria Be?—The public views risks differently than does a statistician, an
the perception and acceptance of risks is a very subjective and sometimes emotional issue. For instance,
the benefit that is received may persuade one to "overlook" the risk. However, if there is no personal ben-
efit, then little risk may be tolerated. If the risk involves "acts of God," concern and reaction should the
event actually occur will likely be very different than if it is caused by a person, corporation, or
government. For example, people continue to build residences near airports and on beaches, but after a
hurricane one does not hear serious cries demanding that the beach be closed, as has happened after a
major air crash adjacent to an airport. Events which involve spectacularly visual consequences or major
loss of life will be viewed differently from events with one or a few casualties, e.g., the space shuttle
explosion or the Bhopal, India chemical leak vis-a-vis one-car or two-car traffic fatalities.
Equally subjective is the way that quantitative probabilities for occurrences having serious conse-
quences are perceived. It seems that a one-in-a-million occurrence is viewed as being incredible in that
people may not be aware of its happening, or think that it would happen only to the "other person."
Although people take note of a one-in-a-hundred-thousand occurrence, such as a drowning, a blow from
a falling object, or an aircraft accident, only a few actually alter their lives in response to such a risk (e.g.,
refusing to travel by air); most do not. When the probability of being killed is on the order of one in ten
thousand, most people are willing to spend money—as long as it is public money—to decrease the
hazard. For example, fences are built to prevent falls and safety campaigns are waged with public
approval. Few hazard levels of one in a thousand exist for the population since most are willing to spend
their own money and effort to correct or eliminate them. This level of hazard for an event of serious con-
sequence *appears not to be* acceptable to anyone.
Given the assumption that an accident has occurred, then consideration of criteria (threshold values)
smaller than 1 in 10^6 for abnormal environment nuclear detonation safety would be almost surrealistic.
One in a million occurrences are about at the outer limit of what humans can personally observe (or com-
prehend) in nature, and as mentioned earlier, most would presume such occurrences would not happen,
at least in their lifetime. It is likely that those who would propose changing the criteria to 1 in 10^7 or 1 in
10^8 are, in fact, seeking assurance that the occurrence can never happen (probalility of zero), and this is a
common public misconception. Since events with a nonzero probability of occurrence really do happen,
if the motivation for making the criteria more stringent (reducing the probability for occurrence) is to
ensure that an unintended nuclear detonation cannot occur, then quantitative criteria should be
replaced by absolute statements of intent (with the implications presented below). Carrying this line of
reasoning a little further, if nonzero quantitative criteria remain desired, then the criteria should be at
least as stringent as *1 in 10^6* (for abnormal-environment *nuclear* detonation safety), and philosophically,
1 in 10^6 is sufficient in that it is viewed as being nearly incredible. We will see in the following that 1 in 10^6
is about the best we can do with sealed-pit weapons.

Can More Stringent Criteria Be Met?—Credibilty that can be attributed to the judgment of
an analyst depends on his experience, etc. Probabilities of 10^{-8} or less are beyond human capability or
experience, if not beyond human understanding. Thus, one may say categorically that if there is no
empirical evidence that will support a probability of 10^{-8} (or less), then no such probability should be
claimed. It is very expensive and difficult to conduct sufficient testing to obtain data that will support

---

*This accident involved a Titan II missile having a Mk 6 reentry vehicle/W53 warhead. The missile developed a
propellant leak which led to the destruction of the missile and missile silo and the ejection of the warhead several
hundred feet from the silo. There was no nuclear yield or radiation contamination although the warhead was
extensively damaged.

component performance probabilities in abnormal environments at the 1 in 10^3 level, much less 1 in 10^6. Therefore, multiple safing subsystems are incorporated and shown to be independent of common failure paths in order to achieve threshold levels of 1 in 10^6. That is:

> If we let ND represent an unintended nuclear detonation, and SS1 and SS2 two abnormal-environment safety subsystems, then the probability of an unintended nuclear detonation, P(ND) is given by,
>
> $$P(ND) = P(SS1) \times P(SS2),$$
>
> where P(SS1) and P(SS2) are the probabilities that SS1 and SS2 will fail to perform their safing functions. Note that the equation holds only if P(SS1) and P(SS2) are independent of each other. Now if we can show that the probabilities of failure for each of the two safing subsystems are of the order of 10^{-3} or less, then we may conclude that the probability for an unintended nuclear detonation is no greater than 10^{-6}. The problem, of course, is that great care must be taken that some single event was not overlooked which has a probability of occurrence of say order 10^{-5} or less and which could cause both SS2 and SS1 to operate.

That is the real problem of trying to design to criteria exceeding 1 in 10^4. Since it is impractical to prove a piece of hardware has a failure probability of that order, multiple independent subsystems would be needed. For the same reasons, it is difficult to prove that some event having smaller probability than that of each of the independent subsystems but greater than the criteria which would either compromise the independence of the subsystems or cause a nuclear detonation directly does not exist.

The preceding discussion might suggest that little or no progress has been made in nuclear detonation safety design since the introduction of the enhanced theme involving the exclusion region, strong links, weak links, unique signals, and IHE in the early 1970s. While that design philosophy is still operative, several significant improvements in its implementation have evolved. Instead of the requirement for transferring electrical energy via mines through the exclusion barrier in order to allow proper arming, firing, and fusing signals into the exclusion region, the concept of a "wireless" firing set has been engineered. Electrical energy can be transferred into the exclusion region only after rotating a composite metal disk (which physically separates two parts of a transformer) having magnetic "windows" so that the primary and secondary of the transformer is coupled. The proper alignments are controlled by an electromechanical device which requires a unique signal to operate. The fuzing signal is transmitted through the barrier optically. Another change currently being made to the original concept is to have two exclusion regions instead of one, with each region firing only one of the weapon detonators (here a two-point nuclear system is assumed). The idea is that both exclusion regions would have to be breeched for a nuclear detonation to be electrically initiated. One other innovation that has been fielded is the mechanically safed detonator, or MSAD. The concept here was to move one of the safety subsystems even closer to the nuclear package. An HE pellet drives a small flyer into a contained powdered explosive with enough energy to initiate the powdered explosive and hence the main HE charge. The HE pellet is normally kept out of alignment with the flyer until a mechanism driven by a unique signal causes the correct physical alignment to take place. While each of the above developments is considered to have improved nuclear detonation safety, none of them changed the threshold safety criteria which the weapons were judged to meet, i.e., not greater than 1×10^{-4}. Rather, the improvements increased the confidence that the safety subsystems are truly independent, and improved one part of the system (the exclusion region) and eliminated another (the Lightning Arrestor Connector) which had to be individually shown to be at the 1×10^6 level.

Could nuclear weapons be fielded with absolute (meaning essentially no risk of) nuclear detonation and radioactive contamination safety assurances? The answer is yes, but! The "yes" is based on designs that would have the fissile material physically separate from any high explosive until that point in the STS where absolute nuclear safety was no longer required. The "but" implies that there are some consequences. The most straightforward way (perhaps the only way) of meeting the requirement would be to have systems which demand human placement of the fissile material before the system would be able to be employed. This would likely entail volume and weight growth of the warhead.

Comments

An attempt has been made up to this point to avoid sweeping judgmental commentary. However, it is the author's opinion that:

- The US nuclear weapon safety program has served the nation well.
- Nuclear weapon safety requires understanding and constant vigilance at all management levels.
- Abnormal-environment safety assessments will always contain subjective judgments which do not lend themselves to rigorous cost-benefit analyses. Decision makers, being aware of this, should be receptive to stockpile safety upgrades when proposed.
- To lower the present nuclear detonation safety criteria (thresholds of risk) would require changes to current nuclear deployments and/or current nuclear weapon/nuclear weapon system interfaces.
- In joint agency judgments, the inclusion of DOE judgments in matters concerning nuclear weapon operations and deployments is equally as important as including DoD judgments in nuclear weapon design reviews.
- Nuclear safety has been enhanced by the courage and efforts of a few key individuals.

Epilogue

Nuclear detonation safety and radioactive contamination safety, the main topics of this report, are extremely important considerations in the US nuclear weapon program. Two equally important aspects are those efforts taken to prevent the unauthorized use of a nuclear weapon/nuclear weapon system and those efforts taken to prevent the unauthorized access to the nuclear weapon/nuclear weapon system. Of the four safety standards discussed under the Post-1959 section of this report, two relate directly to safety (unintentional/inadvertent), one to unauthorized (deliberate) use, and one to physical security. It is irrational to attempt to rank order these considerations; a serious nuclear weapon–related event would have grave consequences regardless of its initiating cause.

Adequate safety, security, and control of nuclear weapons—perceived and actual—directly affects the deterrent value of our nuclear forces in that their continued deployments are permitted because of an assumption of that adequacy. While this paper has examined only nuclear detonation and radioactive contamination safety, similar changes in perceptions, threats, and technologies have taken place in the areas of the unauthorized use of and physical security of nuclear weapons/nuclear weapon systems.

~~OUO E2~~

SPECIFIED EXTERNAL DISTRIBUTION ONLY:

1-30A M0701 US Department of Energy
Energy Library MA232.21
Attn: T & A Station
For: S. R. Foley, Jr., DP-1
D. F. Ofte, DP-2
MG G. K. Withers, Jr. (USA), DP-20
R. N. Brodie, DP-22 (15)
J. W. Culpepper, DP-22
R. J. Ross, DP-221
COL V. D. Kempton (USAF), DP-222
COL W. D. Bitler (USA), DP-223
J. E. Rudolph, DP-224
R. D. Hahn, DP-225
CAPT L. R. Newby (USN), DP-226
M. B. Seton, DP-30
M. B. Seaton, Acting, DP-34
M. J. Dowd, DP-34.1
J. L. Meinhardt, DP-10
C. V. Boykin, DP-40
PO Box A
Germantown, MD 20874

31-62A M0759 Office of the Assistant Secretary of Defense (Atomic Energy)
Attn: R. B. Barker
Room 3E1074, The Pentagon
Washington, DC 20301-3050

63-66A M3274 US Department of Energy
Albuquerque Operations
Office
Attn: T – A Station
For: R. G. Romatowski, Manager
J. R. Roeder, OSS
R. L. Hymer, ODP
C. E. Garcia, Acting, ESHD
PO Box 5400
Albuquerque, NM 87115

67-70A M1994 US Department of Energy
Nevada Operations Office
Attn: Mail & Records
For: T. R. Clark, Manager
J. K. Magruder, Assistant Manager
G. C. Allen, NSD
T. D. Wiard, SHD
PO Box 14100
Las Vegas, NV 89114

SPECIFIED EXTERNAL DISTRIBUTION ONLY (Continued):

71-72A M0798 US Department of Energy
San Francisco Operations
Office
Attn: Defense Programs Division
For: R. A. Duval, Manager
D. R. Picasso, DP
1333 Broadway
Oakland, CA 94612

73-95A M3669 Los Alamos National
Laboratory
Attn: Report Librarian
For: S. S. Hecker, Director, MS A100
J. H. Birely, DDD, MS A102
J. F. Jackson, DDO, MS A101
W. F. Miller, DDR, MS A104
J. C. Browne, ADR, MS A114
J. C. Hopkins, ADWT, MS A105
S. D. Rockwood, ADDRA, MS A110
A. J. Tiedman, ADS, MS A120
J. T. Whetten, ADERA, MS A107
R. W. Selden, CNSS, MS A112
D. V. Giovanielli, ADDRA, MS A110
L. A. Gritzo, M-DO, MS P915
M. G. Henderson, X-DO, MS B218
G. G. Hill, WX-DO, MS P945
F. A. Morse, P-DO, MS D437
D. J. Sandstrom, MST-DO, MS G756
T. T. Scolman, J-DO, MS F670
T. P. Seitz, ADWT, MS A105
D. G. Rose, WT-QA, MS A105
N. Davis, WT-WP, MS A105
E. J. Palanek, WT-WP, MS F634
D. L. Roeder, WT-WP, MS F632
B. P. Shafer, WT-WP, MS A105
PO Box 1663
Los Alamos, NM 87545

96-102A M0830 University of California
Lawrence Livermore National Laboratory
Attn: Technical Information Department
For: R. E. Clough, L-125
S. G. Cochran, L-35
J. D. Immele, L-38
G. S. Miller, L-20
W. F. Scanlin, L-20
W. E. Nelson, L-389
W. B. Shuler, L-6
PO Box 808
Livermore, CA 94550

SPECIFIED EXTERNAL DISTRIBUTION ONLY (Continued):

103A	M4461	Deputy Commander USA Nuclear & Chemical Agency Attn: Top Secret Control Officer For: COL E. B. DeBoser, Jr. (USA) 7500 Backlick Rd, Building 2073 Springfield, VA 22150-3198
104A	M4986	Commander, USA ARDEC Attn: Restricted Data Control Officer For: SMCAR-SSN-T (Vanness) Dover, NJ 07801-5001
105A	M4412	Commander, US Army Material Command OPM Nuclear Munitions Attn: AMCPM-NUC (Lapibus) Dover, NJ 07801-5001
106-107A	M1517	Directorate of Nuclear Surety/SNA Attn: COL J. R. Richardson (USAF) Kirtland Air Force Base, NM 87117-5000
108A	M0649	Commander, Field Command Defense Nuclear Agency Attn: FCSAC For: CMDR A. A. Nichols, PF Kirtland Air Force Base, NM 87115-5000
109-110A	M0857	Commanding Officer Naval Weapons Evaluation Facility Attn: Code 12 For: R. Tillery, Code 50 Kirtland Air Force Base, NM 87117-5000
111A	M0654	Director, Defense Nuclear Agency Attn: SSAB For: COL B. Burke, OPSM Washington, DC 20305

SPECIFIED EXTERNAL DISTRIBUTION ONLY (Continued):

112-138A	M0800	SNLL Attn: Document Control For: R. S. Claassen, 8000 P. W. Dean, 8024 E. E. Ives, 8100 J. D. Gilson, 8130 H. M. Witek, 8131 W. R. Hoover, 8132 J. B. Wright, 8150 C. B. Layne, 8151 J. C. Swearengen, 8152 L. A. Hiles, 8153 D. J. Bohrer, 8160 M. H. Reynolds, 8161 A. S. Rivenes, 8162 W. G. Wilson, 8163 P. G. Heppner, 8164 R. A. Baroody, 8180 R. J. Detry, 8200 P. L. Mattern, 8300 R. C. Wayne, 8400 J. Vitko, Jr., 8430 H. Hanser, 8440 J. F. Barham, 8460 R. J. Tockey, 8461 R. I. Peterson, 8462 M. A. Gusinow, 8463 A. L. Hull, 8464 R. L. Rinne, 8470
139A	1	I. Welber
140A	20	O. E. Jones
141A	30	L. E. Bray
142A	100	P. M. Stanford
143A	400	A. N. Blackwell
144A	1000	W. F. Brinkman
145A	1100	F. L. Vook
146A	1200	J. P. VanDevender
147A	1400	E. H. Barsis
148A	1420	G. J. Simmons
149A	1500	W. Herrmann
150A	1510	J. W. Nunziato
151A	1520	W. Herrmann, Acting
152A	1530	L. W. Davison
153A	1800	R. L. Schwoebel
154A	2000	L. K. Anderson
155A	2100	B. L. Gregory
156A	2300	J. L. Wirth
157A	2310	M. K. Parsons
158A	2320	J. H. Renken
159A	2330	J. H. Stichman
160A	2340	M. W. Callahan
161A	2360	P. A. Longmire
162A	2500	H. J. Saxton
163A	2510	D. H. Anderson
164A	2520	N. J. Magnani
165A	2530	D. B. Hayes
166A	2540	G. N. Beeler
167A	2560	J. T. Cutchen
168A	2600	L. D. Bertholf
169A	2800	W. E. Alzheimer
170A	4000	M. R. Kestenbaum
171-180A	5000	E. H. Beckner
181A	5100	J. C. Crawford
182A	5110	C. C. Burks
183A	5111	D. L. McCoy
184A	5112	L. J. Merrell
185A	5113	R. W. Jorgensen
186A	5114	W. D. Ulrich
187A	5120	W. R. Reynolds
188A	5121	D. F. McVey
189A	5129	G. C. Novotny
190A	5140	C. M. Tapp
191A	5150	K. D. Hardin
192A	5151	W. C. Nickell
193A	5152	J. L. Duncan
194A	5153	S. L. Jeffers
195A	5154	R. D. Christopher
196A	5155	R. C. Hartwig
197A	5160	G. R. Otey
198A	5161	K. D. Nokes
199A	5164	D. H. Schroeder
200A	5165	S. D. Meyer
201A	5200	W. C. Myre
202A	5210	J. J. Baremore
203A	5220	A. A. Lieber
204A	6000	D. L. Hartley
205A	6200	V. L. Dugan
206A	6300	R. W. Lynch
207A	6320	J. E. Stiegler
208A	6400	D. J. McCloskey
209A	6410	N. R. Ortiz
210A	6440	D. A. Dahlgren
211A	7000	R. L. Peurifoy
212A	7100	C. D. Broyles
213A	7110	J. D. Plimpton
214A	7130	J. D. Kennedy
215A	7200	H. W. Schmitt
216A	7210	R. E. Sonnenberg
217A	7220	R. R. Prairie
218A	7230	J. F. Ney
219A	7231	H. D. Bickelman
220-222A	7232	S. D. Spray

SPECIFIED EXTERNAL DISTRIBUTION ONLY (Concluded):

223A	7233	R. E. Smith
224A	7250	J. A. Hood
225A	7260	C. H. Mauney
226A	7400	J. C. King
227A	7500	D. M. Olson
228A	9000	R. L. Hagengruber
229A	9010	W. C. Hines
230A	9100	R. G. Clem
231A	9110	P. A. Stokes
232A	9120	M. M. Newsom
233A	9140	D. J. Rigali
234A	9200	L. D. Smith
235-239A	3141	S. A. Landenberger
240A	3151	W. L. Garner (For NWD index)