A Robust Approach to Nuclear Weapon Safety

SAND 2011-4123 C

Alton P. Donnell, Jr., MEng, MBA; Sandia National Laboratories, Albuquerque, New Mexico, USA

Keywords: nuclear, weapon, safety

Abstract

Because of the vast destructive capabilities of nuclear weapons, there has always been an intense interest in ensuring safety, consistent with operational requirements. Over 60+ years of history, we learned important lessons from our accidents, incidents and tests; specifically, we needed robust approach to nuclear weapon safety. This paper outlines some of that history and describes our philosophical approach to nuclear weapon safety, which includes the concept of assured safety and the design principles of isolation, incompatibility, and inoperability.

Introduction

Amongst the many weapons in our arsenal, the safety of one, the nuclear weapon, remains paramount. Our operational history with nuclear weapons and the design evolution forced us to change how we thought about safety. Our philosophical approach to nuclear safety, developed through the 1970s and 1980s and maintained since then, has provided us with the necessary tools to meet the national policy to prevent accidental or inadvertent use of a nuclear weapon. The Sandia National Laboratories Surety Policy captures the basics in a concise sentence: *Assured nuclear weapon safety will be designed into nuclear weapons using the Nuclear Safety Design Principles of isolation, incompatibility, and inoperability that provide safety in a predictable manner when subjected to normal and abnormal environments.* These terms and a summary of the implementation approach are discussed as are some challenges and opportunities for the future.

How Did We Get To Where We Are?

Before the advent of sealed-pit weapons in the late-1950s, weapons were inoperable when the fissile material was separated from the main charge high explosive. These weapons were inherently safe until assembled. Obvious examples are Little Boy (Hiroshima) and Fat Man (Nagasaki) where the assembly occurred on Tinian Island just before intended use. After assembly in both designs, a "green" plug shorted the electrical circuits and kept the system safe. A "red" plug was then inserted to complete the circuits before release.

Later nuclear weapon designs used "separable" components, but could be assembled in flight either manually or mechanically. Electromechanical switches later replaced the red or green plug but performed the same function. Sealed-pit designs provided environmental protection to the fissile material and allowed the full integration of the pit and high explosive package into. This required much less maintenance, was more efficient and could be designed to be more responsive to service alert requirements.

Throughout our history with nuclear weapons there have only been 32 accidents[1] that resulted in detonation of the high explosive, burning of

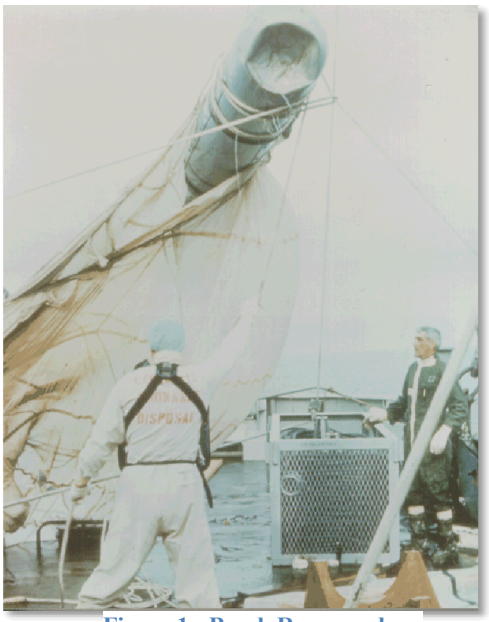

Figure 1 - Bomb Recovered Near Palomares, Spain, 1966

[1] An accident involving nuclear weapons is defined as an unexpected event involving nuclear weapons or nuclear weapons components that results in any of the following:

- Accidental or unauthorized launching, firing, or use, by U.S. forces or supported allied forces, of a nuclear-capable weapons 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; or
- Public hazard, actual or implied. (Ref 1)

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

the high explosive, or radioactive contamination. None of these resulted in even a partial nuclear detonation, despite extreme environmental conditions. B-52 crashes while flying airborne alert over Palomares, Spain in 1966 and Thule, Greenland in 1968 did result in significant radiological contamination.

In the late 1950s, a military commission concluded that more needed to be done to ensure safety for these fully integrated designs, but only minor incremental changes were made, most of which were focused on preventing deliberate unauthorized use by an adversary or an insider. Early safety was based on assumptions, unsupported by a technical basis, about how weapons would behave in abnormal environments[2]. Assumptions that soldered joints would open or that a short circuit to ground would create a dud were made. In fact, some short circuits could lead to other propagating faults and more dangerous situations.

Accidents in the 1960s highlighted the need for more robust safety systems for the prevention of inadvertent nuclear detonation. Two of the most significant were at Goldsboro, NC and Bunker Hill, IN. The following is extracted verbatim from the unclassified DoD report (ref. 1).

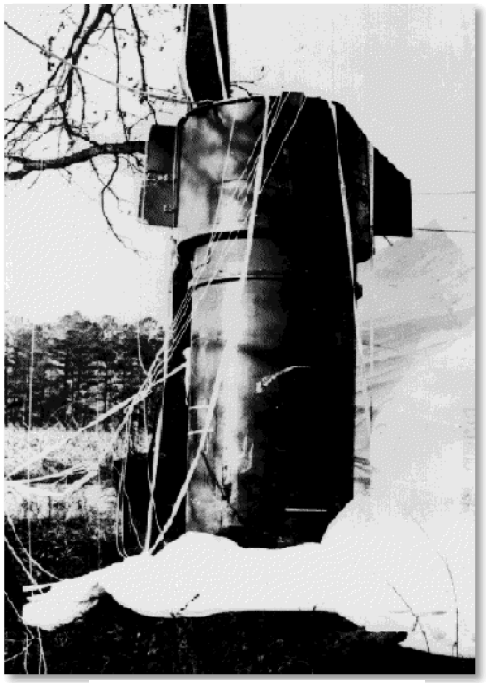

Figure 2 - Bomb recovered at Goldsboro, 1961

January 24, 1961/B-52/Goldsboro, North Carolina

During a B-52 airborne alert mission, structural failure of the right wing resulted in two weapons separating from the aircraft during aircraft breakup at 2,000 - 10,000 feet altitude. One bomb's parachute deployed and the weapon received little impact damage. The other bomb fell free and broke apart upon impact. No explosion occurred.

December 8, 1964/B-58/Bunker Hill (Now Grissom) AFB, Indiana

Strategic Air Command aircraft were taxiing during an exercise alert. As one B-58 reached a position directly behind the aircraft on the runway ahead of it, the aircraft ahead brought advanced power. As a result of the combination of the jet blast from the aircraft ahead, the icy runway surface conditions, and the power applied to the aircraft while attempting to turn onto the runway, control was lost and the aircraft slide off the left hand side of the taxiway. The left main landing gear passed over a flush mounted taxiway light fixture and 10 feet further along in its travel, grazed the left edge of a concrete light base. Ten feet further, the left main landing gear struck a concrete electrical manhole box, and the aircraft caught on fire. Portions of the five nuclear weapons on board burned; contamination was limited to the immediate area of the crash and was subsequently removed.

As a result of these accidents, several important insights were gained. Accidents, like Goldsboro, may mimic the flight environment. Accidents are complex and unpredictable; a variety of harsh environments like fire, crush, shock, and unintended electrical energy may occur in a single accident and should be assumed to occur concurrently and, potentially, sequentially in the worst possible order. Subsequent testing on components such as cable wiring, printed circuit boards and the electromagnetic replacements to the "red plug/green plug" discovered that they performed unpredictably in abnormal environments allowing electricity available on the weapon system to propagate through to the charging circuits for the weapon. The conclusion that hardware relied on for safety may not perform when required unless it was specifically designed to be robust against abnormal environments was key to implementing changes to the stockpile.

Several important changes were begun in the late 1960s. Recognizing that the drop of a bomb, whether intentionally or accidentally, created essentially the same environment, something else needed to be done. The solution was the implementation of a unique signal that would provide unambiguous indication of human intent while being

[2] Abnormal Environment defined: Those environments in which the weapon is not expected to retain full operational reliability but is expected to remain safe.

extremely difficult to mimic in an abnormal environment. Another was the development of the concept of "assured safety" (discussed in detail later) that ensures that a weapon must fail safe in a manner where it cannot function when exposed to an abnormal environment such as fire or shock and credible combinations of these environments.

The Sandia design approach addresses these types of environments and meets the -recently developed requirements from the President and the Department of Energy discussed below.

Nuclear Weapon Safety Design Requirements

Requirements that drive nuclear safety begin with Presidential Executive Orders. The most recent (ref. 2) states:

> "Given the profound implications of their potential use, nuclear weapons must be subject to the most precise and stringent command and control, safety, and security possible.
>
> …
>
> We must also prevent accidental, inadvertent, or unauthorized access to or use of U.S. nuclear weapons and protect against their loss, theft, or seizure.
>
> …
>
> …measures shall be consistent with operational requirements and shall be continually assessed against existing and emerging threats as well as technological opportunities for improvement."

The Department of Energy (DOE)/National Nuclear Security Administration (NNSA) and Department of Defense (DoD) share a joint responsibility for addressing nuclear weapon surety[3] throughout all phases of the weapons life cycle. (ref. 3) This commitment has been fundamental to the weapon design agencies and their close relationship with the DoD in support of the nuclear weapon stockpile.

As a result, both the DOE/NNSA and DoD provide qualitative standards and requirements as well as quantitative criteria for nuclear weapon safety design. (refs. 4, 5)

Specifically, the policy established by the DOE is to "… prevent unintended/unauthorized detonation … of nuclear explosives." The overall goals governing nuclear weapon design are the DOE/NNSA and DoD nuclear surety and/or safety standards.[4]

Common to both sets of standards is the requirement for nuclear weapons to possess design attributes or features (called positive measures by the DoD) to prevent a nuclear detonation in the event of an accident or unauthorized act.[5] Similar qualitative design requirements exist to ensure adequate security and to prevent deliberate unauthorized use.

DOE's "Nuclear Explosive and Weapon Surety Program," (ref. 4) specifies numerical requirements similar to those specified by the DoD in the Military Characteristics (MCs) for a specific design.[6] Other specific quantitative or qualitative design requirements are provided for one-point safety, fissile material dispersal, use control, and nuclear-criticality. Design requirements for unintended multipoint initiation in abnormal environments have not been developed, but the potential for and the associated consequences of unintended multipoint initiation must be evaluated.

---

[3] Surety defined: safety, security and use control. The DoD also includes reliability.

[4] The DOE and DoD nuclear safety standards are used by the respective review departmental groups to determine whether a weapon meets the overall need for the departments, recognizing that the implementation of safety in a particular design may not meet a particular, prescribed requirement. The specific wording in the standards has diverged. The DoD safety standards are still broad and encompass what the DOE refers to as surety. The DOE's fifth standard on design expands beyond preventing nuclear yield and includes preventing high-explosive detonation or deflagration for which the implied consequence is explosive fissile material dispersal.

[5] This is consistent with Morgan Sparks' statement as President of Sandia in 1977 that "We are trying to accomplish a design which will have a vanishingly small risk of a nuclear detonation" (in SAND2001-0600).

[6] "The following are design requirements for nuclear weapons delivered to DoD:

> 1. Normal Environment. Prior to receipt of the enabling input signals and the arming signal, the probability of a premature nuclear detonation must not exceed one in a billion (1E-09) per nuclear weapon lifetime.
>
> 2. Abnormal Environment. Prior to receipt of the enabling input signals, the probability of a premature nuclear detonation must not exceed one in a million (1E-06) per credible nuclear weapon accident or exposure to abnormal environments."

Customer-generated qualitative and quantitative design requirements are normally contained in the MCs and supporting Stockpile-to-Target Sequence (STS). These design requirements may encompass both general requirements and those specific to particular types of hardware, such as electro-explosive devices. Negotiation for the MC and STS occurs during the development phase of the weapon.

Nuclear Weapon Safety Design Policy

Sandia's formal nuclear safety design policy is encompassed within the Laboratories Nuclear Explosive and Weapon Surety (NEWS) Policy statement. (ref. 6)

> "SNL's surety objective is to drive the likelihood of the unacceptable consequences as low as reasonably practicable, with the appropriate balance of surety design features that are tailored for the nuclear explosives, nuclear weapons and weapon-related products, and considering the environments and threats they may encounter throughout their lifetimes, consistent with our customer's operational requirements.
>
> …
>
> Assured nuclear weapon safety will be designed into nuclear weapons using the Nuclear Safety Design Principles of isolation, incompatibility, and inoperability that provide safety in a predictable manner when subjected to normal and abnormal environments."

Nuclear Weapon Safety Fundamental Design Requirements

The following nuclear weapon safety fundamental design requirements outline what must be done as part of design development—not how to do it. Elaboration on each of the five core requirements follows.

Assured Safety

Assured safety for a high-consequence system requires a design that is safe regardless of the accident scenario and whether or not that scenario has been specifically accounted for in the design. The implementation of assured safety must be built around the need to detonate nuclear weapons when properly authorized and with exceptionally high reliability.

Sandia recognized more than 40 years ago that assured safety for nuclear weapons could be achieved if, at some severe environmental level, the weapon could no longer work. Assured safety[7] uses the Nuclear Safety Design Principles to develop a safety theme that ensures isolation of compatible energy from nuclear detonation-critical components[8] until the weapon fails safe. Another way of expressing the concept is that assured safety is achieved as long as isolation is maintained or if a detonation-critical component becomes irreversibly inoperable before isolation is lost.

The design of a system that provides assured safety requires safety subsystems and components that perform specific safety functions. Assured safety at other than the overall system level means that the subsystems and components predictably[9] meet their identified nuclear safety requirements.

Nuclear Safety Design Principles

Achieving assured safety relies on the interrelated Nuclear Safety Design Principles of isolation[10], incompatibility[11], and inoperability[12]. (ref. 7, 8) Two of these, isolation and inoperability, are always used to achieve assured safety. Further, isolation is always part of the implementation because of 1) the need to prevent detonation through the design pathway except when properly authorized, and 2) the current paradigm of sealed-pit designs that requires

---

[7] Assured Nuclear Weapon Safety defined: Isolation of compatible energy from nuclear detonation-critical components of an operable nuclear weapon until after the weapon becomes irreversibly inoperable.

[8] Nuclear Detonation-Critical Component defined: A weapon feature that if rendered inoperable precludes nuclear detonation.

[9] Predictable means certain to happen based on knowledge and experience. To be predictable, knowledge and experience must be based on identifiable, analyzable, testable, controllable, and verifiable attributes.

[10] Isolation defined: The predictable separation of weapon elements from compatible energy.

[11] Incompatibility defined: The use of energy or information that will not be duplicated inadvertently.

[12] Inoperability defined: The predictable inability of weapon elements to function.

protecting detonation-critical components against bypass pathways. Isolation builds on and requires the support of incompatibility and inoperability.

Unique signals, properly implemented throughout the weapon system, provide unambiguous indication of human intent and provide energy pathways that permit authorized use during prearming. These signals are specially designed such that their duplication in an accident environment is highly unlikely—information incompatibility. Other prearming, arming, and firing signals are used that do not match the usual electrical signals found in the delivery system and common sources of abnormal electrical energy—energy incompatibility. Regardless of the barrier chosen to provide isolation, there is always some leakage; therefore, energy incompatibility defines what needs to be isolated and how much leakage can be allowed.

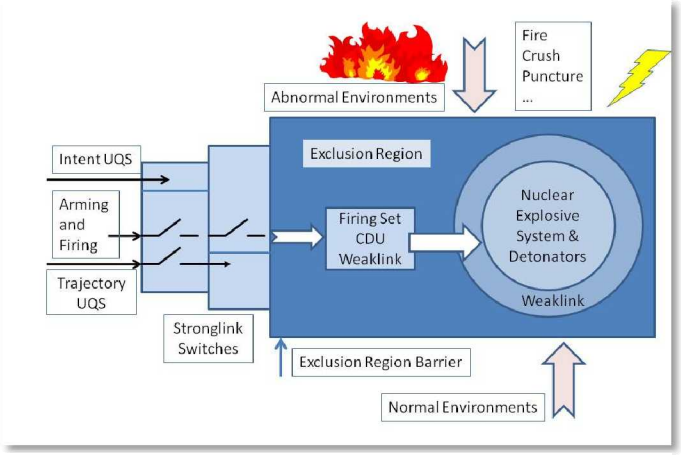

Figure 3 - Nuclear Detonation Safety Architecture

Implementation of the design principles requires the creation of an "exclusion region" from which energy capable of creating nuclear yield is excluded. Within the exclusion region are the nuclear detonation critical components needed to produce nuclear yield. To be able to use the weapon, switches block energy from the exclusion region and remain locked until the unique signal is received.

With today's modern sealed-pit designs, which are inherently operable, assured safety is achieved only when one or more nuclear detonation-critical components become irreversibly inoperable before isolation in abnormal environments fails. This component is called a *weaklink*.[13]

The first principles of physics and chemistry[14] are used to support the Nuclear Safety Design Principles. First principles are used, for example, in the weaklink design, in which a fundamental characteristic of the material is relied on to ensure the weaklink becomes predictably and irreversibly inoperable.

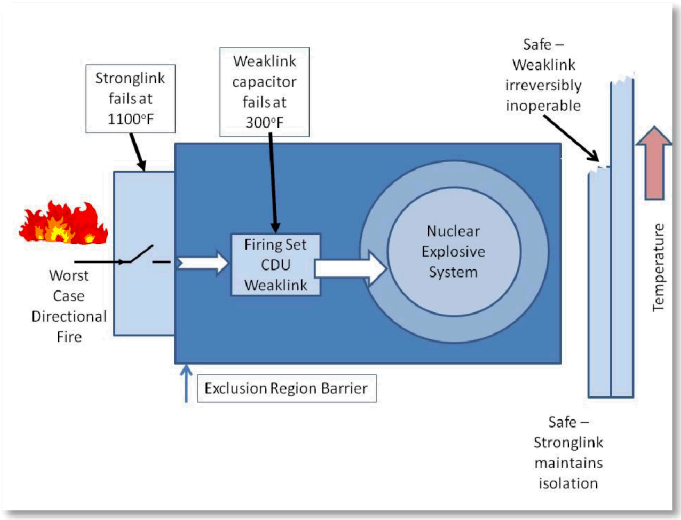

Figure 4 - Weaklink-Stronglink Concept Provides Assured Safety

Nuclear Safety Theme – The "What"

Designers must develop a Nuclear Safety Theme, a high-level, concise expression of how the nuclear safety design principles are used to provide assured safety, using the Nuclear Safety Design Principles of isolation, incompatibility and inoperability.

Nuclear Safety Theme Implementation – The "How"

Supporting requirements have been identified as necessary for successful implementation and are levied on the subsystems, components and other features that constitute the nuclear safety system. These include:

- Use multiple independent safety subsystems. At least three safety subsystems are required; usually two for abnormal environments and one for normal environments.
- Design nuclear safety-critical features to be passive, to fail safe, and to be verifiable.
- Minimize the number of features critical to nuclear safety while ensuring completeness.

---

[13] Weaklink defined: A nuclear detonation-critical element of a weapon system that fails *predictably* and *irreversibly* in specific abnormal environments based on first principles of physics and chemistry.

[14] First Principles of Physics and Chemistry defined: Inherent physical and chemical characteristics (for example, melting temperature, electrical conductivity, tensile strength) that provide a *predictable* response when subjected to specified stimuli.

- Demonstrate nuclear safety assurance without precise definition of abnormal environment scenarios.

Implementing the Nuclear Safety Theme requires identifying all design features (subsystems, components, etc.) necessary to provide assured safety in normal and abnormal environments. As these nuclear safety-critical features are identified, the designer continually checks to ensure that the "how" of the implementation is consistent with the "what" of the Nuclear Safety Theme. These features are critical to meeting nuclear safety requirements in an assured and predictable manner.

Fault tree analyses of systems, subsystems, and components help to systematically and coherently identify safety-critical features (first order faults and, occasionally, second order faults) that require higher levels of change control in design and manufacturing. A variety of other analytical techniques such as Failure Modes and Effects Analysis (FMEA) are also used.

Sound implementation relies on the flow-down of requirements from the overall system to the nuclear safety-critical features to ensure traceability to the system requirements. To ensure that these requirements are met, all nuclear safety features are designed and implemented in accordance with formal processes and procedures.

Positive verification that as-built hardware meets abnormal environment requirements often results in destruction of the hardware. Therefore, those aspects of the nuclear weapon design necessary to meet the system's nuclear safety requirements must be explicitly "built-in." There is little opportunity for requirements verification after manufacturing, although destructive testing during stockpile life provides some confirmation that components are performing as expected.

It is impossible to test-in safety for a variety of reasons. Destructive testing to the specified abnormal environments is prohibitively expensive, the required facilities to test to those environments are lacking, and even if the tests are possible, no number of destructive tests could provide an adequate basis given the uncertainty associated with all of the possible accident environments.

After the system has been designed, controls are placed on all safety-critical subsystems, components and features to ensure they are manufactured as intended. These controls include:

- Identification of the nuclear safety-critical features and Pentagon S [/S/] designation.
- Enhanced design definition change control.
- Enhanced manufacturing process and materials verification.
- Stockpile sampling and testing throughout a weapon's life-cycle.

Nuclear Safety Specification

The system-level Nuclear Safety Specification documents how the Nuclear Safety Theme and its implementation meet the nuclear safety design requirements for a specific weapon design. The NS documents the approach for meeting the nuclear safety qualitative and quantitative requirements in all Manufacturing-to-Retirement sequence (MRS) environments, which envelope the normal and abnormal environments specified in DoD's STS. The NS explains in detail how independent, passive safety subsystems and associated components are integrated into a system to provide assured safety.

The Role of Peer Review and Independent Assessment

Throughout the design process, the architecture, design, documentation, and production is subject to rigorous review, both by peers within organizations and by independent assessors both within and external to the design organizations. The system designers have the sole responsibility to "prove the design is safe;" all others provide aggressive challenges to that assertion. The intent is to ensure a healthy and creative tension between the designers and those who review the designs as early in the process as possible. While some of the reviews lead to adjustments in the designs, there are always some aspects of the designs that can never live up to the perfection implied by "assured safety." These reviews lead to better informed executive management within the laboratories, and ultimately the DOE/NNSA and DoD.

Future Opportunities and Challenges

A variety of potential technological advances are available as part of the refurbishment of existing systems. Many of our safety components in the existing stockpile are first-generation devices developed in the 1970s – we have learned much from these devices, and have identified significant design improvements over time. Concepts like

detonator safing and direct optical initiation offer significant safety improvements, and can likely be certified without the need to return to underground testing.

A variety of additional operational capabilities (for example, location enablement that would preclude the detonation of a weapon unless it was at the correct location and at, potentially, the correct time) could be developed if there is the military need. Similarly, a significant improvement in overall surety could be gained by fully integrating safety and use control systems in a much more coherent manner.

Similar concepts can be developed and implemented for conventional systems. An auto-destruct mechanism can be built in to destroy the missile that veers off course. Warheads can be developed to recognize those authorized to employ them and destroy themselves, either violently or passively, if tampered with by an unauthorized person.

Summary

Our operational history with nuclear weapons and the design evolution forced us to change how we thought about safety. Our philosophical approach to nuclear safety, developed through the 1970s and 1980s and maintained since then, has provided us with the necessary tools to meet the national policy to prevent accidental or inadvertent use of a nuclear weapon.

Many opportunities exist for making our systems, both nuclear and conventional safer and more secure.

References

1. "Narrative Summaries of Accidents Involving U.S. Nuclear Weapons," Department of Defense, May 1981.
2. NSPD-28, "Nuclear Weapons Command and Control, Safety, and Security (U)", President George W. Bush, June 2003.
3. Secretaries of Defense and Energy, "Joint Policy Statement on Nuclear Weapons Surety," June 27, 1991.
4. U. S. Department of Energy, DOE Order 452.1D, *Nuclear Explosive and Weapon Surety Program*, April 14, 2009.
5. U. S. Department of Defense, DoD Directive 3150.2, *DoD Nuclear Weapon System Safety Program*, December 23, 1996 (certified current March 8, 2004).
6. "Nuclear Explosive and Weapon Surety (NEWS) Policy," Sandia National Laboratories, Albuquerque, New Mexico, 2011.
7. SC-DR-72 0492, *Approaches for Achieving Nuclear Weapon Electrical System Safety in Abnormal Environments,* August 1972 (originally published as SC-DR-71 0772).
8. S.D. Spray, *Nuclear Weapon Safety from Production to Retirement*, SAND2001-0600, May 2001.

Biography

Alton P. Donnell, Jr., MEng, MBA; Sandia National Laboratories, PO Box 5800, MS0492, Albuquerque, New Mexico, 87185 USA, telephone – (505) 845-7813, e-mail – apdonne@sandia.gov

Mr. Donnell is a Certified Nuclear Explosive Safety Study Group member for the Department of Energy and conducts internal nuclear safety assessments for Sandia National Laboratories. He continues to support surety improvements for transportation on nuclear weapons. Before joining the laboratories, he spent 14 years as a nuclear safety consultant and 20 years in the U.S. Army, where he completed his career as a nuclear weapon specialist.