SAND2012-0793C

The Enhanced Nuclear Detonation Safety Theme – an Introduction

Raymond B. Wolfgang[1], Sandia National Laboratories[2]

Abstract

The United States, in order to maintain a viable and robust nuclear deterrent, needs to support a safe, reliable, and predictable stockpile of nuclear weapons. How can it be assured that over the course of a weapon system‟s lifetime, which can be up to 30 years or more, the workers on these weapons as well as the surrounding community remain safe? At stake are the continued functioning of the complex, the world‟s confidence in the United States‟ ability to maintain a stockpile for itself and its allies, and most importantly the safety of nuclear weapons workers and surrounding communities. This paper first discusses some accidents early in the United States‟ nuclear weapon program, and then lists the safety requirements (Walske criteria) that arose as a reaction to those accidents. The bulk of this paper outlines the current version of this safety theme –Enhanced Nuclear Detonation Safety (ENDS). The theme described here is comprised of three principles – Isolation, Incompatibility and Inoperability – and is assisted by the concept of Independence. Examples of the theme for both normal and abnormal (i.e. accident) environments are presented to illustrate requirements. Designing weapons to this theme helps to solve the problem of keeping personnel and the environment safe while storing, transporting, and maintaining weapons in the stockpile – a stockpile that is key for US national security and the protection of US-allied nations.

---

[1] Sandia National Laboratories, Albuquerque, New Mexico. Raymond is a systems engineer for the W76-1 Life Extension Program. Contact info: (505) 284-2486, rwolfga@sandia.gov . This report # is SAND2012-0793 C.

[2] 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.

Introduction

Even a small nuclear weapons accident that involved nuclear yield would be catastrophic to the local community, the operation of the nuclear weapon complex, and the world‟s confidence in the United States‟ ability to safely maintain a sustainable deterrent. These consequences drive the need to assure there are absolutely no US nuclear detonations resulting from anything else than a declared launch by the US President. Fortunately there have not been any inadvertent nuclear detonations in US history, but there have been several other accidents without detonations as well as inadvertent radiological dispersals. This paper describes the requirements that were levied on US nuclear weapons laboratories as a result of these accidents in the 1950‟s and 1960‟s (Walske criteria). This safety policy led to the design theme used today by the US weapon design laboratories (Los Alamos, Lawrence Livermore, and Sandia) to build and refurbish nuclear weapons – the Enhanced Nuclear Detonation Safety (ENDS) theme. The theme, formed by the three pillars of Isolation, Incompatibility and Inoperability, will be described along with the concept of Independence, which is used to help implement the safety design. First, an analysis of early nuclear weapon history is required to examine the motivation behind the Walske requirements.

History

Accidents

No US nuclear weapon accident has involved an inadvertent nuclear detonation (IND) of any yield (i.e. no “blinding white flash”). The most severe accidents have involved radiological dispersal from the detonation of the high explosive (HE) in the weapon. When radioactive material is scattered by the force of the HE blast, it is referred to as an HE Violent Reaction (HEVR). Some of the more severe accidents are described below, with emphasis on those parts of the accident that motivated a set of quantitative safety requirements being levied on all new and refurbished weapon systems. These new requirements, referred to as the Walske Criteria, prompted the development of the Enhanced Nuclear Detonation Safety theme. These criteria were first promulgated in a letter by Carl Walske, then chair of the Military Liaison Committee (precursor to today‟s Nuclear Weapons Council), to the Atomic Energy Commission (early precursor to today‟s Department of Energy) [3]. The Walske criteria, as originally expressed in the letter are listed below:

> *"The probability of a premature nuclear detonation of a bomb (warhead) due to bomb (warhead) component malfunctions (in a mated or unmated condition), in the absence of any input signals except for specified signals (e.g., monitoring and control), shall not exceed:*
>
>> *Prior to receipt of prearm signal (launch) for the normal** *storage and operational environments described in the STS, 1 in* 10^9 *per bomb (warhead) lifetime.*

---

[3] “The Walske Letter”, Memo from the Department of Defense Military Liaison Committee, (Carl Walske) to the Atomic Energy commission (General Edward B. Giller), March 14, 1968.

> *Prior to receipt of prearm signal (launch), for the abnormal*[**] *environments described in the STS, 1 in* 10^6 *per warhead exposure or accident."*

> [*]*Normal environments are those expected logistical and operational environments, as defined in the weapon's stockpile-to-target sequence (STS) and military characteristics (MCs) in which the weapon is expected to retain full operational reliability."*
>
> [**]*Abnormal environments are those* [unexpected] *environments, as defined in the weapon's stockpile-to-target sequence (STS) and military characteristics (MCs) in which the weapon is not expected to retain full operational reliability."*

A prearm signal, is a signal that must be sent to the weapon firing system before final arming, fuzing and firing of the weapon can occur; it is most often incorporated as a safety feature to prevent accidental arming of a warhead. In the Walske letter, the prearm signal was the physical acceleration experience by the weapon during launch; once such acceleration was felt by the warhead, subsequent arming and firing steps could take place. A more thorough analysis of nuclear weapon safety as they relate to the Walske criteria is presented in [4]. The goal of the Walske criteria, and implementing the safety theme to meet them, is to prevent non-standard events of any type during warhead handling - particularly HEVRs or INDs.

Early Safety – Removable Capsules

One early design of nuclear weapons involved a removable capsule of nuclear (fissile) material, as shown in Figure 1. This design required that, before deployment, the nuclear part of the weapon be physically inserted into the body of the weapon casing; this would usually happen inside the aircraft bomb bay during flight. Most designs required that this capsule, also known as the *pit*, be stored separately from the weapon in a special storage container called a *birdcage*. The advantage offered by this design was in the event of an accident, a high explosive detonation did not necessarily produce any radiological dispersal, since it was possible to transport weapon cases without any nuclear material on board the transport plane. Among the 32 nuclear weapon accidents [5] in US history, several had high explosive detonations without a live capsule present and several others had weapons and capsules on board without the capsules inserted. These latter accidents – even though HEVR occurred – did not involve any radiological dispersal. Two accidents, each with capsules and weapon cases in the same transport vehicle, only involved contamination limited to the immediate accident area. There was also an accident with only two capsules on board, but no weapon case with high explosive to cause dispersal. Finally, not every accident in the capsule-era resulted in a HE explosion, although one such accident resulted in slight alpha contamination of a firefighter‟s clothing.

---

[4] Kidder, R. E., "Report to Congress: Assessment of the Safety of U.S. Nuclear Weapons and Related Nuclear Test Requirements," Lawrence Livermore National Laboratory report, UCRL-LR-107454, July 26, 1991.

[5] United States Department of Defense, *Unclassified Narrative Summaries of Accidents Involving U.S. Nuclear Weapons, 1950 – 1980.* (1981).

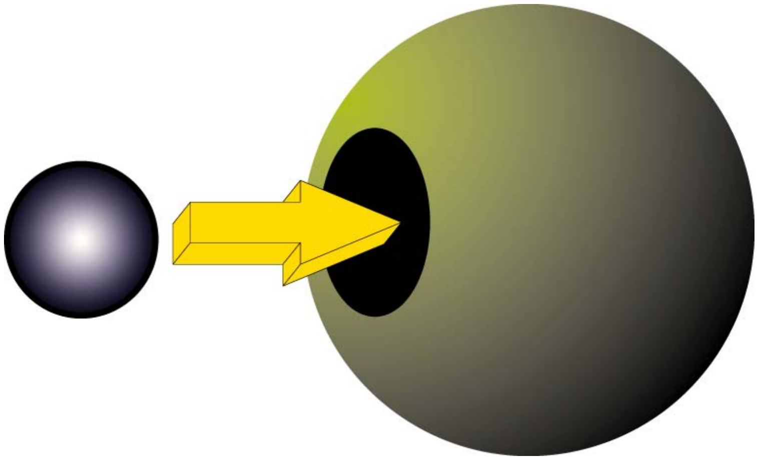

Figure 1. Nuclear Capsule, or “pit”, (left) inserted into Weapon Case.

There were many substantial disadvantages to separable-pit weapons, including difficulties associated with tracking the nuclear material, increased radiation exposure to workers, and the limitation of designs to bomb-type weapons. Later weapon designs were “sealed-pit” weapons, where the nuclear material is placed inside the weapon during manufacture (Figure 2), and is not removable during normal operation. This type of weapon is much easier to maintain, and avoids the potentially dangerous and fallible operation of inserting the capsule while the aircraft is mid-flight. This design also allows delivery of weapons via intercontinental ballistic missile (ICBM), since it is not realistic from an engineering standpoint to insert a capsule into a warhead during missile flight, and have the warhead meet a reasonable yield requirement.

Sealed-pit weapons present a different safety challenge, since the high explosive and the nuclear material are now within the same bomb casing. An example of the new risk that this poses was seen in an accident over Goldsboro, North Carolina.[6] Here, two weapons separated from the aircraft during a structural failure of the right wing. One bomb‟s parachute deployed and the bomb underwent only minor damage as shown in Figure 3; the other bomb broke apart. Neither bomb‟s HE detonated on impact, avoiding certain substantial radiological dispersal. A separate accident involved weapons mounted on an airplane taxiing on the tarmac.[7] Due to a runway accident in icy conditions, the bombs experienced both extreme cold and then intense heat from the ensuing fire. Parts of the five weapons on board burned up, and contamination was limited to the immediate area of the accident and subsequently removed. More importantly, this accident provided an example of a bomb experiencing an environment (simultaneous hot and cold) not anticipated by the original designers. This drove the need for a systematic way to design safety into a weapon, instead of designing a weapon specifically to certain environments.

---

[6] Ibid. January 24, 1961 / B-52 / Goldsboro, North Carolina

[7] Ibid. December 8, 1964 / B-58 Hustler / Bunker Hill (now Grissom) AFB, Indiana.

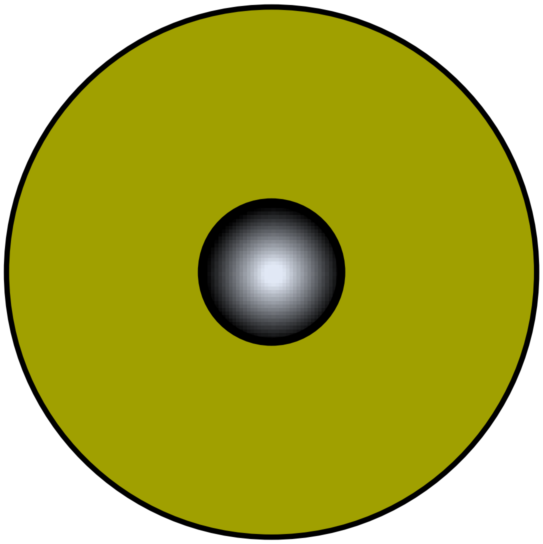

Figure 2. Sealed Pit Weapon; Nuclear Material in Center.

To this point, most of the accidents had not resulted in nuclear material dispersal. Those that had were sufficiently minor that the radiation was confined to the immediate area of the accident: the wreckage, the crater and the immediate area, or someone"s clothing. In all contamination cases, the spread was confined to the property of the military base involved. This changed in the late 60"s with two accidents – one over Palomares, Spain[8] and the other near the airbase in Thule, Greenland.[9] Descriptions of the two accidents are below:

> *January 17, 1966. A B-52 bomber and KC-325 refueling tanker collided during a routine high altitude air refueling operation. Both aircraft crashed near Palomares, Spain. Four of the 11 crew members survived. The B52 carried four nuclear weapons. One was recovered on the ground and on April 7, one was recovered from the sea* (Figure 4). *Explosive materials exploded on impact with the ground releasing some radioactive materials. Approximately 1400 tons of slightly contaminated soil and vegetation were removed to the United States for storage at an approved site. Representatives of the Spanish government monitored the cleanup operation.*
>
> *January, 21, 1968. A B-52 crashed and burned some 11 miles southwest of the runway at Thule AB, Greenland, while approaching the base to land. Six of the seven crew members survived. The bomber carried four nuclear weapons, all of which were destroyed by fire. Some radioactive contamination occurred in the area of the crash which was on the sea ice. Some 237,000 cubic feet of contaminated ice, snow, and water with crash debris were removed to an approved storage site in the U.S. over the course of a 4-month operation. Although an unknown amount of contamination was dispersed by the crash, environmental sampling showed normal readings in the area after the cleanup was completed. Representatives of the Danish government monitored the cleanup operations.*

---

[8] Ibid. January 17, 1966 / B-52 & KC-135 / Palomares, Spain.

[9] Ibid. January 21, 1968 / B-52 / Thule AB, Greenland.

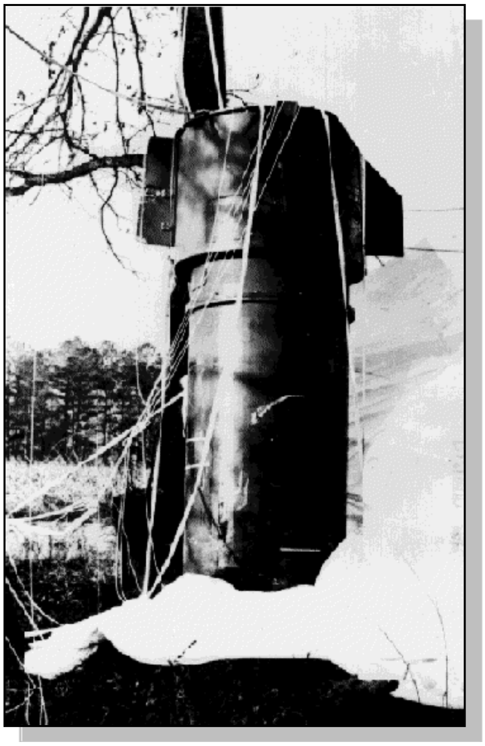

Figure 3. One of the Goldsboro bombs.

Figure 4. Palomares: January 1966

These were the only two accidents that resulted in widespread dispersal of nuclear materials, and both occurred during the period of airborne alert, where the US had airborne bombers loaded with nuclear weapons in the event of an attack. Later in 1968, airborne alert was terminated the day after the Thule accident.[10] These two accidents also resulted in a policy change by the top-level government committee governing all aspects of the nuclear weapons complex, the Military Liaison Committee (MLC), precursor of today‟s Nuclear Weapons Council.[11]

Safety

Walske Criteria

While the airborne alert was cancelled in 1968, there was still concern at the policy level on whether there would be another accident. Carl Walske, then chair of the Military Liaison Committee (MLC), led a group of military and civilian officials which had the ability to levy requirements on any and all nuclear weapon development, maintenance and retirement activities. The MLC passed onto the US Military and the Atomic Energy Commission (AEC), precursor to today‟s Department of Energy (DOE), the following safety-related requirements for all new weapon development and refurbishment projects. These are known as the Walske Criteria. The Walske Criteria set the following parameters for safety prior to launch in "normal" and "abnormal" environments.

---

[10] Grant, Rebecca, "The Perils of Chrome Dome," Airforce-magazine.com, http://www.airforce-magazine.com/MagazineArchive/Pages/2011/August%202011/0811dome.aspx.

[11] Asst. Sec. of Defense for Nuclear Matters, *Nuclear Matters Handbook*, expanded edition, Appendix A (May 2011) http://www.acq.osd.mil/ncbdp/nm/nm_book_5_11/index.htm.

1. *In normal storage and operational environments*, … the probability of nuclear yield greater than 4 lbs. equivalent TNT shall not exceed one in one billion (or 1 in 10^9) per warhead lifetime.
2. *In abnormal environments* as described in the system Stockpile-to-Target sequence … the probability of nuclear yield greater than 4 lbs. equivalent TNT shall not exceed (one in one million (or 1 in 10^6) per warhead exposure to the environment or accident.

To put the probability of failure in a normal environment into perspective, one billion (10^9) seconds would last 31.7 years. One billion minutes into the past, the Roman Empire was still in existence. For abnormal environments, a failure probability of one in one million is roughly equivalent to the probability that one word was misspelled among 136 pages of text in Encyclopedia Britannica (without spaces). One million US dollar-bills weighs approximately 1,000 kg, and one million seconds is equivalent to 11.6 days. Abnormal environments may include lightning events, underwater submersion, fires involving either petroleum-based fuel or missile propellant, or even extreme heat, cold, or humidity experienced during storage.

The Walske Criteria impose stringent safety standards which pose significant engineering and production challenges to the national laboratories responsible for weapon design, production, and surveillance.

The Laboratories' Response

The national laboratories that deal with nuclear weapon design are Los Alamos National Laboratory (LANL), Lawrence Livermore National Laboratory (LLNL), and Sandia National Laboratories (SNL),. Additionally, Sandia is responsible for the overall system integration and thereby the safety of the overall nuclear weapon system. The following history is excerpted from [12], and a fuller version of the history is available in [13,14]. In 1968, Sandia Executive VP Jack Howard formed the Independent Safety Assessment Group (ISAG); Stan Spray, a Division Supervisor under Jack Howard at the time, led a study of weapon safety in abnormal environments. This study soon led to a stockpile-wide review conducted jointly by Sandia and the Energy Research and Development Administration (ERDA) in the early to mid-70‟s. ERDA was the precursor to today‟s Department of Energy. The conclusions of the review were that, in light of Palomares and Thule, safety improvements could be made – either by ending airborne alert, retrofitting active systems, or retiring systems from the stockpile. From these studies (late 60‟s, early 70‟s), ISAG also worked with systems and components groups at Sandia to develop a new approach to designing weapon systems and refurbishments that would address some of the new safety concerns: the Enhanced Nuclear Detonation Safety (ENDS) theme.[15] This approach involves following certain design rules and guidance in the selection of weapon parts and in the overall weapon architecture. The ENDS theme may also drive the selection of material, safety

---

[12] Spray, S.D., "Nuclear Weapon Safety from Production to Retirement," SAND2001-0600, Section 1: Background. Official Use Only; distribution limited.

[13] Spray, S. D., "History of Nuclear Weapon Safety at Sandia: Personal recollections. Vol. 1. SAND2008-2881. Official Use Only; distribution limited.

[14] Spray, S. D., "History of Nuclear Weapon Safety at Sandia: Personal recollections. Vol. 2. SAND2008-2879. Official Use Only; distribution limited.

[15] David W. Plummer and William H. Greenwood, *The History of Nuclear Weapon Safety Devices*, Sandia report SAND98-1184C. American Institute of Aeronautics and Astronautics (AIAA) report AIAA-98-3464, OSTI ID: 671923. http://www.osti.gov/bridge/servlets/purl/671923-JYRvMV/webviewable/671923.pdf

features, and subcomponent design. For refurbishing a weapon, the safety theme drives the design of the replacement parts.

Enhanced Nuclear Detonation Safety (ENDS)

Three "I"s: Isolation, Incompatibility, Inoperability

Three pillars support the ENDS theme: isolation, incompatibility, and inoperability. Isolation may be considered the first among equals, as the other two principles support isolation in different ways.

1. **Isolation**: The effort here is to isolate detonation-critical components from unintended energy (electrical or mechanical). Isolation components may include metal "exclusion barriers", steel enclosures, or safety switches that stay in the off position until activated.
2. **Incompatibility**: This entails designing "enabling stimuli" – signals that eventually turn off safety features, arm the fuze, and fire the weapon – to be unique relative to signals found in nature. For instance, the theme directs the designer against using 440 Volt, 3-phase signals, since that is a common commercial power supply voltage.
3. **Inoperability**: This requires the labs to design the weapon so that critical detonation features become inoperable beyond repair before the isolation features succumb to an abnormal environment. Inoperability may be considered similar to "fail-safe" features of key detonation-critical components. Another example is the small (often red in the US) tube that melts in order to activate commercial sprinkler systems. (This tube melts away early in a fire so the water may start to flow. To be effective, the tube must melt away long before the steel sprinkler head starts to melt and malfunctions from the heat of the fire.)

Independence

One aspect of implementing the ENDS theme that has evolved with continued weapon development and production is the use of multiple, independent subsystems for the safety features. While independence is not formally part of Carl Walske"s requirement set, the concept allows engineers to design two systems with failure probabilities $\leq 10^{-3}$ instead of $\leq 10^{-6}$ which is much more difficult and expensive to build. The two systems would then be placed in series, one following the other in the system, to achieve the required assurance level. Systems with failure probabilities $\leq 10^{-6}$ are also almost impossible to verify. Specifically, far more parts would be required for testing and qualification – on the order of tens or hundreds of thousands – than would ever be produced for the weapons themselves.

Terminology

Several terms must be defined. "Exclusion Barrier" refers to a device that implements isolation of some type of energy – electrical, mechanical or thermal. Exclusion barriers keep energy that could be compatible with firing the weapon outside of those regions containing arming and firing circuitry, while letting that same energy pass through in the event of authorized use. A "stronglink" refers to a safety subsystem that is designed to withstand different types of environments and still function normally – thus forming a „strong link" in the safety system. A "weaklink" may be considered a first-failure device, or a device that ensures the larger assembly of the weapon fails safely. Both stronglinks and weaklinks are in the essential pathway of signals needed to arm, trigger and physically fire the weapon. A top-level description of the stronglink-weaklink relationship may be found in Chapter 10 of [16] and in Section 5.4 of [17].

Normal Environments

The ENDS theme is meant to lead to a weapon design that is safe, can be produced efficiently, and can withstand normal operating environments over the course of the system lifetime. The components that implement the theme in these normal environments can be seen in the warhead schematic in Figure 5. Starting with the outer barrier in the diagram, this represents the thermal barrier of the warhead. Note that all figures in this paper are strictly notional and do not represent any US weapon design. The inner rectangle represents the outer exclusion barrier, which is the underside of the warhead‟s outer shell and acts as the electrical barrier to the outside environment.

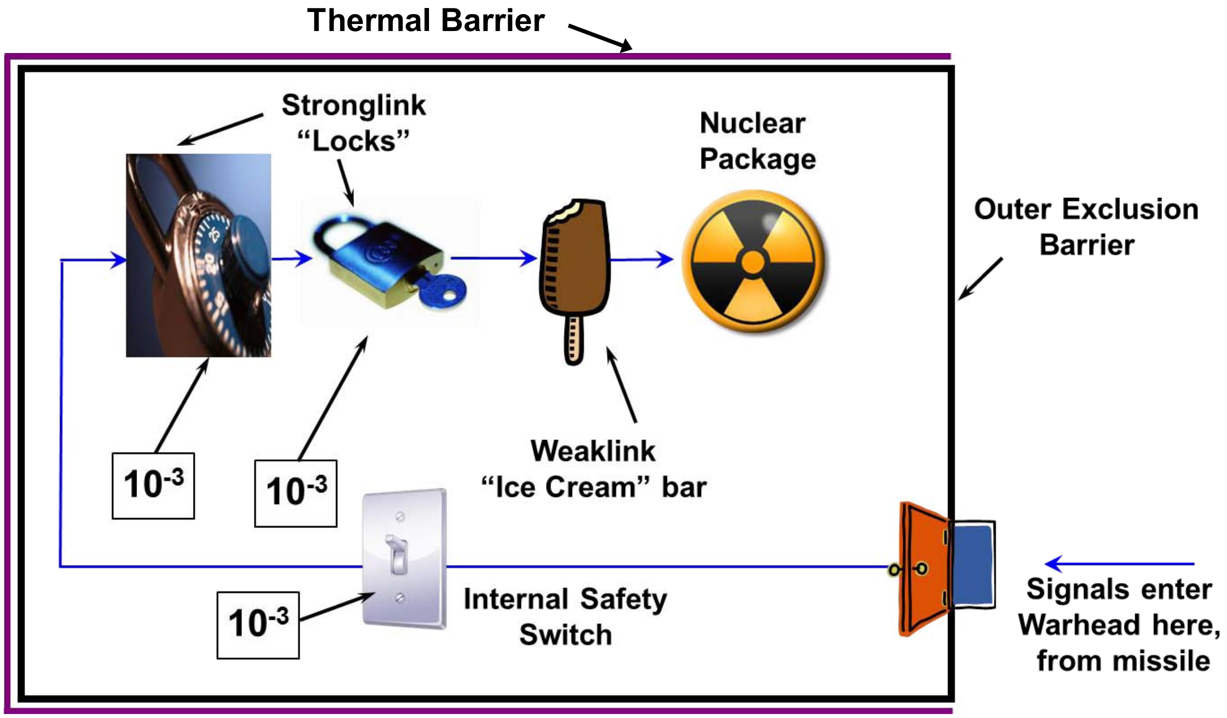

Figure 5. The ENDS theme in Normal Environments

In Figure 5, starting from the lower right, by the door, we see communication signals enter the warhead from the host missile. A similar diagram could be drawn for a bomb being carried in an airplane. The details of these signals do not affect the theme and are outside the scope of this paper; however these signals must pass into the warhead for proper operation. Once the signals

---

[16] Loeber, C. R., "Building the Bombs: A History of the Nuclear Weapons Complex," Second Ed., SAND2005-5648P. 2005 Sandia National Laboratories.

[17] Nuclear Matters Handbook, Expanded Edition. Deputy Asst. Sec. of Defense for Nuclear Matters. http://www.acq.osd.mil/ncbdp/nm/.

enter the warhead, they must pass through different switches. A switch must be unlocked or "enabled" for the signal to pass through and perform its intended function in the warhead.

The first switch is an internal safety switch, perhaps an on/off variety, which has a 10^{-3} or less chance of failure. Failure of a switch in this case means the switch is prematurely enabled. After this switch, the signals must pass through a second switch (shown as a combination lock), then finally through a third switch (represented by the padlock). Like the first switch, both of these stronglink switches have a probability of failure of 10^{-3}. The path is not yet complete, however. After the third switch the signals must detect the intact presence of the weakink device, here symbolized as an ice cream bar, in order to arm the fuze and detonate the nuclear package. The weaklink must absolutely be intact, of the correct size and shape, and fully functional for the weapon to work.

When 1) the signals pass through all the switches successfully, 2) the weaklink is functional and intact, and 3) the weapon has had a nuclear package inserted, then the weapon may then be armed and then fired. Equally important is that during the normal handing, storage and transport of the weapon, the weapon does not detonate and remains safe to 10^{-9} levels. In normal environments, the weapon is also required to meet its reliability requirements levied by the military. The other scenarios consist of abnormal environments – i.e. potential accidents. The theme is the same.

Abnormal Environments

If the weapon is involved in an accident, the military requirement is no longer that the weapon function normally if pressed into service; thus, reliability is no longer an issue. However, the weapon must still remain safe to 10^{-6} levels per the Walske criteria. This is a challenge from an engineering perspective, since the abnormal environments are far more stressing to the weapon than normal ones.

Electrical Environments

There are many different accident scenarios that a unit could face. One such environment is electrical – such as exposure to a downed power-line in the course of a transport accident (Figure 6) In this case we assume that the internal safety switch has been damaged and bypassed by the nature of the accident. In an abnormal environment, all three safety subsystems are not expected to survive. The two abnormal-environment safety features are still operable and protect the weapon. These are the two stronglinks of the system.

A unique feature of this electrical environment is that the weaklink (the ice-cream bar), which is a detonation-critical component, remains intact. Fortunately in this case, both stronglinks are still fully functional and operate as expected – providing isolation and insulation against the electrical energy present from the power line. The next section describes an environment where the weaklink does not survive: a fire.

Thermal

In the case of electrical insult, the two stronglinks operated as designed and together provided 10^{-6} safety – which met the requirement of Walske. If the accident scenario is expanded to include a fire (perhaps a fuel fire from the transport vehicle) together with a downed power line, then at some point the two stronglinks will no longer each provide 10^{-3} isolation since they will eventually fail in a fuel fire. This situation is illustrated in Figure 7. The question arises, if both stronglinks are lost, would the weapon still meet the 10^{-6} safety requirement?

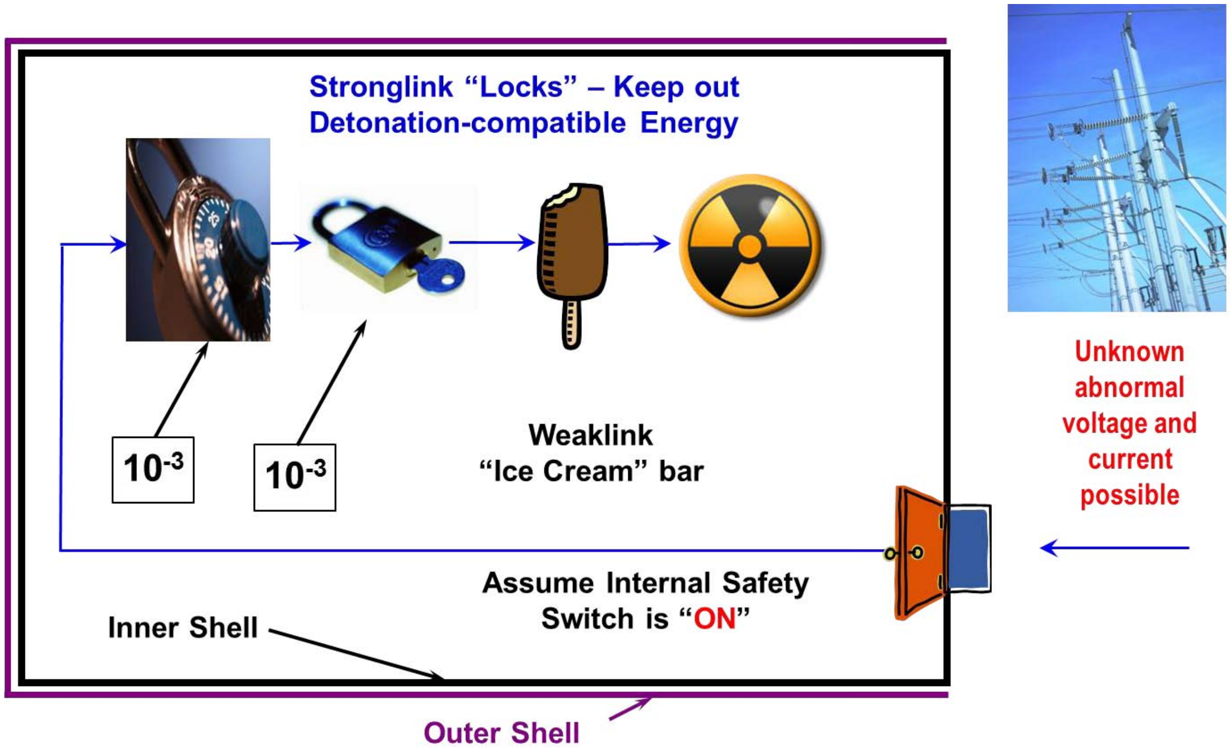

Figure 6. Abnormal Environment - Electrical only. Both stronglinks function as intended.

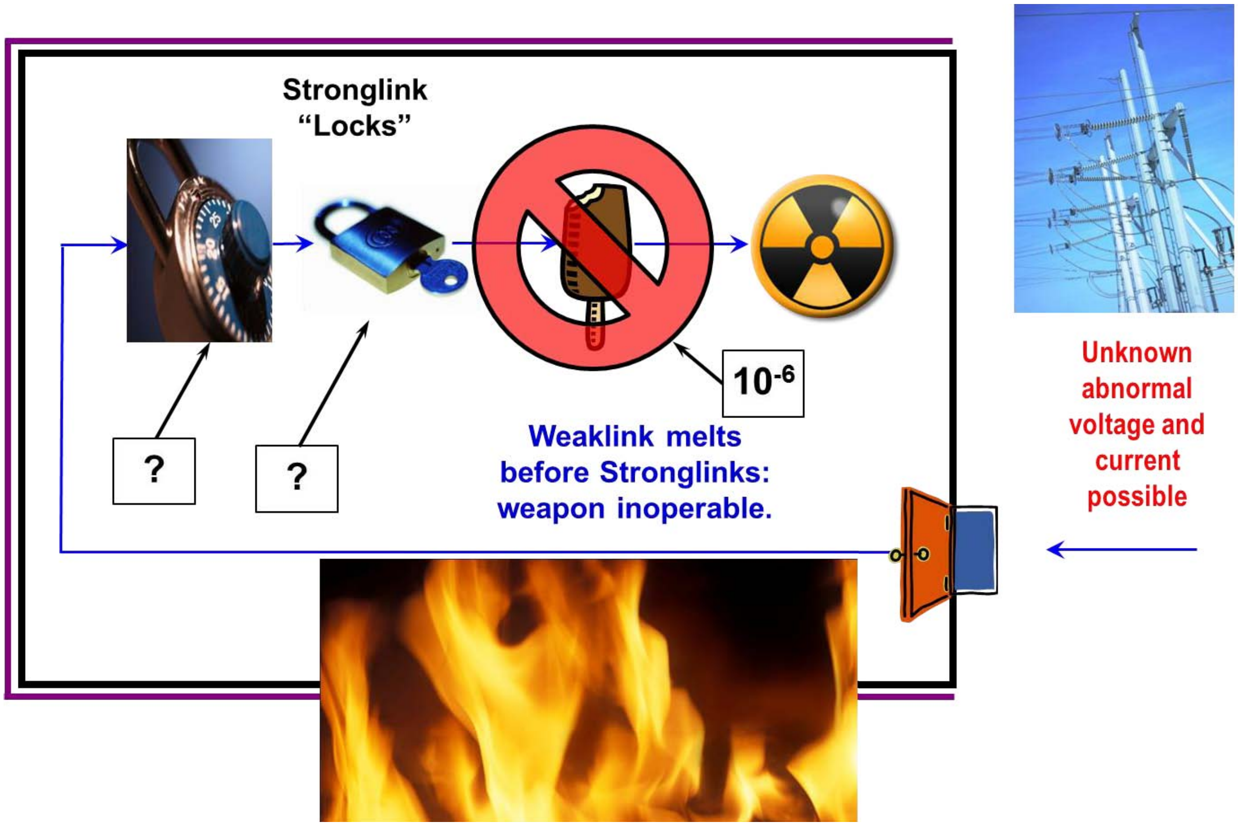

Figure 7. Abnormal Environment: Electrical + Fire. Weaklink provides the 10^{-6} safety.

This example demonstrates, with a sufficiently unstable environment, isolation can no longer be assured. In the presence of the fire, the two stronglinks move from assured, 10^{-3} safety (for each system), to an unknown but lesser safety level. To compensate for this situation, while maintaining 10^{-6} safety in credible abnormal environments, weapon designs include a weaklink device. The key to weaklinks is that they make the device irreversibly inoperable far sooner than the stronglinks fail for the same accident scenario. By the time the two locks become „soft‟ and they can no longer be assured to stay locked, the weaklink has long since lost its ability to function and, thus, so has the device as a whole. In other words, the ice cream bar had melted away. At this point, it doesn‟t matter if the stronglinks cannot provide isolation since without the weaklink, the weapon cannot work. This is sometimes called the “thermal race” – the race to failure by the weaklink vs. the stronglinks. Notionally this thermal race may be viewed as, „Which will melt faster in a fire, a steel combination lock or an ice cream bar? The thermal race must be won for each weapon.

Conclusion

The design, manufacture, and deployment of two nuclear weapons in the early and mid-40s in wartime were gargantuan endeavors.[18] It is no smaller or less complex a pursuit to build and maintain an entire stockpile of weapons that are ready to use on a moment‟s notice, with a shelf life of multiple decades, in a safe and secure manner. The problem this paper addresses is how to build this latter type of stockpile. An escalating series of accidents in the 1950s and 1960s, which happened in the course of then-normal transport of weapons and weapon parts, caused brought about new safety requirements issued by Carl Walske and the Military Liaison Committee in 1968; the "Walske criteria" led to the development of the Enhanced Nuclear Detonation Safety (ENDS) theme. Weapons designed according to this theme could be asserted to have met the new safety requirements.

This paper has discussed the Walske criteria, the ENDS theme, safety features such as exclusion barriers, stronglinks, and weaklinks, as well as normal and abnormal environments. The basics of the ENDS theme were presented: Isolation, Incompatibility, and Inoperability. This was followed by a discussion of Independence – the use of several independent subsystems in series to achieve safety requirements. ENDS in normal environments followed, after which two accident scenarios were introduced: electrical only, and electrical in combination with fire. Each scenario (normal, electrical, and electrical with fire) showed how the ENDS theme helps designers build a weapon that can remain safe in multiple abnormal environments. An ENDS-designed weapon may also protect against scenarios engineers have not thought of: this is why it is important to design to a theme, rather than to specific accident scenarios. Modern weapon systems in the US stockpile all adhere to the ENDS principles, with newer systems implementing the theme in more technologically advanced ways. While no weapon is one hundred percent safe, ENDS allows a program to meet its nuclear safety requirements while minimizing nuclear safety risks inherent in maintaining a reliable, deployable, and safe nuclear weapon stockpile.

---

[18] Richard Rhodes, *The Making of the Atomic Bomb* (New York: Touchstone, 1986).