SAND2014-16545J

One in a Million, Given the Accident: Assuring Nuclear Weapon Safety

Jason M. Weaver[1]

Since the introduction of nuclear weapons, there has not been a single instance of accidental or unauthorized nuclear detonation, but there have been numerous accidents and "close calls." As understanding of these environments has increased, the need for a robust nuclear weapon safety philosophy has grown. This paper describes some of the methods used by the Nuclear Weapon Complex today to assure nuclear weapon safety, including testing, modeling, analysis, and design features. It also reviews safety's continued role in the future and examines how nuclear safety's present maturity can play a role in strengthening security and other areas and how increased coordination can improve safety and reduce long-term cost.

Introduction

Designing a "safe" nuclear weapon seems at first a bit of an oxymoron. Yet, one of the most important factors in maintaining an effective deterrent is assuring that weapons will operate when needed, but never when unintended. This must be true for the normal life of a nuclear weapon, from assembly to retirement. But it must also hold across such varied scenarios as aircraft accidents, natural disasters, and human error during production or maintenance. Over such a wide and unpredictable range of possible abnormal environments, it would be impossible to plan for and design against every scenario, yet nuclear weapons must remain safe across these scenarios nonetheless. The Nuclear Weapons Complex follows a robust philosophy of nuclear weapon safety to assure that the likelihood of an inadvertent nuclear detonation is "vanishingly small"[2].

This paper examines the role nuclear weapon safety plays in the design, refurbishment, and deployment of the U.S. nuclear arsenal. A brief overview is given of the evolution of the nuclear weapon safety philosophy, including nuclear weapon accidents, the "Walske criteria" requirements on assured safety, and the advent of Enhanced Nuclear Detonation Safety (ENDS) architecture. The current "principles-based" approach to assuring nuclear weapon safety is described, showing how designing in passive safety features allows safety to be claimed at levels like "one in one million" and "one in one billion" with no underground weapon testing and only limited non-nuclear testing[3].

Also considered is the question of what role nuclear weapon safety should play in the larger scope of maintaining a nuclear deterrent. Recommendations are given on how increased coordination between nuclear safety and other related areas (command & control, use control,

---

[1] Jason Weaver is a Senior Systems Engineer at Sandia National Laboratories. The views expressed in this paper are those of the author and do not necessarily reflect the views of Sandia National Laboratories.

[2] Morgan Sparks to Major General Joseph K. Bratton, 1 June 1977, quoted in Stanley D. Spray, *Nuclear Weapon Safety From Production to Retirement* (Albuquerque: Sandia National Laboratories, 2001), SAND2001-0600, 27.

[3] For related commentary on the role of human factors in nuclear weapon safety, see Elise Rowan, "A Perfect Record: Assessing Risk and the Human Factor in Avoiding Nuclear Catastrophe," *Nuclear Scholars Initiative: A Collection of Papers from the 2014 Nuclear Scholars Initiative*, (Washington: CSIS/Rowman & Littlefield, 2014).

etc.) can lead to a safer nuclear arsenal even within the current political environment. The possible benefits and risks of sharing technology and information about nuclear weapon safety with other nuclear weapon states is also examined.

A Brief History of Nuclear Weapon Accidents

Five years after the atomic bomb entered the stockpile, the United States experienced its first recorded nuclear weapon accident[4]. On February 13, 1950, a B-36 carrying a nuclear weapon on a mission from Alaska to Texas developed mechanical problems over British Columbia. The crew flew over the Pacific Ocean, jettisoned the weapon, and bailed out as the airplane crashed. This accident was followed by four other similar cases the same year: three airplane crashes and one emergency bomb release over water[5]. From 1951 to 1960, over 30 additional accidents and incidents occurred[6]. These early accidents, though frequent, did not pose a risk of nuclear detonation; the weapons involved were designed with "removable cores," where the nuclear material was kept separate from the weapon until shortly before intended use.

In the late 1950s, however, weapon design moved to a "sealed pit" architecture, where warheads are manufactured and stored with the nuclear material already in place[7]. This new design has many benefits, including improved personnel safety and increased readiness, but made the existing safety protocol of removing the nuclear material infeasible. Instead, switches and other components were used to isolate the nuclear material from the energy needed to cause detonation.

Accidents in this new era became more worrisome. Safety devices like "ready/safe" switches and "environmental sensing devices" (ESDs) were supposed to assure that firing signals were kept away from detonation-critical components, but accidents and testing showed new ways to bypass or spoof these systems[8]. Many ready/safe switches were operated via small motors powered by a 28-volt signal from the airplane. In theory, this would only happen when the crew flipped the switch to arm the bomb. Instead, in an accident, loose wires or shorts in the airplane or weapon could connect, apply a voltage to enable the switch, and then energize the firing circuit. The switch could be enabled inadvertently by a crewmember bumping the control or playing with it when bored. Environmental sensing devices, typically forms of accelerometers or barometers,

---

[4] William L. Stevens, *Report D: A Summary of Accidents and Significant Incidents Involving U.S. Nuclear Weapons and Nuclear Weapon Systems*, (Albuquerque: Sandia National Laboratories, 1986), J-3. The report quotes the DoD definition of an "accident involving nuclear weapons" as an unexpected event involving nuclear weapon or nuclear weapon components that results in accidental or unauthorized use of a nuclear-capable weapon system, nuclear detonation, non-nuclear detonation or burning of the weapon or components, radioactive contamination, loss of the weapon or components, or other public hazard.

[5] Shaun Gregory, *The Hidden Cost of Deterrence: Nuclear Weapon Accidents*, (Exeter: B.P.C.C. Wheatons Ltd., 1990), 147-148.

[6] Ibid., 148-156.

[7] David W. Plummer and William H. Greenwood, "The History of Nuclear Weapon Safety Devices," *34th AIAA/ASME/SAE/ASEE Joint Propulsion Conferences* (July 1998): 1, doi: 10.2514/6.1998-3464.

[8] Ibid., 2-3.

were supposed to enable only when they sensed the proper environment (acceleration or altitude). But if a bomb were accidentally dropped out of an airplane, how would the ESDs distinguish between an accidental drop and deliberate use?

A prime example of this occurred on January 24, 1961, when a B-52 carrying two nuclear weapons broke apart over Goldsboro, North Carolina. The two bombs separated from the aircraft. One of the bombs fell free and broke apart upon impact. No explosion occurred. The other bomb's parachute deployed and the weapon received little impact damage[9]. As Sandia Laboratories engineer Parker Jones later noted in a memo, the bomb had four safety mechanisms, but three were damaged or activated by the aircraft breakup and fall. The weapon only failed to detonate because a single ready/safe switch was set to "safe," preventing the firing signal from reaching the explosives. "One simple, dynamo-technology, low voltage switch stood between the United States and a major catastrophe!"[10] Jones further pointed out that this switch was hardly fool proof—several instances were discovered where weapons were flown with the switch enabled as a result of shorted wires or human error. When newly appointed Secretary of Defense Robert McNamara learned of the accident, "the story scared the hell out of him"[11].

As airborne global alert programs kept B-52s in the air around the clock in the 1960s, accidents continued with increasing frequency. The role of nuclear weapon safety finally gained widespread public attention with accidents in Palomares, Spain and Thule, Greenland. In January 1966, a B-52 collided with its refueling tanker and both aircraft crashed near Palomares Spain. The B-52 carried four nuclear weapons. One was recovered on the ground; and one was recovered from the sea on April 7 after extensive search and recovery efforts. Two of the weapons' high explosive materials exploded on impact with the ground, releasing some radioactive materials. Approximately 1,400 tons of slightly contaminated soil and vegetation were removed to the United States for storage at an approved site. The Pentagon put the bomb recovered from the ocean on display for reporters, hopeful that actually seeing the recovered weapon would quell the bad press and reassure the public[12].

Two years later, a B-52 crashed and burned some seven miles southwest of the runway at Thule Air Force Base, Greenland, while approaching the base to land. The bomber carried four nuclear weapons, all of which were destroyed by fire. Some 237,000 cubic feet of contaminated ice,

---

[9] Plummer and Greenwood, "The History of Nuclear Weapon Safety Devices," 1.

[10] Parker F. Jones, *Goldsboro Revisited, or How I Learned to Mistrust the H-Bomb, or To Set the Record Straight*, (Albuquerque: Sandia Laboratories, 22 October 1969), 1-2. This document was originally classified Secret/Formerly Restricted Data; a redacted, unclassified version was released to Eric Schlosser via a Freedom of Information request and published online by *The Guardian* at http://www.theguardian.com/world/interactive/2013/sep/20/goldsboro-revisited-declassified-document

[11] Eric Schlosser, *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*, (New York: Penguin Press, 2013), 247.

[12] Ibid., 314-319.

snow and water, with crash debris, were removed to an approved storage site in the United States. The day after the Thule accident, the airborne alert program was canceled, permanently[13].

The most recent nuclear weapon accident occurred on September 19, 1980 in Damascus, Arkansas. In a Titan II silo, an Air Force repairman dropped a heavy wrench socket, which rolled off a work platform and fell toward the bottom of the silo. After seventy feet, the socket bounced and struck the missile, causing a leak from a pressurized fuel tank. Eight and a half hours later, fuel vapors within the silo ignited and exploded. The nuclear warhead was recovered intact. There was no radioactive contamination. Nevertheless, the accident resulted in serious injuries and one death[14].

Even today, nuclear weapons continue to be susceptible to these types of scenarios. Numerous "incidents," where fires, crashes, or other abnormal situations occurred but did not damage or affect the nuclear weapon itself (and thus be classified as an "accident"), continue to be reported in the years since 1980[15]. In 2008, for example, a maintenance crew entered a Minuteman III silo at F. E. Warren Air Force Base to investigate a faulty sensor reading. They found the wires to the sensor had been shorted out in a fire five days earlier—a fire that, until then, nobody had known about. A power interruption, a battery charger leaking hydrogen gas, a lack of circulating fresh air, a nearby flammable shotgun case (filled with ammunition) and an abundant use of duct tape on the missile's umbilical cables had combined to result in a brief but serious fire. The heat had destroyed the umbilical cables and pressure monitor cable leading to the missile. Fortunately, the majority of the missile and the warhead itself were undamaged[16].

Enhanced Nuclear Detonation Safety (ENDS)

At the beginning of the nuclear era, the Atomic Energy Commission (AEC) was responsible for safety during the production, transportation, and storage of nuclear material. This nuclear material remained separate from the weapon until shortly before use; thus, the possibility of accidental nuclear yield during peacetime was very low[17]. However, competing demands for reliability and readiness during the Cold War led to the development of the sealed pit design. With the ingredients for nuclear yield now permanently assembled within the warhead, a more disciplined approach was needed to assure these weapons remained as safe as possible.

In the 1950s, the Department of Defense (DoD) and the AEC began instituting standards for nuclear weapon safety. Policy maintained that nuclear weapons "require special consideration

---

[13] Schlosser, *Command and Control*, 320-325.
[14] Ibid., 6-7.
[15] Gregory, *The Hidden Cost of Deterrence*, 177-183.
[16] *United States Air Force Missile Accident Investigation Board Report, Minuteman III Launch Facility A06, 319 Missile Sq., 90 Op. Group, 90 Missile Wing, F. E. Warren AFB, Wyoming, May 23, 2008*, Robert M. Walker, President, Accident Investigation Board, 18 September 2008, 1:1-18.
[17] Stanley D. Spray, *History of U. S. Nuclear Weapon Safety Assessment: The Early Years*, (Albuquerque: Sandia National Laboratories, 5 May 1996), SAND96-1099C, 2-3.

because of their political and military importance, their destructive power, and the potential consequences of an accident…. The search for increased weapon system safety shall be a continuous process beginning as early as possible in development, and continuing throughout the life cycle of a nuclear weapon system"[18]. The use of "positive measures," or features included in the design specifically to prevent arming or firing a weapon, was strongly encouraged.

However, two issues stunted the progress of nuclear weapon safety. The first was an over-confidence in the effectiveness of existing designs and practices. It was assumed that highly complex, dangerous systems like nuclear weapons could be safely governed merely through careful design and strict adherence to procedures in the field[19]. Despite the many nuclear weapon accidents, no weapon had ever gone off unintentionally, so it could be argued that the status quo was working just fine. Post-accident statements by the military like "the possibility of an accidental nuclear explosion taking place is essentially impossible" or "[the chances are] so remote that they can be ruled out completely"[20] perpetuated the public belief that these weapons were safer than they actually were.

The second obstacle to improving nuclear safety was the perceived trade-off between safety and reliability. This is the "Always/Never"[21] problem—assuring that a nuclear weapon will always work when you want it to, but never go off otherwise. Any additional feature added to the system to prevent accidental or unauthorized use would also be a potential point of failure that could dud the weapon during authorized use. When engineers at Sandia started pushing for ESDs on ballistic missile warheads in the late 1950s, the Army pushed back, claiming that adding an additional switch would hurt reliability[22]. Even up through the 1970s and 1980s, it would routinely take years, even decades, to get approval from the military and funding from Congress to implement what was seen by design engineers to be rather urgent safety improvements[23].

Slowly, safety became a more visible priority. In 1957, Sandia conducted the first comprehensive look at all nuclear weapon accidents up to that point. It was clear that nuclear weapons were not and really never could be made completely safe. Instead, any nation with a nuclear arsenal was fundamentally "playing percentages"[24]. The military attempted to determine what those odds would be; what would be acceptable to the American people. An initial DoD study assumed the public would accept accidents with frequency similar to major natural disasters like earthquakes. It gave a recommended maximum probability of an accidental nuclear explosion at one in 100,000 per year for hydrogen bombs, one in 125 per year for atomic bombs. A second study

---

[18] Spray, *History of U. S. Nuclear Weapon Safety Assessment*, 4.
[19] For an analysis of this perspective, see Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, (Princeton: Princeton University Press, 1993), 14-52.
[20] Hanson W. Baldwin, "Chances of Nuclear Mishap Viewed as Infinitesimal," *New York Times*, March 27, 1966.
[21] Peter Douglas Feaver, *Guarding the Guardians*, (Ithaca: Cornell University Press, 1992), 12-20.
[22] Schlosser, *Command and Control*, 196-197.
[23] Ibid., 453-454.
[24] Ibid., 171.

gave a probability of one in 10 million for any given weapon over its lifetime, if kept in storage. However, if the weapons were loaded onto planes, the study's probabilities for a weapon going off every decade was one in five for an hydrogen bomb and 100% for an atomic bomb[25].

By the late 1960s, there were many different methods being used to determine the safety of nuclear weapons probabilistically. Some agencies took a conservative approach, determining the probability of producing nuclear yield with the assumption that an accident had occurred. Others held the view that the probability of the accident itself could be rolled into the calculations. It was unclear whether a stated probability was for a single weapon or for all weapons, for each year or for a weapon's lifetime. This was leading to confusion as to whether individual weapon designs were in fact meeting the required probabilities. In 1968, the assistant to the secretary of defense for atomic energy, Dr. Carl Walske, codified the safety standard for nuclear weapons:

> The probability of a premature nuclear detonation of a bomb [or warhead] due to bomb [or warhead] component malfunctions, in the absence of any input except for specified signals (e.g. monitoring and control) shall not exceed:
>
> (1) Prior to receipt of the pre-arm signal, for normal storage and operational environments described in the STS (Stockpile-to-Target Sequence), 1 in 10^9 (one in one billion) per bomb [or warhead] lifetime.
>
> (2) Prior to receipt of the pre-arm signal, for the abnormal environments described in the STS, 1 in 10^6 (one in one million) per bomb [or warhead] exposure or accident.[26]

Walske also stipulated that all nuclear weapons in the stockpile must be "one-point safe;" that is, the weapon must have a probability of less than one in one million of producing a nuclear detonation if a detonation of the high explosives originates from a single point (as would likely happen in a crash or fire). These "Walske Criteria" are essentially the same standards that are followed today by the Nuclear Weapon Complex and the DoD for all nuclear weapons.

About the same time, Sandia Laboratories formed a safety department to examine whether current design practices were sufficient for nuclear safety. The group determined that even with the more precise wording of the Walske criteria, it was still virtually impossible to accurately gauge probabilities using existing methods. The number of nuclear weapons exposed to accidents was simply too low to generate any statistically significant conclusions. The fact that weapons had survived several fires, crashes, etc. was not sufficient to make a meaningful calculation of how likely they were to survive all future accidents. The space of possible accident scenarios and abnormal environments was too vast, and the behavior of current safety components across all environments was essentially unknowable. As Richard Feynman would

---

[25] Schlosser, *Command and Control*, 172.

[26] U.S. Dept. of Energy and U.S. Dept. of Defense, *Glossary of Nuclear Weapons Materiel and Related Terms, TP4-1*, 31 May, 2005.

later say about the Challenger shuttle explosion, "The fact that this danger did not lead to a catastrophe before is no guarantee that it will not the next time, unless it is completely understood. When playing Russian roulette, the fact that the first shot got off safely is little comfort for the next"[27].

Instead of relying only on probabilistic analysis, the safety engineers proposed developing a more thorough understanding of component behavior in abnormal environments. As they began to experiment, the results were shocking, even to the safety engineers. Fundamental assumptions about how materials and components would behave in certain environments were proven false. To demonstrate the flaws in current hardware, the department assembled a "burned board room" that they could show to Sandia management and visiting DoD officials. Circuit boards, wires, and switches that were supposed to keep electrical energy away from critical areas of the weapon were shown to behave unpredictably in fires and other abnormal environments—wires on opposite sides of the warhead could come into contact; circuit boards could melt and short to other locations; switches could be forced closed through mechanical impact or stray electrical signals. The evidence was indisputable, and within two years, a new plan for assuring nuclear safety was formulated. This new philosophy was termed Enhanced Nuclear Detonation Safety, or ENDS. ENDS depends on three fundamental nuclear safety principles: *isolation*, *incompatibility*, and *inoperability*.

In ENDS, to assure that a nuclear weapon remains safe, critical components like high explosives, detonators, and firing sets must be kept *isolated* from any energy that could set off the detonation sequence. The primary focus is electrical energy, but could also include any other types of compatible energy, like heat or mechanical impact. These detonation-critical components are enclosed by robust barriers that form complete Faraday cages, preventing electromagnetic energy from reaching the interior "exclusion regions."

However, in order for the weapon to function, there must be some way for the proper arming signals to be delivered to the detonation-critical components. Thus, the design must assure that signals that can activate the weapon for intended use are *incompatible* with signals resulting from other sources in normal or abnormal environments. For example, the ready/safe switches previously described could easily be enabled by accidental application of DC power from the aircraft. ESDs are more appropriate for driving incompatibility, since they can only be enabled by specific environments, like a predetermined barometric pressure or acceleration. Yet even these devices are not very robust in accidents—many common accident environments can replicate the enabling environments. ENDS recommends using devices called "strong links" to regulate what signals are passed through the barriers to the detonation-critical components. A strong link is a mechanical switch designed to always fail safe—it remains in a safe state when

[27] Richard Feynman, "Personal Observations on the Reliability of the Shuttle," *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, 1986, Appendix F.

exposed to an insult that damages it to failure. The only way to enable a strong link and allow arming signals through is to send it a specific complex pattern called a "unique signal." This unique signal is engineered to be extremely unlikely to be found anywhere in normal or abnormal environments The signal is not stored anywhere in the weapon until the weapon is deliberately armed by the aircraft or missile crew. If an incorrect unique signal or a similar but different signal from the environment is received by the strong link, the device immediately and permanently locks up in the safe state.

Combining isolation and incompatibility allows the weapon to passively control what signals and energy types are allowed to reach the detonation-critical components. Yet there is still a major concern: no barrier or strong link can be designed sufficiently robust to survive every possible accident scenario. Of particular concern are thermal environments. Accidents involving fires from jet fuel or rocket propellant are among the most common accidents encountered. Even the most exotic alloys may weaken or melt in such a scenario, creating breaches in the isolation barriers and strong links. The solution to this limitation is the principle of *inoperability*. In an accident, at some point before isolation may be lost, one or more of the detonation-critical components must be rendered inoperable. This is often done by including in the component a key material known to melt at a specific temperature well below the failure temperature of the barriers and strong links. A detonation-critical component that is assured to become permanently inoperable in certain environments is called a "weak link." A weapon system using ENDS typically includes at least a thermal weak link, with other types of weak links (like ones that become inoperable in certain mechanical impact or crush environments) also encouraged.

In addition to *isolation*, *incompatibility*, and *inoperability*, there is also a fourth "I" used in ENDS: the principle of *independence*. It is extremely difficult, often impossible, to design, build, and test devices that can be shown to be reliable to levels of one in one million or billion. Instead, an ENDS safety architecture will include multiple sets of strong links, weak links, and barriers nested within one another, with each safety subsystem largely independent of the others. If the different subsystems are sufficiently independent, the respective assurance levels for each subsystem can be multiplied together to get an overall system assurance level. Two one-in-one thousand safety subsystems can be combined to yield a system assurance of one in one million; three can be combined to provide one in one billion. This method of multiplying probabilities is only possible if the failure modes for each safety subsystem are truly independent from each other, which becomes more and more difficult as more complexity is added.

Because the positive measures used in ENDS are passive and designed to fail safe, the designers more fully understand how the weapon will behave in an accident, even though some specifics about the environment are unknown. Thus, a properly implemented ENDS safety architecture can assure that the weapon meets the one in one million and one in one billion levels mandated by the Walske criteria, *regardless of the accident type encountered*.

Assuring Nuclear Weapon Safety Today

Implementing ENDS into the nuclear stockpile was a slow and painful process. Almost every weapon in the 1970s stockpile needed some sort of alteration to fully meet ENDS, but both the DoD and the weapons labs were reluctant to take the drastic and expensive measures needed for such a retrofit. Thus, the primary means for implementing ENDS was one weapon system at a time, as new ones were designed and existing ones were retired or modernized. As late as 1990, over two decades after ENDS was first recommended, only half of the weapons in the stockpile were equipped with ENDS[28]. As the Cold War ended in the late 1980s and early 1990s, focus finally shifted from meeting the Soviet threat to cost cutting, modernization, and responsibly shrinking the stockpile. With aging weapons and new constraints on budget and testing, there was a major push to determine how to better assure that the stockpile as a whole remained safe, secure, and reliable.

Today, several life extension programs and alterations are in various stages of development: the W76-1 and B61-12 life extension programs, the W88 Alteration 370, and the W87 fuze program. Several more are being planned, detailed in the "3+2" long-term schedule proposed by the Nuclear Weapons Council[29]. For every one of these programs, the major intent is to replace limited-life components, increase safety and reliability by upgrading components and safety architectures, and decrease lifetime costs by making them easier to manufacture and inspect.

This new generation of weapons, beginning with the W76-1 currently in full production, will include strong links and weak links much more sophisticated and foolproof than the first generation of ENDS weapons. Future weapons may include features that support safety even more strongly, such as more sophisticated strong links and weak links, insensitive high explosives, fire-resistant pits, and improved fabrication and inspection techniques.

There are limitations to what can be done for safety, however. The Nuclear Weapons Complex no longer has a blank check for weapon development. Even though the enterprise makes up only a small portion of the defense budget, every line item is inspected and negotiated. The possibility of bureaucratic wastefulness, both within the Nuclear Weapons Complex and within the military and government in general, increases the overall reluctance to spend billions of dollars to upgrade weapons that appear to already meet their requirements satisfactorily. The moratorium on underground testing and the restriction that refurbished weapons often must reuse nuclear material and various other components also limits what improvements are possible.

---

[28] *The Report of the Nuclear Weapons Safety Panel, Before the House of Representatives Committee on Armed Services ("The Drell Report")*, 101st Cong. 10 (1990) (statement of Sidney D. Drell, Chairman, Nuclear Weapons Safety Panel.

[29] *Fiscal Year 2015 Stockpile Stewardship and Management Plan*, (Washington: U.S. Department of Energy, April 2014), 1-2 – 1-4.

In light of these restrictions, how do engineers at Sandia, Los Alamos, and Lawrence Livermore National Laboratories demonstrate safety today? The weapons labs approach this analysis from several angles. First, extensive computer modeling is done at system, subsystem, and component levels. These models are far more sophisticated than anything available when previous generations of weapons were being designed. Mechanical, thermal, and electrical models can simulate the behavior of the weapon systems in a wide variety of accident scenarios. These simulations are reinforced by physical testing, also performed at system, subsystem, and component levels. These tests are used to calibrate and confirm the simulations, and they give insight into complex abnormal environments that cannot be accurately modeled. Both physical testing and computer modeling begin early in the design process, and continue long after production ends, taking into account continued aging and any information discovered through stockpile surveillance. And of course, the passive, fail-safe features found in ENDS architectures provide confidence that the weapons remain safe even in those accidents that defy our expectations.

The American Association for the Advancement of Science and the Union of Concerned Scientists recently published a summary of opinions expressed at their 2012 workshop on nuclear weapon safety and security[30]. The consensus appeared to be that nuclear weapon safety in the U.S. stockpile is reasonably mature: "In general, participants were not greatly concerned about the safety of existing warheads. A few participants noted that improved safety was beneficial…but overall, as one participant noted, safety 'is not something I lose sleep over.'" The participants in the workshop, in general, felt that cost, command & control, and evolving threats to security (particularly cyber security and use control) were areas of far greater concern.

The Continuing Role of Nuclear Weapon Safety

The safety of the U.S. nuclear arsenal has improved greatly in the last half century, and it now seems fairly robust. What, then, is the role of nuclear weapon safety assurance going forward? Is safety being neglected due to budget constraints, or are currently planned spending levels for nuclear safety sufficient or even excessive to maintain a safe stockpile? If all the current weapon systems meet the Walske Criteria and have ENDS architectures, what is there left to do?

The question of how much to spend refurbishing our nuclear weapons is, of course, complicated. The multi-billion dollar B61-12 program has drawn attention to the question of what level of spending can be justified for these life extension programs[31]. The B61-12 will feature new strong links and weak links, as well as other incremental safety improvements. However, other more substantial safety proposals for the weapon were tabled due to projected cost and required development time. This trend will likely continue in future life extension programs—minor

[30] *Summary Report: Workshop on U.S. Nuclear Weapons Safety and Security, December 12, 2012*, American Association for the Advancement of Science and the Union of Concerned Scientists, September 2013, 1-2,13-20.
[31] Ibid., 9-10.

improvements will be implemented as the opportunity arises, but major design changes that would dramatically improve safety margin will have difficulty finding support. Often, such changes fall outside the limited scope of individual programs or require lead-time and research investment far beyond what any one program is willing to support. Sandia National Laboratories attempts to address the second problem by devoting part of its funding to long-term research, separate from the individual weapon programs, thereby providing a means to develop concepts to sufficient maturity so they can be implemented down the road.

It is vital that nuclear weapon safety remain tightly integrated into both the design of new weapons and the surveillance of the existing stockpile. There are two main points to consider. The first is that continued vigilance is necessary to prevent unsafe designs or practices from creeping in. As experienced designers, manufacturers, testers, and handlers are gradually replaced by new personnel, the lessons from the past are likely to be forgotten unless carefully passed down to the next generation. The weapons labs have been forced to deal with this issue already—from the time that new weapon design stopped in the early 1990s until work started on the W76-1 in the mid-2000s, much experience was lost as the workforce contracted and shifted to other priorities. As a result, new engineers tasked with designing the W76-1 had a substantial learning curve as they tracked down the rationale for previous design choices and formulated their own safety architectures. A detailed record of past programs and a competent workforce must be maintained at each of the weapons labs to avoid repeating mistakes of the past or accidentally overlooking a potential safety concern.

The second reason nuclear safety must remain a core focus of research is that our understanding continually grows as new knowledge comes to light. Remember, most of the engineers in the 1950s and 1960s believed that their designs were safe too. It was not until accidents revealed possible flaws and key tests were performed that a paradigm shift occurred and changes were made. Although the Nuclear Weapons Complex maintains that the current stockpile is safe, future accidents or studies may reveal gaps in our understanding—accidents previously deemed infeasible, manufacturing flaws discovered in the field, unanticipated byproducts of design choices, or behavior by those handling the weapons not consistent with what is established in documented processes. Some of these may merely show the wisdom of future upgrades in the next round of life extension programs; others may possibly necessitate immediate removal of some weapons from the stockpile for repair or retirement.

Beyond the core responsibility of designing and maintaining safe weapons, the nuclear weapon safety community can contribute to the nuclear community in other ways. As seen previously, command & control has often been mentioned as an area of concern. Though the situation is much better coordinated than it has been in the past, it remains an area where substantial safeguarding and improvement is possible. The lessons learned in developing assured nuclear weapon safety may in many cases be carried over into this field. In particular, aspects of the command & control structure could be redesigned incorporating more design features that fail safe (minimizing false positives) without hampering the ability to transmit and verify legitimate

messages. Better communication and coordination between those designing safety into the weapons themselves and those managing safety, security, and control administratively can help assure that instead of hardware and actual behavior possibly neutralizing each other's effectiveness and introducing holes to the system, they can work together to keep the arsenal predictably safe and secure.

The nuclear weapon safety community can fulfill an important function in public outreach as well. As is apparent by the interplay between the military and the public during past nuclear weapon accidents, there is a long history of mutual distrust, with the military often understating the severity of accidents. Some level of security is of course necessary to preserve classified information; representatives from the weapons laboratories (particularly the accident response teams) could be seen by the public as a more safety-oriented voice clarifying the background of any future accident and explaining the steps taken to ensure the public's safety.

Finally, an interesting opportunity may exist to share some level of nuclear weapon safety design with other nuclear-armed states. Studies by Sandia National Laboratories[32] and a NATO research workshop[33] in the mid-1990s examined the merits and risks of opening a dialog among the five recognized nuclear weapon states discussing best practices in nuclear surety. They concluded that such an exchange would be beneficial. Possible risks or hindrances could include adversaries using the exchange as a platform for other issues, giving an adversary increased readiness or reliability as a result of enabling safer designs, or unwittingly revealing non-surety-related information. It was agreed that a formal, summit-type meeting would be counterproductive, but that informal exchanges should be actively pursued and documented. This has been pursued to some extent under mutual defense agreements[34] and papers presented in public forums[35], but more likely can be done, particularly with newer nuclear-armed states like India and Pakistan (while carefully considering the risks above). An accidental nuclear weapon detonation would affect everybody. Improving the assured safety of all nuclear weapons, even those of our adversaries, is a noble goal that would make the world just a little bit safer.

---

[32] Steve Parker and Jessica Glicken, *A Vital Issues Report: The Merits of Conducting an International Exchange on Nuclear Surety Topics Among the Five Acknowledged Nuclear Weapon States*. (Washington DC: Sandia National Laboratories, 24 July 1995), 1N.2958, 5-20.

[33] Scott D. Sagan and Benjamin A. Valentino, *Nuclear Weapons Safety After the Cold War: Technical and Organizational Opportunities for Improvement; A Report of a NATO Advanced Research Workshop*, (Stanford: Stanford University, 1994), 4-7.

[34] For example, Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for Co-operation on the Uses of Atomic Energy for Mutual Defence Purposes, U.S.-U.K., Aug. 4, 1958, T.I.A.S. 4078.

[35] For example, G. K. Hansen, S. Lydersen, and H. Sandtorv, eds., *Safety and Reliability: Proceedings of the ESREL '98 Conference, Trondheim, Norway, 16-19 June 1998*, (Rotterdam: Balkema, 1998).