US Nuclear Weapon Safety and Control

Grant Elliott*
MIT Program in Science, Technology, and Society
(Dated: December 12, 2005)

In light of the devastating political and social effects of an accidental (or intentional, but unsanctioned) nuclear detonation, an intricate network of safety and control mechanisms has been implemented in the US nuclear arsenal. We discuss these measures, including technological solutions to restricting the use of weapons and preventing accidents, as well as procedural solutions which attempt to mitigate the risk of mistakes or intentional misuse. Technologies covered include Environment Detection Sensors (EDS), Permissive Action Links (PAL), Enhanced Nuclear Detonation Safety (ENDS), Insensitive High Explosive (IHE), and Fire Resistant Pits (FRP).

1. INTRODUCTION

To appreciate the public's fascination with nuclear weapon safety, one must look no further than the cinema. In Kubrick's classic *Dr. Strangelove or How I Learned to Stop Worrying and Love the Bomb*, a deranged US officer succeeds in launching a nuclear attack on the Soviet Union without authorization. Countless other films place stolen nuclear weapons in the hands of terrorists who use them to hold cities hostage. Clearly, popular culture reflects popular concern—the US armed forces were so concerned with the effect Kubrick's film could have on the populace that they required it to be prefaced with a disclaimer stating the impossibility of the events depicted.

But how safe are nuclear weapons in practice? Could a deranged officer launch or detonate a warhead? Could a terrorist? We examine these questions in terms of safety and control features maintained on the US arsenal of nuclear weapons. In this context, safety features are those which prevent disasters in the event of accidents while control features are those which prevent disasters as the result of deliberate misuse. As we shall see, the two often overlap with systems serving both safety and control purposes.

The history of these features, in many respects, corresponds to concerns of the day. While several safety features were born from severe accidents in the 1960s, most control systems were developed as a result of political concerns, including the deployment of nuclear weapons to potentially unstable countries. As a result, these features reflect the history and politics of the weapon itself.

1.1. Accidents

While there have been dozens of accidents involving US nuclear weapons, not one has resulted in even a partial nuclear detonation. In two cases, however, the devastation of a warhead resulted in the dispersal of radioactive material, contaminating the area of the accident. These accidents are described here as evidence for the need for safety devices on warheads. Most safety technology (see Section 2) focuses on preventing dispersal of this kind, rather than the less likely case of an accidental nuclear detonation.

1.1.1. Palomares

The best known nuclear accident occurred over Palomares, Spain in January, 1966 when a B-52G bomber collided with a tanker aircraft during a refueling operation. The tanker exploded and the B-52G broke up, dropping its four B28 thermonuclear bombs, some of which deployed parachutes[1]. One landed safely on the ground and another was recovered several months later (see Figure 1) by an unmanned submersible (see [8] for an account of the recovery). The conventional explosives of the remaining two weapons detonated on impact with the ground, spewing plutonium into the small farming village.

The decontamination effort involved the removal of more than 1,400 tons of contaminated soil over more than a square mile (see Figure 2) and hundreds of residents underwent medical tests for the next 30 years. Air monitoring and soil sampling continued for several years as well. The monetary cost of the accident is estimated at just $120 million[1]. The political cost could potentially have been much higher, but General Franco was determined to downplay the significance of the accident.

Had the B28 warheads been equipped with insensitive high explosive (IHE; see Section 2.2.2) and fire resistant pits (FRP; see Section 2.2.3), the Palomares accident would have been far less severe. These safety mechanisms protect the nuclear material in the pit from extreme environments. In this case, had the high explosives of two of the weapons not detonated, the radioactive material would have remained safety encapsulated within the weapon and the contamination would have been avoided.

*Electronic address: gelliott@mit.edu

FIG. 1: **The B28 warhead recovered from the ocean floor following the Palomares accident.** Notice the damage to the nose caused by the impact. The underwater search effort for this weapon lasted 80 days. This image is also noted as one of the earliest publicly available photographs of a US thermonuclear weapon. Image from [12]

FIG. 2: **Contaminated soil and vegetation following the Palomares accident.** 1,400 tons of material was packaged in barrels and shipped to the US for disposal. The cleanup and subsequent monitoring cost $120 million. Image from [12]

1.1.2. Thule

Less well known, but equally serious was an accident at Thule Air Base, Greenland in 1968. Another B-52G, already suffering from a fire which had disrupted its power, crashed into the North Star Bay and burst into flame. High explosives on all four of its B28 bombs detonated, contributing plutonium, uranium, and tritium to the burning debris[1].

The cleanup, dubbed Project Crested Ice, required the removal of 10,000 tons of snow, ice, and debris prior to the spring thaw. Part of one weapon melted through the ice and had to be retrieved by submersible from the lake below. The effort is reported to have cost $9 million dollars and potentially exposed hundreds of workers to dangerously high levels of radioactivity. Long term monitoring of the workers' health was not performed, so it is impossible to know the extent of the human damage caused. It is known that the Danish workers experienced a much higher incidence of cancer in addition to many other dehabilitating ailments, though an attempt to sue the US Government was disallowed[1].

As in the Palomares accident, modern safety features could have minimized this devastation. The aircraft burned for approximately twenty minutes. Even at the temperature of burning jet fuel, modern insensitive high explosives would not have detonated in this short time.

1.2. The Politics of Safety and Control

The issues of safety and control are seen today as being about protecting the population, either from accidents or from adversaries and madmen; in fact, they are far more complicated. As described in Section 2.2.4, the first motivation for installing PAL locks on missiles was to prevent the weapon's use not by an adversary, but by an ally. With the growing need to deposit weapons on foreign soil, the US needed to maintain control over them and PAL was born.

Similarly, it is doubtful that safety systems would have come as far as they have were it not for the accidents described in Section 1.1 and the dozens of other near misses. The political ramifications of a large scale nuclear accident or nuclear detonation, particularly if it happened abroad, would be devastating. Nuclear safety measures are as much a product of politics as they are of concern for safety.

Most significantly, it is important to realize that all failsafes and safeguards represent a tradeoff between usability and security. Consider the infamous Minuteman PAL codes. As Secretary of Defense to the Kennedy and Johnston administrations, Robert McNamara had seen to it that PAL locks (see Section 2.2.4) be installed on all Minuteman missiles. While the locks were installed, the Strategic Air Command (SAC) in Omaha had all of the codes set to 00000000, in order to ensure that the safeguard not interfere with their ability to launch quickly in a time of crisis. The locks were not activated until 1977, nearly 20 years after they been installed[4].

Quick launch capability is at odds with most control systems. The elaborate procedures which precede all nuclear launches, from silos to submarines, represent delays which could potentially prevent the launch of the weapon. One can further imagine scenarios which appear to render the launching of nuclear weapons impossible, such as the partial destruction of a silo's launch control center making access to PAL codes impossible.

Similarly, one may ask how PAL codes should be distributed. If one level of command maintains all codes, then destruction of that center or a loss of communication could render the entire stockpile useless. At the same time, the farther down the chain of command PAL

codes are allowed to reside, the more likely it becomes that the codes be compromised, possibly resulting in an intentional, albeit unauthorized, nuclear detonation.

These tradeoffs lie at the heart of the technical problems of safety and control. Ultimately, choices must be made and the middle ground will surely come at some cost to peace of mind. No technological solution can solve the fundamental problems of securing a weapon while maintaining its usability. Weapon control will always be a human issue.

2. THE BOMB

While launch and storage site security and procedures (see Section 3) should preclude the accidental (or deliberate, though unsanctioned) launch or theft of a nuclear weapon, the possibilities cannot be ignored. Further, in light of past accidents (see Section 1.1), a nuclear weapon must be designed to withstand extreme conditions, such as impact and fire, without detonating its nuclear payload. As such, a variety of safety and control features are built into weapons in an effort to prevent detonation in an accident or at the hands of an adversary.

2.1. Early Weapons

The earliest nuclear weapons were poorly secured by today's standards, often relying on an accident to "manufacture a safety device or feature", to borrow the wording of Plummer and Greenwood of Sandia National Laboratories[14]. It was not uncommon to assume, for instance, that a fire would melt solder joints in such a way as to render the weapon impotent or that mechanical damage causing ground faults would similarly destroy electronics safely. Engineers of the time were not concerned with such accidents. Rather, they focused on designing arming and disarming mechanisms, so that weapons could be activated only when needed. The techniques used were not poor—they were simply incomplete—and several have been incorporated into modern safety and control systems.

2.1.1. Separables

The most basic way of rendering a weapon harmless is to dismantle it and this is exactly how the United States secured its earliest nuclear bombs. Fissile material was kept in a capsule separate from the weapon itself[11]. This capsule was to be inserted by the crew of the bomber while enroute to the target and removed prior to landing if the mission were to be aborted. Without it, the weapon was reduced to the conventional explosive charges ordinarily used to implode the pit.

When weapons began being carried on the wings of aircraft in 1952, assembly by the crew became an impossibility. Instead a screw-jack was developed to perform this assembly operation[11], under crew control. Only a few years later, in 1957, the policy was abandoned altogether. Since then, nuclear weapons have been produced intact and sealed, relying on far more intricate safety mechanisms (see Section 2.2).

Of course, the method of separables was only effective while the two components are physically separated. During the portion of flight between installation of the capsule and deployment of the bomb, an accident could potentially lead to a nuclear detonation. Further, if an adversary were able to obtain both parts (which could be stored in separate, albeit nearby, facilities), the weapon would be quite viable. As such, the technique of separables was incomplete.

2.1.2. Safety Switches

Even the earliest nuclear weapons also employed simple arming switches, including both switches mechanically operated switches and switches controlled by onboard DC motors. These safety switches effectively disabled the detonator electronics and in many cases restricted physical access to the nuclear components. During transport, these switches were shorted in the disarm position by a wire so that they were not inadvertently armed by movement. Motor controlled switches were also operable directly from aircraft power so that the weapon could be armed in flight[14]. These switches, in a sense, were the first stronglinks (see Section 2.2.1).

In addition to simple arming switches, most early nuclear weapons employed mechanical combination locks which needed to be unlocked in order to arm the weapon. These locks were predecessors to the modern Permissive Action Links (PALs), which are typically electromechanical or entirely electronic (see Section 2.2.4).

As an alternative to the simple arming switch, some warheads, such as the W47, included a cadmium-boron wire in the pit[3]. In theory, this wire would absorb neutrons, preventing or at least damping a nuclear chain reaction leading to an explosion. Its removal was necessary in order to arm the warhead. Unfortunately, this wire tended to become brittle over time and could break during an arming attempt, making its complete removal nearly impossible. As a result, this scheme was abandoned and the W47s in service were modified.

Safety switches could do nothing to prevent accidental detonation in the event of an accidental release following arming, though this problem could be minimized by arming immediately prior to reaching the target, through the use of motorized switches controllable from the aircraft's cockpit. Unfortunately, even an unarmed weapon may be detonated in the event of an accident (owing to the effects of impact and fire), as discussed in Section 2.2.1. Further, only the combination lock (which allowed unlimited unlocking attempts) served to prevent an adversary from arming the weapon.

Designation	Type	Delivery	Yield	PAL	AMAC	IHE	FRP	ENDS	Details
B61-3	Bomb	Fighter Bomber	Variable to 170 kT	CAT F	Yes	Yes	No	No	
B61-4	Bomb	Fighter Bomber	Variable to 45 kT	CAT F	Yes	Yes	No	No	
B61-7	Bomb	B-2A Bomber	Variable to 340 kT	CAT D	Yes	Yes	No	Yes	Laydown Bomb. The first weapon in the current stockpile to incorporate ENDS.
B61-10	Bomb	Fighter Bomber	Variable to 80 kT	CAT F	Yes	Yes	No	Yes	Converted from the Pershing II W-85 Warhead, based in turn on the B61-3 and B61-4.
B61-11	Bomb	B-2A Bomber	Variable to 340 kT	CAT D	Yes	Yes	No	Yes	Earth Penetrator based on the B61-7.
W62	MIRVed Warhead	Minuteman	170 kT	Unknown	N/A	No	No	No	
W76	MIRVed Warhead	Trident I/II	100 kT	Unknown	N/A	No	No	Yes	
W78	MIRVed Warhead	Minuteman	350 kT	Unknown	N/A	No	No	Yes	
W80-0	Cruise Missile	Sea Launched	Variable to 200 kT	CAT D	No	No	No	No	Based on the B61.
W80-1	Cruise Missile	B-52H Bomber	Variable to 170 kT	CAT D	No	No	No	No	Based on the B61.
B83-1	Bomb	B-2A Bomber	1.2 MT	CAT D	No	Yes	Yes	Yes	With the W87, one of only two weapons to incorporate both IHE and FRP. The PAL is capable of destroying vital components as a control measure.
W87	MIRVed Warhead	MX Peacekeeper	300 kT	Unknown	N/A	Yes	Yes	Yes	The first warhead to incorporate both IHE and FRP, the W87 was praised at its introduction as the safest nuclear weapon ever built.
W88	MIRVed Warhead	Trident II	475 kT	Unknown	N/A	No	No	Yes	IHE was considered, but not used due to size and weight concerns. Uses a magnetically coupled stronglink.

TABLE I: **Safety and Control Features of the US Nuclear Stockpile circa 2005.** The nature of PALs on silo based missiles (sometimes referred to as PELs for Permissive Enable Links) is unclear. The story of setting the Minuteman PALs to 00000000 (see Section 1.2) implies 8 digit codes, inconsistent with any of the PAL Categories typically described. Specific delivery vehicles listed for bombs and missiles indicate the preferred vehicle, though other options may exist. PAL—Permissive Action Links (Section 2.2.4). AMAC—Aircraft Monitoring and Control (Section 2.2.4). IHE—Insensitive High Explosive (Section 2.2.2). FRP—Fire Resistance Pit (Section 2.2.3). ENDS—Enhanced Nuclear Detonation Safety (Section 2.2.1). Information compiled largely from *The Bulletin of the Atomic Scientists* and *The Nuclear Weapon Archive*[10][11][7][14][9][16][17][18][2][19].

2.1.3. Environmental Sensors

The most sophisticated of the early safety and control systems, environmental detection sensors (EDSs) demanded that the weapon undergo the expected sequence of physical motions before the warhead is completed armed. The Genie Air-to-Air Missile, for instance, demanded periods of acceleration and deceleration while many gravity bombs could not be armed below a specified altitude.

Environmental sensing is highly effective in preventing accidental detonation, but only if not accompanied by an accidental launch or release. Similarly, an adversary who has obtained access to a nuclear weapon with environmental sensing would be required to launch it in the expected fashion. While clearly imperfect, environmental sensing does improve the situation and the technique is used ubiquitously today. In fact, many weapons use environmental sensing as both an interlock and a fuse. For instance, a gravity bomb may arm only if it first reaches a specified altitude then begins freefall and subsequently detonate once it reaches a different altitude or experiences a sudden deceleration.

2.2. Refined Approaches

Following the accidents of the 1960s and 1970s (see Section 1.1), safety features of nuclear weapons began to be treated more seriously. Modern weapons are designed both to withstand the severe environments which may accompany an unintended release or crash and to thwart the efforts of the most determined and technologically sophisticated adversary.

2.2.1. Enhanced Nuclear Detonation Safety

The Enhanced Nuclear Detonation Safety (ENDS)[1] initiative outlines a set of principles for ensuring predictable nuclear safety in abnormal environments. In accordance with ENDS, the detonation systems of a nuclear warhead must be isolated from other components by an energy barrier. The region protected by this barrier is referred to as the exclusion zone. So-called stronglinks govern the breaching of the energy barrier so that a detonation signal may enter. This detonation signal, in turn, must be distinguishable from any naturally occurring signals. This is often referred to as the use of a unique signal generator. If stronglinks or the energy barrier fail, as in severe environmental conditions such as fire, it must be ensured that detonation has already been rendered impossible. This is done by using weaklinks—components designed to fail well before the stronglinks and energy barrier and without which detonation cannot occur. These directives are referred to as isolation (of the detonator from the environment), incompatibility (of the trigger signal from naturally occurring signals), and inoperability (of the weapon if the energy barrier is compromised)[14].

Arming a nuclear weapon with ENDS requires producing the unique arming signal, assuming additional interlocks such as PAL (see Section 2.2.4) have already been unlocked. Like PAL, the ENDS isolation scheme is designed to make detonation of a nuclear weapon physically impossible until the proper arming sequence has occurred. ENDS mechanisms, therefore, are designed to disconnect or separate components necessary for detonation until the weapon is armed. As a result, ENDS functions for both control and safety; by causing physical changes within the bomb, this implementation severely reduces the likelihood of an accidental nuclear detonation, but it also makes the use of a weapon without the proper PAL access codes and unique signals effectively impossible. It is important to realize, however, that stronglinks are first and foremost safety devices, designed to make detonation in atypical environments impossible.

Stronglinks are always mechanical devices, not dissimilar from the motor controlled switches in early nuclear weapons (see Section 2.1.2). A simple AC or DC signal is used to drive mechanical actuators, called drivers, in a specified sequence of events (generally 24) which are monitored by a single-try discriminator. This sequence is designed to be incompatible with any sequence which could be generated by typical or atypical environments. If the sequence is incorrect, the discrimator locks and will permit no further activation attempts. If the sequence is correct, the discriminator activates an energy control element, which is also mechanical and may involve electrical contacts, explosive pellets, ferrite buttons, or optical fibers and prisms[14]. Stronglinks are sometimes described as mazes; the unique signal encodes the path out of the maze and controls the driver to follow that path. As such, a stronglink is nothing more than an elaborate mechanical discrimator which operates an energy control element. Only once all energy control elements are activated, is it possible to detonate the warhead. Table II describes several common stronglinks, two of which are depicted in Figures 3 and 4.

The mechanical complexity of stronglinks makes it difficult to imagine an accidental activation. Particularly in the event of an accident which damages the weapon, it is unlikely that all of the necessary systems would still operate, let alone inadvertently receive the unique control pattern. Further, two different stronglinks are generally used in series. Presumably, a factor which compromises one stronglink will not, coincidentally, also compromise a stronglink of completely different construction. The first stronglink is an intent stronglink, the unique signal for which must be provided from outside the weapon.

[1] ENDS is sometimes referred to as Enhanced Electrical Isolation (EEI). The two are equivalent; the ENDS terminology is simply more inclusive.

Discrimator	Driver	Energy Control Device	Energy Form
MC2969	Rotary Solenoids	Electrical Contacts	Electrical
MC2935	Rotary Solenoids	Electrical Contacts	Electrical
C Mod	Rotary Solenoids	Interrupted Transformer	Magnetic
D Mod	Rotary Solenoids	Interrupted Transformer	Magnetic
MSAD	Linear Solenoids	Explosive Pellet	Kinetic
DSSL	Rotary Solenoids	Explosive Pellet	Kinetic
Pin in Maze	Stepper Motor	Prism Alignment	Optical
Leaf Spring	Stepper Motor	Paste Explosive Valves	Chemical

TABLE II: **Common stronglink mechanisms,** including drivers and energy control devices[15].

Human intent arms this link. The second is a trajectory stronglink. Its unique signal is stored onboard and must pass through the first stronglink's energy control element[15].

More likely than accidentally activating the stronglinks an accident may breach the energy barrier, by fire for instance. Weaklinks are devices crucial to detonation which are designed to fail prior to this occurrence, so that nuclear detonation remains an impossibility. Capacitors which must be charged by the detonator circuit are common examples of thermal weaklinks; they are intentionally designed to be destroyed in fire.

2.2.2. Insensitive High Explosive

Although most conventional explosives are susceptible to accidental detonation as a result of impact or fire, it is highly unlikely that a warhead could experience a nuclear detonation following such an accident. These weapons rely on finely timed (resolution on the order of hundreds of nanoseconds) detonations to compress the nuclear fuel to supercriticality. An accidental explosion simply could not do this. It could, however, rupture the pit and aerosolize the nuclear fuel. As at Palomares (see Section 1.1), the resulting contamination would be both dangerous and politically disastrous. For this reason, considerable effort has been invested in developing insensitive high explosives (IHEs) designed to withstand impact and fire without detonating.

Although a veritable laundry list of insensitive munitions have been developed for both explosives weapons and boosters, only PBX-9502, developed at Los Alamos, and LX-17, developed at Livermore, are approved as insensitive high explosives for use in nuclear weapons[6]. Both are based on triamino-trinitrobenzene (TATB). With an energy density higher than that of TNT, though still only two-thirds that of the conventional explosives it replaces, TATB is considered to have thermal and shock stability greater than any other high explosive with similar density. PBX-9502 and LX-17 have been available since the late 1970s, but IHEs are far from ubiquitous in weapons produced since then. Their comparatively low energy densities demand an increase in the weight and

FIG. 3: **The MC2935 Stronglink.** Two rotary solenoids are used as drivers. The discriminator connects electrical contacts. The MC2935 was used as a trajectory stronglink; the MC2969, with similar operation, was used as an intent stronglink. Image from [14]

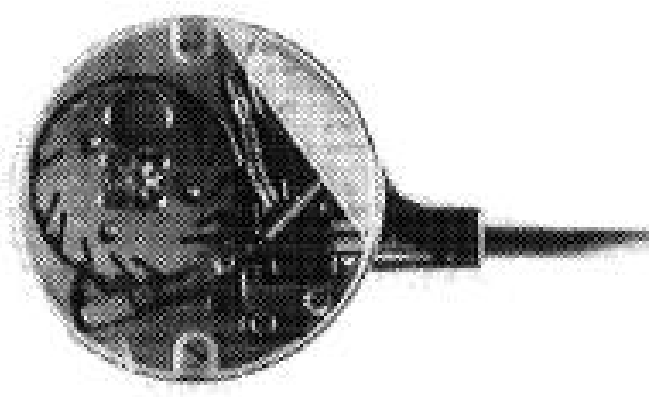

FIG. 4: **The MSAD Stronglink.** Two linear solenoids (not shown) are used as drivers. The discriminator rotates an explosive pellet into position between a slapper detonator and the main explosive charge. The pellet also serves as a thermal weaklink. Image from [14]

size of the warhead. As a result, this safety feature must be weighted against practical issues of construction feasibility and military planning. The W88 warhead lifted by a Trident missile, for instance, does not incorporate IHEs out of concern for the military capabilities of the missile[11].

2.2.3. Fire Resistant Pits

The pit of a nuclear weapon may also be encased in a metal shell with a high melting point. These fire resistant pits (FRPs) are intended to withstand a jet fuel fire for several hours. Since such a safety mechanism is only serviceable if the conventional explosives do not detonate, fire resistant pits are intended for use with insensitive high explosives (see Section 2.2.2) which should not detonate in a fire.

Fire resistant pits are incorporated into the B83 bomb and the W87 warhead, which rides the Peacekeeper ICBM[11][19]. The inclusion of a fire resistant pit, insensitive high explosives, and Enhanced Nuclear Detonation Safety (ENDS; see Section 2.2.1) mechanisms led to the Peacekeeper's being praised as "the safest, most advanced warhead in the active stockpile"[5].

2.2.4. Permissive Action Links

Perhaps the most striking (and most well known) safety and control feature of modern nuclear weapons is the Permissive Action Link (PAL). A PAL is, at first glance, a fairly simple concept; a security code, the number of digits of which varies from 4 to 12 with different PAL versions and which is typically divided between two users, must be entered into the weapon before it can be armed or detonated. The actual implementation of a PAL, however, requires that it be impossible to bypass or reverse-engineer. A nuclear weapon, quite simply, should be unusable in every sense without the PAL code.

Early mechanical combination locks (see Section 2.1.2) were, in a very crude sense, the first PALs. In the early 1960s, the first electro-mechanical PALs, known as CAT A, were introduced. These PALs used 4 digit codes entered by a handheld device [3] and allowed unlimited attempts. They were meant to prevent unauthorized use, but typically assumed the weapon remained in relatively safe hands; a rogue officer would not be able to try every possible combination, although an adversary with a stolen weapon would be able to. CAT B and CAT C PALs introduced longer codes (up to six digits) and limited the number of allowed attempts.

It was not until the 1980s that PALs became notably more powerful. CAT D and CAT F PALs permit the use of multiple arming codes, so that different subsets of weapons may be armed using different codes. Training codes, which cause the weapon to behave as it would if it were armed, without actually arming, are also supported. Most interestingly, CAT D and CAT F PALs are also capable of violently disabling the warhead, in addition to simply locking down. This feature may also be controlled remotely[13]. The details of this mechanism have not been released publicly and speculation abounds. Without substantiating any of the various claims, one proposed mechanism involves the detonation of an explosive charge which changes the shape of the pit, rendering the weapon useless until it can be remachined[3].

Speculation also abounds regarding the inner workings of PALs themselves. Proposed possibilities include encrypting detonator timing information or scrambling wires[3]. It is known that recent weapons do incorporate microcontrollers, an addition which suggests cryptographic calculations. Further, PALs are known to be buried deep within weapons, to prevent easy bypassing, and are covered by a tamper resistant skin. In the event that this skin is pierced in an attempt to tamper with the detonation electronics, the PAL may disable or destroy the weapon.

At first glance, a PAL is a simple security feature, which prevents the unauthorized use a nuclear weapon. The history of the device, however, is far more specific; the first PALs appear to have been installed in order to maintain control over American nuclear weapons deployed abroad. National Security Action Memorandum 160[20] suggests several sets of states to which PALs should be deployed, including those considered potentially unstable or possible early captures in the event of total war. Ultimately, PALs permitted the US more freedom in deploying nuclear weapons, as it could now maintain complete control over their use simply by limiting distribution of PAL codes. Ironically, this safety measure actively promoted weapon proliferation.

Starting with CAT B, it became possible to arm a weapon by remote control from an aircraft cockpit [3] using a system known as Aircraft Monitoring and Control (AMAC). As a result, weapons could be armed immediately prior to release, maintaining the security afforded by the PAL. On some aircraft, such as the B1 bomber, AMAC is not used and the PAL must be unlocked prior to takeoff. In this case, an additional coded switch system must be unlocked by the crew before the bomb can be released. These codes may be retained by ground support until such a time as they are necessary.

As described in Section 3, PALs are not the only codes necessary to arm a nuclear weapon. On submarines, they may not used at all or may be unlocked before leaving port. Security instead relies on a complex scheme requiring most of the crew (see Section 3.3). Similarly, the coded switch system used in silos likely varies from the PALs used in aircraft munitions. In all cases, a set of authentication codes are to be verified by the controllers of the PAL codes if any launch order is to be accepted. It is important to recognize that while access to a PAL code makes it possible, in theory, to arm a nuclear weapon, it far from ensures that doing so is possible. A wide range of addition controls, including redundant verifica-

tions, make the arming of a weapon by a rogue official extremely unlikely.

3. THE HUMAN FACTOR

The human factor introduces perhaps the weakest link in nuclear weapon safety and control. From the deliberate actions of military officers or others persons who have gained access to the facility to the accidental misuse of otherwise effective systems, safety and control is constrained most by the people who use it. We consider the safeguards and procedures in place for assuring the continued safety of the US nuclear stockpile at the hands of those directly responsible.

3.1. Launch Control Centers

A Launch Control Center (LCC) is responsible for authenticating launch commands and, ultimately, launching silo based missiles. It is also responsible for maintaining the security of the silos. Security systems maintain a perimeter about the entire complex and notify all LCCs on the site in the event of a breach, at which time armed security police are dispatched. In keeping with the two man rule of the armed forces, an LCC is staffed by two crew members who must both turn their keys in order to launch a missile. We examine in more detail the functioning of the Launch Control Centers for the Minuteman missile.

A Minuteman squadron consists of 50 missiles divided into 5 flights of 10 missiles, each with its own LCC several miles from the silos themselves. Each LCC contains a range of sensitive materials including two launch keys, presidential launch order authentication codes, and keys and access codes to the silos themselves, to permit maintenance crew access.

In the event that a command for action is issued, the two member crew will receive an Emergency Action Message (EAM) over a secure line and must authenticate the message using codes stored in the LCC safe which requires keys from both crew members to open. They may then take whatever actions were directed of them, possibly including unlocking the PAL, arming the missile, or launching it by turning both of their keys. Most likely, an EAM will simply request that missiles be brought to launch readiness with further instructions to follow.

A launch attempt must also be independently initiated by a second LCC from the squadron. Without this secondary confirmation, a launch may still be initiated, but will be time delayed by several hours. With the approval of two launch crews, a missile will fly within seconds.

Blair[4] outlines a variety of ways in which LCC crew members could interfere with the workings of this system. Conspiring crew members could, if positioned properly in the LCC structure, facilitate the theft, sabotage, or launch of a thermonuclear weapon. Possibly more frightening, aberrant crew members could initiate a sequence of false launch requests contrived either to appear as authentic presidential codes or simply to invalidate the entire inventory of authentication codes. The latter would temporarily ground the missiles, providing a strike opportunity for an adversary.

As Blair points out, security at Launch Control Centers has not always been as tight as one might expect. Visitors were generally approved with relatively little authentication and once they were inside, the on duty crew was considered to be in control of any such personnel. In light of the fact that as many eights visitors might be authorized in an LCC with only two crew members, the ability of the crew to thwart a seizure attempt is doubtful. Fortunately, this situation has been improved in recent years.

3.2. Aircraft

Aircraft may routinely fly with live weapons as a deterrent; there is not necessarily any intent to use them. Alternatively, bombers may be flushed in response to an EAM demanding military action. In either case, it is critical that the arming of the onboard weapons be well controlled. As discussed in Section 2.2.4, nuclear armed aircraft generally take flight with the PALs of onboard nuclear weapons securely locked. PAL codes will be sent via EAM and the crew will receive authenticated commands after takeoff. These commands may include PAL codes to be entered through the AMAC system (see Section 2.2.4) as well as information needed to unlock any additional coded switch systems. As a result, PAL codes may be kept at a secure location until they must be disseminated down the chain of command and to the aircraft.

3.3. Submarines

Communication with submarines is problematic and generally restricted to very low frequency (VLF) and extremely low frequency (ELF) bands which permit only a few bits of information per second. As a result, all communications must be very short. Knowing the proper communication bands and identification codes for a given submarine at a given time is considered a form of authentication in itself, but the relatively short EAMs sent to submarines are still authenticated using codes kept in a two key safe on board the vessel.

The submarine's Weapons Officer controls access to another safe which contains the trigger mechanism. The remainder of the crew is needed to bring the vessel to firing readiness, including reaching depth, attitude, and speed within a fairly narrow range. The missile may then be armed (which may require a PAL or similar code) and fired.

The launch procedures for submarines are designed to require minimal communication, while still implementing a high degree of security through the required intervention of the majority of the crew. In addition to those officers who control access to authentication codes, arming codes, and the trigger mechanism, the entire crew is needed to prepare the submarine for the launch. As with LCCs, the submarine's crew could, in theory, conspire to launch its missiles, since no codes from the outside are strictly prerequisite to a launch.

4. CONCLUSIONS

The US nuclear arsenal is certainly safe and secure, but this is not to say that nothing can go wrong. It is, and will likely always be, possible for a small group of military officers with the proper clearances and positions to launch, disable, or steal a nuclear weapon. It is, fortunately, considerably less likely for an outsider to do so. This level of security is maintained both by policies and procedures that ensure consensus and authorization before action is taken and by technologies, such as PAL, which restrict access to and use of the weapons themselves. Still other procedures and technologies, such as ENDS, IHE, and FRP, help to prevent devastating nuclear accidents.

Ultimately, all of these systems represent a change in the control structure that governs nuclear weapons. Coded switch systems require additional communication and dissemination of access codes. Every safety device introduces a small risk of failure. It is not surprising that attempts to control a weapon will limit its use; what is surprising is that the political freedom gained by implementing these measures may actually act to promote the construction of more weapons. Once a government is confident that its weapons are securely within its control and the people are confident those weapons are unlikely to accidently injure them, a major roadblock to proliferation is lifted. Safety and control quickly becomes a double-edged sword.

[1] "Atomic Audit: The Costs and Consequences." *The Brookings Institute*. 1998. <http://www.brook.edu/fp/projects/nucwcost/Box7-3.htm>.

[2] "The B83 Bomb." Nuclear Weapon Archive. 11 Sept. 1997. <http://nuclearweaponarchive.org/Usa/Weapons/B83.html>.

[3] Bellovin, Steven M. *Permissive Action Links*. 3 Jan. 2005. Columbia University. <http://www.cs.columbia.edu/$\sim$smb/nsam-160/pal.html>.

[4] Blair, Bruce G. "Keeping Presidents in the Nuclear Dark (Episode #1: The Case of the Missing Permissive Action Links)." *Bruce Blair's Nuclear Column* 11 Feb. 2004. <http://www.cdi.org/blair/permissive-action-links.cfm>.

[5] Department of Energy. Office of Science. *The Enrico Fermi Award*. 2003. <http://www.sc.doe.gov/fermi/html/Laureates/2000s/ssack.htm>.

[6] "Insensitive High Explosives." *GlobalSecurity.org*. <http://www.globalsecurity.org/military/systems/munitions/explosives-im.htm>.

[7] Kiddler, R. E. *Report to Congress: Assessment of the Safety of U.S. Nuclear Weapons and Related Nuclear Test Requirements*. July 1991. UCRL-LR-107454.

[8] Moran, Barbara. "The Day They Lost The H-Bomb–and How They Got It Back." *Invention & Technology* Fall 2004.

[9] Norris, Robert S., Hans M. Kristensen, and Joshua Handler. "The B61 Family of Bombs." *Bulletin of the Atomic Scientists* 59.1 (Jan/Feb. 2003): 74-76. <http://www.thebulletin.org/article_nn.php?art_ofn=jf03norris>.

[10] Norris, Robert S. and Hans M. Kristensen. "U.S. Nuclear Forces." *Bulletin of the Atomic Scientists* 61.1 (Jan/Feb. 2005): 73-75. <http://www.thebulletin.org/article_nn.php?art_ofn=jf05norris>.

[11] Norris, Robert S. and William M. Arkin. "U.S. Nuclear Weapons Safety and Control Features." *Bulletin of the Atomic Scientists* 47.8 (Oct. 1991): 48-49. <http://www.thebulletin.org/article_nn.php?art_ofn=oct91norris>.

[12] "The Palomares Broken Arrow, January 1966." *The Brookings Institute*. 1998. <http://www.brook.edu/FP/projects/nucwcost/palomares.htm>.

[13] "Principles of Nuclear Weapon Security and Safety." Nuclear Weapon Archive. 1 Oct. 1997. <http://nuclearweaponarchive.org/Usa/Weapons/Pal.html>.

[14] Sandia National Laboratories. Safety Components and Instrumentation Center. *The History of Nuclear Weapon Safety Devices*. By David W. Plummer and Willian H. Greenwood. Albuquerque, New Mexico: 1998.

[15] Sandia National Laboratories. Safety Components and Instrumentation Center. *A Primer on Unique Signal Stronglinks*. By David W. Plummer and Willian H. Greenwood. Albuquerque, New Mexico: 1993.

[16] "The W-62 Warhead." Nuclear Weapon Archive. 26 Sept. 1997. <http://nuclearweaponarchive.org/Usa/Weapons/W62.html>.

[17] "The W-78 Warhead." Nuclear Weapon Archive. 1 Sept. 2001. <http://nuclearweaponarchive.org/Usa/Weapons/W78.html>.

[18] "The W-80 Warhead." Nuclear Weapon Archive. 1 Sept. 2001. <http://nuclearweaponarchive.org/Usa/Weapons/W80.html>.

[19] "W87" *GlobalSecurity.org*. <http://www.globalsecurity.org/wmd/systems/w87.htm>.

[20] The White House. *National Security Action Memorandum 160*. Washington, DC, 6. June 1962.

APPENDIX A: EDITING NOTE

The LaTeXtemplate used in this document causes it to appear much shorter than it actually is (approximately 25 standard MS Word pages).