NAWCWD TP 8431

SAFETY AND ARMING DEVICE DESIGN PRINCIPLES

by

Steven E. Fowler
Ordnance Systems Division
Ordnance Systems

MAY 1999

NAVAL AIR WARFARE CENTER WEAPONS DIVISION
CHINA LAKE, CA 93555-6100

Approved for public release; distribution is unlimited.

Naval Air Warfare Center Weapons Division

FOREWORD

This report documents the efforts conducted at the Naval Air Warfare Center Weapons Division (NAWCWD), China Lake, California, over the last 30 years to develop a sound methodology for the development of safety and arming devices. This narrative draws from the experiences of countless experts in the area of fuzing.

Support for this development was provided under the auspices of the Ordnance Systems Director, Mr. John Robbins. This report was reviewed for technical accuracy by Mr. Randall Cope.

Approved by
J. M. ROBBINS, *Head*
Ordnance Systems
13 May 1999

Under authority of
CHARLES H. JOHNSTON
CAPT., U.S. Navy
Commander

Released for publication by
K. HIGGINS
Director for Research and Engineering

NAWCWD Technical Publication 8431

Published by ..... Technical Information Division
Collation ..... Cover, 14 leaves
First printing ..... 70 copies

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 1999	Summary

4. TITLE AND SUBTITLE

SAFETY AND ARMING DEVICE DESIGN PRINCIPLES (U)

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)

Steven E. Fowler

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Air Warfare Center Weapons Division
1 Administration Circle
China Lake, CA 93555-6100

8. PERFORMING ORGANIZATION REPORT NUMBER

NAWCWD TP 8431

8. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Naval Air Warfare Center Weapons Division
1 Administration Circle
China Lake, CA 93555-6100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

(U) This report documents the principles that have been used by fuze designers at the Naval Air Warfare Center Weapons Division, China Lake, Calif., for over 30 years in the creation of safety devices for warheads in missiles and free-fall weapons.

(U) The underlying philosophy in implementing safety and arming (S&A) device design safety requirements is very conservative. This approach is dictated by two factors: 1) the extremely severe consequences associated with safety failures; and 2) the difficulties in determining—with adequate confidence—what the safety failure rate is for any given system while considering all possible manufacture-to-target scenarios up to, and including, accidents and combat.

(U) This report describes the most sound methodology to approach the design of an S&A device that meets as closely as possible the requirements for safety and reliability.

14. SUBJECT TERMS

Safety and Arming Device, S&A, Explosive Train, Initiator, Interrupted Explosive Train, Non-interrupted Explosive Train, Armed, Fail Safe, Safety Features

15. NUMBER OF PAGES

26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

CONTENTS

INTRODUCTION

The purpose of this report is to document the principles that have been used by fuze designers at the Naval Air Warfare Center Weapons Division (NAWCWD), China Lake, Calif., for over 30 years in the creation of safety devices for warheads in missiles and free-fall weapons. With the continuing reduction of funding to the Laboratories for safety and arming (S&A) device development programs, the opportunity for newly hired engineers at China Lake to learn the design principles by "doing it" becomes less feasible. These principles were not developed overnight but are based on the results of many years of experience. The recent trend from mechanical to electronic S&A devices emphasizes the importance of using basic principles to develop a methodology that would ensure the safety of new systems. S&A devices would not exist if there were not a real need to enhance explosive weapon system safety. Thus, to a large extent, the role of an S&A device engineer is that of a safety advocate who must understand and communicate these principles to function effectively.

S&A DEVICE SAFETY DESIGN PHILOSOPHY

The underlying philosophy in implementing S&A device design safety requirements is very conservative. This approach is dictated by two factors: 1) the extremely severe consequences associated with safety failures; and 2) the difficulties in determining—with adequate confidence—what the safety failure rate is for any given system while considering all possible manufacture-to-target scenarios up to, and including, accidents and combat. The latter aspect is a natural consequence of the extremely small probabilities that are considered acceptable for safety failures—normally two to three orders of magnitude smaller than those acceptable for reliability failures. Normal design practices are often unacceptable from a safety design standpoint. These factors have led to a conservative approach in the development and implementation of safety requirements. Decisions are, therefore, based on the safest practical alternative—rather than accepting a more expedient alternative that cannot be proven safe. Thus, a considerable amount of judgment and discipline is required in the safety design process. Design requirements and solutions that are acceptable in an application that involves constraining performance requirements or environmental limitations may not be acceptable in another application. The fact that inconsistencies occur in acceptable safety design solutions from one application to the next is compatible with a conservative safety design philosophy. Unfortunately, this philosophy is difficult to employ in the present day weapon development environment. The intent of this document is to identify and clarify the safety design principles that accompany this philosophy, as well as aid in their future application.

MIL-STD-1316

MIL-STD-1316 (Reference 1) describes the safety design requirements for fuzes and S&A devices that are subsystems to fuzes. However, this standard does not address reliability issues. While MIL-STD-1316 uses the term *fuze* throughout, its design requirements apply only to the S&A device, which becomes a fuze in applications in which the target-detecting function is included in the S&A device. The design

safety requirements of MIL-STD-1316 normally do not apply to the target-detecting function. In addition, MIL-STD-1316 does not dictate the way an S&A device should be designed, but it does present complementary sets of general and specific design requirements that must be followed. Where possible, the general requirements allow flexibility in the design approach while ensuring an appropriate review of any proposed design. An example is the requirement for the determination of safety system failure rates that must be predicted via safety analyses. Prior to intentional initiation of the arming sequence, the safety system failure rate must not exceed one failure to prevent arming or functioning in one million opportunities. However, this requirement—very broad in scope—does not drive the design approach. Because there is some subjectivity involved in determining whether or not a device meets this criterion, additional issues must be addressed to ensure that a design is adequately safe. Design requirements are specific for safety-critical areas. For example, the explosive sensitivity requirements for lead and booster explosives are so detailed that they are covered under an additional military standard. This complementary approach offers balance between imposing fundamental safety design requirements and giving needed discretion to the fuze designers. This valid approach represents the years of cumulative experience of people throughout the fuzing community. Therefore, any deviation from this approach should be implemented with extreme caution and only with validated proof of the safety of the new method.

KEY PRINCIPLES FOR S&A DEVICES

The following are commonly used terms and definitions in S&A device design. In addition, key concerns and the applicable principles are addressed.

S&A DEVICE

An S&A is a device that keeps the ordnance section of a munition from arming during shipping, handling, and storage. The device also arms the ordnance section at the proper time through sensing that a predetermined set of conditions has been met. The S&A device will cause the high explosives to initiate when the munition senses that it has either hit or is in a close proximity to the target.

The S&A device has two sometimes conflicting requirements that create design challenges that differ from those of other weapon system components—a very low safety failure rate (no greater than 1×10^{-6}) and a very high reliability value (up to 0.995 at 90% confidence). Normally, making an S&A device safer does not make the device more reliable, and vice versa. Moreover, the S&A device safety requirements are unique in that they must be satisfactorily demonstrated prior to the S&A device being placed on a weapon system with a live ordnance section.

A key point to remember when working with explosive devices is that all explosives are inherently hazardous. The function of the S&A device is to mitigate (to an acceptable level) the hazards associated with the initiation of the explosives. This objective is accomplished by isolating the initiating stimuli from the insensitive secondary explosives during times when equipment or people are within the hazard area. An acceptable level of hazard has been determined to be one inadvertent explosive initiation in one million opportunities. The initiating stimuli can be heat, shock, light, static electricity, or any other mechanism that transfers enough energy to initiate the explosives. Figure 1 shows an example of a basic S&A device in which the initiating shock stimulus is provided by a relatively sensitive detonator. A mechanical barrier that blocks the explosive shock wave when the S&A device is in the safe condition supplies the isolation.

Another key principle in S&A device design is that the device must be maintained as a stand-alone configuration item. There are several reasons for this approach. The design challenges associated with conflicting requirements normally entail some compromises in design solutions. Moreover, the ability to find satisfactory solutions decreases almost exponentially when constraints, associated with additional functions, are integrated. This circumstance is true for any design that is excessively constrained. The inclusion of other functions in the design also raises the possibility of diluting or losing the emphasis on the safety aspects of the S&A device—a situation that is inconsistent with a conservative safety design philosophy. When other functions are combined with those of the S&A device, it is difficult to justify and maintain the expense associated with the conservative approach.

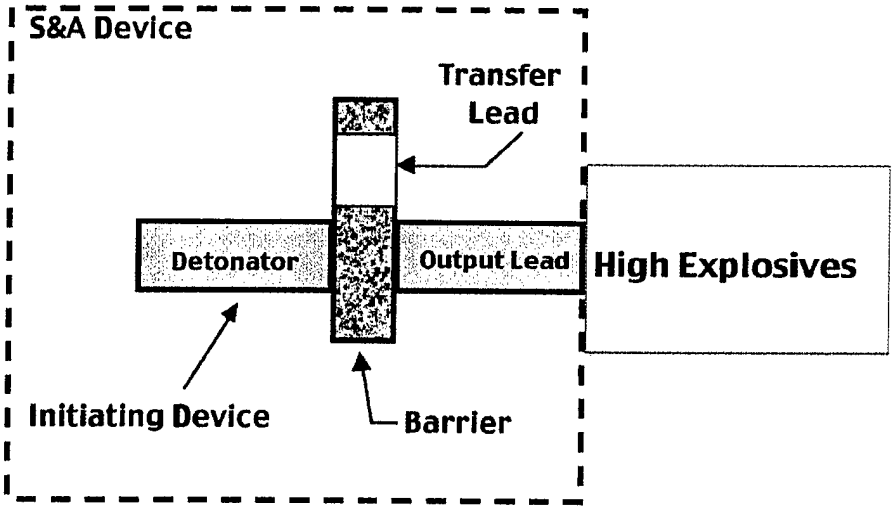

FIGURE 1. Basic S&A Device.

EXPLOSIVE TRAIN

The explosive train is the detonation or deflagration train beginning with the first explosive element and terminating in the main charge. In other words, the explosive train is that part of the S&A device that transfers a detonation wave from the most sensitive explosive element (usually a detonator) to the least sensitive explosive element (usually the warhead). An important question is

> What is the first explosive element?

For a conventional S&A device with a hot wire detonator packaged with a primary explosive, the answer is fairly simple—the detonator is the first explosive element. This determination becomes more difficult if the initiating element for the train is made up of more than one component. Thus, in an effort to simplify this issue for all applications, the first explosive element in the explosive train is defined as the most sensitive energetic element side of the explosive train. Figure 1 shows an explosive train. The first explosive element in this train is the detonator. The other elements in the train are the transfer lead (out of line when the S&A device is safe and in line when the S&A device is armed), the output lead, and the high explosives.

INITIATOR

The initiator is the component or components that convert the firing energy (electrical, mechanical, or optical) into a detonation wave that begins the detonation or deflagration of an explosive train. The initiator is a device capable of directly causing functioning of the explosive train. In the event that the energy conversion occurs in a physically different component from the first element, all energy conversion components, the first explosive element, and any connections between them shall be considered part of the initiator. The first explosive element of the explosive train will always be considered as part of the initiator. In other words, the sole responsibility of the initiators within the S&A device is to convert the appropriate energy input into the firing and to begin the incrementally escalating energetic function that will result in the weapon system warhead functioning. In terms of safety requirements, this definition becomes important when considering the requirements for initiator sensitivity. The key is to ensure that the requirement for a high degree of isolation from inadvertent initiation of the explosive train is maintained. In non-interrupted explosive train implementations, the initiator—consisting of only highly insensitive initiation components—provides isolation from unintended firing inputs. If the initiator contains sensitive components that can lead to explosive train initiation, some form of interruption must isolate them. Explosives, for example, must be qualified to strict secondary explosive requirements to be used in in-line systems. Otherwise, a mechanical barrier must isolate them. The electrical sensitivity of initiators used in systems without interruption must also meet strict insensitivity requirements. These prerequisites lead to two types of initiators that must be considered and understood. The first type is the low-voltage or low-energy initiator; the other is the high-voltage or high-energy initiator.

Low-Voltage or Low-Energy Initiator

The low-voltage or low-energy initiator is activated by fewer than 500 volts of direct current (VDC) or it contains a primary explosive. An example is a hot wire detonator that uses a primary explosive like lead azide to generate a detonation wave. Another example is a low-voltage laser diode that begins lazing at voltages below 500 VDC and, therefore, generates a detonation wave in the explosive train of which it is a part. A final example is a stab detonator that contains a primary explosive sensitive to shock inputs.

When the firing train (initiator and explosive train) incorporates a low-voltage or low-energy initiator, at least one physical firing train interrupter is required. The arming process must remove the interrupter. If the first explosive element is positioned so that safety is dependent upon the presence of the interrupter, the design must include a positive means to prevent the S&A device from being assembled without the properly positioned interrupter. If the first explosive element is positioned so that omission of that interrupter will prohibit transfer of its explosive output to the explosive train, a single interrupter is acceptable. The effectiveness of the interruption prior to initiation of the arming sequence should be demonstrated by testing and also determined numerically.

High-Voltage or High-Energy Initiator

The high-voltage or high-energy initiator cannot be activated by voltage equal to or less than 500 VDC and it contains only approved secondary explosives. Examples are an exploding foil initiator (EFI) and a laser with a lazing threshold of 500 VDC or greater.

When the firing train incorporates a high-voltage or high-energy initiator, no physical interrupter is required. However, all energy inputs must be controlled to preclude unintentional arming and/or firing. For the Navy, the Weapons System Explosive Safety Review Board (WSESRB) guidelines for non-

interrupted explosive trains require that at least two energy interrupters, each controlled by an independent safety feature, shall prevent arming before the munition is intended to be launched. The initiator must not be capable of functioning in the absence of, or as a result of, static failure of any or all of the energy interrupters. (See the section on safety features later in this report and Table 1.)

TABLE 1. Safety Feature Type Combinations for Electronic Safety and Arming Devices.

Safety Feature Type	Combination Options			
	A	B	C	D
Mechanical Safety Features	2	1	0	0
Dynamic Electrical Safety Features	0	1	2	1
Non-Dynamic Electrical Safety Features	0	0	0	2

INTERRUPTED EXPLOSIVE TRAIN

An interrupted explosive train is an explosive train in which the explosive path between the primary explosives and the lead and booster explosives is functionally separated until arming. The key point is that, if the initiator can be readily functioned by common environmental conditions, it must be separated physically and isolated from the less sensitive but more energetic elements of the explosive train. For example, the typical hot wire detonator is subject to inadvertent functioning for two reasons. First, the functioning stimulus energy requirement is small and is present in most environments. Second, the primary explosives used are susceptible to inadvertent initiation via shock, thermal input, etc., or by the absence of a fully energetic firing stimulus. Because of these factors, S&A devices incorporate a barrier between the hot wire detonator and the next component of the explosive train. This configuration prevents the detonation wave from propagating even if the detonator should function.

NON-INTERRUPTED EXPLOSIVE TRAIN

A non-interrupted explosive train is an explosive train in which the explosive path between the first explosive element and all other explosive elements in the train is functionally fixed without separation or barrier. This type of explosive train requires that only secondary explosives be used for each element of the train. While the explosives used in non-interrupted explosive trains are required to be approved secondary explosives and are extremely unlikely to be initiated inadvertently, the S&A system can still be unacceptably hazardous if the initiation mechanism is not properly controlled. Therefore, because this is a key principle, MIL-STD-1316 specifically covers fuze arming control requirements for non-interrupted explosive trains. Whether interrupted or non-interrupted explosive trains are used is not the key safety question. The pertinent question is

> Could the S&A device become a safety hazard due to natural environmental stimuli?

At present, all non-interrupted explosive train warhead applications use EFIs that incorporate only secondary explosives and require a specific and unique firing pulse for initiation. This unique firing pulse ensures that the possibility of inadvertent initiation is equivalent to that of inadvertently initiating a secondary explosive. Future developments may result in devices capable of initiating secondary explosives without a unique firing pulse. In this event, an equivalent means of isolating the firing pulse from the initiator will be required.

ARMED FUZE

A fuze is considered armed when any firing stimulus can produce fuze function. As part of a conservative safety philosophy, a fuze that is inadvertently armed is a safety system failure, whether or not the explosive train of the fuze generates an explosive output.

Figure 2 shows an example of an armed interrupted explosive train. The key point to note is that the explosive train is armed when the barrier between the primary explosives (detonator) and the other explosive components has been removed sufficiently to allow the propagation of the detonation wave to the secondary explosives (transfer lead and output lead). Any sufficient energetic firing input, intended or unintended, that initiates the detonator will result in an output from the fuze's explosive train.

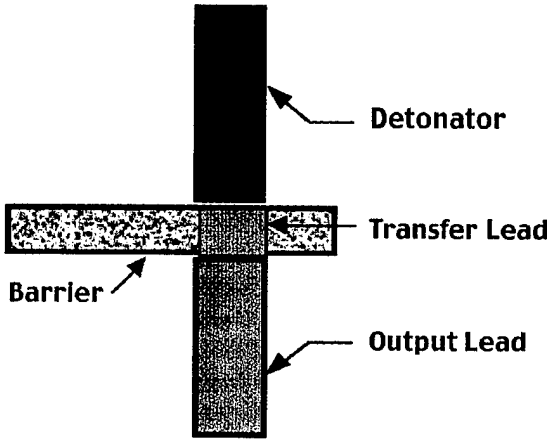

FIGURE 2. Armed Interrupted Explosive Train.

Figure 3 shows an armed non-interrupted explosive train. The key point to note is that the explosive train is armed when the firing capacitor has a large enough charge to initiate the EFI with a probability of one in a million (or exceeds the minimum no-fire voltage). This state is equivalent to removing the barrier in the interrupted explosive train example. Any stimulus, intended or unintended, that activates the spark-gap switch will result in an output from the fuze's explosive train.

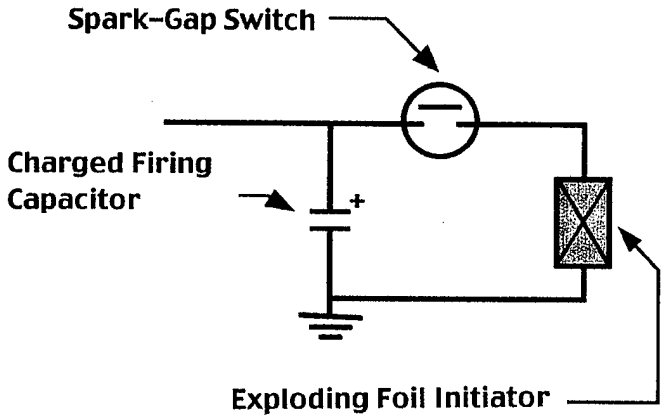

FIGURE 3. Armed Non-interrupted Explosive Train.

ARMING DELAY

An arming delay is the time elapsed or distance traveled by the munitions from launch to arming. It is required that all S&A devices shall delay arming, starting at the time the weapon is intentionally launched and ending after the weapon has left an imaginary volume of space known as the safe-separation envelope, as shown in Figure 4. The safe-separation envelope is the volume of space immediately around the launch platform at which a hazard from an inadvertent detonation of a warhead creates an unsafe environment for the launch platform and personnel. The intent here is to prevent the blast and fragments from a functioning weapon from becoming an unacceptable hazard to the launch platform and personnel. In some applications, compromises to this envelope are required to balance the potential hazard from a retaliating target on the launch platform to the hazard created by the weapon being detonated while in the safe-separation envelope.

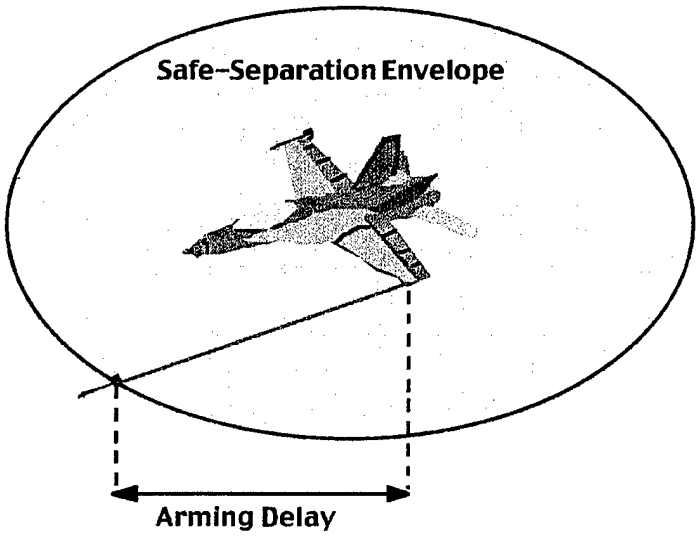

FIGURE 4. Warhead Arming Scenario.

SINGLE POINT FAILURE

A single point failure is the failure of one element in the system that results in the entire system failing. An example of an unacceptable single point failure in an S&A device is an element that fails, a condition that causes the S&A device to arm prematurely and, thus, become a safety hazard. A very serious failure can only be tolerated if its possibility of occurrence were fewer than one in one million opportunities. This factor is driving the requirement in MIL-STD-1316 for two independent safety features that prevent arming. Because the foregoing tolerance level is very difficult to demonstrate, the best practice is to eliminate the possibility of all single point failures of this type (by proper design). Another example is a scenario in which the S&A device permanently duds. While this instance may not create a safety problem, the failure can result in reliability problems and should be avoided or minimized.

A single point failure of an interrupted explosive train S&A device, as shown in Figure 5, can occur if a barrier connected to a spring that is biased pulls the barrier out of the gap between the explosive components. Only the solenoid lock keeps the barrier from moving. Therefore, if the solenoid lock fails to hold the barrier in the safe position, the explosive train is pulled into the armed condition.

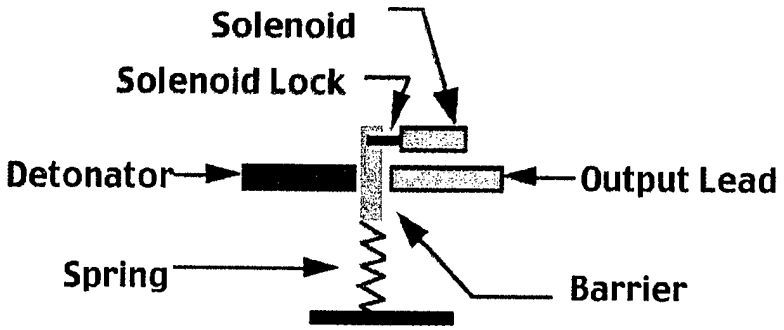

FIGURE 5. Interrupted Explosive Train Single Point Failure.

An example of a single point failure of a non-interrupted explosive train S&A device is shown in Figure 6. A single switch keeps the charge off the firing capacitor. If the arming switch fails in the electrically shorted condition, the capacitor charges and the S&A device is armed.

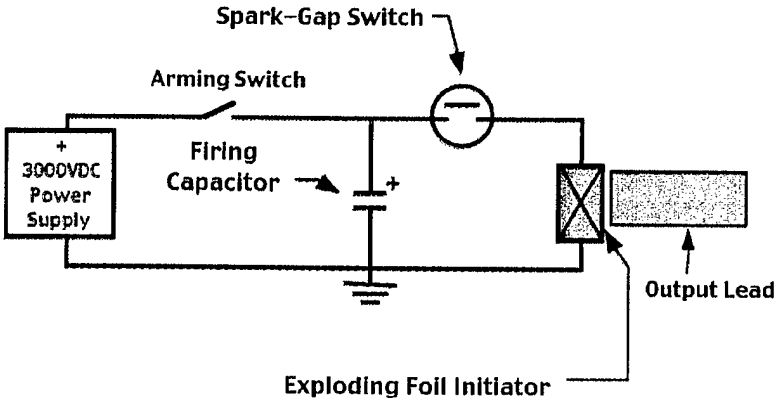

FIGURE 6. Non-interrupted Explosive Train Single Point Failure.

COMMON MODE FAILURES

Common mode failures are multiple failures that result from or are caused by seemingly unrelated failures or an adverse environment. One example is the failure of two gates on a digital integrated circuit due to the loss of the ground lead to the chip. Another example is the failure of two transistors due to exposure to a high-temperature environment. Multiple failures caused by a single factor or event are as bad as, or equivalent to, a single point failure. This problem can be especially insidious when working with the input signals to electronic S&A devices, as shown in the example in Figure 7.

The inputs to this system appear to be from unique and independent environments. However, because a direct current (DC) voltage represents both of the signals, a single 28-VDC signal can cause the S&A device to react as though both environments have been satisfied. This mode failure is common because a single input, in this case the coupling of an inadvertent DC signal into the input lines, can compromise both safety features.

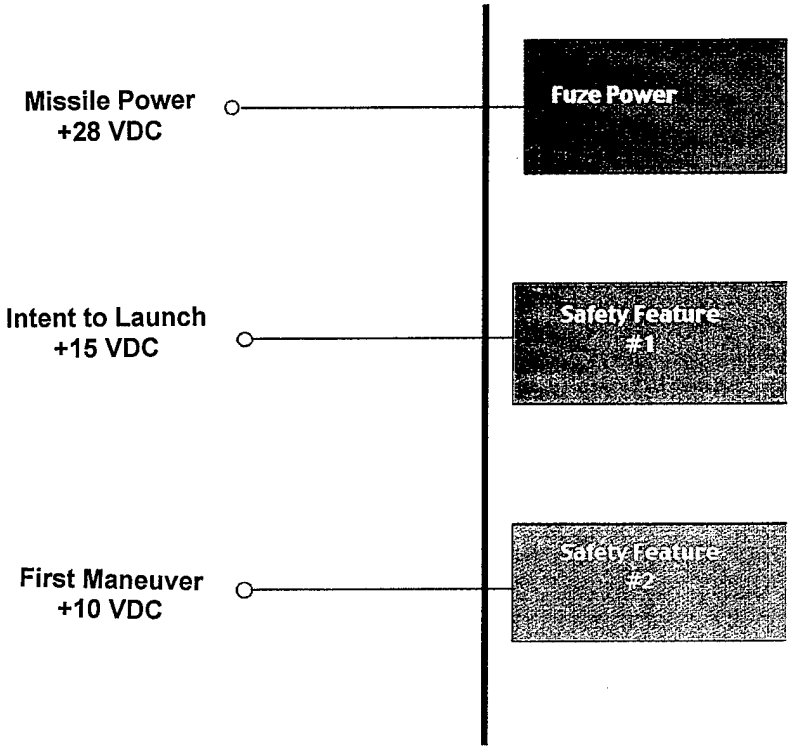

FIGURE 7. Common Mode Failure Example.

FIRMWARE

Firmware is the combination of a hardware device and computer coding or computer data that reside as read-only information or coding on the hardware device. The information or coding cannot be readily modified under program control. It is important to note that firmware can be used with other logic devices besides computers. The most common form of firmware is a read-only memory that provides the coding for a microprocessor or a sequential logic device. There has been a recent trend to use write-once, read-only memories to contain the firmware. This approach is acceptable from a not-readily-modifiable point of view but has other concerns that must be addressed to be sufficient. If this approach is employed, the user must be able to ensure that errors have not been encoded during the write process. Finding encoding errors is very difficult with this type of hardware because it is programmed one device at a time, as opposed to a masked programmable read-only memory that has an approved mask layout.

CREDIBLE ENVIRONMENTS

A credible environment is an environment that a device may be exposed to during its life cycle. These include extremes of temperature and humidity, electromagnetic effects, line voltages, etc. Combinations of environments that can be reasonably expected to occur must also be considered within the context of credible environments. All S&A devices are exposed to unique sets of credible environments based on the anticipated manufacture-to-target sequence. Each weapon system application dictates the unique set of credible environments in which its S&A device must be designed to survive. When an

existing S&A is considered for a new application, the set of credible environments to which the S&A has been qualified seldom completely overlaps the new application's credible environments, and a "delta" qualification for the new environments is required.

As an important step in the design or selection of an S&A device, the credible environments determine the arming stimuli that are available for sensing by the S&A device to determine if arming should be allowed. The selection and uniqueness of the available arming environments are normally the biggest driving factors in the complexity and cost, as well as the level of safety, of the S&A device. In general, the S&A device's design is improved with the uniqueness of the selected arming environments. To illustrate, bomb fuze safety systems tend to be much more complex than guided missile fuzes due to the lack of unique post-launch environments for bombs. When considering an existing S&A device in a new application, investigators find that it is not unusual for a qualified S&A device to be unsuitable or unusable in that new application because the credible arming environments have changed. An example is the use of an acceleration-armed S&A device in an application in which the munition acceleration never exceeds $1g$. In this case, munitions acceleration is no longer a feasible arming environment.

There is a temptation to use environments that are easy to sense, but this approach is not appropriate if the weapons system is potentially exposed to those same environments at other times during its life cycle. It is important that the environment sensed be unique to the launch, or post-launch, cycle so that the safety feature is enabled only after committing the weapon system to be launched. When selecting enabling environments, designers encounter the additional temptation of using a non-unique signal that represents that environment as an enabling signal, such as a voltage level alone to represent a commit-to-launch environment. The problem with this approach is that the S&A device can easily be exposed to a similar environment any time during its life cycle. Voltage-level environments are considered to be very susceptible to common mode failure problems if their lack of uniqueness is not addressed.

Another point to remember, when selecting enabling environments, is not to use environments that are a direct result of an action within the weapon. An example of this scenario is one in which a thermal battery is used. There is a possibility that the battery may be initiated inadvertently (this is a known thermal battery failure mode). This condition results in the enabling environment coming into existence when it has not been intended, thus reducing system safety. A better approach is to use environments such as acceleration, air pressure, physical motion associated with launch, or any other unique event external to the weapon system that will result in a commitment of the weapon system to be launched.

DUD

A dud is a munition or munition component that has failed to function, although functioning was intended. The best example of a dud is a fuzing system that received all the correct stimuli for arming and firing but did not initiate the warhead. There are many possible causes for this failure, such as a circuit malfunction or a non-compliant or defective explosive train component. The key point is that the fuze was intended to function, conditions were correct for functioning, and yet it failed to function. This scenario should not be confused with the case in which a fuze properly sensed that the environments for arming were wrong and remained in the safe condition after the launching of the weapon. This outcome is a dudded munition, but the fuze was not a dud. In this case, the fuze worked as designed.

FAIL-SAFE DESIGN

A fail-safe design is a characteristic of a fuze system or part thereof designed to prevent fuze function when components fail. When things go wrong (and they will), the S&A device has been designed

with a bias to fail in a manner that will not result in an unintended arming or output from the explosive train. A successful design requires the use of fault tree analysis; sneak circuit analyses; and failure modes, effects, and criticality analyses. These analyses should be conducted early in the process before the design has been finalized and/or committed to hardware.

BOOSTER AND LEAD EXPLOSIVES

Booster and lead explosives are compounds or formulations, such as those explosives listed in Table I, paragraph 6.9, MIL-STD-1316D, which are used to transmit and augment the detonation reaction. For inclusion in the approved explosive list, the explosive composition must be endorsed by all the services. A new explosive, even after approval by one service, normally takes several years to be approved by the other services—a time frame that depends upon their first use of the explosive. Approved booster and lead explosives should only be used in a position leading to initiation of a higher explosive main charge without interruption. To be approved in this category, a candidate explosive must show—by way of a comprehensive test series—that it is insensitive to a variety of potential stimuli. Because of this required test series, inadvertent initiation of approved lead and booster explosives is not expected when they are subjected to stimuli normally present in the environment. The distinction is between compounds that are inherently highly hazardous and those that only become hazardous when a unique stimulus is present. Because initiation of these explosives automatically results in the initiation of the entire explosive train regardless of the response of the rest of the S&A device, these explosives' selection and configuration must be tightly controlled. If there is a small change—of any type—to one of the approved explosives, the new configuration must be qualified before it can be used. An example is adding more binder to an explosive. The resulting explosive may have different characteristics than the compound originally approved and, therefore, must be requalified. Table 2 gives a list of approved explosives.

TABLE 2. Approved Explosives.

Explosive	Specification
Comp A3	MIL-C-440, Composition A3 and A4
Comp A4	MIL-C-440, Composition A3 and A4
Comp A5	MIL-E-14970, Explosive Composition A5
Comp CH-6	MIL-C-21723, Composition CH-6
PBX-9407	MIL-R-63419, RDX/Vinyl Chloride Copolymer Explosive Composition (PBX 9407)
PBXN-5	MIL-E-81111, Explosive, Plastic-Bonded Molding Powder (PBXN-5)
PBXN-6	WS-12604, Explosive, Plastic-Bonded Molding Powder (PBXN-6)
DIPAM	WS-4660, DIPAM Explosive
HNS Type 1 or Type 2 Gr A	WS-5003, HNS Explosive
HNS-IV	WS-32972, Material Specification for HNS-IV
Tetryl*	MIL-T-339
Tetryl Pellets*	MIL-P-46464

* No longer manufactured and not for use in new developments.
PBX = plastic-bonded explosive; RDX = cyclotrimethylenetrinitramine; DIPAM = hexanitrodiphenyldiamine; HNS = hexanitrostilbene; Gr A = Group A.

SAFETY FEATURES

A safety feature is an element or combination of elements that prevents unintentional arming or functioning. In mechanical systems, a safety feature is normally a mechanical locking system that prevents the rotor, shutter, or slide from moving out of the safe position. In the definition of a safety feature for configuration control or safety analysis, everything critical to maintaining safety must be included. An acceleration-based safety feature, for instance, includes the inertial mass; bias springs; and the portions of the rotor, shutter, housing, etc., necessary to and involved in preventing arming. In electronic systems, the safety features include the energy interrupter—normally a switch—and the associated sensors and logic that control that switch.

In the selection of arming stimuli and safety feature design, there are several commonsense safety principles that should be followed when practical.

1. Safety features should be fully contained within the S&A device to ensure that the safety-related design decisions are not diluted by requiring design trade-offs with other physical and functional requirements. Internal implementation of the safety features normally minimizes their exposure to external actuation. There are also cost advantages because the stringent testing and configuration control issues, which are unique to S&A devices, are not imposed on non-safety-related hardware.

2. Arming stimuli should be sensed within the S&A device whenever possible to minimize the potential for unintentional generation or coupling of a false arming signal into the S&A device via external events. This precaution also minimizes the amount of hardware involved in providing the safety function and, therefore, its associated cost and complexity.

3. The coupling between the arming stimulus and the safety feature should be as direct as possible to eliminate the need for intermediary signal processing hardware, which may inadvertently produce or distort the arming stimuli.

4. The arming stimuli should be chosen so that they do not occur anywhere else in the service environment. This choice makes the stimuli's presence an excellent indicator that the weapon has been launched and that arming was appropriate.

5. Energy levels that enable safety features should be maximized to lower the risk of inadvertent generation.

6. The arming energy should be derived from a post-launch environment whenever possible to minimize the possibility of receiving arming energy prior to launch.

7. Arming stimuli should be of sufficient magnitude and duration that safe separation distance can be verified prior to the disappearance of the stimuli. This course allows the designer to delay the enabling of the associated safety feature until after safe separation.

8. Restricting the arming stimuli to a small window in time and requiring arming stimuli to occur in a specific sequence are both effective techniques in reducing the possibility of the safety feature being inadvertently enabled.

Launch acceleration, if unique to the manufacture-to-target sequence, is an almost ideal arming environment for implementation in a mechanical S&A device. The most successful family of Navy S&A devices, the Mark Series, has demonstrated this concept. Starting with the Terrier Missile's Mk 6 Mod 1

S&A device, which was developed in 1957, there have been over 175,000 Mark Series S&A devices placed in service without a single safety failure. Central to this remarkable safety record is the launch acceleration arming stimuli. Launch acceleration as an arming stimulus in the Mark Series is an excellent illustration of the application of the safety principles. While all of the safety principles are not applicable to launch acceleration, those that do apply are addressed in the paragraphs that follow.

Principles 1 and 2: Acceleration can be sensed within the S&A device—a state that allows the safety features to be contained within the S&A device without requiring additional transmission hardware. Moreover, the safety features are easily protected from external activation.

Principle 3: The coupling between the arming stimulus and the safety feature is very direct. Therefore, no intermediary signal processing/enhancing hardware, which may inadvertently produce or distort the arming stimuli, is required.

Principle 4: The launch acceleration level is a unique service environment and represents an excellent indicator that the weapon has been launched and that arming is appropriate.

Principle 6: The arming energy used to move the rotor from the safe position can be derived directly from the arming stimulus—a configuration that ensures arming energy is derived from the post-launch environment. Additionally, the movement of the rotor can serve as verification that the arming stimulus is present.

Principle 7: Acceleration profiles in these applications are of sufficient magnitude and duration that safe separation distance can be verified prior to final commitment to enable arming of the explosive train.

As weapon systems evolve, the application of electronic S&A devices (ESADs) with non-interrupted explosive trains is becoming more common. The implementation options available to ESAD designers allow much more sophisticated solutions than those of mechanical S&A devices. As design complexity increases, so does the complexity of interpreting basic safety principles as they apply to those designs. In addition, the possibility of overlooking the basic safety principles contained in this document (i.e., ensuring that the safety features are truly independent and preventing single point or common mode failures) increases. Because of these factors, implementation of safety features for ESADs requires even more attention by the design and review community to ensure that the basic safety design principles contained in this document are emphasized and consistently followed.

INDEPENDENT SAFETY FEATURE

A safety feature is independent if the function or malfunction of other safety features does not affect its integrity. If a high degree of independence is not maintained, the possibility of single point failures or common mode problems is increased. And, while each safety feature should act independently, total independence is not possible. For example, two mechanical locks that rely on the integrity of a common housing structure for their functionality are not independent. Thus, in evaluating this concept, a designer must consider the following: physical separation, type of arming stimuli and inputs, implementation methods/parts, and type of energy. Again, proper selection of the arming stimuli is a key to implementing independent safety features.

SAFETY REDUNDANCY

The safety system of the fuze must contain at least two independent safety features to prevent unintentional arming of the fuze. The stimuli enabling a minimum of two safety features are derived from different environments. Designers should avoid using environments and levels of stimuli to which the fuze may be exposed prior to initiation of the launch cycle. Operation of at least one of these safety features depends on sensing an environment after first motion in the launch cycle or on sensing a post-launch environment. An action taken to initiate launch may be considered an environment if the signal generated by the action irreversibly commits the munitions to complete the launch cycle.

The requirement for two independent safety features must be emphasized, as it makes the fuze considerably safer. This requirement is also reasonable from a design verification standpoint. The allowable system safety failure rate is no greater than 1×10^{-6} in an S&A device—a difficult requirement to assess because of the impracticality of verifying occurrences that happen so infrequently. On the other hand, when two independent safety features are required, each safety feature need only demonstrate a failure rate of 1×10^{-3}—more easily achieved and demonstrated. Moreover, this failure rate is more in line with the reliability requirement for the system. However, the validity of splitting the allocation of the safety failure rate requirements to individual safety features is applicable only if the concept of independent safety features discussed earlier is strictly adhered to. If there is any interdependence between the safety features, their individual failure rates cannot be multiplied to obtain a 1×10^{-6} overall failure rate ($[1 \times 10^{-3}] \times [1 \times 10^{-3}]$). As mentioned earlier, the concept of independence applies to the environments that are used to enable the safety features. In addition, practicality also plays a role. Examination of the resources available to designers shows that obtaining two unique and independent arming stimuli from most launch environments is practical and feasible.

In the development of design requirements that satisfy safety feature redundancy for electronically controlled non-interrupted ESADs, adjustments must be made to accommodate the technology. Because there is no mechanical interruption in the explosive train of an ESAD, at least two energy interrupters—controlled by two safety features—are required to prevent inadvertent arming. This prerequisite is directly comparable to at least two safety features directly locking the mechanical interrupter in the safe position for mechanical S&A devices. The *WSESRB Technical Manual for Electronic Safety and Arming Devices with Non-Interrupted Explosive Trains* (Reference 2) provides additional guidance for the minimum number of safety features required, based on the implementation used. This guidance is shown in Table 1.

The reader should note that safety feature implementations are not equivalent. The WSESRB manual requires two non-dynamic (i.e., static) electrical safety features to replace one mechanical or one dynamic electrical safety feature. Most ESAD designs use one dynamic safety feature—which is accepted as equivalent to two mechanical safety features—or two static safety features. The reasoning is that a single static energy-interrupter-based safety feature does not provide the same level of safety as the other safety feature types. Failing in the closed condition is one of the two predominant failure modes for the switches used to provide the energy interruption. With the use of redundant static energy interrupters, the risk is reduced to an acceptable level. In other words, if the design has ensured that the interrupters are truly independent, at least one of the static energy interrupters will work properly. Dynamic energy interrupters are equivalent to mechanical safety features because the interrupter must actively function in order to prevent inadvertent arming.

FUZE SAFETY SYSTEM

The fuze safety system is the aggregate of devices (e.g., environmental sensors, launch event sensors, command function devices, removable critical items, or logic networks, plus the initiation or explosive train interrupter, if applicable) included in the fuze to prevent arming and functioning of the fuze. Arming and functioning must not occur until a valid launch environment has been sensed and the arming delay has been achieved. This concept is extremely important and sometimes difficult to define. Determining what the safety system exactly is, for a given situation, has at times been very controversial. For the purpose of clarification, the following two examples are provided.

The basic pneumatic fuzing system consists of two subassemblies, the guided missile fuze (shown in Figure 8) and the pressure probe. Fuze safety is maintained with the explosive train in the out-of-line or safe position during handling, storage, and the phase of the flight prior to reaching the safe separation from the launch platform. At launch, the rotary solenoid is energized to remove the safety feature that locks the rotor in the safe position. Concurrently, an arming wire is pulled from the pressure probe (not shown)—a condition that permits the probe switch closure that delivers missile power to fire the probe squib. Squib firing erects the probe into the missile air stream—an effect that shears two fuze air tube manifold tips and makes possible the connection of the tubes to the pressure probe. The probe senses pressure differential between the dynamic ram and the static ports and transmits this pressure differential to the fuze piston. When the pressure differential force exceeds the bias and arming spring forces, the piston is stroked, and energy is stored in the arming spring. When the piston reaches the fully stroked position, the second safety feature, which locks the explosive rotor, is removed—a configuration that enables the rotor movement to begin. The rotor is driven by the arming spring and is retarded by the escapement and the rotor return spring. Near the end of the rotor rotation, the detonators are switched into the firing circuitry. When the rotor rotation is complete, the forward solenoid cam depresses the rotor-locking ball into the rotor slot—an arrangement that locks the rotor in the armed position. The explosive train is now aligned, and the fuze is not only mechanically and electrically armed but also locked in the armed condition.

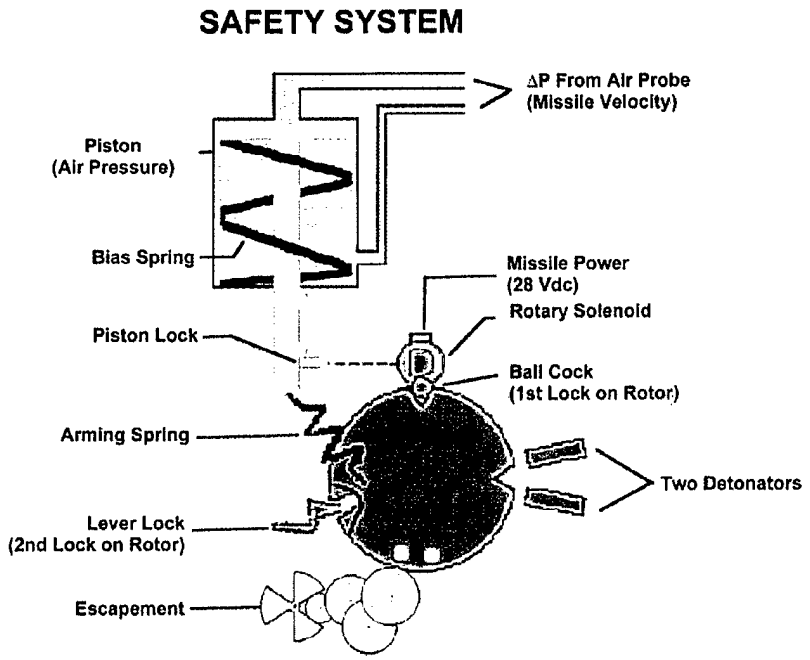

FIGURE 8. Example 1, Pneumatic Fuze.

At first glance, it might appear that the safety system for this pneumatic fuze consists of the guided missile fuze and the pressure probe. But, in actuality, only the S&A device portion of the pneumatic fuze constitutes the safety system. All of the safety features are located inside and the sensing of the arming stimuli occur in the fuze. The probe creates an environment to be sensed, yet all safety determinations take place in the fuze. This concept is important because having the safety system components at several different locations is highly discouraged. To reinforce this notion, discussions with fuze engineers who participated in the early development of MIL-STD-1316 have reported that "included in the fuze" used in the definition above means, "the fuze safety system would be contained wholly within the fuze." This concept is intended as a requirement because it is judged to be the safest design approach.

The generic ESAD (Figure 9) consists of two sections—usually contained in the same package. The first section is the safety circuitry and the second section is the high-voltage fireset. Fuze safety is maintained by prohibiting power from the high-voltage circuits. This design does not require the explosive train to be interrupted because no primary explosives are being used in the explosive train. The safety system provides isolation of the initiating stimulus, a unique high-power electrical pulse, from the explosive train by preventing accumulation of high voltage in the fireset. Launch provides the first environment and is sensed by the ESAD, a state that enables the first safety feature. This phase closes static switch 1 and simultaneously satisfies one condition for the dynamic switch safety feature. After launch, the second environment is sensed by the ESAD and enables the second safety feature. This condition closes static switch 2 and simultaneously provides the second input to the dynamic switch safety feature. Once the safe separation delay requirement is satisfied, the dynamic safety feature is totally enabled; dynamic switch begins operation and causes the fireset to be charged. When the voltage on the fireset passes the minimum no-fire voltage for the EFI, the ESAD is armed. The safety system in this example consists of the environmental sensors, the logic and control circuitry, the three energy interrupting switches, the high-voltage transformer, and the capacitor.

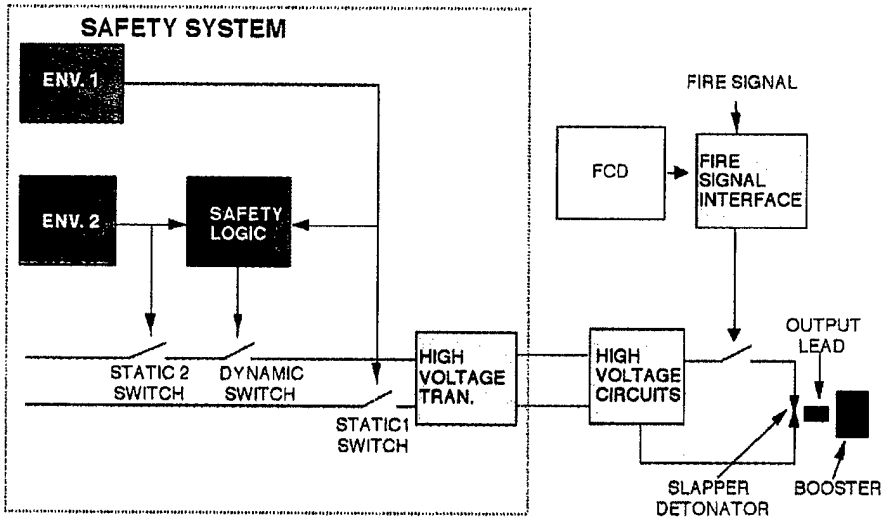

FIGURE 9. Example 2, Generic ESAD.

ENVIRONMENTAL SIGNAL TYPES FOR ESAD

The best practice is that the environmental sensors inside the ESAD determine the validity and integrity of the external environmental signals. However, for some applications, this approach is not

feasible. In these instances, the architecture becomes even more important. The following discussions are intended to provide some guidance for these cases based on the form of the arming/enabling signal available to the ESAD from the environmental sensor. Table 3 contains the different types of arming/enabling signal forms that can be used as inputs to an electronic S&A device.

TABLE 3. Signal Types.

Type	Description	Example
Type 1	Simple analog or digital signal, static or single transition.	Direct sensor output or static logic output associated with a distinct moment in time is utilized.
Type 2	Dynamic signal	Continuous time-related signal that follows an expected profile is utilized.
Type 3	Synthetic signal	Dynamic-type signal created by the sequential execution of a computer program is utilized.
Type 4	Intelligent signal	Synthetic-type signal is generated in such a manner that the validity of the signal can be verified.
Type 5	Processed signal	Processed signal indicates when thresholds have been met. Signal has unique coding.

Most ESAD fuze designers prefer Type 1. In this case, the associated safety feature uses unfiltered/unprocessed information from a sensor. The safety feature checks the validity of the signal by verifying that the characteristics of the signal are within the acceptable boundaries. Signal validity is limited to verifiable characteristics. If a simple or common signal is used, the sensor producing it should be dedicated to the safety function. Additionally, to minimize the chances of inadvertent enabling of the safety feature, the sensor should be contained within the ESAD and directly coupled to the safety feature.

In a Type 2 signal, the encoded data are time or frequency dependent. This signal requires a safety feature that can detect and verify time-related as well as other arming stimulus characteristics. The acceptability of this signal is highly dependent on how unique its characteristics are and how the dynamic signal is being generated. The best Type 2 signals are those that are unique and created within the weapon system only as a result of a post-launch environment. An example is the signal generated by an alternator on a turbine engine.

Type 3 is a Type 2 signal that is artificially created by a computer program. Generally, this signal should not be used because of the inherent inability of the associated safety feature to determine the validity of the input initiating the execution of the computer program. This signal should be utilized only when there are no other means of providing an environmental input.

Type 4 is similar to the Type 3 signal, except that the encoded information allows the S&A device to verify the validity of the generated signal. The additional complexity of this configuration is justified when remote sensors must be used and verifiable characteristics of the expected signal are lacking.

The Type 5 signal is unique in that it may be required in future distributed initiation or submunition applications and can be used in a command arm configuration. The safety thresholds/characteristics of the arming environments are already verified externally to the command arm module. This signal is encoded so that its validity can be determined. This approach involves some safety and cost compromises because extra hardware is required to encode, transmit, and decode the unique signals.

Figure 10 shows a conventional ESAD architecture. This approach represents a design that has been used successfully on mechanical S&A devices for over 30 years with a perfect safety record and very high reliability. As the preferred approach, it should be used whenever possible. The safety system has environmental sensors that are part of the fuze package. Because the ESAD is self-contained, it is not dependent on any other part of the smart weapon to make the decision to arm. The only input to the fuze is a potential data link that can be used to select fuzing modes.

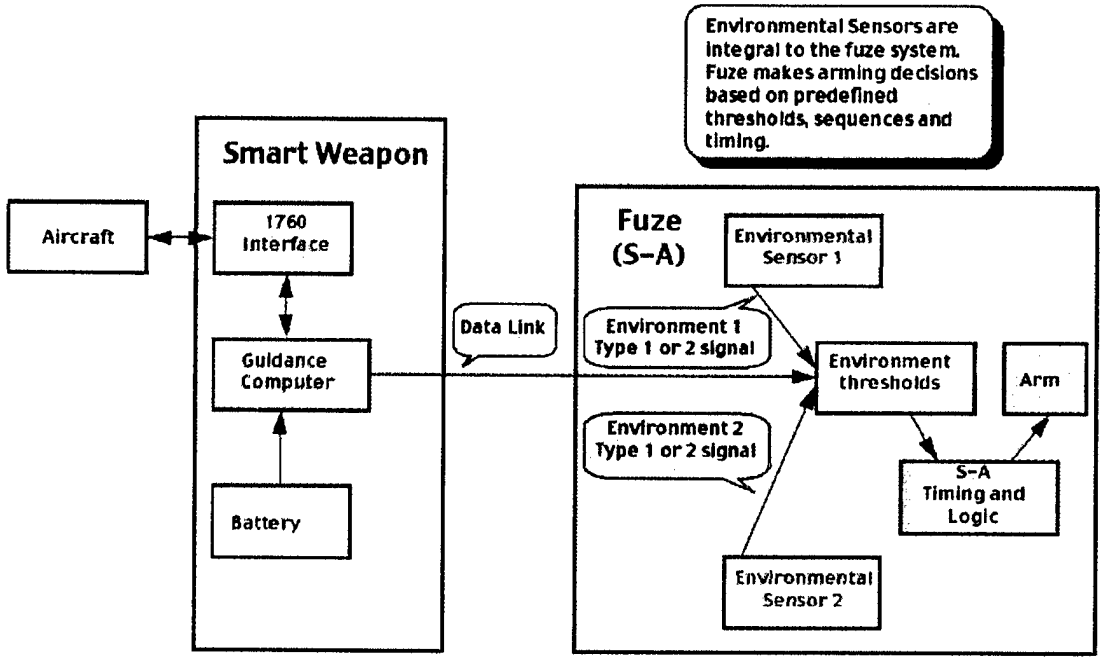

FIGURE 10. Conventional ESAD (Sensors Part of the Safety System).

In the application in Figure 11, the sensors used in another location in the smart weapon are shared with the fuze system. The outputs from the sensors are directly connected to the fuze—a condition that makes them Type 1 or Type 2 signals. The major concern in this application is the integrity of the signals to the fuze. Care should be taken to ensure that the signals processed by the fuzing system are unique enough to provide adequate safety and cannot be inadvertently altered.

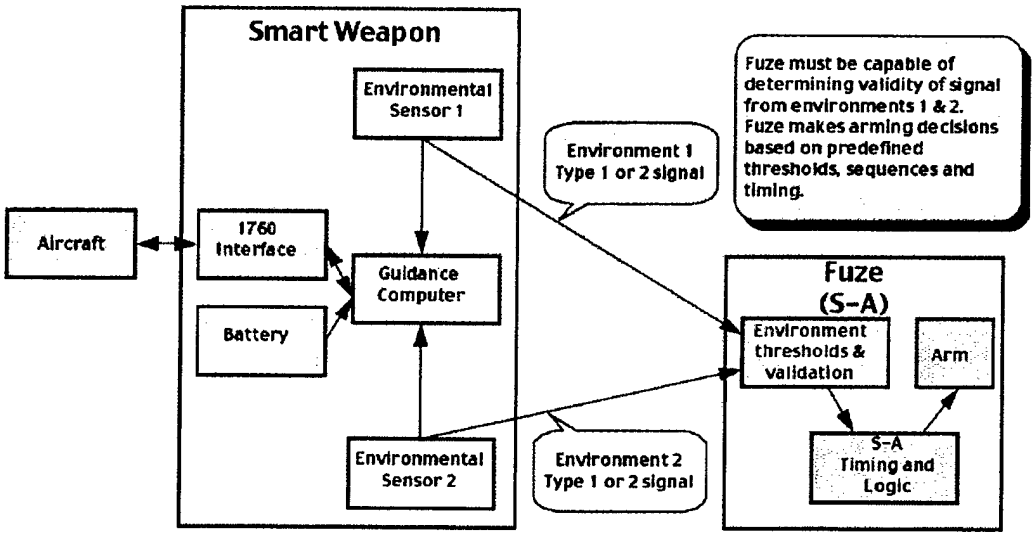

FIGURE 11. Shared Sensor (Independent of Guidance Computer).

In the application in Figure 12, the guidance computer is tracking the events occurring in the weapon system. The guidance computer generates two Type 3 signals sent to the fuze as environmental inputs. One of the problems encountered is how the fuze verifies that the signals received are valid inputs rather than signals generated by an out-of-control computer. To be an acceptable approach, a reliability safety failure rate of no greater than 1×10^{-6} is required from the guidance computer. In most cases, this requirement is cost prohibitive. Therefore, this approach should be avoided. While in theory this approach appears to be workable, it has proven to be impractical in application.

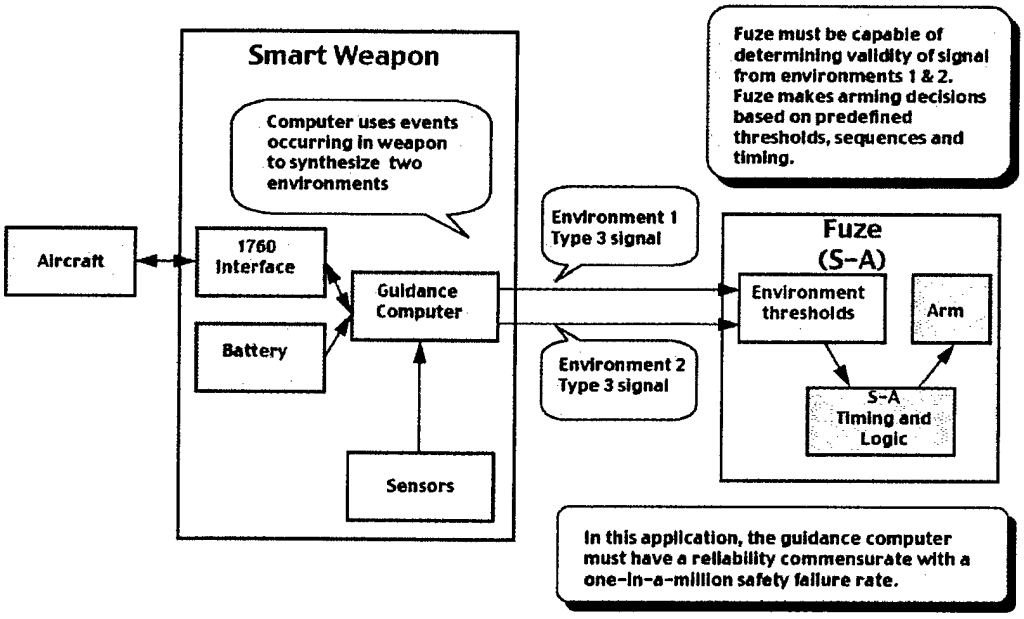

FIGURE 12. Computer-Processed Environment (Synthetic Environments).

The approach in Figure 13 is quite similar to that of Figure 12 except that a Type 4 signal is used. Unique information from the environmental sensors is encoded onto the signal being generated by the guidance computer. In this application, the fuze system determines the integrity of the received signals based on the additional information. This approach requires that the encoding technique be secure enough to preclude a malfunctioning computer from generating encoded signals that, in actuality, have not occurred.

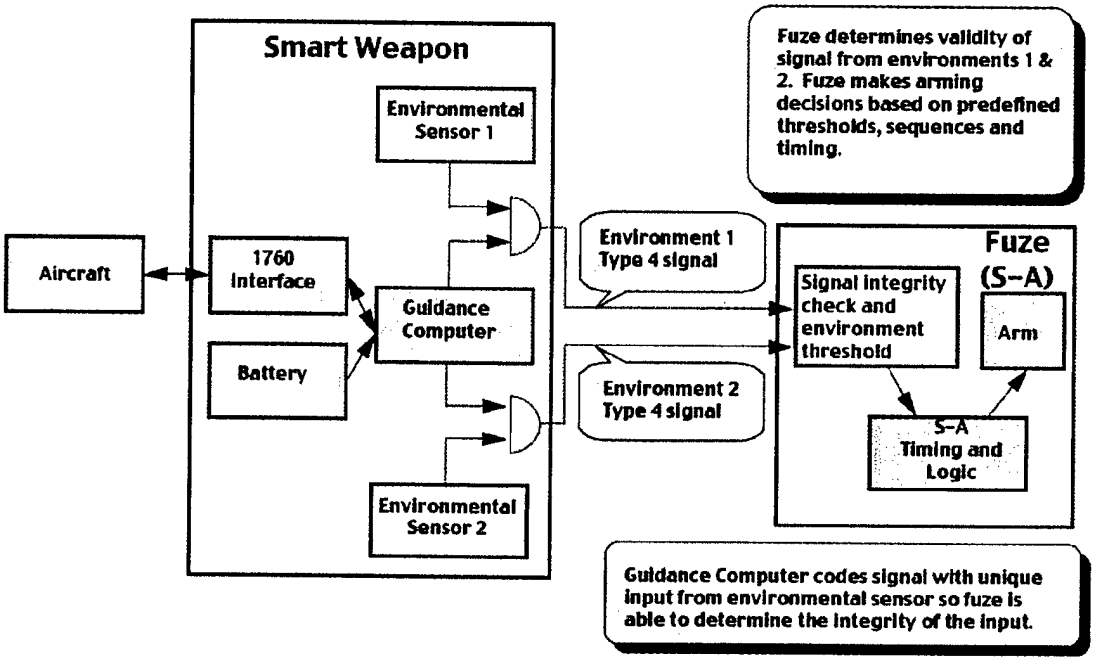

FIGURE 13. Computer-Processed Environment (Unique Coded Signals).

The approach in Figure 14 is the most controversial because it deals with the concept of distributed safety systems. In other words, the safety logic is not in the same location or package as the fire circuits but is centrally located. The safety logic, along with inputs from environmental sensors and the guidance computer, determines when arming the warhead is appropriate. The signal from the safety logic to the command arm fuzes is encoded so that a false signal is highly unlikely. Each command arm fuze has the ability to verify the integrity of the command arm signal and arms based only on the proper reception of an actual or valid arm command.

The controversy revolves around whether the single input can provide adequate safety. One argument is that a single command into the fuze at the wrong time could cause the system to arm the warhead before it is safe to do so. Another argument is that, because the input signal is encoded, a false arm command is not a single failure but actually two failures—namely, a signal is generated at the wrong time, and the encoding is correct but for a false signal. This argument cannot be resolved by evaluating a block diagram. Only assessment of the final design circuitry will determine whether there is a single point failure potential.

The bottom line is that this approach is unacceptable if a single output is required (because of the complexity of the design). However, because the requirement for multipoint initiation demands more and more outputs, this type of approach may become more common.

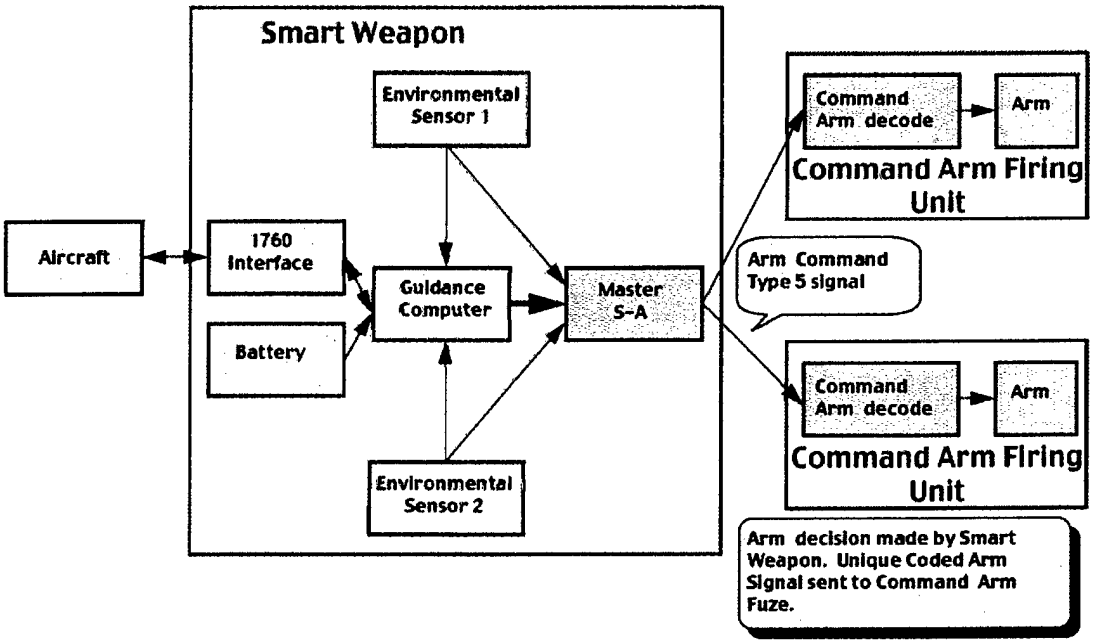

FIGURE 14. Command Arm (Smart Weapon With Safety System That Commands Satellite Fuze).

It is intended that two key principles are clarified by this discussion. First, it is unacceptable to have a design in which the environmental signals cannot be validated. This deficiency makes it almost impossible to determine the safety failure rate for the system when the integrity of the environmental signals is unknown. Second, distributed safety systems are generally an unsuitable practice. While a distributed safety approach is possible, in most cases, there are better and usually less costly ways to meet performance requirements. Another concern, when dealing with multiple firing units, is that the safety system failure rate requirement is less than 1×10^{-6}. Thus, if there are two firing units, each firing unit must have a safety failure rate of less than 5×10^{-7} ([1/N × system safety failure fate] = unit failure rate, where N is the number of units). As the number of firing units increase, the safety failure rate requirement for each individual unit becomes smaller. Obviously, this limitation will become a problem for the designer if the number of firing points becomes even moderately large.

PRODUCTION EVALUATION TEST PHILOSOPHY

S&A devices contain sensitive explosive elements that initiate the warhead. These devices are used with modern missile ordnance sections to provide a measure of safety during the pre-launch handling, carrying, loading, and launching of the missile and during initial travel of the weapon system to its target. In modern weapons, the S&A device is installed in the warhead during the assembly of the weapon at a weapons station and remains in the warhead throughout the weapon's life cycle. While an arming failure of the S&A device will result in a dud warhead, the unintentional arming of the S&A device might initiate the warhead with disastrous results. The foregoing discussion makes it clear that the S&A device is a critical component in the ordnance section of a weapon system.

MIL-STD-1316 establishes the design safety criteria for S&A devices and fuzes. The safety failure rate should not exceed one failure in a million opportunities for all phases—from manufacture to the designated service endpoint. From the time of manufacture to intended functioning, this safety level must be sustained while maintaining a system-assigned reliability of at least 99.5 % after exposure to all service environments over a service life of at least 20 years. These safety and reliability requirements are very high. Therefore, the S&A device design is critical; and the manufacture of the S&A device must be performed in strict accordance with the documented design. The testing and the manufacturing requirements are contained in the fabrication specification and the drawing package. The technical design agency has the responsibility to develop a design that meets all requirements and then document it so that any competent manufacturer of precision electromechanical devices can build the S&A device.

It is clearly evident that end-item testing to demonstrate safety failure rates of less than 1×10^{-6} or to demonstrate reliability levels of 99.5% after 20 years of service is so expensive that it becomes unfeasible. Over the years, NAWCWD has developed a system of coordinated, stringent, in-process inspections, in-process tests, and limited end-item tests. The theory is simple—if the S&A device is designed correctly and built as designed, it will perform as required. The soundness of the design is determined by collective inputs from the most knowledgeable people available based on past experience and extensive formal laboratory testing and evaluation. However, determining that the S&A device has been built as designed is a different matter.

The specification and drawings call out a large number of certifications, inspections, in-process tests, and end-item tests for critical or important functional features. In practice, the government does not critically review every certification, witness every test, or inspect every component. However, the evolution of a combined test and evaluation program gives the Fleet the best assurance of receiving S&A devices that will perform as designed. This conviction is backed by the following precautions.

1. During production of the S&A device, the manufacturer forms inspection lots consisting of 151 to 500 units. The manufacturer conducts functional tests on each unit in the lot, records the performance data, and removes all non-conforming units (a record is kept of all removed units). To verify that all non-conforming units were removed, the lot is sampled to a 0.4 acceptable quality level on a double-sampling plan (each sample is 80 units). These units are subjected to end-item tests in the presence of a government quality assurance representative (QAR). These tests verify that the manufacturer properly performed the tests, that all units function as required, that all the non-conforming units have been removed from the lot, and that the lot may be accepted for further evaluation by the government.

2. A 15-unit lot evaluation sample, frequently called the lot acceptance test (LAT) sample, is randomly selected by the QAR from the entire lot. This sample is tested by an independent test facility in accordance with the fabrication specification. These tests evaluate the S&A device's ability to withstand extreme life-cycle environments, as related to both reliability and safety. A sample size of 15 units, of which only a few units may be exposed to all these environments, is not statistically adequate to describe the entire lot. However, destructive testing of adequately large samples on a routine basis during production is uneconomical and considered unnecessary.

The time lost during lot sample evaluation testing is also a concern. However, this time is predictable and can be scheduled. In any event, the combination of tight delivery schedules and failure to meet acceptance test requirements cause major problems in delivery. If an S&A device's performance deviates from the test requirements, the cause of the anomaly or its failure to permit proper evaluation must be determined. While this assessment takes time, it is critical in determining the life-cycle performance of the S&A device.

In any discussion about acceptance testing, the question arises—why not draw up a list of all possible failures and establish an accept–reject or rework criteria? This is a logical question—particularly after conducting a failure analysis. Several attempts have been made to establish clear-cut accept–reject criteria. The problem is that making a correct determination of when an item will fail is quite complex. Also, safety experts have found it almost impossible to quantify the different degrees at which a device will fail.* Moreover, there are many failures that have never been encountered and cannot be predicted.

The following is a scenario of an unexpected problem that had never before been encountered. In heat treating, the launch latch was inadvertently case hardened. Upon quenching, minute cracks (not readily visible) developed. The technician failed to report his mistake. The latch broke in both drop and safety tests—and yet the unit had passed all the MIL-STD-331 (Reference 3) test requirements.

Cost also drives the emphasis placed on S&A device reliability. A guided missile can cost from $50 K to $1500 K while the S&A device costs from $0.5 K to about $15 K—or a relatively small percentage (1%) of the total cost. Yet, if the S&A device fails to function, the missile cannot detonate its warhead on target. The cost of a failure to function also includes the cost of damage done by the target. The S&A device is a one-shot item that cannot be recalled readily and retested after delivery to the Fleet. Obviously, the present unit cost of $0.5 K to $15 K is cost effective if it buys a highly reliable S&A device.

The importance of safety cannot be overemphasized. In order to improve the reliability of guided missiles, they are assembled and tested as all-up rounds at the weapons depots. The S&A device is, therefore, also installed in the warhead at that time. If a warhead is accidentally initiated during these tests, it can do extensive damage. If the warhead is initiated accidentally in a ship's magazine, it can result in lost lives or a sinking ship. Additionally, some of the fuzing circuits used on guided missiles apply a series of firing pulses to the S&A device immediately after the launching of the missile. Were the warhead to be initiated at this time, it would certainly damage the launch vehicle. Therefore, the S&A device must keep the warhead safe from accidental initiation during assembly, storage, carrying, and loading and after launch during travel within a safe separation distance from the launch vehicle. In the latter case, the S&A device may be the only warhead safety device functioning on the missile.

No other component of the ordnance section of the weapon system has such critical and stringent performance requirements. For this reason, the test and evaluation programs for S&A devices must be extremely thorough.

---

* Possible questions: If an S&A device arms too fast (early), it may present a safety hazard. However, there are many questions to consider. Would safety personnel accept, reject, screen, or rework a lot if one sample unit armed 0.010 second early? What if it armed 1 second early? What if it armed early and the cause was found to be a defective gear? What if the S&A device cost $500 apiece in a lot size of 500 units with another 500 following in a few days and the Fleet needs missiles? What if it takes 30% of the new cost to rework the lot and to submit and test another lot evaluation sample? What if the S&A device cost $2,000 each and the lot size is 200?

SUMMARY

This report documents the philosophy that has been used by experienced fuze designers at NAWCWD for over 30 years. It is hoped that the readers find this account useful in their quest to understand basic S&A design principles. The author also hopes that this document will help accomplish the following goals:

1. Avoid, or at least minimize, exposure of personnel and/or equipment to unacceptable hazard levels.

2. Provide a highly reliable method of initiating explosive trains containing sensitive or high explosives.

3. Aid future S&A device designers and reviewers in performing their roles.

In closing, the readers should remember that many other methods are valid in the design of S&A devices. However, the techniques presented herein represent an accepted and time-tested methodology. Therefore, any drastic departures from these basic principles should be undertaken with extreme caution.

REFERENCES

1. Naval Air Systems Command. *Fuze Design, Safety Criteria for.* Washington, D.C., NAVAIR, 9 April 1991. (MIL-STD-1316D, document UNCLASSIFIED.)

2. Naval Sea Systems Command. *Weapons System Explosives Safety Review Board Technical Manual for Electronic Safety and Arming Devices with Non-interrupted Explosive Trains.* Washington, D.C., NAVSEA, 30 September 1990. (NAVSEA, document UNCLASSIFIED.)

3. Naval Air Systems Command. *Fuze and Fuze Components, Environmental and Performance Tests for.* Washington, D.C., NAVAIR, 1 December 1989. (MIL-STD-331B, document UNCLASSIFIED.)

INITIAL DISTRIBUTION

2 Naval Air Systems Command, Patuxent River
  Code 4.T
    Gehris (1)
    S. Shumway (1)
1 Naval Sea Systems Command, Arlington (PMS-422-16, N. Bazarko)
2 Naval Air Warfare Center Weapons Division, Point Mugu
  Code 473310E
    F. Becker (1)
    Don Morgan (1)
2 Defense Technical Information Center, Fort Belvoir

ON-SITE DISTRIBUTION

4 Code 47BL000D (3 plus Archives copy)
1 Code 47CA00D, W. Doucette
1 Code 47CA70D, A. Thompson
1 Code 47C000D, J. Robbins
30 Code 478000D, S. Fowler
1 Code 478A00D, N. Fasig
3 Code 478C00D
  B. Bartels (1)
  R. Cope (1)
  G. Hennings (1)
1 Code 478200D, L. Brauer
20 Code 478300D, M. Tyler
1 Code 478400D, C. Halsey