

UNCLASSIFIED

AD NUMBER
AD875185
NEW LIMITATION CHANGE
TO Approved for public release, distribution unlimited
FROM Distribution authorized to U.S. Gov't. agencies only; Administrative/Operational Use; 18 MAY 1970. Other requests shall be referred to United States Naval Ordnance Lab., White Oak, MD.
AUTHORITY
USNOL ltr, 12 Dec 1972

THIS PAGE IS UNCLASSIFIED

J. Lott
625-110

NOLTR 70-94

2

AD-875185

FUZE SAFETY CONCEPTS

By
Allen M. Corbin

NOL

18 MAY 1970

UNITED STATES NAVAL ORDNANCE LABORATORY, WHITE OAK, MARYLAND

NOLTR 70-94

ATTENTION

Each transmittal of this document outside the agencies of the U S Government must have prior approval of NOL.

FUZE SAFETY CONCEPT

Prepared by:
Allen M. Corbin

ABSTRACT: Weapon safety is defined as "the probability of freedom from the destructive effects of one's own weapon in any conditions which may occur before intended launch and safe separation." This report concentrates on fuze safety since the fuze is frequently the most sensitive component with respect to the weapon safety or reliability. When this definition is compared to the definition of reliability, "the probability that an item will perform its intended function for a specified interval under stated conditions," it is evident that there is a cross-purpose of safety and reliability goals. But only the purposes are opposites. The techniques for improving reliability when applied with safety in mind can improve safety. The parallel path redundancy to improve reliability becomes an additional series barrier when the redundancy is to improve safety. It then becomes evident that much of the spade work for improved formal safety programs has been done in the advancement of the reliability disciplines. The challenging task is to give the designer information and objectives pertinent to safety which are comparable to what he now expects for reliability. The author presents his views on how to determine pertinent safety objectives and the means to avoid safety bypasses in the safety system design. The necessity for a safety-reliability balance suggests that an activity which is designing and developing hardware, such as a fuze, should have a close working relationship between its safety and reliability organizations.

PUBLISHED 18 MAY 1970

U. S. NAVAL ORDNANCE LABORATORY
WHITE OAK, MARYLAND

NOLTR 70-94

18 May 1970

FUZE SAFETY CONCEPTS

The preparation of this report was one of the recommendations of an ad hoc group consisting of representatives of the Naval Ordnance Laboratory, the Naval Weapons Center, Corona Annex, and the Naval Weapons Laboratory, Dahlgren, which, in 1965, studied fuze safety objectives and recommended changes to take advantage of modern methods and technology. When the Working Party for Fuzes of the Joint Technical Coordinating Group for Air Launched Non-Nuclear Ordnance (JTCC/ALNNO) explored the possibility of developing joint service fuze safety criteria, an early draft of this report, dated 9 January 1968, was made available to the Working Party members. This helped to provide the rationale for the Navy's long-range plans, formulated by the ad hoc group in 1965, so that these plans would be adequately considered in the tri-service coordination.

Work on the program of modernizing fuze safety design objectives in NOL is being performed under Task A532-5323/292-5/0246-0000-03 Work Unit A53233A-2.

GEORGE G. BALI
Captain, USN
Commander

R. E. Grantham
R. E. GRANTHAM
By direction

CONTENTS

	Page
PREFACE	v
Chapter 1 - FOUR ACCIDENTS	1
Chapter 2 - SAFETY DEFINITIONS	3
Chapter 3 - SAFETY AND RELIABILITY	6
Chapter 4 - SAFETY-RELIABILITY BALANCE	9
Chapter 5 - DIFFERENT SAFETY APPROACHES	14
Chapter 6 - SAFETY OBJECTIVES	17
Chapter 7 - SAFETY SYSTEM DESIGN	25
Chapter 8 - EXPLOSIVES SAFETY	47
Chapter 9 - A SAFETY PROGRAM IN DEVELOPMENT	58
Chapter 10 - SUMMARY	78
REFERENCES	81
APPENDIX A	A-1
REFERENCES	A-8

ILLUSTRATIONS

Figure	Title	Page
4.1	Simple Reliability Model	10
4.2	Simple Safety Model	10
4.3	Possible Safety Model for Two Series Safety Devices	11
4.4	Safety Device Added to Simple Reliability Model	11
4.5	Parallel Redundancy to Improve Reliability	11
4.6	Series Redundancy to Improve Safety	12
6.1	Examples of Potential Hazards Analysis Worksheets	21
6.2	Symbolic Purpose of Potential Hazards Analysis	23
7.1	Weak Link, Switching Analogy	32
7.2	Weak Link Fail Safe Logic	32
7.3	Alternate Safety Design Solutions - Acceptable Equivalence	35
7.4	Event Order by Procedure	39
7.5	Event Order by Design	39
7.6	Safety Component Orientations	42
9.1	Conceptual Safety - Potential Hazards Analysis Solution	60
9.2	Reliable and Safe System Concept	62
9.3	Hardware Weaknesses - The Safety Bypasses	64
9.4	Safety Analysis Diagrams	67
9.5	Preliminary Design Review	72
9.6	Design Review at Design Freeze	73

PREFACE

On 30 June 1964 at the Third Annual Reliability and Maintainability Conference held in Washington, D. C., a paper was presented entitled "Systems Safety-Reliability's New Associate." This association of safety and reliability was intriguing because at first it appeared to contradict a prevalent impression that these two important characteristics are diametric, suggesting that different approaches are necessary. The material presented in this report will not change the impression that safety and reliability are diametric in certain important aspects; however, it will suggest that the same or similar disciplines are applicable to improvement of quality of both characteristics. In other words, the tools of the reliability engineer, with little or no change, can be applied to improve and control designed safety. But these tools must be applied to achieve different, and frequently opposite, results. In theory, the author has found no exceptions to this. Practical applications are a different matter, for the degree of difficulty of applying some operations to safety is much greater.

The comparison of reliability and safety disciplines had to start with a feeling for the breadth of safety problems leading to an acceptable definition of safety. To illustrate this, four quite different accidents are described. Weapon safety is then defined as "the probability of freedom from the destructive effects of one's own weapon in any conditions which may occur before intended launch and safe separation." From this point on it was quite simple to present the similarities to reliability in regard to redundancy, design objectives, human engineering, and the roles of analysis and testing.

Since much has been said about reliability, it is not surprising that even in a brief treatise of safety, much had to be said. This prompted the writing of a summary at the end of each of the longer sections presenting the main points in condensed form. Finally a section summarizing the entire report was added.

FUZE SAFETY CONCEPTS

Chapter 1

FOUR ACCIDENTS

1. On 6 March 1953 an F4U aircraft returned aboard a carrier with a hung 250-pound general purpose bomb. On arrested landing the bomb tore loose and tumbled. It bounced twice on the deck, damaging or breaking the tail fins. On the third impact with the deck, on the bomb nose, it exploded. The casualties as reported on the day of the accident were two critically injured, two seriously injured, and five with minor injuries. One officer pilot was injured. The explosion blew a hole approximately four feet by eight feet in the number three elevator. The F4U aircraft was severely damaged and was a total loss. Two F9F aircraft parked at hangar bay 2 were punctured by flying fragments and leaked gasoline onto the deck. Fortunately, there was no fire.

2. The following is quoted from OP 1014, (reference (a)):

"An important lesson to learn about accidental explosions is that the force initiating explosions varies widely. In one instance, 12 TNT-filled bombs were dropped from a height of 2,500 feet onto concrete. Only one exploded, and that was a 'low order' explosion. In contrast, a fall of a mere six inches set off a similar depth bomb." Several paragraphs later the article continues: "The depth bomb which exploded after falling only six inches was aboard an aircraft carrier in 1945. Ordnance men were transferring Mk 54 bombs from one type aircraft to another being readied for patrol. An aviation ordnance man, second class, placed two bombs on a skid not fitted with a safety wire. He had to push the skid over an arresting gear wire. The skid tilted. Both bombs slid off and fell six inches to the deck. They struck tail vane first. One exploded. Fifteen feet directly in front of the exploding bomb, a man working on a plane was struck and killed. Six others were injured. Torpex on the deck began burning, but was quickly extinguished. Two aircraft were damaged."

3. During a rapid salvo-fire support mission a five-inch projectile exploded in the barrel of a gun. Before this approximately 34 rounds had been fired from the gun in a 30-minute period. The explosion removed approximately 18 inches from the gun at the muzzle. Flying pieces caused light damage to the bridge, an anti-aircraft station, the starboard hedgehog launcher, and antenna arrays on the foremast. One seaman was killed. Witnesses said that at least one round was fired after the muzzle explosion and it functioned normally on target.

4. The following accident is also described in OP 1014 (reference (a)). In 1929 a Marine failed to comply with instructions to turn in hand grenades after a patrol. He kept one live grenade and a dummy grenade. Later during some horseplay, and in an attempt to frighten other marines, he pulled the pin of what he thought was the dummy grenade. He lost four fingers and suffered wounds in his right shoulder and thigh.

5. This report discusses what designers can and can't do to reduce the number of accidents like those described above. A safe weapon isn't so by accident. It is safe because a great deal of thought went into the design of its safety features and the procedures established for its use and handling. When safety problems arise they raise the question of whether or not experience, knowledge, and thought are being used to best advantage, and in particular, are being applied to the design of safety systems. This report is intended to stimulate some thought, impart some knowledge, and cite some experience which can be used to enhance safety in future weapons.

Chapter 2

SAFETY DEFINITIONS

1. Webster defines safety as freedom from danger or hazard. He also defines a weapon as something to fight with. Therein arises a paradox. Weapons are designed to kill and destroy and yet it is desired that they be safe. History shows that man has not always been as successful in this as he would like to be. Reference (b) contains a quotation which expresses the concern of a Civil War General that his own ammunition might be doing him more harm than good. Confederate General D. H. Hill wrote the following blunt note to his Secretary of War: "There must be something very rotten in the Ordnance Department. It is a Yankee concern throughout and I have long been afraid there was foul play there. Our shells burst at the mouth of the gun or do not burst at all." The problem of muzzle bursts, so prevalent with the first explosive shells, has been pretty well mastered, and now, muzzle bursts are quite infrequent. But new weapons employing ingenious technological advances are constantly being devised, and with them come new and unfamiliar hazards. How successfully man avoids being the victim of his own devices depends on his ability to recognize these hazards and harness the conditions which create them. As a start, an attempt should first be made to define the problem and some of its ramifications.

2. Many definitions of safety have been written. Kanda listed sixteen definitions in addition to Webster's in a paper presented at a system safety symposium in June 1965 (reference (c)). Most of these were more specialized than any general definition and applied to such things as missiles, military aircraft, and automotive equipment. He concluded there was no set definition of safety and explored some of the problems involved in expressing it as a probability. There are at least a dozen published definitions that he didn't list. Consequently, there should be no harm in suggesting a few more, the purpose being to identify different aspects of safety and suggest where design responsibilities start and end.

3. Referring to the first accident described one might conclude that:

"Safety is a good fuze."

The investigation of the accident revealed the following. Pieces recovered after the accident indicated that when the bomb was tumbling and hit on the tail, the vane assembly tube and arming stem were sheared. This released the fuze firing plunger which functioned normally on the subsequent nose impact. These indications were later

verified in tests. The accident was attributed to a deficiency in the fuze design. A better fuze design would have avoided this accident and at least one other from the same cause.

4. The second accident described suggests that:

"Safety is a trustworthy explosive."

To say that any explosive is trustworthy can be done only in a relative sense. But experience gives a sense of relative trust. A feeling for this is actually expressed in the description of the accident. At the start of World War II, TNT was the standard explosive filler. But during the progress of the war a great deal of pressure was put on the Bureau of Ordnance to supply weapons containing an explosive with more punch. With some misgivings because of known greater sensitivity to bullets and shell fragments the Bureau gave interim approval to the use of Torpex while continuing the effort to develop powerful explosives with less sensitivity. The description of the accident compares a 2,500-foot drop to a fall of a mere six inches to drive home the point that extreme care must be exercised in the handling of explosives. Since TNT-filled bombs were involved in the 2,500-foot drop and a Torpex bomb in the six-inch fall, it is doubtful that this particular comparison is really valid. In fact, in published properties of military explosives, such as reference (d), Torpex is more sensitive than TNT in all comparable tests. There were many disastrous accidents with Torpex. About all that anyone can say is that some of these probably would not have happened if a more trustworthy explosive, such as TNT was, or HBX is pictured to be today, had been in the weapons.

5. Another possible definition is:

"Safety is constant quality."

The muzzle bursts which caused the dismay of the Confederate General are no longer common occurrences. There are occasional reports. These changes were brought about by advancing the knowledge of explosives and the designs and safety concepts of fuzes. The safety record in World War II, when projectiles were fired in huge quantities, is evidence that the design problems were well in control. But no matter how good a design may be, its effectiveness may be jeopardized if the intended quality is not maintained in production. Information is not at hand to lead to the conclusion that the accident described in Chapter 1 can be attributed to lowered quality. The cause of this accident may not have been identified, and it may never be. The example was used only because it is the kind of accident that could easily have been caused by failure to detect a flaw or deficiency on the production line. The stresses which a projectile experiences in a gun are tremendous. At various times muzzle bursts have been attributed to cracks in the filler explosive, gas leaks around a base seal, and omission or breakage of vital parts of the fuze. Consequently, any lowering of quality may result in a part which cannot withstand the tremendous stresses of gun firing. If the part is vital, the projectile becomes a potential muzzle burst.

6. Many ordnance accidents are caused by horseplay. This suggests another possible definition:

"Safety is a reliable buddy."

It is a wonder that the marine who caused the accident described in Chapter 1 was not killed. Perhaps the grenade was a practice rather than a service round. However, there have been many instances where, not only the culprit, but innocent bystanders were killed or seriously injured by foolish acts of this type. Russian roulette, souvenir seeking, horseplay, and overconfidence cause numerous ordnance accidents, killing and maiming the guilty and innocent alike. The reliability, or unreliability, or people is an important factor in safety.

7. Good design of a weapon cannot create complete "freedom from danger or hazard" but it should do its fair share. This report discusses concepts and logic, and cites examples of good practices and rules which are useful guides in designing safety into weapons. The arguments presented are developed on the basis that safety is best expressed as a probability. This probability should be high when it is a measure of freedom from hazard. Some people prefer to think in terms of a small number, a safety failure rate. This is the probability which is unsafety, a measure of exposure to hazard. It will be shown later (see Appendix A) that obtaining a numerical measure of safety requires more data than are available today. In spite of this, a designer can often be quite sure of the effect on safety of a design change. That is, he can be quite sure that his design change is improving safety or degrading it, without knowing beforehand how safe or unsafe the system was. Methods similar to those used in reliability engineering can be of great assistance in this. A discussion of safety and reliability similarities and differences will help to make this clear.

Chapter 3

SAFETY AND RELIABILITY

1. Since safety is defined as a probability, it is important to consider its relation to reliability. MIL-STD-271B (reference (e)) gives the following definition of reliability: "The probability that an item will perform its intended function for a specified interval under stated conditions." Thus for any particular weapon it is necessary to define the intended function, the specified interval, and the conditions under which this functioning is expected to occur. These are the success criteria. Using them, tests are conducted to obtain a measure of reliability. If the success criteria are not defined, the basis for measuring reliability is lacking.

2. It is particularly important to note that "conditions" must be defined. Broadly speaking, there are two types of conditions: conditions before launch and conditions after launch. Conditions before launch are those which make the hardware "old and tired." This includes handling, storage, transportation, and the like. The normal limits of environments in these phases can be predicted. Consequently, their degrading effects can be investigated. When something unusual happens which damages the weapon it is withdrawn or repaired. It is not expected to perform in the damaged condition. Conditions after launch are usually even easier to define. Most weapons have a fixed delivery mode and therefore fixed limits of delivery environments and conditions.

3. The measure of reliability is expressed as a probability. Acceptable weapon reliabilities vary considerably depending on weapon complexity, effectiveness, and the unfavorable environments in which the weapon must operate. Acceptable reliabilities may range from below 0.80 to above 0.999. In this range it is usually considered feasible to demonstrate the reliabilities by conducting tests.

4. It is theoretically possible to treat safety in an identical manner, but the practical problems are extremely severe. The reasons for this will be clearer after safety is defined. Weapon safety is here defined as: "The probability of freedom from the destructive effects of one's own weapon in any conditions which may occur before intended launch and safe separation.* For those who prefer the small

*In these definitions reference to "hazard" has been intentionally dropped. In the definition of "unsafety," which will serve to explain this point, the probability of concern is not the probability of being in danger or peril but is the probability of being destroyed. Danger or peril can pass without destruction. The term "hazard" is used more correctly in reference to conditions which produce high risk or danger and is used in the term "hazard analysis."

number, weapon unsafety is defined as: "The probability of experiencing the destructive effects of one's own weapon resulting from any conditions before intended launch and safe separation."

5. To place reliability on a measurable scale it was necessary to define the intended function, the specified period, and the expected conditions. To place safety on a measurable scale it will be necessary to define the destructive effects, the period when safety is required, and the conditions in which safety is needed. The first of these, the destructive effects, is not quite as easily defined as the intended function in reliability. For example, two major destructive effects of an all-up missile are warhead detonation and motor burning. Accidents involving these may originate from quite different events. In seeking measures of safety these two would have to be considered separately. The second is the period when safety is required. It is all time prior to use or disassembly and removal from service. This may be a matter of many years. But as a time period it is no more difficult to define than the logistics cycles in reliability. The third is the most difficult problem. It is defining the conditions in which safety is needed. Reliability deals with normal conditions and it is possible to place upper bounds on these. Safety deals not only with normal conditions but also with abnormal conditions. In reliability it is possible to define a series of normal conditions, apply these in sequence as a single set of conditions, and follow this with a test for score. In safety, the abnormal conditions, and there are many, cannot be applied in sequence as a single set of conditions because there is no definable sequence and the abnormal conditions can be independent isolated events. As a result of this, tests for safety would have to be far more numerous than for reliability if the two are to be put on a comparable basis.

6. Another factor discourages the measurement of safety. Earlier it was pointed out that acceptable reliabilities generally fall between numbers such as 0.80 to 0.999. The most quoted number for unsafety comes from criteria for conventional fuzes. It is a safety failure rate not to exceed one in one million. Put in terms of the probability which is safety this is 0.999999. Although this number is not necessarily the proper number for every weapon, it does show that safety should be several orders of magnitude greater than reliability. At present it is not considered feasible to demonstrate safety experimentally with statistically meaningful numbers.

7. The prospect for safety measurement is not quite as dark as the foregoing discussion may have implied. This is because there is a low expectancy of encountering abnormal events. The probability, which is unsafety, associated with a particular abnormal event is the product of the probability of encountering the event and the probability of experiencing the destructive effects of the weapon as a result of the event. If the probability of encountering an abnormal event is extremely small, the probability of experiencing the destructive effects as a result of the event, which is what could be measured by tests, may not have to be so very small. Then, for this particular event, the number of tests required might not be prohibitive. However, the relief this provides to the overall problem

is only slight. There are many abnormal events and consequently there would have to be many different tests. There is also the problem of normal events where reliability testing provides only a fraction of the total data which are needed to demonstrate the much higher safety level.

8. A more complete discussion of safety measurement and the important parameters involved appears in Appendix A. The brief discussion given here is to make the following points:

a. Like reliability, safety (or unsafety) can be expressed as a probability.

b. Unlike reliability, the measurement of safety is not demanded because the practical problems involved are enormous.

The similarity between reliability and safety has been emphasized to show that the disciplines required to obtain high quality in these two important characteristics are similar. The disciplines applied to obtain good reliability are aimed at increasing the probability of satisfactory performance. The disciplines applied to decreasing unsafety must be essentially the same. They must be aimed at decreasing the probability of encountering the destructive effects of one's own weapon. The numbers which evolve in reliability are only measures of the success with which these disciplines have been applied in the engineering and development of the system. The lack of numerical measure of success in safety does not remove the responsibility for diligent application of controls, studies, reviews, and quality engineering. If anything, it emphasizes the need.

9. SUMMARY. Weapon safety is defined as "The probability of freedom from the destructive effects of one's own weapon in any conditions which may occur before intended launch and safe separation." A correspondence to reliability is seen when this definition is compared to the accepted general definition of reliability: "The probability that an item will perform its intended function for a specified interval under stated conditions." Both are probabilities. The "destructive effects" of the safety definition is usually the "intended function," when delivered to the enemy, of the reliability definition. The conditions of the safety definition are broader, being "any conditions before intended launch and safe separation." It is this multiplicity of conditions adding to the need for a very high number, which makes the measurement of safety so difficult and costly.

Chapter 4

SAFETY-RELIABILITY BALANCE

1. From time to time reference is made to safety-reliability balance. OPNAV Instruction 8020.9A (reference (f)) in the statement of policy contains the following: "The current operational requirement to maintain a high state of readiness to provide an immediate nuclear retaliatory capability makes it mandatory that a conscientious effort be made by all agencies to achieve a balance between safety and operational readiness so that an operational capability will not be jeopardized by undue restraints dictated by safety considerations taken alone." Such statements imply that too much safety hurts reliability. If this is true, there must be a proper balance between safety and reliability. Since this report deals with safety, this balance must be discussed.

2. The word "balance" implies the existence of scales which permit the comparison of two objects or quantities. But it is not clear what is being compared in the safety-reliability balance. The preceding section discussed the difficulties in obtaining a measure of safety. Since measurement of safety is impractical, the balance cannot be the comparison of measured safety to measured reliability. Instead, it must be a judgment based on the premise that too many devices placed in a weapon to obtain safety, and too many restrictions placed on a weapon's use to assure safety, would seriously hurt reliability and operational readiness. This is logical, but it is not obvious. The concern of General Hill when he said "Our shells burst at the mouth of the gun or do not burst at all" was for a lack of both safety and reliability. There have been many other examples of weapons which were neither safe nor reliable. So good safety does not necessarily mean poor reliability, and poor safety does not necessarily mean good reliability. Even though the existence of a safety-reliability balance can be accepted as logical, it does not mean that in every case there must be a trade-off of one for the other.

3. The relation between safety and reliability is best explained by using reliability and safety models. Figure 4.1 is a simple reliability model. It shows that events A and B and C and D and E and F and G must occur successfully in order that the system function. If any one of these events does not occur, the series is broken and the system does not function. Each of these events may be the functioning of a mechanism which is a component of the system. Event G, which has been purposely set apart by being placed in a circle, could be the functioning of a safety device. It is quite likely that this device is in the system only for safety and contributes nothing but an additional event to the reliability problem. It is one more component

which must work if the system is to function successfully. On this basis its presence presents a reliability-safety trade-off.

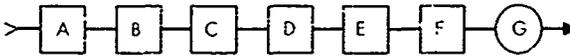


FIG. 4.1 SIMPLE RELIABILITY MODEL

4. This trade-off may not result in a satisfactory safety-reliability balance. There are many ways in which the safety device represented by event G may fail or be bypassed so that it does not provide the intended safety. An important part might be left out, or it might malfunction, or it might be left in the operated position after a test, or it might be susceptible to a particular environment, or it might be accidentally operated during handling. Because there are many ways in which a safety device may be defeated or bypassed the safety model tends to be parallel events. Figure 4.2 is a simple safety model. It shows that events a or b or c or d or e or f can lead to unsafety. If there are too many such events or any one of them is too likely, the system safety may not be acceptable. One solution to such a problem is to add another safety device. With the addition of a second device the safety model is changed. How it is changed depends on the nature and characteristics of the two safety devices and no simple generalized safety model can be drawn. However, Figure 4.3 is one possible model. In this model events a or b or c or d cannot be the sole causes of unsafety. Unsafety can result only if one of these events is followed by events g or h or i or j which represent failures or bypasses of the second safety device. Events, such as e and f, may still bypass both devices. But if the probability of these events is low enough, the system safety has been materially improved by the addition of the second device. The effect on the reliability model of the addition of a second safety device is illustrated by Figure 4.4. The simple model of Figure 4.1 has become longer by one event, event H, which is functioning of the second safety device. This has certainly not helped reliability but was done to improve safety. This is the safety-reliability trade-off.

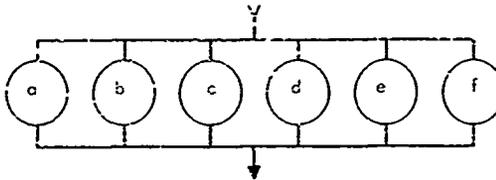


FIG. 4.2 SIMPLE SAFETY MODEL

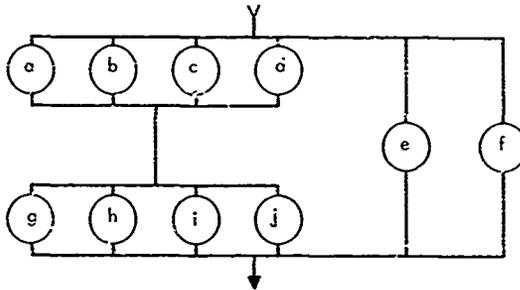


FIG. 4.3 POSSIBLE SAFETY MODEL FOR TWO SERIES SAFETY DEVICES



FIG. 4.4 SAFETY DEVICE ADDED TO SIMPLE RELIABILITY MODEL

5. The addition of event H is redundancy to improve safety. It is interesting to compare redundancy when its purpose is to improve reliability to redundancy when its purpose is to improve safety. Referring again to Figure 4.4, let us suppose that the functioning of components represented by events A and B are not reliable enough. To improve reliability redundancy is used. This may affect the reliability model as shown below.

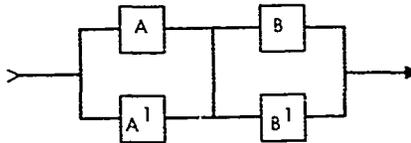


FIG. 4.5 PARALLEL REDUNDANCY TO IMPROVE RELIABILITY

Now in case event A does not occur, the system can still function if event A^1 occurs, and similarly for B and B^1 . The components added to perform the functions of A^1 and B^1 may be identical to those performing functions A and B, or may be entirely different.

Reliability literature contains many arguments presenting the cases for and against identical redundancy. An important argument for this discussion is: when the component failure is likely to be the result of effect of a normal environment, dissimilar redundancy using a component less sensitive to the environment is best. An example might be the backing up of an electronic timer with a mechanical timer because the electronic timer, although more accurate, is too sensitive to high temperature. Backing up the first electronic timer with a second identical timer would have the disadvantage that, if temperature rose high enough to cause failure of the first timer, failure of the second timer would be very likely. Since the purpose of the redundancy is to improve the probability that the sequence of events leading to operation will not be interrupted in the set of conditions when operation is wanted, dissimilar redundancy appears to be the better solution for the example just given.

6. The purpose of safety components is to provide controlled interruption in the operating sequence so that operation will not occur at the wrong time and place. Another way to say this is that the purpose of safety redundancy is to increase the probability that the sequence of events leading to operation will be interrupted in the set of conditions when safety is wanted. Compare this purpose to the purpose of reliability redundancy and it is evident it is exactly opposite. Consequently, it is logical that safety redundancy should be the opposite of reliability redundancy. It is the addition of series events in the reliability model as shown in Figure 4.6

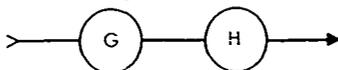


FIG. 4.6 SERIES REDUNDANCY TO IMPROVE SAFETY

7. The approach to analyzing the need for redundancy is identical whether the redundancy is for reliability or safety. Conclusions based on the analysis are frequently different. Identical redundancy is frequently adequate to improve reliability because the failure mode is independent of the set of conditions in which reliability is required. In other words, identical redundancy is frequently used to compensate for "lemons" and its success depends on seldom putting two "lemons" into the same device. Identical redundancy is usually not adequate to improve safety because the set of conditions in which safety is required vary so widely that failure modes cannot be independent of these conditions. Safety failures are more likely to be the result of stress of the accident environments than the result of "lemons." Therefore, it is simply the different nature of the two problems which leads to different solutions.

8. Reliability and safety models and safety-reliability trade-offs do not explain the greater unreliability and unsafety of Civil War projectiles as compared to modern projectiles. Today's weapons are more complex. There are more series events in the reliability models. Because of the complexity there are probably more parallel

paths in the safety models. Yet they are safer and more reliable. This change has come about because of improved quality. Explosives are better. Inert materials are better. Designs have improved. Engineering is more advanced. Production is more carefully controlled. New techniques have been developed. Knowledge has increased and experience has taught many lessons. In brief, the remarkable change between General Hill's shells, which burst at the mouth of the gun or not at all, and modern projectiles, which are not frequently involved in muzzle bursts was brought about by technological advances. This leads to an interesting observation regarding the relationship of safety and reliability. By employing technological advances,* both the safety and reliability of a weapon or weapon system may be improved. In the absence of any technological advance, safety can be obtained only at the expense of reliability and reliability can be obtained only at the expense of safety.

9. From what has been said it is clear that the need for a proper safety-reliability balance is real. Since a weapon is developed employing existing technology and disciplines, the safety-reliability balance is a matter of trade-offs at that level of technological advances. The design and development of future weapons will not be constrained by today's limitations and should strive for improved reliability and safety, and balance of these at the more favorable technological level.

10. SUMMARY.

a. The proper safety-reliability balance for a weapon system is achieved by safety-reliability trade-offs at the current level of technological advances.

b. The concurrent improvement of both safety and reliability can be achieved only by the use of advanced technology.

c. Redundancy to improve reliability is parallel redundancy. Redundancy to improve safety is series redundancy. Since series redundancy degrades reliability the proper amount of redundancy is a safety-reliability trade-off.

*Technological advance here refers to any or all disciplines whose application results in better quality or control or relationship to environments.

Chapter 5

DIFFERENT SAFETY APPROACHES

1. A little thought about widely different types of weapons leads to the conclusion that the methods of obtaining safety vary considerably. The safety of a hand grenade is the responsibility of the user. It contains a safety pin which the user removes. Firing is prevented by a safety lever which the user holds until the grenade is thrown. Firing is then delayed by a time fuse* which permits the grenade to be thrown far enough away from the user for his safety. Except for the delay of the time fuse, every step leading to the firing of the grenade, and consequently every feasible giving safety depends on proper use. Therefore, safety of a hand grenade is a very personal responsibility.

2. The firing train of the modern gun projectile is in the fuze. Most such fuzes prepare to fire by responding to forces developed by the gun. A common feature of these fuzes is a setback pin. To use some common values in the example, this detent may function when it experiences acceleration in excess of 3000 g, whereas the fuze will probably experience setback in excess of 12,000 g. Another common feature is the spin detent. This detent may unlock when it experiences spin in excess of 120 rps whereas the fuze will probably experience spin rates in excess of 200 rps. Frequently these two features are used in the same fuze. Then both must function to permit arming of the projectile firing train. The user is not responsible for operating these safety devices. In fact, they are usually designed and constructed so that it is virtually impossible for him to operate them. They are instead designed to function automatically as the result of forces developed in the gun.

3. Means of obtaining safety can vary all the way from complete reliance on the user to complete reliance on automatic mechanisms. In most weapons, safety is obtained by some combination of these. What is best for a particular weapon system depends on the nature of the system. The degree to which reliance is placed on the users of the weapon or on automatic mechanisms is not dictated by, but is certainly influenced by the following factors:

*In this report "fuse" is spelled with an "s" to denote (a) a length of combustible material, and (b) the protective melting element in an electric circuit. "Fuze" is spelled with a "z" to denote the device designed to initiate ammunition.

a. Launch Conditions of the Weapon: To cite an example, a gun projectile cannot depend on gentle handling for safety. The acts of hoisting from the magazine, ramming into the gun, and firing of the gun are extremely rough. The most dangerous instant is when the projectile is experiencing the high forces of setback and spin. This is where safety is needed most. The situation dictates the need for automatic mechanisms to separate the fuze, which contains the most sensitive elements, from the main charge, which represents the destructive power. Furthermore, the situation is well suited to mechanized safety devices. The forces available to operate the devices are large and practically invariant from one shot to the next. So relatively simple devices can be designed to respond to the forces, and the forces can be counted on to exist in every normal shot.

b. Cost and Simplicity: Mechanisms for safety usually increase cost and complexity. Consequently, every development involves decisions on how far to go in trusting the user to protect himself and those around him with simple safety devices which he can operate. The hand grenade is a simple weapon which is produced in large quantities. Individual cost is important. Suppose that a small zero-g device were developed for hand grenades. Incorporating this device would certainly increase the cost of each grenade. Because of the large quantities produced, the total cost would be sizeable. Would this cost be balanced by accidents prevented? The man who pulls the pin and releases the lever of what he thinks is a dummy grenade will probably not be saved, because he will figure out a way to beat the zero-g device, too. The man who accidentally snags the pin or pulls it out because of sheer ignorance will be saved. So the real value of the zero-g device depends on how often these accidents result from ignorance and chance.

c. Reliability and Training of Personnel: There is no doubt that when the personnel who handle and use a weapon are very reliable and well trained there is less need for built-in-mechanized safety. This is because, to a certain degree, mechanized safety is protection against foolish or careless acts. However, the need for specially trained and selected personnel to obtain weapon safety should be avoided to the extent possible. It does not make sense to impose the never ending training and selection of personnel simply to compensate for poor design of safety features. If special personnel are required, it should be because they are required for other reasons or because there is no other known way to obtain the needed safety.

d. Multiple Use and Multiple Purpose Weapons: The weapon which can be launched in a number of different ways and can be used effectively against many different targets is very attractive. It eases supply and storage problems. However, it is much more difficult to design a weapon with these characteristics. Effectiveness becomes a matter of compromise; as a matter of fact, so does safety. Since the safety components in a multiple-use weapon must be designed to operate in conditions common to all uses, the available choices of operating forces are drastically limited. Invariably the result is that more of the responsibility for the weapon safety is placed in the hands of the user and less reliance is placed on mechanisms.

e. Weapon Quantities: When weapons are of a type which will be used in large numbers, such as HE bombs were during World War II, it is important to minimize dependence on special handling and treatment as a means of obtaining adequate safety. The movement of inert materials in such quantities is difficult enough. Consequently, the weapon should be made as inert as possible. Mechanized safety is frequently a step in this direction.

4. The designer of the safety component, such as the fuze, is usually not in a position to make final decisions regarding the type of safety which is best for a particular weapon. However, he can influence such decisions because he knows best how the use conditions of a weapon affect the design of his safety components. He knows when the operating forces proposed are marginal for operation of an automatic mechanism or when they are ample. He has the best appreciation of approximate cost and complexity. By being aware of the different means of obtaining safety he can suggest back-ups to compensate for the weaknesses of his mechanisms, when these weaknesses are imposed by the factors discussed above.

5. SUMMARY. The means for obtaining weapon safety can vary all the way from complete reliance on the user to complete mechanization making it almost independent of the user. Usually the safety is obtained by a combination of these. However, the choice is not independent of the weapon, since some weapons lend themselves to mechanization better than others. Excessive reliance on the user to compensate for poor design is wasteful, since it demands selection of personnel for stability and reliability and extends the period of training.

Chapter 6

SAFETY OBJECTIVES

1. If safety is to keep step with reliability, which is one thesis of this report, it must be possible to state clearly the requirements and objectives for safety at the outset of any weapon development. What is needed will be clearer if the general categories of information available for application to reliability are reviewed. Then it will be possible to decide whether or not the information presented is applicable, without change, to safety or whether safety needs its counterpart. The categories listed are performance, numerical reliability goal, environments, size and weight, and cost. This is not an exhaustive list but is enough to present the arguments.

a. Performance. In the category of performance are such things as definition of target or targets, warhead size and characteristics, kill probability against specific targets, errors and accuracy of delivery, and limitations imposed by alternate delivery systems.

b. Numerical Reliability Goal. The numerical reliability goal is the statement of the acceptable probability of performing the intended function for a specified interval under stated conditions. It is generally listed as a requirement, although it is frequently set too high to be realistic in this respect. In this regard it is a demand for quality which the customer may not really expect to get, but which he would like to have. Demonstrating the achievement of this goal, or the failure to reach it, is often a part of the development test program.

c. Environments. Environments and environmental magnitudes are listed for every phase which the weapon will experience. These are important to such things as choice of materials, structural design, finishes and surfaces, insulation, and sealing. The environments referred to here are the so-called normal environments which the weapon will experience and after which, or during which, it must function properly. Since the level of any environment which a weapon encounters will vary from one weapon to the next, the levels listed are the expected extremes of the normal environments. That every weapon will experience the extreme level of every environment is, of course, unlikely. Nevertheless, this is the premise which must be accepted by designers to give adequate assurance that the weapon will not fail as the result of one of the environments. The expected life of the weapon is usually listed separately. But an important effect of this statement is to indicate how long the weapon must endure the above environments and how many cycles it will experience. These things

also have strong influence on choice of materials, sealing, mounting, and the like.

d. Size and Weight. There will be restrictions on size and weight of the weapon determined by such things as how it is to be launched, where it is to be stored, how it is to be handled, and what existing equipment is to be used with it. To remain within these restrictions, the size and weight of subsystems and components must be fixed by reasonable apportionment. This has a significant effect on design considerations.

e. Cost. Cost has an important effect on design approaches. We cannot afford to spend dollars on the nickel and dime items for the arsenal. We also can't expect to get dollar values by spending only the nickel or dime. Consequently, the cost of weapon components is fixed quite rigidly by the ultimate worth of the weapon. The cost of a component is a big factor in determining how it must be designed.

2. The above list illustrates the extent of information available to the designer which bears on how components are designed to meet functioning performance requirements. Some of the information categories mentioned are equally applicable to safety. Such things as performance on target, size and weight, and cost, as presented in current design objective documents,* need no further elaboration to be equally meaningful in designing for safety. Where information has been deficient for safety design is in the areas of a numerical safety goal and safety environments.

3. The problems involved in measurements leading to a safety number, expressed as a probability, were discussed in Chapter 3. It was concluded that measurements of a safety number to any reasonable accuracy is impractical. This is a situation which will probably continue for a long time, perhaps indefinitely. Without the capability of measurement and demonstration, most of the usefulness of a numerical safety goal is lost. Since the "Basic Safety and Arming Design Objectives for U. S. Navy Fuzes" (reference (g)) were issued in 1953 there has been some use of "a safety failure rate not to exceed one in one million" as a safety design goal for fuzes and on occasion for other type weapons. However, discussions with several designers who have had such a numerical goal at the outset of design indicates that the number had very little influence on their choice of design, or materials, or any other aspects of their safety devices. This is because of two things. First, the small size of the number removes it from the realm of most human experience. Second, the implied, but undefined scope, covering all situations prior to launch and safe separation, cannot help but prove frustrating to one who has more than he can do without the added burden of systematic and thorough listing and analysis of these situations. Appendix A discusses measurement of unsafety. It argues that the probability of unsafety must be defined

*The NOL issues a document entitled "Design Objectives," which contains information of the type being discussed. However, much of the same kind of information appears in Technical Development Plans (TDP), Performance and Compatibility Requirements (P&CR) and even in Specific Operational Requirements (SOR).

for specific situations and is then the probability of a safety failure in the situation times the probability of ever encountering the situation. This approach would give much more meaning to each number because it would relate it to circumstances which have been experienced or can be envisioned. Furthermore, in situations having low probability of occurrence, the acceptable failure probability, which would be the primary concern of the designer, could be a number large enough to be in the realm of experience. Unfortunately, there would be as many such numbers as there are situations. Using these numbers profitably would be quite tedious. At this point it can only be concluded that this problem must be investigated further with the hope of uncovering a practical system for presenting useful numerical goals for safety.

4. Safety environments comparable to those listed as expected extremes of normal environments have also been lacking in design objective documents. In the past few years, accident situations were often listed. This was a step in the right direction, but didn't go far enough. The important environments of the situation were sometimes obvious. But when not, they were not singled out. No estimates of environment magnitudes were given. The problem is that the list of safety environments must be preceded by the prodigious task of listing all those things which can happen before the weapon is launched and reaches safe separation. Safety is needed in assembly, handling, checkout, transportation, storage, and preparation for launch. Many things can and do happen in these phases. The normal things can be pretty accurately predicted. The abnormal things are more difficult to predict. But unless some attempt is made to predict what situation and what conditions may arise, the designer of safety devices is at a distinct disadvantage. He must design safety devices without knowing the environments in which safety is needed. This would be intolerable to the reliability engineer. If a flight environment of 400°F were simply omitted from the environment list, and the designers, not knowing this, designed only to 160°F, the reliability would simply be unacceptable. The situation in safety is really no different. The designer must have the best list which can be assembled of those things expected of his safety device.

5. A method for obtaining a comprehensive list of conditions and environments which must be design objectives for safety is a predesign analysis of potential hazards. This will henceforth be referred to as potential hazards analysis.* The analysis involves the following:

*The term "hazards analysis" has a broad connotation, referring to any analysis which gives a measure of, or an improved understanding of the hazards. An article entitled Hazard Analysis I (ref (h)) appears in *Biometrika*, Vol. 51, June 1964. The AFSC Design Handbook DH 1-6 (ref (i)) on system safety uses such terms as system/subsystem Hazard Analysis, Preliminary Hazard Analysis, and Design Hazard Analysis. The failure modes and effects analysis (FMEA), the fault tree analysis (ref (c)), and the RAP Analysis (ref (o)) are methods of hazards analysis. Consequently it is necessary to define the method since each has its particular purpose.

a. A listing of all phases of the manufacture-to-target sequence.

b. A listing under each phase of those things that do happen (normal events) and those things that can happen (abnormal events).

c. Expression of these events in terms of environments, personnel actions, or other descriptors best suited for protective devices design considerations.

d. Assignment of weighing factors to the abnormal events so that likely events are given precedence over unlikely events for safety design considerations.

6. When this procedure has been completed it becomes the basis for safety design requirements and objectives. The reasoning is the following. The procedure produces a list of events in which the weapon must be safe. Because of the systematic approach, and if done thoroughly, the list is more comprehensive than any which can be drawn from general specifications or design guides. Furthermore it is tailored specifically to the weapon to be developed. The designers are then faced with the problem of developing safety mechanisms which will prevent weapon functioning in the listed events. These are engineering problems. They are basically the same as reliability problems. For example, to obtain reliability an engineer must design his component to function properly despite the effects of a normal environment. To obtain safety the engineer must design his safety component to prevent functioning despite the effects of an abnormal environment. In either case he needs to know something of the nature and magnitude of the environment.

7. The potential hazards analysis does more than just develop safety environments. It also considers the actions of people. It gets into the realm of human engineering. Many accidents are caused by carelessness or bravado. Often, the way a device is designed makes it more or less susceptible to these human actions. The analysis lists the common types of human errors in appropriate situations. The designer can then think about ways to make his mechanism so that these errors are less likely to contribute to accidents. In human engineering for reliability a similar problem exists. Any equipment which is to be operated by people is designed so that the chance that human error will result in system failure is minimized.

8. Since procedures for conducting a potential hazards analysis are to be described in a separate report, only a brief description will be given here for purpose of familiarity. Figure 6.1 is an abbreviated example of a potential hazards analysis worksheet. This worksheet is prepared by taking the phases of the Factory-to-Target Sequence (FTS) and, under each phase, listing the events which can occur. The list is not limited to abnormal events but these will predominate, because the abnormal events are more likely to lead to unsafety. Normal events will be pretty thoroughly analyzed during development as part of the reliability program and will therefore require less attention in the potential hazards analysis. Each event

Phase: Assembly

HAZARDOUS EVENT	LIKELIHOOD	ENVIRONMENT OR CONDITION	DESIGN CONSIDERATIONS AND/OR PROCEDURES	REFERENCES
1. Bent connector pins	L	1.1 Electrical shorts & grounds	1.1.1 Pin assignments 1.1.2 Pin straighteners 1.1.3 Multiple keys on connector shell	1. UR-67-XX
2. Omission of parts	L	2.1 Critical part missing 2.2 Structural weakness	2.1.1 100% inspection 2.2.2 Make part necessary for assembly 2.2.1 Design to shear at a safe point	

21

Phase: Transportation (Truck)

HAZARDOUS EVENT	LIKELIHOOD	ENVIRONMENT OR CONDITION	DESIGN CONSIDERATIONS AND/OR PROCEDURES	REFERENCES
1. Fire		1.1 High temperature (1500-1800°F)	1.1.1 Thermal disconnect	
2. Collision	0.38/100,000 vehicle miles	2.1 Shock (ΔV 90 fps At 10-1000 ms) 2.2 Crushing; To 1/2 original dimensions 2.3 Tumbling: 10 rad/sec. 2.4 Rolling: 20 rad/sec.	2.1.1 Avoid shock sensitive devices 2.1.2 Rugged design 2.2.1 Fail-safe weak link 2.3.1 Avoid inertial device 2.4.1 Avoid inertial device	2. Merrill K.C., Auto-matic Crash & Field Demonstration Conf.

Figure 6.1 Examples of Potential Hazards Analysis Worksheets

is then described in terms of environments, personnel actions, or other appropriate descriptors. Collectively, hazardous environments and dangerous personnel actions can be called hazardous events. By estimate or calculation, magnitudes are determined for the environments. As a result of this process the designer can be supplied with information applicable to safety design which is comparable to that now developed for reliability. He will have the problem of designing safety devices to provide safety, by not functioning or by failing safe in an intended manner, in known environments of known magnitudes. And he will have the problem of designing safety devices which will resist identified dangerous personnel actions. These are his safety design objectives.

9. The purpose of the potential hazards analysis is illustrated by Figure 6.2. In this figure the rectangles on the left represent the listed environments, personnel actions, or other conditions which could cause accidents unless the design includes provisions to protect against these events. The circles on the right represent the design solutions, i.e., the safety devices which give the system its safety in all situations. As depicted, one safety device will frequently protect against many different events. But when an event is encountered for which the first device does not provide protection, a different device must be chosen or a second device added. Addition of the second device usually duplicates protection for a number of events. If the safety devices are checked systematically against the events, as illustrated by Figure 6.2, it is unlikely that an event will be overlooked. When an event pops up for which there is no protection, like the last line of Figure 6.2, the system must either be changed or the event must be prevented by procedures or warnings. The unlikely nature of many of the hazardous events presents one of the most difficult problems. The Air Force goes so far as to say there should be protection in "credible abnormal environments." Unfortunately, since it has not been possible to attach probabilities to the occurrence of these events, the difference between "credible" and "incredible" is very much a matter of personal opinion.

10. SUMMARY

a. Safety objectives have lacked the preciseness and detail of reliability objectives. In many instances, it has appeared that telling the designer that the weapon design must be safe was considered adequate, as if the designer would know what to do to obtain the desired safety in the desired conditions. On the other hand, the same designers were trusted less to have equal success with their intuitive feel for reliability. Instead, they were given precise objectives in terms of environmental levels which their devices were to withstand without undue wear and tear or in which their devices were to perform successfully.

b. Listing safety environmental objectives is more difficult and this is a primary reason they have been neglected. There are two principal difficulties. First, safety objectives must deal with the unusual and abnormal as well as with the commonplace and normal events. It is much more difficult to name these abnormal events and determine

HAZARDOUS EVENT
ENVIRONMENT OR
PERSONNEL ACTION

DESIGN SOLUTION
PROTECTIVE
SAFETY DEVICE

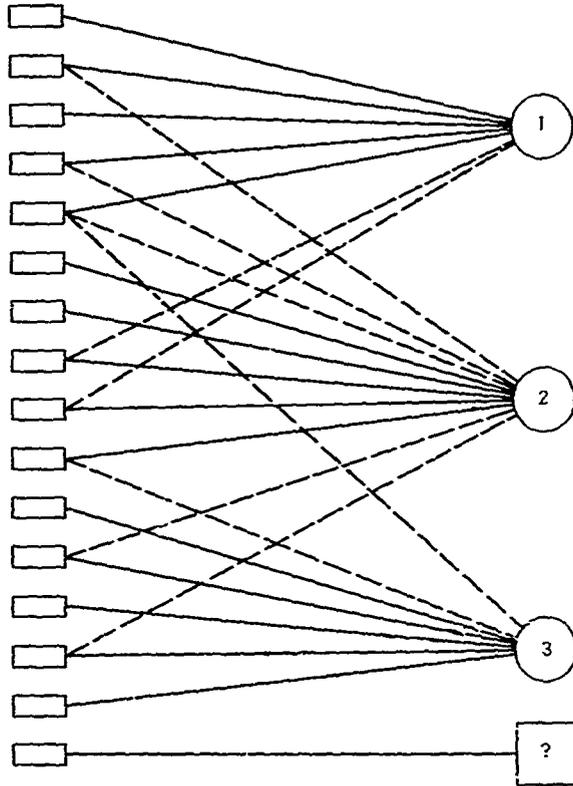


FIG. 6.2 SYMBOLIC PURPOSE OF POTENTIAL HAZARDS ANALYSIS

environmental levels. Second, the abnormal events are likely to occur infrequently or even never in the life of a weapon. Design protection then takes on the aspect of insurance with the ever present question of whether or not the risk is great enough to warrant the cost of insurance.

c. In spite of the difficulties, it must certainly be evident that safety cannot reach the level of refinement of reliability unless a substantial attempt is made to improve the quality and engineering value of safety objectives. The listing of safety environmental objectives is an important step in this direction. The potential hazards analysis is recommended as a systematic procedure for accomplishing this. The potential hazards analysis is a systematic procedure in which normal and abnormal events which will or can happen in the life of the weapon are listed, environment magnitudes are assigned to these events, and a "credible" list of safety environmental magnitudes is developed and becomes a part of the safety design objectives. The reason that the term "credible" becomes important is because designed protection in all abnormal environments is neither possible nor practical. Reasonable and achievable goals must be set for the designer, and this is a matter of judgement based on the state-of-art and the other constraints which influence the course of a weapon development.

Chapter 7

SAFETY SYSTEM DESIGN

1. WHAT IS A SAFETY SYSTEM?

A safety system is the aggregate of safety devices or safety components in the weapon. A more specific definition is the following:

An electrical, mechanical, or electromechanical system consisting of one or more of the following:

- a. Environment sensors
- b. Launch event sensors
- c. Command functioned devices
- d. A logic network, comprising electrical switches and/or mechanical interlocks and timers, utilizing inputs from a, b, or c.

It functions to arm the weapon (by closing switches and/or removing interrupters) at a safe distance from, or a safe time after, the point at which a normal launch is started.

The safety system should more appropriately be called a subsystem. Its purpose is to provide interruption in a normal or abnormal operating sequence so that operation of the weapon will not occur at the wrong time and place. The wrong time and place is any time that operation of the weapon will hurt the user or his allies rather than the enemy. In this sense, a weapon could be said to have ideal safety if the probability of operation at the wrong time and place were zero. Such a weapon could be assembled, handled, transported, stored, and checked out with complete safety. Unfortunately for safety, there is also the demand that the weapon have a destructive capability when used against an enemy. Therefore, ideal safety does not exist. All that any safety system design can hope to do is take advantage of every technique to reduce the probability, which is unsafety, without unduly limiting the destructive capability. This section discusses ideas and concepts which can, in many cases, improve design for safety with little or no reduction in reliability.

2. THE "UNIQUE" POST-LAUNCH ENVIRONMENT

For many years it has been recognized that one of the best ways to obtain good safety is to use a unique post-launch environment to

operate one of the safety devices. This is good common sense. If the post-launch environment is unique, it will not occur before launch. It will not occur in anything that can happen during assembly, handling, transportation, storage, check out, and preparation for launch. A safety device designed to operate on this unique post-launch environment will not experience its operating stimulus until after launch. Such a device provides excellent safety. It is defeated only if it is bypassed or compromised so that it does not perform in its intended manner. Even if the post-launch environment is not unique, but is unusual, and not very likely to occur before launch, this design approach for safety is to be recommended. It gives protection in most of the environments which can occur before launch, and where it is vulnerable, it can usually be backed up by another safety device working on some other principle.

Another way to look at the post-launch environment is that it is a signpost which indicates that the weapon is on the right road and arming should be permitted. If it is not a unique sign but is instead a common one, it is not an adequate identification of the road. Other familiar landmarks are needed to give positive identification. If the safety system is to prevent operation before launch and permit operation after launch, it must be designed to have the capability of identifying launch and separating it from things which can occur before launch. Using the unique or unusual post-launch environment is one of the best ways to obtain this capability.

Examples of the use of unusual post-launch environments* occur in the designs of projectile and rocket fuzes. The projectile fuze uses the setback and spin experienced in the gun barrel to supply the energy for arming. For the projectile, the ride in the gun barrel is a truly unique experience. The setback of 12,000g or more and spin of 200 rps or more are experiences which are practically nonexistent in handling, transportation, gun ramming and the like. When a projectile accident occurs it is probably not because the arming devices have been operated. It is because they have been bypassed by such things as omission of parts, gas leaks around the projectile base seal, voids in the cast explosive, or hitting the projectile too hard with a sledge.

Rocket fuzes commonly use the acceleration experienced during rocket motor burning to operate an arming device. The thrust and burning time of motors vary considerably. But for purpose of illustration assume the motor burns for one second and during that time produces constant acceleration of 40g. At motor burn-out the rocket will be moving at a velocity of almost 1300 feet per second. Are there any accidents during handling and transportation which can produce a velocity change of 1300 feet per second? The crash of a transporting aircraft might come close, but everything else is far below this value. To say the least, the boost from rocket motor burning is an unusual experience for the rocket fuze.

*The meaning of "post-launch environment" is frequently stretched to include launch environments since these are often the last available to supply adequate forces to operate simple and rugged safety devices.

Employing a safety device which operates on a unique or unusual post-launch environment is a big step toward good weapon safety. But sometimes this does not give the safety that was intended. Sometimes unintended operating modes appear and spoil the happy picture of safety. This leads to the next discussion.

3. HOW DOES THE COMPONENT FAIL?

In discussing how the component fails, the rocket fuze example is a good place to start. In a normal rocket firing the fuze experienced a velocity change of about 1300 feet per second. To assure operation, the fuze would be designed to operate on less. Assume the fuze was designed to require 30g for 0.75 second. This would be a velocity change of about 700 feet per second which would still be very unusual in prelaunch accidents. If this fuze always operated on velocity changes above 700 feet per second and never operated on velocity changes below 700 feet per second, the design would be a huge success. But suppose that a critical part in the fuze breaks and allows it to arm if it receives a sharp impact. To continue with figures, assume that a shock of 10,000g for 0.1 millisecond will break this part. In terms of velocity change, this is only about 32 feet per second. That's quite different from the 700 feet per second velocity change for which the fuze was designed.

A safety mechanism used occasionally in ballistic missiles is a device which operates on pressure changes. It arms when the pressure becomes very low as it would in the ballistic flight. Since zero or near zero pressure is very uncommon on the ground, this device has the attribute of using a "unique" post-launch environment for operation. Studies have indicated that such devices would probably operate if in an unpressurized cabin of a high flying aircraft. This is certainly an unwanted normal operation. But there are also likely to be unwanted abnormal operating modes. The mechanical design of such a device requires using moving parts. These parts have mass. If these parts experience high enough acceleration they may operate inertially. Thus it is possible to design a device to operate on pressure differential and have it operate on shock.

In the design of safety components the unwanted operating modes must be given as much or even more attention than the wanted operating mode. To be sure, reliability will suffer if insufficient attention is given to the intended operating mode. But this is not likely to be the case. The intended operation is the first concern of the designer. It becomes well defined early in design. Unwanted operating modes are not well defined, if defined at all. Safety objectives have usually been the quotation of a few general criteria. Sometimes added to these is a flat statement that "the fuze shall fail safe." The more complete objectives list some accident situations in which the fuze shall be safe. This is coming closer to objectives applicable to the particular device, but falls far short of the explicitness of the operating objectives. In this situation the designer is tempted to devote most of his attention to improving the performance of the device in the normal operating environment. Safety may come as a by-product of his efforts. Since the safety provided by a safety

device is its most important attribute, safety objectives must have top priority. To achieve this, safety objectives must be more explicit. This is the most important function of the potential hazards analysis (Chapter 6). With the type of safety objectives developed by the potential hazards analysis the designer can ask the question, "how does this component fail unsafe or operate when not wanted?", and he can obtain some of these answers while the component is still an idea on paper.

Operating on a "unique" post-launch (or launch) environment is a commendable attribute of a safety device provided the practical problems associated with working hardware do not introduce so many unwanted operating modes, or ways in which the hardware may fail unsafe, that the conceptual advantage of the uniqueness of the environment is lost in the frailties of the hardware. The question, "how usable is this environment?", must be asked. If using it is extremely tricky and pushes the state-of-art, it may have to take a back seat to an environment which can be used with confidence and whose shortcomings can be compensated for by known methods.

4. SYSTEM SAFETY IS THE GOAL

A safe weapon is one in which the safety devices effectively prevent weapon operation in all the unusual events for which they were designed. Warnings and procedures will also play a part. However, the discussion in this section will be limited to the roles of the safety devices. These are the primary interest of the weapon designers.

The discussion of the unique post-launch environment dealt with the attributes and shortcomings of individual safety devices. The attributes are important because, to keep the system simple, it is necessary that a single device provide as broad a safety coverage as possible. The shortcomings are important because these identify safety areas which must be covered by a second or third safety component and therefore establish needed characteristics of these devices. This is complementary safety. Where one device in the system has a weakness, another is chosen which is strong. One device complements another to give broad safety coverage.

Redundancy for reliability and for safety was discussed in Chapter 4. Use of complementary safety devices is safety redundancy. It is dissimilar redundancy which is an indicated solution when a component is likely to be disabled by an environment. It is the common type of redundancy for safety. It is uncommon for reliability. The reason for this is logical and is the following. A component which would be caused to fail by one of the normal environments of the FTS would ordinarily never get into the system. Therefore, redundancy for reliability is seldom a matter of providing another operating path around a component that can't endure a normal environment. It is usually employed when a component exhibits too many random unpredictable failures. These can result from flaws in materials, a lapse in quality of workmanship, and the like. They are the occasional "lemons" which crop up and are not recognized as such until failure

occurs. To improve reliability identical redundancy is used on the basis that putting two "lemons" in the same system is unlikely. Dissimilar redundancy may also be an acceptable solution but is usually rejected because of cost, weight, or space penalties.

Safety redundancy is necessary because finding a component which can survive all accident environments without operating or failing in an unsafe manner is very difficult. A safety device is put into the system even though it is known to be vulnerable in one or more accident environments. Adding an identical device would not correct this situation. It would be vulnerable in the same accident environments. Dissimilar redundancy is called for. The second device should be different, particularly to the extent that it is not vulnerable in these same accident environments. The following table expresses what has been said above.

<u>Cause of Failure</u>	<u>Indicated Solution</u>	<u>Where Used</u>
Reaction to environment	Dissimilar redundancy	Safety design
Random defects not detectable in screening	Identical or dissimilar*	Reliability design

*Seldom used because of cost, weight, or space penalties.

There is an analogy which may be helpful in explaining the role of the safety system. The goal is to assemble a system which is least likely to be defeated by any environment or personnel action, normal or abnormal, which can occur in assembly, handling, transportation, storage, check-out, preparation for launch, and launch until after safe separation. That covers a lot of ground. An awful lot of things can happen. It would not be too farfetched to say that the number of things which could happen could be likened to the number of questions which could be asked of a quiz panel with no limitation on subject matter. The panel as a whole (the safety system) would have to be prepared to answer any question on any subject. Easy questions (normal or near normal environments) could probably be answered by any member of the panel regardless of subject. Difficult questions (severe accident environments) would be addressed to the expert in that field. The difficult question in the unusual field not covered by the panel membership (no designed protection because the accident is too unlikely) would go unanswered. Choosing the panel is the equivalent of designing the safety system. Would the panel members all be experts in just sports, or just history, or just nuclear physics? Of course not! Such a panel would be too likely to be stumped by a question in a field outside the expertise of the panel. Should a weapon safety system be designed to provide safety only in the shock environment, or the fire environment, or the human error environment? No! All of these and many more must be adequately covered by the safety system. Like the panel chosen to give broad coverage of subject matter, the safety system components must be

chosen to give broad coverage of all those things which can happen to produce accidents in assembly, handling, transportation, storage, check-out, and preparation for launch. Where the analogy breaks down is in the importance of the selections made. It would be foolish to say that our most knowledgeable people should spend all their time on quiz panels. It is conceivable that there are more important things they should be doing. In fact, stumping the panel is part of the spice and interest of the show. Accidents are spicy too. Many a best seller has been based on the heroism, courage, and endurance of men and women caught in the tragedy of a disaster. But these are painful lessons rather than light entertainment. The analogy is useful only to the extent that it illustrated the common sense approach which must be taken when system safety in all conceivable circumstances is the goal.

5. GROSS DEVICES AND WEAK LINKS

"Gross device" is a term sometimes applied to safety devices. Even though it seems quite descriptive, it probably has a slightly different connotation to each person who uses it. When a safety component is described as a "gross device" it is usually thought of as having been designed to be tough and rugged and capable of withstanding accident environments without breaking, or operating by responding in an abnormal manner. An example would be an accelerometer with a strong and heavy frame designed so that after a forty-foot drop it would be essentially in the same condition as before the drop. "Weak link," on the other hand, implies incorporating an intentional weak point which will react in a predictable manner when stressed beyond a certain point. Examples are fuses* in electric circuits and blow-out plugs in pressure cookers. In most cases there are probably valid reasons for choosing one of these approaches rather than the other. In ordnance there seems to be a prevalence of gross devices. However, there may be many instances where the weak link would give better safety than the gross device.

To use the weak link approach, a designer must know the nature of the environment which threatens to cause an accident, and the level of the environment where he wants the weak link to be stressed to failure. In the electric circuit the fuse is designed to melt and interrupt current before the circuit wires become hot enough to present a threat of fire. This level is predictable. Fuses or circuit breakers are rated on the safe current of the circuit. The blow-out plug of a pressure cooker is designed to blow out and relieve pressure before the failure point of the entire cooker is reached. The blow-out plug itself is a hazard, but is located where its direction of travel is most likely to be harmless. It presents a much smaller hazard to the housewife than pressure bursting of an entire pressure cooker. Just as in the case of the fuse, the safety failure level for the plug can be determined. It is quite likely that one reason the designers of safety

*In this report "fuse" is spelled with an "s" to denote (a) a length of combustible material and, (b) the protective melting element in an electric circuit. "Fuze" is spelled with a "z" to denote the device designed to initiate ammunition.

devices for weapons have not often used the weak link approach in their designs is that they have seldom had the kind of information which would disclose the nature of the environment and permit calculation of a reasonable fail-safe level. This problem of listing safety environments was discussed in Chapter 6. There it was argued that the potential hazards analysis would produce the kind of information which the designer could use as engineering goals. So it is possible that increased use of the potential hazards analysis may encourage more use of the weak link approach to safety device design.

Lack of engineering data cannot be the only reason for avoiding weak link designs. There have been many instances where the designer was primarily concerned with designing to pass a series of safety tests. In these cases he could ask for no better definition of the environment and its level. Yet in most cases he was designing to pass the tests with a gross device approach. This suggests that precedence plays a strong part, or that there is a stigma attached to designing for failure even though the failure (the overstressing of the weak link) is for the express purpose of providing weapon safety. If these are factors discouraging the weak link approach, they are not supported by the logical purpose of a weapon safety system. The purpose is to prevent operation of the weapon at any time or place before operation is intended. If a weak link can contribute to this purpose, without unduly reducing the probability the weapon will work when intended, it is a completely satisfactory solution.

A little thought will lead to the conclusion that the gross device approach is not really independent of the weak link approach. The gross device hasn't yet been built which can withstand the extreme stresses of the most severe accidents. However, it is generally a good bit tougher than many other components of the system. Consequently the gross device is judged adequate because, by the time it fails, other devices needed for system operation have failed. The gross device holds the line on safety until a weak link has been overstressed and precludes system operation. In these cases the weak link is still vital to system safety. The weak link may not be a component with listed safety requirements. But in these extreme conditions it is used in this way. There is nothing wrong with this. In fact it is a commendable way to get safety. However, it should be safety by intent rather than happenstance. The weak link should have a predictable failure level placed on it as a requirement for safety.

Smaller and lighter components are very important to many weapons where every extra ounce cuts down on range and capability. Gross safety devices are very unpopular in such systems because they represent bulk and weight. It appears that the only promising solution for this problem is greater emphasis on the weak link approach for safety component designs. However, simple reference to fuses and blow-out plugs is not enough to explain the logic of the weak link approach. To do this, a switching analogy will be used. Assume for a moment that a circuit contains two switches. The circuit is safe if no current flows. It is unsafe if current flows. Originally switch 1 is open and switch 2 is closed. How is switch 1

closed safely? The answer is obvious. Switch 2 must be opened before switch 1 is closed. This is illustrated in Figure 7.1.

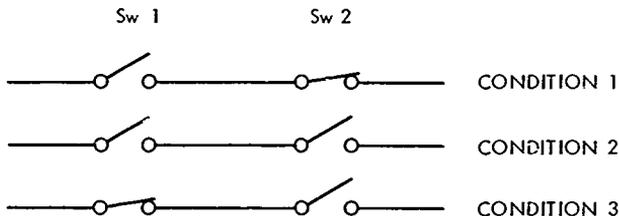


FIG. 7.1 WEAK LINK, SWITCHING ANALOGY

Now replace switches 1 and 2 by A and B which are devices of the safety system. When A is providing safety it is in condition " \bar{a} " (not a). When it is not providing safety it is in condition "a". The same is true for device B; i.e., " \bar{b} " is safe and "b" is unsafe. The devices A and B are designed to provide safety in environment E. The initial condition of the system is " $\bar{a} \bar{b}$ " and exists in normal levels of E. When E reaches an abnormal level the condition becomes " $\bar{a} b$." If E continues to an even higher abnormal level the condition becomes "a \bar{b} ." This is illustrated in Figure 7.2.

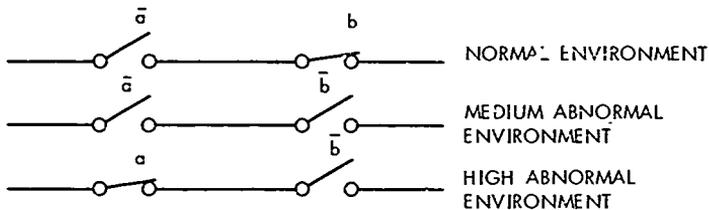


FIG. 7.2 WEAK LINK FAIL SAFE LOGIC

Safety in environment E is assured if the system responds in the order " \bar{a} , b," " $\bar{a} \bar{b}$," "a \bar{b} ." Safety is not assured if the system responds in the order " $\bar{a} b$," "a b," "a \bar{b} ," since the condition "a b" is unsafe. Two examples will be given to illustrate this logic.

a. **THERMAL DISCONNECT.** In this example it will be assumed that a normal type of safety device (such as an accelerometer, a zero-g device, or a decelerometer) is designed to provide protection up to a

temperature of about 1200°F. However, above this temperature some of the materials will carbonize or burn and it is questionable whether or not it will continue to interrupt the critical circuit. How can protection in this thermal environment be assured? One answer is a thermal disconnect located on or near the safety device. Assume this thermal disconnect opens the critical circuit at 800°F. Thermal protection is then obtained as shown in the following table.

<u>Temperature</u>	<u>Protective Devices</u>	<u>Logic Condition</u>
Below 800°F	Safety Device	$\bar{a} b$
800°F to 1200°F	Safety Device and Thermal Disconnect	$\bar{a} \bar{b}$
Above 1200°F	Thermal Disconnect	$a \bar{b}$

Location of the thermal disconnect is important. The progression from " $\bar{a} b$ " through " $\bar{a} \bar{b}$ " to " $a \bar{b}$ " is assured if the two are located close together so that they are always at about the same temperature. But if they are located far apart in the system, they might be at quite different temperatures, and it would be possible to go through the condition " $a b$ " which is not safe. The thermal disconnect does not need to be a fuse or bimetallic strip or any of the other devices suggested by the term. It can be any device with a predictable thermal failure where the failure is such to prevent system operation. It is important, however, that the failure not be a reversible one when the temperature is later reduced (a characteristic recently discovered in a type of transistor being used as a thermal weak link). This would permit the protective devices to end up in the condition " $a b$."

b. CRUSHING PROTECTION. Crushing of components is common in certain kinds of accidents. Designing components so they will be safe if crushed is very difficult because crushing can occur in so many different ways. It can occur slowly or rapidly and the crushing forces can come from many different directions. If a safety component becomes unsafe if crushed, some other safety must be included in the system. This additional safety might be another device so located that it will not be crushed if the first device is crushed. Or it might be a feature added to the first device which disables it in a safe way before crushing can progress to the extent of defeating its designed safety. If the component provides safety by an open electrical switch, the most common thought is a circuit guillotine which must sever the critical circuit before the open switch is endangered. If the component is mechanical, it is conceivable that a rigid interference can be driven into a critical part of the mechanism to cause a fail-safe condition. The weak link approach for crushing protection is a challenge to ingenious design. But it is a logical approach because crushing must progress through stages to reach the unsafe degree. If features can be added to force a safe condition before crushing has progressed to this unsafe degree the order " $\bar{a} b$ " to " $\bar{a} \bar{b}$ " to " $a \bar{b}$ " can be fixed.

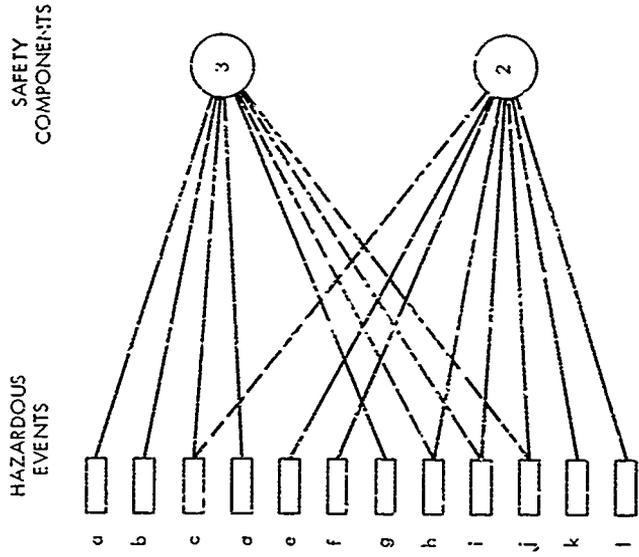
The real benefit of the weak link approach is that it can be set to operate at any level above normal environmental levels. This assumes that when a normal environmental level is exceeded the weapon is no longer expected to be functionable but is expected to be safe. The weak link operating level must be high enough so that it will not occasionally dip into the normal level and hurt reliability. But it can be well below the extreme abnormal levels, and this may permit use of smaller and lighter components.

6. WHEN SAFETY COMPONENTS ARE EQUIVALENT

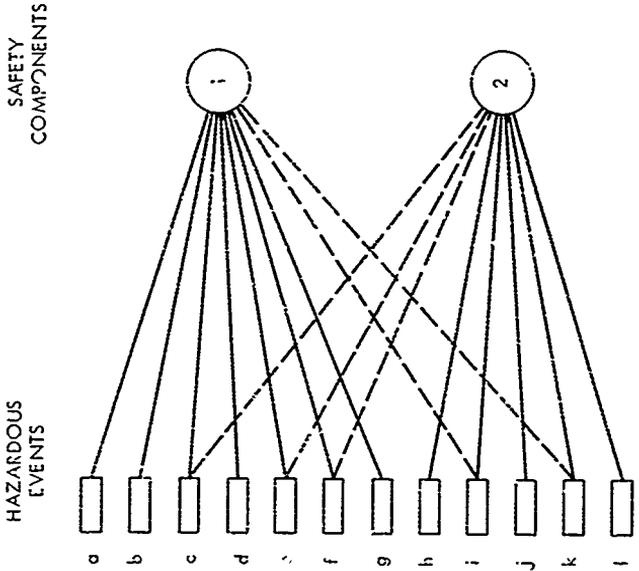
When the possibility of substituting one safety component for another is considered, the question of equivalence must be faced. Each safety component has two primary functions. One is to contribute its share to system safety. The other is to operate on an assigned signal as part of weapon functioning. Comparison must be made on both counts.

Invariably the first questions asked are the reliability questions. Will the substitute component work satisfactorily on the signals which were available to operate the first component? Will the component perform the same operating function for the system? For example, an accelerometer is being considered as a possible substitute for the accelerometer now in a safety system. Naturally there would be differences or the substitution would never be considered in the first place. The candidate accelerometer must have some advantages. It might be lighter, smaller, cost less, or have other advantages. So it is not a matter of physical interchangeability but instead, functional interchangeability. Will one operate as well as the other on the acceleration during motor burning? Can it close the necessary circuits? If it can, there is temptation to say it can do everything the original accelerometer can do. However, this ignores safety aspects entirely.

To be exactly equivalent two safety components would not only function on identical signals but would also provide identical safety. Since it is very unlikely that two different components would be identical in all these aspects, further discussion of exact equivalence is rather pointless. But acceptable equivalence is a different matter. In Chapter 6 the use of the potential hazards analysis to obtain safety design objectives was discussed. Figure 6.2 illustrated the manner in which protection in various hazardous events was assigned to specific safety components. It also showed that in some cases two or three safety components of the system would provide protection in particular hazardous events. This occurred because after the selection of the first device, a hazardous event would be encountered which required a second device, and this second device would give duplicate protection in some events covered by the device. A third device would give protection in some events covered by both the first and second. The result is double and triple protection in some events. This is illustrated again in Figure 7.3 which, for simplicity, shows a two-component system. Figure 7.3a is the original safety design solution employing components 1 and 2. This system gives double protection in hazardous events c, e, f, i, and k. It is



b. ALTERNATE SOLUTION



a. ORIGINAL SOLUTION

FIG. 7.3 ALTERNATE SAFETY DESIGN SOLUTIONS - ACCEPTABLE EQUIVALENCE

then decided to substitute component 3 for component 1. This results in the alternate solution shown in Figure 7.3b. This second system gives double protection in hazardous events c, h, i, and j. The difference is that the alternate system does not give double protection in events e, f, and k which the original system did. However, the alternate system gives double protection in events h and j which the original didn't. Is component 3 an acceptable equivalent for component 1?

Much judgment is needed in deciding if one safety component can be substituted for another. If in Figure 7.3 the substitution of component 3 for component 1 had resulted in no protection for one or more of the hazardous events, component 3 would not be an acceptable equivalent of component 1. But when the substitution simply changes the amount of protection for certain events, which was the case in the example given, it is a matter of judgment. However, there are factors which assist in the judgments. Hazardous events are likely to occur infrequently. Some occur more frequently than others. There is certainly some logic in doubling or tripling protection for events which occur frequently. If in Figure 7.3a events e and f are common and h and j are very uncommon, there would be reason to feel that the system employing components 1 and 2 was superior to the system employing 3 and 2. The first system gives double protection for the common events and single protection for the uncommon events; the second system gives single protection for the common events and double protection for the uncommon events. But if e and h are common events and f and j are uncommon, the decision is more difficult.

Two different components may give protection in the same hazardous events, but to different degrees. For example, component 1 might give protection in shocks to a level represented by a half-sine pulse of 1000g amplitude and 2 millisecond base. Component 3 might give protection to a level represented by a half-sine pulse of 2000g amplitude and 10 millisecond base. In such shocks the quality of protection afforded by component 3 would be better. This would not necessarily show up in a diagram like Figure 7.3 but would be an important factor in comparing the safety equivalence of the two devices.

Judging the equivalence of two different safety components as alternates in a safety system is not a simple matter. To judge that they are equivalent only on the basis that they will operate on the same input signals is a gross misunderstanding of their primary purpose. A safety component is put into the system to provide safety. An alternate component is equivalent in this respect only if it provides the same safety. Two different components, as alternates, are very unlikely to supply exactly the same safety to a system. Each will have its own advantages and disadvantages. The effects of these on the system safety must be the deciding factor.

7. HOW TO AVOID SAFETY BYPASSES

Safety bypasses are the unintended ways of getting around the safety which a safety component is trying to provide. Every system

has them; some more than others. Some are unavoidable. A thick-skinned weapon with an HE warhead is going to explode if it sits long enough in a hot fire. No amount of fuze safety will prevent that, for the fuze is completely bypassed. But many bypasses are avoidable. The omission of a critical part which allows a fuze to arm on a normal handling environment could be avoided if inspection or presence of the part were infallible or if the design were such that it couldn't be assembled if the part were omitted. The shorting out of a safety switch because of a bent pin in a connector could be avoided if the pin were so located that no amount of bending could cause it to contact the return circuit. The number of avoidable bypasses is almost unlimited because each device has its own characteristic bypasses. Consequently only a few general guidelines with examples will be presented in this section.

e. PUT SAFETY BARRIER NEAR DANGER AREA. This is the basis on which the interrupted explosive train has been such a valuable safety device. It is a safety barrier located as close to the warhead as possible. Regardless of what may happen ahead of it, as long as the barrier is there, the progression toward a warhead detonation is stopped. By its very nature the explosive train interrupter must be near the warhead. So it is not a good example of a device which, by choice, could be placed close to the warhead or far from it. A switch in an electric detonator circuit is a better example because it could be located anywhere in the firing circuit. If the switch is located adjacent to the detonator, it will not be bypassed by anything except its own deficiencies. But if it is so located that there is much wiring, many connectors, and proximity to live circuits between the switch and the detonator, it can be bypassed by short circuits, bent connector pins, and many other faults as well as its own deficiencies. A good general rule is, don't leave room for bypasses.

b. USE SIMPLE AND DIRECT SAFETY LOCKS. The indirect, roundabout safety lock is reminiscent of Rube Goldberg inventions. There are many things that can go wrong. To illustrate, a safety pin is usually accepted as a direct and positive lock assuring safety as long as it is inserted. It may directly lock the explosive train interrupter, or firing pin, or arming shaft. When it is inserted there is strong assurance that the weapon is safe. But a safety pin can also be very indirect in the safety it provides. There is one fuze in which the safety pin, when inserted, closes an electrical switch. If the fuze battery is energized when the switch is closed, the fuse burns out and disconnects power from the fuze electronics. The fuze is then inoperable. The problem with this safety pin is that its presence does not give the usual high assurance of safety. If the switch fails to make or there is an open anywhere in the fuse circuit, the intended safety is bypassed. This safety pin is not direct enough in its lock on safety.

c. MAKE CRITICAL PARTS SO THEY ARE NECESSARY FOR ASSEMBLY. The omission of a critical part which results in unsafety is a bypass because it results in an unintended way of getting around the safety which the device is trying to provide. The sure formula for avoiding this kind of bypass is to design the critical part so that it is

essential to assembly; an attempt to assemble without it would fail. It is frequently not practical to do this but the scheme is always worth considering during early design. When it is not possible to make the part essential for assembly, it is necessary to fall back on inspection to assure its presence. This too requires special design considerations.

d. MAKE EXTERNAL PARTS DIDDLE-PROOF. Projecting parts, which are necessary in most weapons, are temptations to curious people and play things to thoughtless people. Such things as airvanes, arming stems, and detents are accessible to anyone near the weapon. Although these are intended to be operated by a launch environment, in many cases they can be operated inadvertently (or intentionally) by handling personnel. Avoiding careless or thoughtless operation is a matter of designing to obtain discrimination between the environment operation and the most likely mode of operation by personnel. For example, clutches have been put in airvane shafts so that high rotational velocity is necessary for operation. The high rotational velocity is normal in operation but would be abnormal in thoughtless manual turning of the vane.

e. USE SEPARATE INPUT AND OUTPUT CONNECTORS. Where safety is supplied by an open electrical switch, separation of the input and output wires to this switch is essential. When the switch is part of an operating component it is common to bring the leads to the switch through a connector or connectors. The component design is simpler if a single connector is used. But this puts both sides of the switch on pins of a single connector. The occurrence of bent pins in connectors has been a common source of trouble. Of course, the type of connector makes a difference. But where safety is concerned, the use of separate input and output connectors is a good rule of thumb.

f. ISOLATE MONITOR CIRCUITS. Monitor circuits are considered essential in some weapons. They are needed to give an indication of the condition of the weapon. Unfortunately they are a source of power which under certain circumstances can bypass safety components. Monitor wires may go from one component to another and be potential shorts across safety switches. Since these monitors are needed, the solution is to design these circuits in such a way that their chance of becoming safety bypasses is held to a minimum. This is done by careful physical and dielectric isolation. Current and voltage limiting of these circuits to levels below those needed for critical component operation is also good practice. The same precautions should be followed in the design of fuzing option selection circuits or any other circuits which introduce potential safety switch bypasses into the system.

8. ORDER OF OPERATING

Most weapons function properly as the result of a series of events in a set order. The series may be short or long depending on the complexity of the weapon. The order of the events may be demanded for functioning or may be simply a matter of procedure. The system which follows a set order as a matter of procedure is illustrated by the simple logic diagram of Figure 7.4.

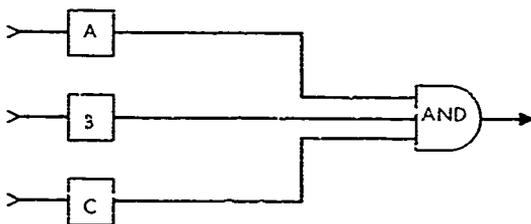


FIG. 7.4 EVENT ORDER BY PROCEDURE

The normal order of events could be ABC but this would be because of an established procedure rather than by design. The logic diagram shows that any order such as BCA or BAC or CBA satisfies the logic. A set order by design is illustrated by Figure 7.5.

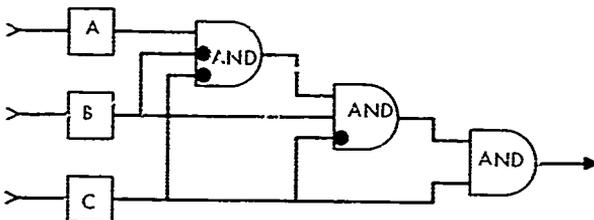


FIG. 7.5 EVENT ORDER BY DESIGN

In this figure the first AND gate is satisfied by the events A and B (read not B) and C. This means that event A must precede events B and C. The second AND gate is satisfied by events A and B and C. This means that event B must precede event C. The last AND gate is satisfied by events A and B and C. However, the order A, B, C has been required by the logic.

The existence of a set order of functioning events can be used to enhance safety in the following way. If the safety devices are so designed that they will operate to remove their safety only if normal functioning events occur in the correct order, then out-of-sequence events will be rejected. This means that the conditions capable of

causing an accident by normal operation of the safety devices would have to duplicate the launch conditions of the weapon.

If there is no fixed order of events, set by design, the safety devices can function on inputs received in any order. In Figure 7.4, the order CBA is just as effective in satisfying the logic as the order ABC. If the order CBA is abnormal and functioning under these conditions is to be avoided, this system does not provide adequate safety.

9. THE TIME GATE

The series of events leading to proper functioning of a weapon may not only occur in a set order but some events may occur within certain time limits. It is abnormal for these events to occur outside these time limits, and this may be a clue that weapon operation is undesirable or dangerous. If the safety devices are designed so that they will function only if these key events occur within the proper time gate, the safety of the system is tied more closely to the events of a normal launch. Out-of-sequence or out-of-time events are rejected. An example may help to illustrate this. Suppose that a ground launched missile fuze is designed so that when a launcher detent is withdrawn motor pressure must appear within 0.01 second or the fuze will not arm. This means that in normal use there has to be a fixed relation between launcher detent removal and motor pressure. It is quite possible that this same fixed time relation may exist in some accident situations. In such situations safety has not been improved by the time gate. It is also possible that there may be a number of situations where the launcher detent will be withdrawn and motor pressure will appear but not within the normal time span. In these cases the time gate has materially improved safety.

The value of a time gate depends on how well it distinguishes normal conditions from abnormal conditions. If the conditions of many accidents satisfy the time gate just as well as the normal conditions of launch, the time gate is supplying very little safety. Safety may be greatly improved if a time gate can be chosen which is rarely satisfied by the conditions of accident situations.

10. COMPONENT ORIENTATION

In designing for safety much attention must be given to abnormal and unintended operating modes of components. Frequently the intended operating mode becomes secondary in a study of whether or not the system is safe. Assume that a safety system consists of three safety components. One component is operated by acceleration, one by reduced pressure, and one by the centrifugal force of spin. Conceptually this is a very safe system. What kind of accident could combine acceleration, low pressure, and spin? On the basis of designed operation it appears that nothing but launch and flight of the weapon could cause this safety system to operate. It is therefore only necessary to make sure that each component is in the system, is working properly, and is not bypassed by some sneak path.

But the above conclusion about the system is based on how it is supposed to work. Note that each one of these safety devices has moving parts. The accelerometer and the spin operated device are inertial devices. They contain weights which move when experiencing inertial forces. The component operated by low pressure has moving parts which react to changes of pressure. These parts have mass and will therefore also react to inertial forces. It is therefore quite conceivable that a very high accidental shock (one many times higher than normal operating forces) having a large vector in the line of operation of each device could defeat the safety of this system.

This kind of safety defeat can be prevented. Notice what happens if two diametric spin operated devices are used instead of one. Figure 7.6 illustrates this. The normal operating forces, shown as vectors A and B are completely opposite. This is perfectly satisfactory for normal operation. But now it is not possible for a single accident shock to produce vectors in the direction of operation of both. Any shock producing an operating vector in one of the spin devices produces a vector tending to safe the other.

The pressure device can also be made orientation safe from shocks. Figure 7.6 shows the internal portion of a pressure device. It shows the orifice which communicates to outside pressure, and a manifold which delivers this pressure to two bellows operating in opposite directions. All of this would be sealed in a constant pressure container with only the orifice communicating to outside pressure. At reduced pressure the bellows would move in the directions C and D. Again there is no single accident shock which will tend to move both bellows in the direction of operation. The tendency for one to move in the direction of operation is accompanied by the tendency for the other to move away from operation.

Since pressure can be used to produce motion in any desired direction, there is never a need to place the moving parts of a pressure device and an inertial device on the same axis where they may both be susceptible to a single accident shock. In spite of this it is sometimes done because it simplifies design problems and interfaces. When it comes to component orientation, there will always be trade-offs between the best safety orientations and the practical limitations of space and mechanical or electrical interfaces. The best solutions for a particular weapon will be a compromise, but the compromise should take advantage of the maximum practical safety benefits of component orientation. If orientation is considered from the outset, it will generally be possible to use it to advantage.

11. MULTIPLE SIMPLE DEVICES

The launch-to-target sequence of some weapons provides many environments and forces which can be used to control or operate safety devices. The intercontinental ballistic missile has been described as such a weapon. The discussion of this section is pertinent to such weapons. It is not pertinent to weapons where environments or forces for arming are extremely limited.

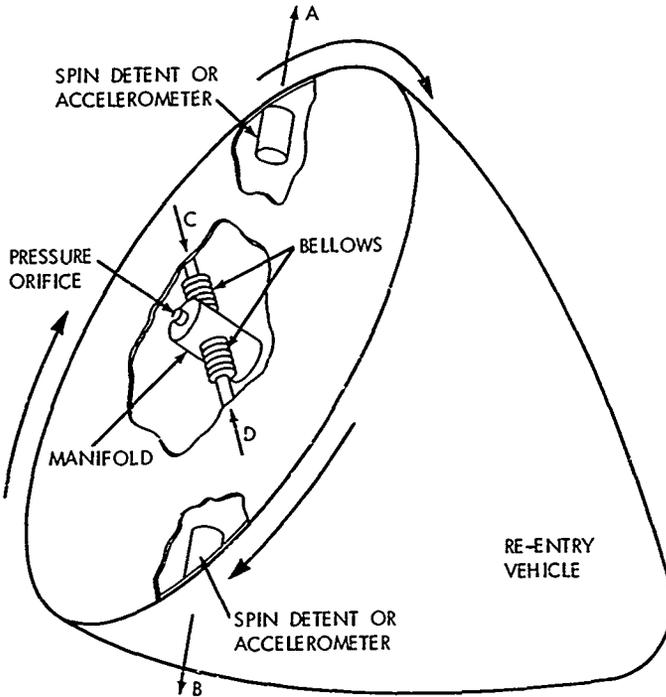


FIG. 7.6 SAFETY COMPONENT ORIENTATIONS

The following environments are a part of the launch-to-target sequence of an intercontinental ballistic missile reentry vehicle:

- a. Acceleration of powered flight
- b. Weightlessness
- c. Vacuum above the atmosphere
- d. Aerodynamic heating of reentry
- e. Reentry drag or deceleration

Compared to some other weapons this represents an abundance of usable post-launch environments. Each of these has very predictable characteristics. Each of them can be used to operate a safety component. Usually two are used and the others are ignored.

The purpose of using the post-launch environments is to give the system the ability to distinguish between accident environments (where operation of the system is not wanted) and launch-to-target environments (where operation of the system is wanted). If this distinction can be made with great accuracy, the weapon will always reject accident environments and will always accept launch-to-target environments. The arming and fuzing device for the intercontinental ballistic missile reentry vehicle mentioned above would make this distinction most accurately if it functioned to arm the warhead only if (1) powered flight acceleration had the proper magnitude and duration, if (2) weightlessness lasted for the proper time, if (3) vacuum trajectory lasted for the proper time and was in proper time relationship with weightlessness, if (4) skin temperature reached the proper level at the proper time, and if (5) reentry deceleration magnitude and duration were proper and in the correct time relationship to the other environments. The safety system to do this would be very complex. It would undoubtedly be unacceptable from a reliability standpoint. Each of the safety components, in order to identify proper characteristics of its operating environment, would have to be quite sophisticated. Getting the needed high reliability from a series of five components of this level of sophistication is beyond present state-of-art.

The solution has been to use two post-launch environments, detect them with sophisticated safety components, and ignore the other environments. Thus the identification of a proper flight is made with less than half of the information available. There is no evidence yet to show that this has not been satisfactory. When enough is known about the nature of the two environments, which is the purpose of using sophisticated components rather than simple components, most of the doubt that they are the result of an acceptable flight has been removed.

A solution which has not been used is to sample each of the five environments with simple components. Simple components would have to be used so that five such components in series would have high enough

reliability. In fact, the five simple components should be no less reliable than the two sophisticated components. Each simple component would obtain a much less complete picture of its operating environment. It might do no more than just determine that the environment existed. But the determination that all five environments existed, even though very little was known about the particular qualities of each one, is strong indication that a normal flight to target has taken place because the mere existence of all five environments in an accident is unlikely. Add to this a simple timer to program acceptance of these five in the order and on the time scale of a normal flight, and a highly intelligent and discriminatory safety system results from the use of multiple simple components.

The relative merits of a pair of sophisticated components versus multiple simple components cannot be argued on the basis of experience. The latter system, as described here, has never been used. It appears to be good on the basis of common sense. Much of its attraction as a concept comes from ordering of component operation as discussed in paragraph 8, time gating as discussed in paragraph 9, and the use of as many post-launch environments as possible. Both ordering of operation and time gating can be applied to systems employing the sophisticated components. Also a sophisticated component can be combined with simple components in a system. It is apparent that quite a few combinations are possible. What is an optimum choice from the outset depends on the nature of accident environments and conditions in which the safety system must provide protection. It appears that as experience with the potential hazards analysis increases, the basis for such decisions will improve.

12. MINIMIZE EFFECTS OF CARELESSNESS

In an East Coast shipyard an electrician was standing near a ship's power distribution board. Clipped to his belt was a ring holding a large assortment of keys and a pocket knife. The terminals on the distribution panel were exposed. As the electrician turned away from the board there was a bright flash and a sharp report. The terminals were mostly melted away. Several keys on the ring were welded together.

Carelessness causes many accidents. In spite of training and warnings and admonitions a certain amount of it persists in every individual. Carelessness is human and can't be completely eliminated. But the effects of carelessness can and should be controlled by design. Designing so that carelessness is less likely to cause accidents is human engineering for safety. The accident described above would have been prevented if the terminals on the distribution board had been covered, or if the bundle of keys and knife had been in an insulated pouch.

Since ordnance items are recognized as dangerous, they are given better protection from careless acts than the electrical distribution panel. But examination of various ordnance items shows there is room for improvement. Some ordnance devices are initiated by the pull of a lanyard. The lanyard comes as part of the ordnance, already attached,

and ready to actuate the ordnance if a safety pin is out and the lanyard receives sufficient pull. Snagging or tripping over the lanyard under these conditions could actuate the device. There is reason to believe that one very costly accident, which took 44 lives and crippled an aircraft carrier, may have been caused by a careless act of this type.

The lanyard example given was, of course, an extreme case. Most ordnance is designed to operate on events more intimately related to a real and desired launch sequence. But the lesson to be learned can be applied to any safety device. Devices which can be operated by handling personnel should, to the extent possible, be designed so that operation is accomplished only if the operator follows a procedure requiring thought. In other words, there should be just enough of a trick to operation of the device so that it requires an intentional premeditated act as distinguished from an unintentional thoughtless act. Suppose, for example, that the lanyard came as a separate item not attached to the firing mechanism, but attachable at the appropriate time. Suppose also that attachment was accomplished by snapping a plug into a recess (to avoid a projection which could be snagged) in the firing mechanism and that this were a reversible process. Now the lanyard could be completely separate from the firing mechanism until attachment was made just before launch. If the device was not launched, the lanyard could be removed. Only when the lanyard was attached would it be a hazard with regard to snagging by one means or another. Attachment of the lanyard would require an intentional, premeditated act associated with final preparations for launch. Detachment of the lanyard would be a safety precaution prior to returning the item to a storage area. Prior to attachment of the lanyard and after detachment the probability of actuation by a careless act would be much reduced.

13. SUMMARY

a. A safety system is defined as the aggregate of safety devices or safety components in the weapon. There are a number of rules of thumb in the design of a good safety system. A number of the general rules are enumerated.

b. Operating one of the safety devices by a "unique" post-launch environment has proved to be an excellent way to obtain good safety. However, in the choice of the safety device much attention must be given to unwanted operating modes because these can rapidly dilute the effectiveness of the device operating on the "unique" post-launch environment.

c. The various devices in a good safety system complement each other. Where one device has a weakness, another is strong. This is the dissimilar redundancy which is most common in safety systems.

d. Safety devices must either resist the extreme stresses of accident environments or fail predictably in a preconceived safe manner. This latter device is the "weak link" and much can be said

in its favor. The "weak link" must be strong enough to withstand the extreme of normal environments but must have a predictable failure level in the greater extremes of accidents. The "weak link" is teamed with another device designed to withstand the "weak link" failure level. In this way there is no gap in the protection afforded by the team in the environment of concern.

e. Two safety components are equivalent when they provide the same protection and are functioned by the same energy. Too often components are erroneously called equivalent only because they will operate on the same stimulus. This is ignoring the primary function of the component which is to provide its share of the system safety.

f. Safety bypasses are the unintended way of getting around the safety which a safety component is trying to provide. Some rules of thumb for avoiding these bypasses are: Put the safety barrier near the danger area. This leaves less room for a bypass. Use simple and direct safety locks. Make critical parts so they are necessary for assembly. Make external parts diddle-proof. Use separate input and output connectors. Isolate monitor circuits.

g. To the extent possible, a safety system should require that operating signals be received in normal order. This system rejects out-of-order sequences. An extension of this is the use of time gates. When these are added, the system not only requires that operating signals be received in proper order but also that these signals be received in proper time references.

h. Three additional ideas for improving system safety are to position components judiciously, use multiple simple devices, and design manual operations to require thought. Some components can operate in any position. These should be positioned to be least susceptible to unwanted operation by some environment other than the normal operating environment. Some weapons give a large choice of environments for operation of safety devices. In some cases using all of these environments to operate simple devices is a better design solution than using just one or two to operate sophisticated devices. To avoid careless operation, normal devices should be designed so that operation is accomplished only if the operator follows a procedure requiring thought.

Chapter 8

EXPLOSIVES SAFETY

1. AK-LINE EXPLOSIVES SENSITIVITY

Explosives are by nature dangerous. Consequently any discussion of their safety is on a relative basis. Some explosives are more easily initiated than others by such things as shock or flame or friction or static spark. These more sensitive explosives would be the cause of many more accidents than now occur, if it were not for the fact that special precautions and design techniques isolate these explosives until their functioning is needed for weapon operation. This sensitive explosives isolation is a fundamental safety aspect of most conventional weapons and, for this reason, is discussed separately in this report.

The difference between the most sensitive and least sensitive explosives is very much like the difference between black and white. But like black and white, there are many shades of gray in between. The common distinction between the sensitive and insensitive explosives is in the classification as primary explosives or high explosives. Reference (b) defines primary explosives as metastable materials that are very sensitive to initiation by impact or heat, and lists examples as mercury fulminate, lead azide, and lead styphnate. High explosives are defined as metastable materials that are relatively insensitive to heat or impact and when properly initiated have detonation velocities higher than about 4000 meters per second. Examples listed are tetryl and TNT. These definitions do not make a clear-cut distinction between primary explosives and high explosives and are not adequate guides in deciding what sensitive explosives should be isolated from insensitive explosives. As would be expected, decisions to isolate or not isolate must be made in the gray area of sensitivity where the distinction between primary and high explosives is not discernible.

The sensitive primary explosives are used as the initiating elements of explosive trains. Reference (b) defines an explosive train as "an arrangement of a series of combustible and explosive elements consisting of a primer, a detonator, a delay, a relay, a lead and booster charge one or more of which may be either omitted or combined. The function of the explosive train is to accomplish the controlled augmentation of a relatively small impulse into one of sufficient energy to cause the main charge of the munition to function." The nature and amount of the energy available to initiate the explosives determines the need for sensitive explosives in the explosive train. If enough energy of proper characteristics can be

made available by nonexplosive means to initiate the high explosives, the sensitive primary explosives would not be required. High-order detonations of unfuzed warheads as the result of fire or drop are examples of putting enough energy in to effect initiation. But such events are hardly practical as normal operating inputs. The nearest thing to a practical input avoiding the need for a sensitive primary explosive is the exploding bridge wire (EBW). This technique is used in a number of applications which can tolerate the relative bulk of the power supply. It may possibly be used in the future in conventional fuzes if the size of power supplies can be further reduced. But today the use of primary explosives and the conventional explosive train is still predominant in fuzes.

Drawing the line on acceptability of explosives to be in-line with the main explosive charge involves many complex problems. Reference (j) discusses a number of these problems. For many years the Navy adhered to a rule, which on the surface, appeared to be a simple solution. This rule was that an explosive more sensitive than standard tetryl was not to be used on the side of the explosive train interrupter which was in direct communication with the main charge. This rule was originated at a time when tetryl was the common choice for leads and boosters. Now there are many other explosives with desirable characteristics. When tetryl was the most desirable explosive for a lead or booster, the rule caused no problem. But now that other explosives are attractive (notably RDX) the rule presents problems. What is or is not more sensitive than tetryl? Reference (j) presents many of the problems involved in answering this question. It shows that the order of sensitivity may easily be inverted on sensitivity scales. In one test RDX may be more sensitive than tetryl. In another test it may be less sensitive. Furthermore the sensitivity of a particular explosive in a particular test can vary widely if such things as particle size and compaction are changed. The term "dead pressed" applies to extreme cases of loss of sensitivity due to compaction to very high densities. Since one explosive may have widely varying sensitivity, even in repetitions of the same test, how can it be said to be more or less sensitive than another explosive which has overlapping sensitivity in the same test?

These questions have undoubtedly contributed to the problems which exist today and which cause considerable concern every time the Navy is asked to use a weapon component developed for one of the other services. The Navy continues to draw the line at the sensitivity of tetryl, in spite of the ambiguities, and has developed the explosive CH-6 (a desensitized RDX) to be less sensitive than tetryl to shock. Army drawings of explosive components frequently call for RDX with a maximum of two percent desensitizer added. It may be the Army's intention that the two percent desensitizer (usually calcium stearate) be added, which would result in a sensitivity very close to CH-6. But the fact that the two percent is listed as a maximum, and no minimum is stated, must be interpreted as permitting the use of RDX without any desensitizer, and this is unacceptable to the Navy.

Is the Navy being pigheaded on this question? There are arguments for and against this. In spite of the possible inversions of test

results, there is undeniable evidence that, when all factors are considered, RDX is definitely more sensitive than tetryl. Therefore, its use beyond the explosive train interrupter as accepted policy would represent some decrease in safety. The Navy cannot knowingly accept a policy which represents a decrease in safety. A fighting ship is an unparalleled concentration of men and material. Any accident may touch off a series of events which may cause loss of the ship and crew. The only condition in which the Navy will knowingly accept a decrease in safety is when it must be accepted to permit use of a weapon which has decided advantages. This is not a factor in the present differences.

On the other hand, the Army has been using RDX in leads and boosters for over ten years. It is not apparent on the surface that this has led to safety problems. Also it is not known how much of this was desensitized RDX and how much was not, and to determine this would require a greater search than is practical for the purposes of this report. If much of this has been pure RDX, all this experience has proved is that the difference between the sensitivities of RDX and tetryl or CH-6 is not a large factor in weapon accidents.

Probably the best hope for solution of this problem lies in the present Navy effort to develop a series of sensitivity tests to determine the acceptability of an explosive for in-line use. This series will include eight tests. These are:

- a. Small-scale gap test
- b. Impact sensitivity test
- c. Impact vulnerability (flying plate test)
- d. Vacuum stability test
- e. Hot-wire ignition test
- f. Bonfire test
- g. Electrostatic sensitivity test
- h. Friction sensitivity test

The procedure for running each test and the equipment to be used will be specified. Each test will have a pass-fail criterion. The sensitivity of the explosive will be acceptable only if it satisfies the criteria of all eight tests. It is very likely that pure RDX will fail to meet the criterion of at least one of these tests. But desensitized RDX will probably be acceptable. So, these tests, if accepted by the Army, will force desensitization of their RDX leads.

2. SEPARATION OF SENSITIVE AND INSENSITIVE EXPLOSIVES

Having defined the difference between sensitive and insensitive explosives, the next problem is to assure separation of these until

they must be brought together for weapon functioning. Historically there have been two primary ways this separation has been achieved. Demolition materials are a good example of one way this is done. It has been standard practice with demolition materials to store and handle the detonators of firing devices separately from the main demolition charges. Separate lockers or magazines are used for storage of these initiating devices. When a demolition job is to be done, the system, including detonators and main charges, is assembled. The detonator is generally inserted as the last step. When completely assembled, the system usually does not have explosive train interruption. The explosive train is completely aligned and ready to function on receipt of the firing stimulus. Therefore, with demolition material the separation of sensitive and insensitive explosives is a matter of policy and procedure which is followed in storage and handling up to the final arming of a demolition setup.

Most fuzed weapons are examples of the second method for separating sensitive and insensitive explosives. Modern fuzes employ interrupted explosive trains. The interrupter is a physical barrier (or a break) in the explosive train between the sensitive and insensitive explosives. It, therefore, isolates the sensitive explosives so that if they should be initiated accidentally, they cannot cause initiation of the insensitive explosives. The isolation is removed, i.e., the weapon is armed, as one of the final steps during launching or planting of the weapon. It is always preferred that this final arming occur after launch but before the weapon can acquire a target. The interrupted explosive train is a safety necessity in weapons which are transported, handled, and stored with all elements for firing contained in the weapon and with an explosive train which is initiated by explosive components containing sensitive primary explosives.

Another practice which frequently has been followed is a combination of separation by procedure and separation by explosive train interruption. There are many examples of weapons where a key element of the firing train can be removed and handled and stored separately from the rest of the weapon. This key element frequently contains an interrupted explosive train. If properly designed, this type of weapon is very good from the safety standpoint. Its disadvantages are operational. There is always the problem of field assembly of the missing arming elements which may be time consuming and may have to be done in unfavorable environments.

For the designer the important thing is that he recognize that the separation of sensitive and insensitive explosives is a policy of long standing and must not be violated. Experienced designers need no reminders. But there have been instances where designers, not experienced in weapon designs, have mistaken the lack of explosive interruption in a demolition assembly as license to design an in-line train in an all-up device. The argument to support such devices has been reference to some previous device which did not contain explosive train interruption. The reference device undoubtedly came into being because of a similar argument, and so on, and so on. Somewhere in this chain of violations of good safety policy is the original violation which was based on ignorance and misinterpretation of the

significance of storage and handling separation. This is not justification to repeat the error even though the devices concerned may be in the Fleet.

There are some new fuzes which are designed to dud if certain out-of-sequence events occur. The purpose is to provide safety, and in this respect the practice is commendable. What must be questioned, in some cases, is the methods of dudding. The method questioned here is dudding by firing the detonator in the safe position. The argument for this practice is the following. Firing the detonator in the safe position is safe because the explosive train is interrupted (this is questionable). After the detonator has fired, the munition is safe to approach and dispose of (this is not questioned). The attraction of this dudding method is the relative ease of disposal by a disposal team. With the detonator fired, there is no longer an active component capable of initiating the explosive train. This kind of dud can be approached with considerably more safety than most duds. On the other hand, the instant when the detonator fires is relatively dangerous. Explosive train interruption is not infallible. Few development programs can go further than to prove that there is a relatively high probability that firing of the detonator in the safe position will not result in explosion of the main charge. The experimental methods described in reference (k) are aimed at developing experimental evidence that the interrupter will be effective. But there are many factors which can change the effectiveness of interruption. Dimension tolerances, materials variabilities, detonator output, and lead or booster sensitivity are all factors which can change and which have a bearing on whether or not the explosive train interrupter will actually interrupt. When a detonator is fired the outcome is in doubt until the experiment is concluded. Consequently, firing the detonator in the safe position, as a means of dudding, is acceptable only if explosion (or other effect) of the weapon is acceptable, because this is a possible outcome of the experiment. If the conditions in which dudding is desired or required is always in a remote area far removed from men and material so that weapon functioning can be accepted as quite harmless, dudding by firing in the safe position could be acceptable. But if the conditions are such that a weapon actuation would be very costly in terms of men and material or use of a facility, then another method of dudding had better be employed. This is usually the case in the Navy where men and material are confined to the small areas and volumes of ships.

3. NOVEL INTERRUPTERS

The usual type of explosive train interrupter is one in which a solid piece of metal occupies a gap in the explosive train. This metal barrier is removed on arming which usually moves an explosive element in line to fill the gap. A different scheme was used in World War II mine extenders and depth charge pistols. The detonator was withdrawn from a well in the booster so that a large air gap existed between the detonator and booster. Arming was accomplished by hydrostatic pressure which pushed the detonator into the booster. This type of separation has not been used in newer devices because it appears that the interposed metal barrier provides more safety. When

withdrawn detonators were fired, the booster would be riddled by small pieces of the detonator cup giving the impression of rather marginal safety.

In recent years a novel interrupter has appeared intended primarily for underwater applications. This is a detonator which will not fire in air but will fire under water. Two different types of detonators were developed to the point of demonstrating that they worked pretty well. One of these was developed by private industry and was called WETDET. This detonator is simply a special configuration of a flexible line charge of insensitive explosive. A loop is configured in the line charge with a controlled gap where the charge enters and leaves the loop. In air, as detonation enters the loop, the blast disrupts the line charge across the gap before detonation can traverse the loop. The explosive column is broken and propagation stops at the break. In water the blast is attenuated and crosses the gap too slowly to break the column and stop detonation.

A second type of air-safe detonator is based on the known fact that certain explosive columns need adequate confinement in order to propagate. In this detonator a small diameter, relatively long column of explosive is very lightly confined. In air, detonation dies out in this column because of the light confinement. In water the confinement is increased adequately to support detonation.

These novel interrupters are not likely to appear attractive for common use applications. But they are examples of schemes employing special properties of certain explosives. New schemes may appear from time to time, and some of these may appear to have fuzing application. Consequently some discussion of these air-safe detonators may help to illustrate the nature of the problem of demonstrating adequate explosive train interruption.

It is seldom possible to conduct enough tests to obtain statistical assurance of the safety demanded of the explosive train interrupter. Usually it is only possible to obtain an engineering type of confidence in the design. This is done by conducting tests which show that the conditions of interruption are not marginal. Reference (k) describes the general approach for tests of this type for the usual type of physical barrier interruption. In these tests the physical configuration is changed so that a safety failure is more likely. If the test does not result in a safety failure, the engineer has gained confidence that the system was not marginal. If the system had been marginal the change he made would have resulted in an unsafe configuration. Penalty testing is a term often applied to this kind of testing.

Penalty testing demands precise knowledge of how the interrupter interrupts the train. Without such knowledge there can be no confidence in what does or does not constitute a penalty test. Even knowledge of the mechanism of operation does not guarantee that an acceptable penalty test can be devised. The air-safe detonators present some difficulties in this respect. The most obvious penalty

test is to demand safety when the device is in a medium more dense than air but less dense than water. For good safety it is desirable that the medium be considerably more dense than air. So an engineer may not be completely satisfied with the choices he has between air and water.

As a general rule the designer should avoid novel interrupter devices unless (1) they offer very decided advantages in his design, (2) the mechanism of operation is well understood and, (3) a good penalty test is readily apparent.

4. DIRECT INITIATION OF INSENSITIVE EXPLOSIVES

In recent years techniques have been developed which permit the direct initiation of insensitive explosives. The exploding bridge wire (EBW) was mentioned above where it was stated that the EBW is the nearest thing to a practical method for direct initiation of the insensitive explosives. The exploding bridge wire is literally that. The small bridge wire is exploded when very high current is forced through it before it has time to melt and disrupt the circuit. The common method for doing this requires high voltage, a source of considerable energy, and a matched transmission line to the wire.* This was accomplished by very efficient use of available energy. The wire explosion has been used to initiate directly such explosives as PETN, RDX, and HMX. These are borderline unacceptable by Navy standards. However, there is considerable promise that as knowledge of the exploding wire is increased the direct initiation of less sensitive explosives will become practical.

In their first applications the EBW devices were heralded as removing the necessity for explosive train interruption. Ignoring for the moment that the explosives which are readily ignited are marginally unacceptable to the Navy, the argument for this premise was valid as far as it went. It was argued that interruption was not needed because the purpose of interruption was protection from the sensitive primary explosives. These were not present in the EBW system. However, the argument did not go far enough. The interrupted explosive train is not just protection from the demonic tendency of sensitive explosives to initiate from receipt of accidental extraneous stimuli. More often than not it is protection from perfectly normal initiations of the sensitive explosive element obtained from the device which was designed to function it. Because of an error, or because of unusual circumstances the firing pin is released and strikes the stab detonator, or a switch is closed supplying firing energy to the electric detonator. Provided that other errors or conditions have not removed the interrupter it stops the propagation of the explosive train and prevents an accident. Just such an incident occurred in the Fleet recently. In fact this type of incident is probably much more common than firing of the sensitive explosives by extraneous and unusual energy inputs.

*Most commercial systems initiate PETN or RDX with one or two joules of energy. However, R. H. Stresau has initiated RDX with as little as 20 millijoules (reference (1)).

An important function of the interrupted train is to protect from normal but accidental initiations of the sensitive elements. The EEW device must also have a normal initiation process. Therefore, it is evident that the EBW device, without explosive train interruption, is practical only if accidental release of normal firing energy to the EBW device is much less likely than it has been in the conventional firing systems. The fact that the wire needs a very special current pulse is not adequate assurance against accidents. The firing unit designed to supply this special pulse is there and ready to go. So it boils down to how easily the firing unit can be armed and triggered accidentally.

Many EBW systems have been advertised by companies seeking to obtain a share of the present and future market. An important selling point is the adaptability of the system to the customer's needs including what electrical power he has available to arm and trigger the firing unit. Systems have been designed to arm and trigger on a common 6 volt d.c. supply, a common 26 volt d.c. supply, and there are undoubtedly others. One system requires 110 volts a.c. for arming and 30 volts d.c. for triggering. In one of the systems using a common power source for arming and triggering, it appeared that there was enough built-in delay in the trigger circuit so that an accident or fault applying arm and trigger voltages simultaneously would assure initiation of the EBW device. It is evident that in such systems the usual fuze objective to have at least two series arming mechanisms requiring independent sources of arming energy is violated.

The safety of present EBW systems has suffered from lack of adequate guidance. The basic safety and arming objectives for U. S. Navy fuzes, which have been in existence for a good many years, were quite naturally slanted toward mechanical devices. Mechanical devices predominated when these objectives were first stated. The problem today is to come up with equivalent objectives applicable to the control of arming and firing of the EBW system. This is one of the assignments of the group working on the modernization of fuze safety policy and design procedures, of which this present report is a part. It may turn out to be the most difficult of the assignments which this group has accepted.

The exploding bridge wire is not the only existing method for direct initiation of insensitive explosives. Another method has been demonstrated as feasible by explosives experts. This is burning to detonation. If a long heavily confined column of an insensitive explosive (such as tetryl or RDX) is given enough of a stimulus to start burning at one end, this burning will build up to detonation. The stimulus to cause burning may be quite small. The energy to start burning may be supplied electrically or by a special mechanical device. It should be apparent that this type of initiation raises a whole host of new questions about the relative of explosives sensitivity to the need for explosive train interruption. No ready solution is available. It is probable that a solution could be reached only after a thorough study of the susceptibility of such devices to initiation by accidental inputs. In the meantime employment of such a device not

followed by explosive train interruption would be considered too adventurous to receive favor of safety conscious designers.

5. PYROTECHNICS AND PROPELLANTS

There are no rules regarding the sensitivity of in-line pyrotechnics and propellants comparable to the rule applicable to the detonating explosives. But there is increasing realization that interruption of the firing train is needed in some weapons. Pyrotechnics are thought of as the military applications of fireworks. Such things as illuminating candles and distress signals come to mind. These devices are thought of as being much safer than high-explosive weapons which are designed for destructive effect. But the serious fire on the carrier ORISKANY in October 1966 which took the lives of 44 men was started by a high intensity flare.

Propellants are explosives which burn rapidly rather than detonate. Their primary use, as the name implies, is to propel projectiles or missiles. They are usually thought of as being less dangerous than the detonating explosives. However, the high-energy propellants can be detonated. Consequently, large rocket boosters are a safety concern not only because of the possibility of burning prematurely but also because of the detonating possibility. Some of these large boosters have explosive train interruption in a safety and arming (S and A) device. Smaller rocket boosters generally have no S and A device. Yet one of the possible causes leading to fire and explosions which almost cost the loss of a carrier and crew was the accidental firing of a small rocket from an aircraft on the carrier deck.

There is increasing awareness that many of the fuzing safety concepts would be good for the safety of pyrotechnic devices and propellant igniter systems. In fact, reference (m), which has existed for nine years, requires mechanical and electrical interruption in the igniters of air-launched guided missiles. Also, several years ago following a couple of accidents, the Air Force invited proposals for a frequency coded armament system employing EBW devices for ignition of air-launched guided missiles. This program never got off the ground, probably because of cost, but it did indicate serious concern regarding accidental ignition of guided missile motors. The same concern should, and often does exist for the accidental ignition of rocket motors.

Many of the safety features which appear in fuzes could be employed in a different manner in rocket and guided missile igniters. The main difference would be in the manner in which safety is removed. In most cases this would have to be commanded by launch personnel. Since lighting off the igniter is the act of launching, there would be no post-launch environment available for arming energy. However, in the case of air-launched rockets and missiles it would be entirely possible to demand some aircraft flight as a prerequisite to arming. This would definitely improve safety on the carrier deck and in any previous phases.

When igniter trains are interrupted, the position of the interrupter is not controlled by rules comparable to those stated for the high-explosive trains. No one has said what materials are acceptable for in-line use in the propellant-ignition train. Furthermore, it is not possible to select igniter materials on the same basis as the detonable high explosives. For example, it is likely that almost any igniter material would not be able to satisfy the criteria of the eight sensitivity tests proposed for the qualification of high explosives for in-line use. This is somewhat disturbing. If the eight tests are the right ones to limit sensitivity in accident-type environments, shouldn't they also be the right ones for igniter materials? Wouldn't the igniter-type materials be expected to encounter the same kinds of accident environments? The only reason that igniter materials might experience less severe accident environments in some cases is because of system configurations; the igniter materials might be better protected by the system. But this would not be true in all cases. Consequently, it would be very desirable to have igniter materials which could meet the same criteria as high explosives. Today it is simply not within the state of the art.

In spite of the problem of material sensitivity, the interruption of igniter trains would be an important improvement in safety for the reasons argued in paragraph 4. The interrupter has frequently prevented an accident when the first element of the train was initiated in a perfectly normal manner by the mechanism designed to initiate it. This kind of safety is independent of explosives sensitivity. It can be designed into igniters as well as into fuzes.

What has been said about propellant materials being unable to meet high-explosive sensitivity criteria applies also to pyrotechnics. And again, it can be repeated, that some accidents could be averted by an interrupted firing train requiring one additional step to set the firing train up for operation. Then accidental ignition of the first element, whether by normal or abnormal means, would not result in ignition of the main pyrotechnic device when the final arming step to remove the interrupter had not been accomplished.

6. SUMMARY

In summary, this chapter has dealt with the following points:

a. The Navy has criteria for determining the acceptability of high explosives for in-line use. The dividing line is at present set by the sensitivity of tetryl. Soon a series of eight sensitivity tests will appear which will control the sensitivity of these explosives without reference to tetryl.

b. The separation of sensitive and insensitive explosives until they must be brought together for functioning is a policy of long standing which must not be violated. The method of separation varies from one of procedure with most demolition materials to designed physical separation by interruption in all-up weapons.

c. Novel interrupter devices should be avoided unless they offer very decided advantages in the particular design and enough is known about how they operate so that a valid penalty test can be devised.

d. Direct initiation of insensitive explosives does not remove the need for explosive train interruption unless the equivalent of the out-of-line safety is put into the firing mechanism.

e. No rules exist regarding sensitivity of propellants and pyrotechnics for in-line use comparable to those which are in effect for high explosives. Furthermore, propellants and pyrotechnics will not pass sensitivity tests which are being used with high explosives. However, the interrupted explosive train would improve safety of igniters because it is capable of preventing an accident when the first element is accidentally initiated in a normal manner by the device designed to initiate it.

Chapter 9

A SAFETY PROGRAM IN DEVELOPMENT¹1. CONCEPTUAL SAFETY

One of the first steps in the orderly development of a weapon is to arrive at a weapon concept which available information indicates will be reliable and safe.* When the criteria stated in 1953 (reference (g)) governed the safety design of fuzes, the fuzing concept was considered safe if it satisfied these criteria. That is, the fuze was conceptually safe if it had the following features:

- a. An interrupted explosive train.
- b. A positive lock on the interrupter in the safe position.
- c. At least two arming mechanisms requiring independent sources of arming energy.
- d. At least one of the mechanisms which derived its energy from environmental conditions after launching and which unlocked and/or armed the interrupted train.
- e. For some fuzes, an arming indicator, visible when the fuze was in the round.

With the present use of the potential hazards analysis to develop weapon-dependent safety objectives, conceptual safety means somewhat more. There are still requirements and objectives applicable to all fuzes which will demand that certain features be present in fuze designs. There may also be requirements for other types of weapons (such as nuclear weapons, mines, torpedoes which are not affected by fuze requirements) appearing in specifications or standards. But regardless of the type of weapon, it is now conceptually safe only if it satisfies applicable standards and includes a safety system which, on paper, appears to provide adequate protection in all the accident events which were developed in the potential hazards analysis. This is illustrated in Figure 9.1.

Figure 9.1 depicts one aspect of the safety design solution by use of the potential hazards analysis which has not been discussed previously. Note that the safety solution for accident events $n + 1$

*This statement is an oversimplification. Other factors which must be considered in the concept are effectiveness, maintainability, anticipated cost, and schedule constraints.

and $n + 2$ is to issue proper procedures and warnings. This is a discouraging fact of life. It is simply not possible to obtain protection from every possible environment or from every conceivable careless act by the design of safety devices in the weapon. Even the best designed weapon must have some constraints placed on what can be done to it. The handling, transportation, assembly and disassembly, inspection and check-out, storage, and launch of weapons must be subject to certain rules and regulations. Since there is no limit to the detail with which accident environments and personnel actions are listed and studied in the process of the potential hazards analysis, it is quite logical that some of these would be of the type best handled by procedures and warnings. Consequently, if the potential hazards analysis is conducted with thoroughness and attention to detail, it will disclose the important safe procedures and warnings which must be part of manuals and other documents.

The discouraging thing about having to admit that procedures and warnings must be a part of the total safety solution for any weapon is that it appears to open the door to excessive use of these. When special procedures and warnings are issued to try to compensate for poor design or deficient safety devices, the procedures become complicated and the warnings are numerous and it is only a matter of time until one is violated and an accident results. A good design is one which holds the need for safe procedures and warnings to a minimum. A good design incorporates features to prevent accidents in most of the accident environments and dangerous personnel actions, and limits reliance on procedures and warnings to those events where safety device protection is beyond the state of the art or would be too complex to permit a satisfactory safety-reliability balance. In other words, reliance on procedures and warnings should be a last resort in the safety solution for a weapon. It should be held to a bare minimum in the concept stage because, as will be shown later, the hardware will have shortcomings not envisioned in the concept which will demand compensation by additional procedures and warnings.

The potential hazards analysis contribution to a safe weapon concept is the choice of safety devices to do the job for a particular weapon. Note that in the first paragraph of this Chapter nothing is said about what kinds of "arming mechanisms requiring independent sources of arming energy" are to be used. The choice of just any two mechanisms which will work in the system is no guarantee of safety. These mechanisms might be easily defeated by hazardous events which are common to the life of this particular weapon. But if the two mechanisms are chosen because they appear to offer good protection in the hazardous events which this particular weapon is likely to experience they are appropriate choices and this results in good conceptual safety.

The systematic listing of accident environments and dangerous personnel actions in the process of the potential hazards analysis will result in a long list of events, some of which will be common and some uncommon. Common sense dictates that the safety system must provide protection in common events. But what about the uncommon events? What about the very unlikely events which a weapon or even all weapons of its kind may never experience?

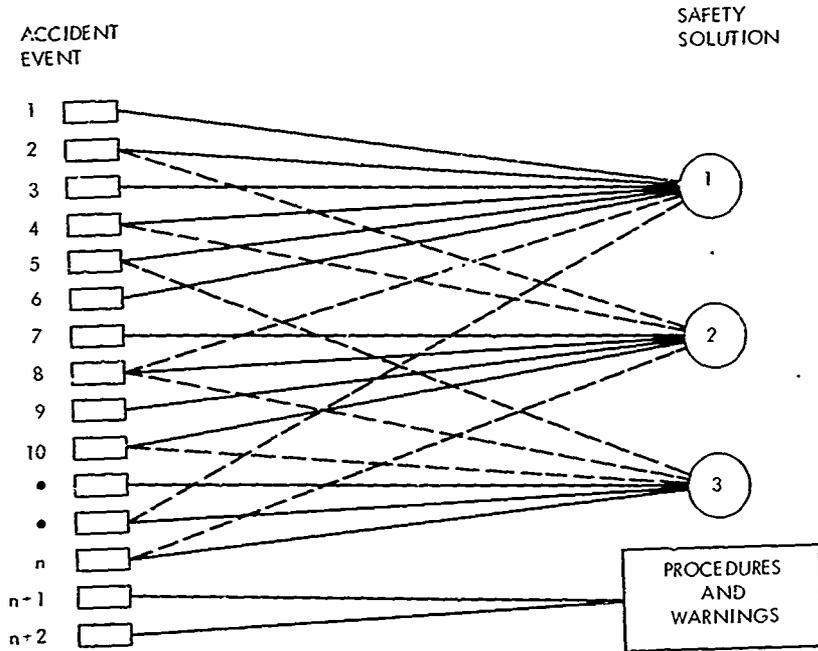


FIG. 9.1 CONCEPTUAL SAFETY - POTENTIAL HAZARDS ANALYSIS SOLUTION

The fact that safety is required in unlikely situations and occurrences as well as in the common ones adds to the complications of developing the proper safety objectives. Similar problems face everyone of us in our daily lives. Today, no responsible car owner would fail to carry liability coverage in his automobile insurance policy. He knows his chances of someday becoming involved in an accident are relatively high. However, the same man would be reluctant to pay premiums for special benefits in the event his property was damaged by earthquake if he lived in an area where an earthquake had never been recorded and was deemed extremely improbable by well known geologists. The same kind of situation exists with the accident events listed in the potential hazards analysis. Some are known to be quite probable because they have been experienced repeatedly in the past. Others are known to be quite improbable because there is no record of such occurrences. Where does one draw the line and how far does one go with the old adage that there is always a first time for everything?

The really satisfactory solution would be to obtain the probability of occurrence associated with each accident event and discard those with a probability below a set cut-off value. In this way a truly uniform criterion would be obtained. All likely events would receive due consideration and too unlikely events would not clutter up the analysis. This is a worthwhile goal. But that is all that can be said for it, because it is not possible to set down a valid number for the probability of occurrence of each of the accident events developed by a potential hazards analysis. A valid number must be based on an adequate number of observations or the known laws of chance such as in the rolling of dice. There are very few accident events where either of these establish a valid number.

Since numbers cannot now be the basis for eliminating the too unlikely events it must be done as a matter of judgment. The Air Force in its Nuclear Weapon System Safety Design Manual (reference (n)) uses the term "credible abnormal environments." This is about all that can be said in general guidelines. The potential hazards analysis must include all credible accident events where events include accident environments and dangerous personnel actions. Whether or not an event is credible must be a matter of judgment.

The conceptually safe weapon system is one which complies with applicable specifications and standards and, on paper, provides adequate protection in the credible accident events developed in the potential hazards analysis. At this stage the entire system is little more than a paper study. As illustrated in Figure 9.2 a series of component concepts are considered for the system. These concepts usually have a definite relation to existing components of known characteristics. But somewhat different functions are to be performed in somewhat different circumstances. This is the stage when engineers are looking at the system composed of some existing components and some new components and gathering the information available to make an initial assessment. If the initial assessment is unfavorable, alternate means to accomplish the functions of the weak links will be

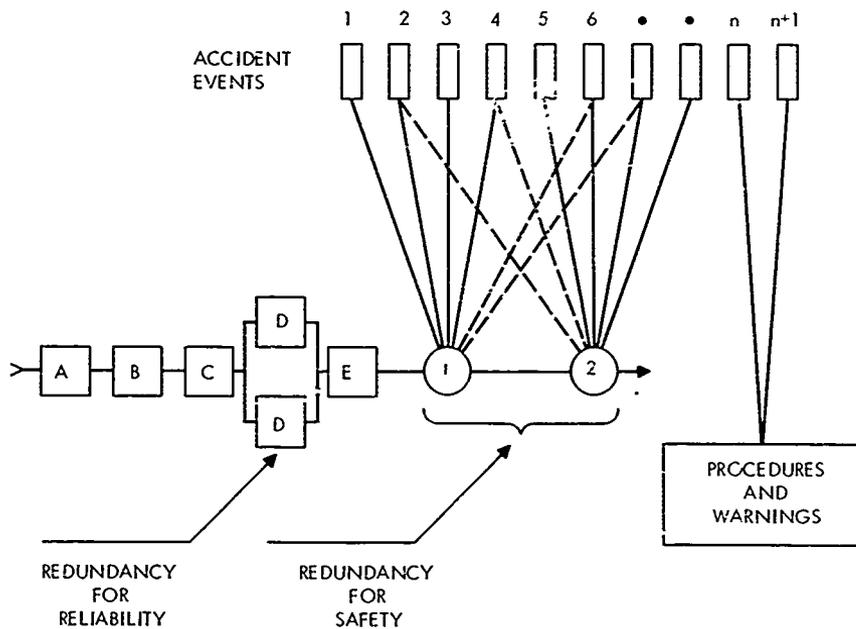


FIG. 9.2 RELIABLE AND SAFE SYSTEM CONCEPT

explored. If the initial assessment is favorable, a hurdle toward development of the system will have been cleared. Therefore, the conceptually safe system is safety's equivalent of reliability's satisfactory initial reliability assessment. Both are green lights to go ahead with development of the system. If either is deficient, the development of the system involves high risk.

2. HARDWARE FALLIBILITY

A good concept does not assure a good weapon. The hardware may not fulfill the glowing expectations of the concept. There was a recent advertisement which went "its not how long you make it; its how you make it long." "How you make it" is important to both the safety and reliability of a weapon. In reliability, the performance of some components may not come up to the level which was expected when it was nothing more than a concept. Failure modes appear which were not expected. Reactions to certain environments are not what was anticipated. If these problems are severe and solutions are not found, the program may be halted even though it showed promise as a concept. In safety the effectiveness of safety components may be less than was hoped for. A component may be designed so that a critical part can be omitted, whereas in concept it was hoped that the designer would find a clever method to make the part necessary for assembly. Thus an additional burden is placed on inspection or the original component concept is discarded in favor of another one. A component may act indirectly rather than directly in performing its safety mission. Then a linkage failure between the component and the safety barrier it controls may nullify the effectiveness of the component. A component may not resist an accident environment as it was expected to. Or the nature of the structure or the presence of wires may offer ways to get around the component in certain situations. All of these, and there are many more, are safety bypasses which are characteristics of hardware. If too many of these bypass problems appear in the hardware and solutions are not found, the program is in jeopardy because it is headed toward developing an unsafe weapon.

Safety bypasses are uncovered through knowledge of the characteristics of the hardware. This knowledge is gained in safety analyses and tests. Figure 9.3 illustrates the effects of safety bypasses which appear when the concept of Figure 9.2 reaches the hardware stage. Components 1 and 2 which are concepts in the stage represented in Figure 9.2 have been designed to the point that hardware models have been made. These models can be examined and tested. This process (the safety analysis and tests) shows that component 1 can be bypassed by paths a, b, c, and d, and component 2 can be bypassed by e, f, g, and h. Furthermore component 1 and component 2 can both be bypassed by paths i and j. The effect of these bypasses is to reduce the effectiveness of components 1 and 2 in providing the intended safety. The ideal would be to have no bypasses but this is not realistic. Any system will have some bypasses.

Even when the safety system was being developed as a concept the existence of some bypasses was recognized. For example, in Figure 9.2 components 1 and 2 are safety components and the fact that there are

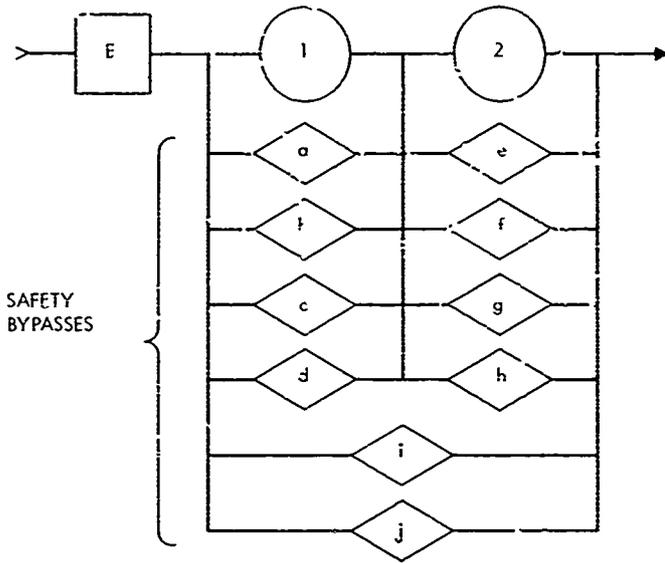


FIG. 9.3 HARDWARE WEAKNESSES - THE SAFETY BYPASSES

two is redundancy for safety. Component 1 was chosen first to provide safety in the accident events of the potential hazards analysis. But an event was encountered for which component 1 was not suitable. So component 2 was added. Component 2 was added because an event was encountered which would bypass component 1. Let's say this event is represented by "a" in Figure 9.3. At this stage the addition of another component 1 would do little good. It would also be bypassed by event "a." Component 2 was chosen because it would not be bypassed by event "a." But it has its weaknesses too. Event "a," for example, bypasses component 2, but in arriving at a safe concept it was concluded that event "e" would not bypass component 1 and that events "a" and "e" did not coexist in the hazardous situations. In short, the recognition of safety bypasses even in concept stage was the primary reason for dissimilar redundancy in the safety system, and the choice of concepts was specifically directed toward avoiding coexistence of the safety component bypasses.

The bypasses which destroy the effectiveness of a safety system are those which have a high probability of coexisting, or those which bypass all safety components. In Figure 9.3 events "i" and "j" bypass both safety components. These might be the two events which in Figure 9.2 were to be handled by procedures and warnings. This would be the most favorable outcome because then these complete bypasses come as no surprise and were considered in a satisfactory original concept. But more often the safety analysis or tests will uncover some which were not anticipated.

Some further assumptions will illustrate the individual component bypass. In the previous paragraph it was assumed that event "a" could not coexist with event "e." Assume now that event "a" also does not coexist with "f" and that "b" does not coexist with "e" or "f." This leaves the following failure paths: ag, ah, bg, bh, ca, cf, de, df, cg, ch, dg, and dh. In other words there are a dozen safety failure paths.

The number of safety failure paths is not in itself an indication of unsafety. A large number of unlikely paths may be less dangerous than one likely path. But a large number of safety failure paths is indication of problems, particularly when they come as surprises as a result of the safety analysis or tests. Too often the likelihood of occurrence of paths cannot be reasonably estimated. This means there is considerable risk that a large number of safety failure paths include some dangerous ones. Chapter 7 discussed some ways to avoid safety bypasses. Because bypasses are so intimately associated with the hardware, it was difficult to give any general rules for avoiding bypasses. Probably the two most valuable general rules are to locate safety barriers near the danger areas (such as the warhead), and to use simple and direct safety locks. Where these have been violated, there has been considerable concern for the safety of the system.

3. SAFETY ANALYSES

The safety analysis is the equivalent of reliability's Failure Modes and Effects Analysis (FMEA). The FMEA is a systematic study of

the effects of hardware failure modes on operation or safety. It generally considers the common failure modes of components exposed to normal stresses. It frequently exposes weaknesses which can be corrected by redesign to give more reliable performance. Every now and then it uncovers a safety weakness which must be corrected by design changes. For this reason the FMEA has rightfully been regarded as an analysis tool which is effective in uncovering safety problems. In fact it may be the best for locating problems due to normal parts failure modes under normal stresses. But there are fundamental difficulties in relying entirely on the FMEA. The FMEA approach is to start with piece parts, consider the ways in which they can fail, and then analyze the effects of these failures on system performance or safety. In this process a number of failures affecting safety are usually uncovered. But the analysis is usually concentrating on failures caused by normal usage or wear and tear. The safety analysis starts with the unwanted event, such as the accident, and methodically develops the paths which can lead to this event. Abnormal events immediately come into the picture because these events produce some of the paths. The FMEA and the safety analysis use different approaches in analyzing the system. In this respect they are an excellent team because they complement each other.

Two safety analysis methods, which have been described in enough detail to bear formal names, will be discussed briefly. One is the Relative Accident Probability (RAP) Analysis which is described in reference (c); the other is Fault Tree Analysis which has been discussed in a number of symposium papers (reference (2)) and is the subject of short courses given periodically at the University of Washington, Seattle. These two analyses are very similar in purpose. Each is a systematic method for tracing the possible accident paths and evaluating their importance. The primary difference between the two methods is in the graphic display of the accident paths. Figure 9.3 illustrates this, using the safety features of an elevator for the example. This figure shows the two principal logic symbols used in the Fault Tree: the AND gate and the OR gate. It also shows the transfer symbol (the triangle) and the conditional input (the oval). The triangle indicates a "transfer in" if the line is from the apex and a "transfer out" by a line from the side. A good description of the Fault Tree Analysis is contained in reference (c) in a paper by R. A. Feutz and T. A. Waldeck of the Boeing Company entitled "The Application of Fault Tree Analysis to Dynamic Systems."

Boolean expressions can be developed for either the Fault Tree or the RAP Analysis situation (an event diagram is prepared for each situation). Consequently, the mathematics for expressing the undesired end event (Fault Tree Analysis) or the likelihood of accident (RAP Analysis) as a probability is straightforward. The problem has been in obtaining data to give valid estimates of the probabilities of the events in the diagrams. The example given in Figure 9.4 may be misleading in this respect. It is possible to calculate safety factors on cables and other equipment and the entire system is fairly well protected from outside forces. Poor maintenance can, of course, contribute to excessive deterioration so that safety factors are no longer valid. But, in spite of this, the

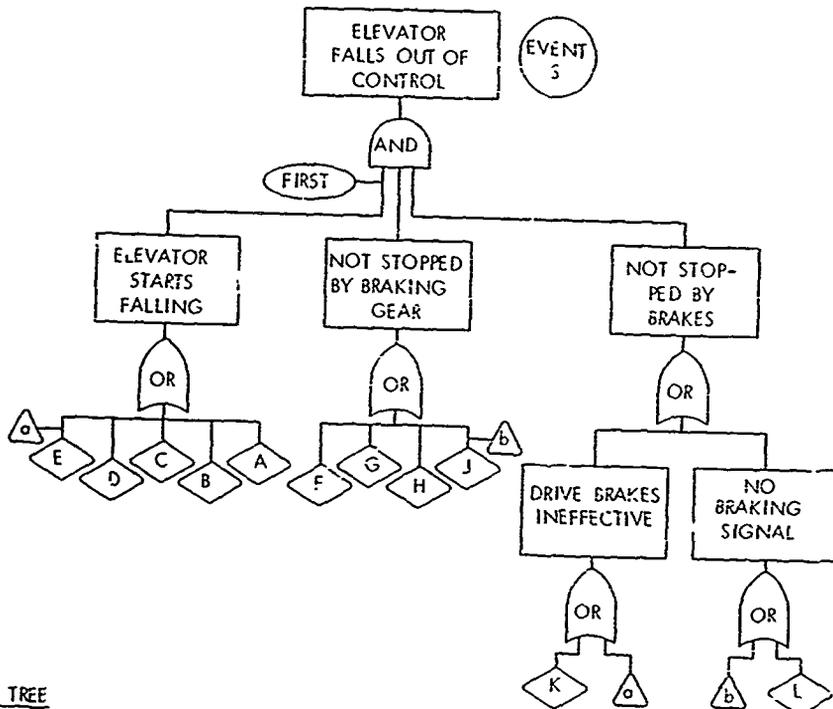
KEY TO ELEVATOR FUNCTIONAL DIAGRAM

- 1 Main Drive Cable Anchors
- 2 Main Drive Cables
- 3 Counterweight
- 4 Main Drive Motors and Brakes
- 5 Main Drive Cable Pulleys
- 6 Governor
- 7 Governor Cable
- 8 Braking Gear
- 9 Braking Gear Cable

DEFINITIONS OF LETTER SYMBOLS USED IN RAP
AND FAULT TREE ANALYSES

- a Transfer symbol: indicates that E will cause two associated failure events
- A Counterweight detaches from drive cables
- b Transfer symbol: indicates that J will cause two associated failure events
- B Drive motor speed control circuits fail
- C Drive cable pulleys detach from elevator
- D Drive cables pull out of either set of anchors
- E All drive cables break (only one needed to hold elevator).
- F Braking gear cable breaks
- G Braking gear defective
- H Governor fails to lock governor cable
- J Governor cable breaks
- K Drive brakes defective
- L Governor electrical circuit defective
- S Elevator falls out of control

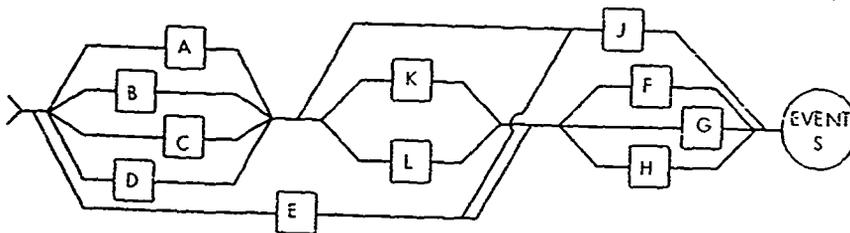
67/68 cont



FAULT TREE

BOOLEAN EXPRESSION (BOTH DIAGRAMS)

$$S = (A + B + C + D) (F + G + H) (K + L) + (A + B + C + D) (J) - (F + G + H + J) (E)$$



RAP ANALYSIS DIAGRAM

FIG. 9.4 SAFETY ANALYSIS DIAGRAMS

elevator is an example where the computation of a safety number appears reasonable. A weapon, on the other hand, will generally have a much more dynamic life. It is a hazard while it is being assembled, handled, transported, stored, checked out, and launched. It can experience fire, crushing, drops, mishandling, flooding, and mistreatment by service personnel due to ignorance or the exigency of circumstances. All of these affect the probabilities of certain events in the event diagrams. Obtaining a measure of these probabilities by tests, calculations, or experience data, as would be done in the case of the elevator is a fantastic undertaking for most weapons. Consequently, the real value of the safety analysis is that it discloses safety weaknesses and suggests means for improvement which otherwise could be overlooked.

As presented in existing documents the RAP Analysis appears to concentrate more on unusual situations while the Fault Tree Analysis seems to deal more with normal situations and stresses. This is not a fundamental difference in the analyses. It very likely resulted from the nature of the problems which were uppermost when the techniques were developed. The RAP Analysis was developed with conventional fuze safety as the primary reference. The Fault Tree Analysis was developed with a large aircraft or a large ballistic missile as the primary reference. The very bulk and weight of aircraft or large ballistic missiles decreases the chance that such devices will experience some of the abnormal environments which a small bomb or projectile is likely to encounter. Either analysis can be adapted to the specific problems of the weapon or system being considered. The method of the Fault Tree Analysis does not confine it to normal events and stresses. It can be used just as well in extremely abnormal events and stresses. By the same token, the RAP Analysis can be used in normal situations as well as in the abnormal accident situations which received emphasis in the first description of the procedure. The temptation to stay in the realm of normal events comes with the improved chances in these cases of finding data which is usable in arriving at event probabilities which permit a numerical expression for safety of the system. However, this is unrealistic. The number means nothing if the abnormal events are ignored, for often they are the most important contributors to unsafety.

There are many ways to analyze problems. Safety analysis methods don't stop with just the RAP Analysis and Fault Tree Analysis. Reference (i) mentions several other safety and hazard analysis approaches. These will not be discussed here. It is the author's opinion that adequate analytical methods for general application are available in the potential hazards analysis followed by the RAP Analysis or Fault Tree Analysis.

4. SAFETY TESTS

Reliability tests are often thought of as those tests which "go for score." For example, if 50 fuzed projectiles are fired under realistic conditions and 49 are scored as successes by the criteria of the applicable reliability definition, the series is considered to have demonstrated a reliability of 0.90 at a confidence level of 95 percent.

Safety tests do not "go for score." As stated previously, it is not economically feasible to set up each of the conditions in which the weapon is expected to be safe, and then conduct enough tests in each set of conditions to demonstrate the small probability which is acceptable for unsafety. Consequently, safety tests have a different purpose. They are more like the isolated exploratory tests which a designer runs on his first models to find out if the hardware performance conforms to his theoretical predictions. Given engineering design goals as safety objectives (such as the magnitudes of accidental shocks, the rate of spin in a special situation, the pressure from a nearby explosion) the designer would, in most cases, want to check to see if his design met these goals. Usually the goals are themselves maximal. So the tests are overtests in this respect. Success in the tests gives engineering confidence.

Standard fuze safety tests considered applicable to nearly all fuzes are the jolt, jumble, 40-foot drop, and static detonator safety tests. These are described in MIL-STD-331 (reference (p)). Reference (p) also describes a number of field safety tests which apply to particular kinds of fuzes. Examples are: jettison tests (five different jettison tests are described), accidental release, muzzle impact safety, impact safe distance, and missile pull off from aircraft on arrested landing. In addition, safety is an aspect of all other tests appearing in the MIL-STD. In such tests as vibration, temperature and humidity, and vacuum-steam-pressure, the fuze is first required to be safe even though operability is the prime consideration. A good fuze would not be expected to become unsafe in the operability tests, but there is always an outside chance of unexpected reaction to the test conditions and, if this results in an unsafe condition, the fuze has failed the test.

These standard tests cover many of the abnormal environments. But it is not possible to cover all abnormal environments with standardized tests. Some weapons will, by their peculiar natures, offer opportunities for unique abnormal environments or events. There is little point in standardizing these in tests. Each test might be applicable to only the one weapon. So in these cases, the need for a test and the nature of the test should result from the potential hazards analysis.

The potential hazards analysis followed by the safety analysis should provide the guidance needed in the selection of safety tests. It would be a rather incomplete analysis that didn't include rough handling and drops as dangerous events demanding design solutions. And the standard rough handling and drop tests should frequently be appropriate to test the adequacy of the safety design solutions. Furthermore, the analyses should also indicate certain hazardous events which are peculiar to the individual weapon and which may call for special types of tests.

In summary, safety tests are not "tests for score." At best they are exploratory to determine whether or not the special safety design provisions are reacting as expected. The safety test program for a particular weapon will include standard tests and special tests as

determined to be appropriate by the analyses. These tests will be overtests in the sense that the weapon will be much more likely to encounter lesser levels of the test environments in accidents occurring in its life span.

5. AN ORGANIZED RELIABILITY - SAFETY PROGRAM

The organized reliability program is a combination of management control and reliability engineering. It will be argued here that a safety program can be managed and engineered in much the same way. This is not a new thought. Safety is an important part of every design review. The FMEA looks for failures with safety implications. Safety objectives are a part of design objectives. And MIL-STD-882 (reference (q)) calls for an organized System Safety Program. Yet, in spite of this, safety has continued to be highly opinionative. The most plausible reason for this is that much less information on which to make safety judgments has been available than in the case of reliability. The potential hazards analysis, safety analysis, this report on fuze safety concepts, and the other documents* being prepared as part of the fuze safety program should help to correct this situation.

The similarity between a reliability program and a safety design program is depicted by the information available to the participants of a design review. Figure 9.5 shows the information which should be available at a preliminary design review of a proposed fuze. The preliminary design review is held at the time a block diagram system is proposed and before first hardware models are built. The information available on safety would be MIL-STD-1316 (reference (r)), the safety concepts presented in this report, and a potential hazards analysis which would have been influential in the choice of safety devices shown as 1 and 2 in the block diagram. This should be considerably more helpful to a design review team than the information available previously, which amounted to little more than the Basic Safety and Arming Design Objectives for U. S. Navy Fuzes stated in 1953 in reference (g).

A later design review is illustrated by Figure 9.6, in this case at a stage called design freeze. The fuze at this stage has been built and tested in modest quantities. The information available for safety review would include safety objectives (obtained from the potential hazards analysis, MIL-STD-1316, and a safe separation study), a safety analysis (based on RAP Analysis or Fault Tree Analysis methods), and the results of some of the planned safety tests. The safety analysis would show and analyze the possible accident paths (the safety bypasses) pertinent to the actual characteristics of the hardware. The safety test results would show whether or not the hardware responded as intended in the tests which were selected on the basis of the potential hazards analysis. Drawings would be available and would show dimensions, tolerances, and materials which would be pertinent in some cases to safety and in some cases to reliability.

*MIL-STD-1316 (reference (r)), sensitivity criteria for in-line explosives (see paragraph 1 of Chapter 8), test methods to determine effectiveness of explosive train interruption (reference (k)) guidelines and test methods applicable to in-line EED's (see paragraph 4 of Chapter 8).

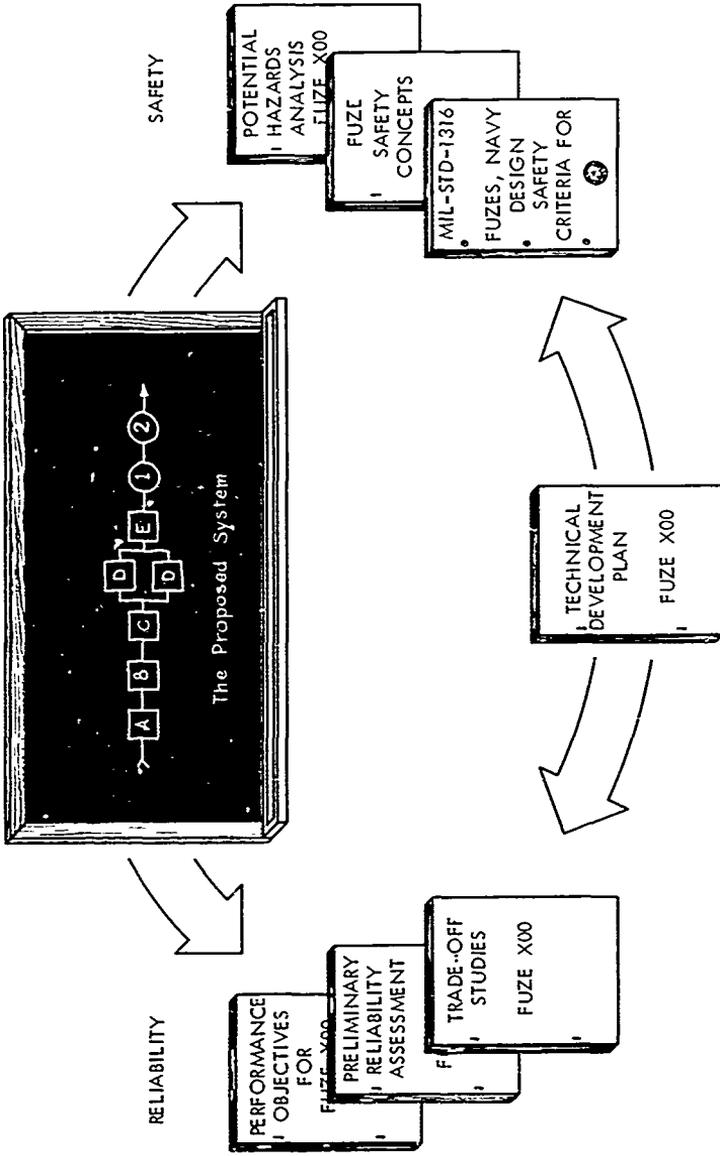


FIG. 9.5 PRELIMINARY DESIGN REVIEW

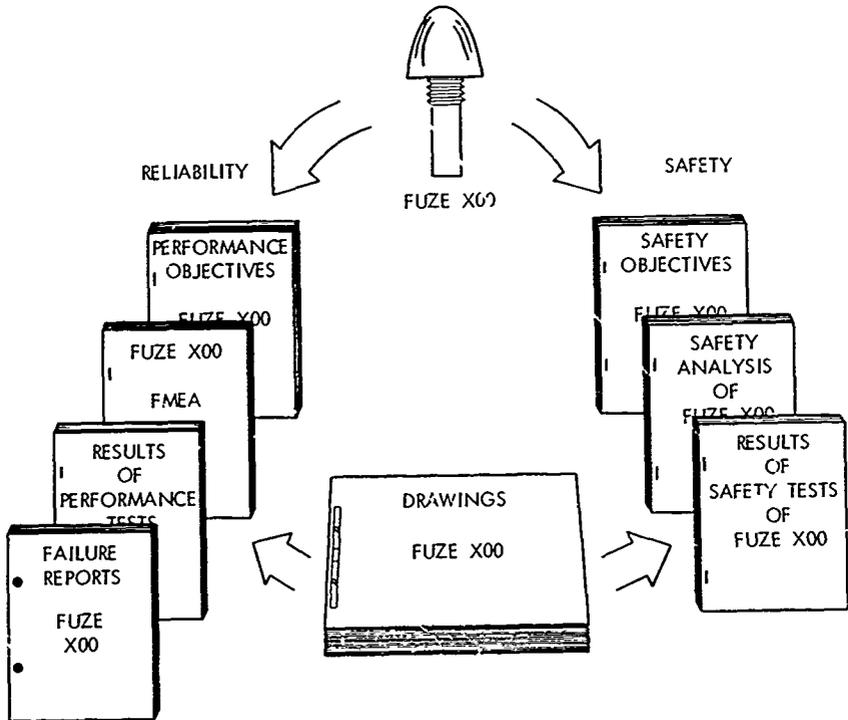


FIG. 9.6 DESIGN REVIEW AT DESIGN FREEZE

It is recognized in the formal reliability program that judgments at any stage must be based on reliable information and relevant experience. The purpose of reliability assessments, FMEA's, failure reports, and the like are to put this information in usable form for decision making. Without these the data would be inadequate and decisions would have to be made in the confusion of conflicting personal opinions. It is the latter situation which seems to have prevailed until recently in safety. The only solution for this is to provide better data. This is the purpose of the potential hazards analysis and safety analysis and their contributions to safety objectives and tests, and a liberal discussion of fuse safety concepts which has been the intent of his report. It is believed that these should contribute materially to the success of formal safety design programs.

In an organization which is designing, developing, and evaluating fuse hardware, there are strong arguments favoring a combined organization for management control of safety and reliability. One of the strongest is the need for a proper safety-reliability balance which was discussed in Chapter 4. There it was argued that safety-reliability trade-offs are necessary. Decisions to make trade-offs must be based on studies of the available safety and reliability information. This information is likely to be most complete if it is being gathered and analyzed in the same organizational unit.

For each reliability program element there is generally a safety counterpart. Some of these may be very similar and some quite different. Differences generally arise from the opposite purposes expressed in the definitions of reliability and safety. The similarities and differences of a number of important program elements can be compared as follows:

Management and Control

Reliability

To assure that an appropriate plan is being followed, that responsible people are aware of status and problems and are taking necessary and timely actions, that adequate data are being obtained as a basis for decisions.

Safety

To assure that an appropriate plan is being followed, that responsible people are aware of status and problems and are taking necessary and timely actions, that adequate data are being obtained as a basis for decisions.

Objectives

Reliability

A clear statement of expected performance; a stated realistic reliability value; definition of compatibility requirements; environmental levels which product must survive and in which it must operate.

Safety

A statement of applicable design controls; definition of constraints imposed by compatibility requirements; environmental levels in which the product must be safe, environments which must be avoided or controlled.

Design Reviews

Reliability

To require that designer organize his thinking about his design and alternate approaches; provide guidance from experienced experts; inform management of technical status and design maturity and readiness to proceed to subsequent development phases.

Safety

To require that the designer compare his design to alternate approaches and compare effects on necessary procedures and warnings; provide guidance from experienced experts; inform management of technical status and design maturity and readiness to proceed to subsequent development phases.

Redundancy

Reliability

To increase the probability of performing as intended by including alternate parallel operating paths where the operating sequence could otherwise be interrupted by component failure.

Safety

To decrease the probability of premature self-destructive operation by including alternate series interrupters where the operating sequence could otherwise proceed because of safety component failure or bypass.

Human Engineering

Reliability

To decrease the probability that human error will result in mission failure.

Safety

To decrease the probability that human error will result in hazard or accident.

Analysis

Reliability

To use systematic analytical procedures to search for and uncover component failure modes under normal stress conditions and study the effects of these on system performance, including safety (FMEA). The FMEA starts with the identification of piece parts failure modes and then analyzes effects of these on system performance and safety.

Safety

To use systematic analytical procedures to search for and uncover out-of-sequence and unwanted component operations and component bypasses under normal and abnormal stress conditions and determine paths so formed leading to system hazard or accident (RAP or Fault Tree Analysis). The RAP or Fault Tree Analysis starts with the unwanted event, usually an accident or hazard, and develops the paths which can lead to this event.

Testing

Reliability

To measure the reliability in the conditions of use and following the environmental exposures which normally precede use. To evaluate relationships between environments or stresses and parameters which influence failure. To eliminate material of unacceptable quality.

Safety

To verify design solutions for specific hazardous environments. To determine effectiveness of safety procedures. To eliminate material of unacceptable quality.

Failure Reporting and Corrective Actions

Reliability

To provide a comprehensive and uniform system for reporting all performance failures and for assuring that corrective actions are taken.

Safety

To provide a comprehensive and uniform system for reporting all failures to meet listed safety objectives and for assuring that corrective actions are taken.

In the brief description of program elements given above it is evident that few design change decisions regarding reliability can be made without some effect on safety and vice versa. Furthermore,

there is a similarity in the elements, even though the goals may be different, which suggests that similar skills and techniques should be employed.

A formal reliability program is a requirement in any weapon development. Military Standard 785 (reference (s)) states the requirements for the reliability program. Formal safety program requirements are given in reference (q). Consequently the prediction made at the Third Annual Reliability and Maintainability Conference on 30 June 1964 has become a reality. System Safety is now Reliability's associate.

Chapter 10

SUMMARY

1. There are many similar aspects to the achievement of fuze design safety and reliability. If there has been confusion on this point in the past, it is because in many aspects they are opposites. This may have led to the idea that entirely different approaches were required. This is not true. The same approaches, applied in a manner to achieve different goals, are quite appropriate for reliability and safety.

2. The opposite aspects of reliability and safety are expressed in the definitions. To show this most clearly, the definition of reliability given in reference (e) can be changed slightly to a definition of weapon reliability: The probability that the weapon will perform its intended function for a specified period under stated conditions. The definition of weapon safety given in Chapter 3 was: The probability of freedom from the destructive effects of one's own weapon in any conditions which may occur before intended launch and safe separation. The "intended function" in the reliability definition is generally the "destructive effect" of the safety definition, with the exception that in the former case it be delivered to the enemy. Thus, it is apparent that reliability tools are used to enhance the probability of unleashing the destructive effects on the enemy, and safety tools are used to decrease the probability of unleashing the destructive effects on oneself. This very definite cross-purpose of safety and reliability goals is the basis for needing a safety-reliability balance.

3. During the advent of the guided missile it was recognized that the difference between the reliable manned aircraft and the unreliable missile was man. Man was the redundant component. Because of his adaptability he could take over the function of many different kinds of components. The well-trained, reliable man could improvise to avoid the disaster which minor failures could lead to if unattended. But in the early guided missiles these minor failures were unattended and usually they triggered events leading to mission failures. Today the failure of a guided missile is more the exception than the rule it once was. The reliability of mechanisms where man is no longer a redundant component has come a long way. Safety is really no different in this respect. It can be entrusted to men or to machines. If entrusted to men, it must be entrusted to reliable, well-trained men. This was a major factor, and still is in the safety of nuclear weapons. If entrusted to machines, these machines must be designed and controlled using all the techniques which gave the guided missile its tremendous lift in reliability. Safety devices must be designed

to meet specific goals. These goals must be determined using the same care and thoroughness which go into the environmental criteria and human engineering aspects for achieving high reliability. Analysis must be used as an adjunct to testing to assure the most complete and thoughtful consideration of possible safety failures. How else did guided missiles reach a point so high on the reliability scale that men are riding them into outer space!

4. There are many guides to the choice of components to do a particular job, and do it reliably. Guides to the choice of safety components are not so common. Some of the guides stated earlier in this report are: keying a safety device to a "unique" post-launch environment; studying the effects of other environments and designing to avoid unwanted operating modes; choosing component designs which give good complementary safety; using "weak links" to protect against the overpowering accident environments; avoiding loose linkages and remote controls which invite safety bypasses; rejection of abnormal sequences; requiring that events occur within the proper time gates; physical orientation of components to reduce chances of unwanted actuations; use of the maximum practical number of characteristic normal environments; and designing so man can defeat the safety only by thoughtful acts rather than thoughtless acts.

5. Since the majority of weapons employ explosives, their characteristics and use are of special concern in the design of weapons. One fundamental rule coming from many years of experience is that the sensitive explosives, used only in small quantities as initiators, should be separated from the insensitive explosives, used in large quantities as main charges. In other words, the initiator should be separated from the large, main charge that it is capable of initiating. The two principle ways this has been done is by storing and handling them separately, which is common for demolition materials, and by interruption of the explosive train, which is common in mechanized weapons. Distinguishing between the sensitive and the insensitive explosives is not a simple matter. There is no natural gap in the sensitivities of different explosives which would permit those on one side to be called sensitive and those on the other side insensitive. The distinction has always been arbitrary, and will continue to be so. Setting the dividing line at tetryl was quite satisfactory when tetryl was by far the best explosive for leads and boosters. But tetryl now has many competitors, and most of these are superior in many ways. Therefore, it appears that the time has come to class an explosive as sensitive or insensitive on the basis of the results of a series of tests. The choice is still arbitrary because the pass-or-fail criteria must be arbitrary.

6. Recent developments in the initiation of explosives have put the alleged purpose of explosive train interruption to a real test. The exploding bridge wire (EBW) and explosive column geometries which permit burning to detonation have made it practical to initiate insensitive explosives without the use of the sensitive initiators. Therefore, if the sole purpose of the explosive train interrupter were to guard against abnormal initiations of the sensitive explosive elements, it would not be needed. But history shows that many an

accident was prevented by the explosive train interrupter when the sensitive explosive element was initiated in a perfectly normal manner by the power source designed to initiate it. In other words, the great reliance placed on the explosive train interruption has resulted in poor quality of other safety features. If this poor quality were to be carried over to the features preventing release of the electrical power to fire an EBW or the energy to start burning to detonation, the results could be disastrous. Consequently it is felt that designers must be made aware that the elimination of explosive train interruption carries with it the responsibility to compensate for this loss of safety with quality safety features elsewhere in the system.

7. Every successful weapon was developed from a sound basic concept. It is very important that the initial concept show promise of being both reliable and safe. At this early stage the safe concept is one which complies with applicable criteria, such as MIL-STD-1316 for fuzes, and appears to offer the protection needed in the abnormal events which experience and analysis show may occur during the life of the weapon. These abnormal events comprise abnormal environments and dangerous personnel actions. The abnormal environments are safety's equivalent of reliability's environmental criteria. They are environmental levels which are goals for safety design. The list of dangerous personnel actions sets goals for human engineering for safety. It is therefore evident that the list of abnormal events, developed by a process herein called the potential hazards analysis, is a prerequisite to the choice of a weapon safety concept.

8. Seldom does hardware live up to the glowing expectations of the concept. Too often unexpected failure modes or safety bypasses appear in the hardware which were not foreseen in the concept. To assure that the maximum number of these are uncovered and corrected, the hardware must be analyzed and tested. This is a continuing process starting with first hardware. The common analyses which are pertinent to safety at this stage are the Failure Modes and Effects Analysis (FMEA) and the R&P Analysis (reference (n)) or the Fault Tree Analysis (reference (c)). The latter two have a common purpose but use somewhat different methodology.

9. Safety tests are designed to explore the reaction of safety devices or systems in abnormal environments. Only in rare cases it is possible to test for safety score. This is a primary difference which is imposed by the high number which is required for the safety probability and the many different conditions in which safety is expected. Therefore safety tests seldom go beyond the purpose of verifying design adequacy in specific abnormal environments. But the wisdom of such verification has been demonstrated many times.

10. A formal reliability program (reference (s)) and a formal safety program (reference (r)) are now a requirement in every weapon development. The importance of safety - reliability balance and the need for safety - reliability trade-offs suggests that common management and control of these programs is a necessity in an agency which is directly engaged in the design, development, and evaluation of hardware such as a fuze. There is, in addition, a need to define the parallelism of reliability and safety events so that decisions which affect both can be based on comparable facts and data.

REFERENCES

- (a) OP 1014, Ordnance Safety Precautions, Their Origin and Necessity, Second Revision, 15 Aug 1965
- (b) ROLR 1111, Ordnance Explosive Train Designers' Handbook (U), Apr 1952
- (c) Proceedings, System Safety Symposium, Jun 1965 (W. E. Classon, W. R. Owens, The Boeing Company, P. O. Box 3707, Seattle, Wash. 98124)
- (d) Picatinny Arsenal Technical Report No. 1740, Properties of Explosives of Military Interest, Apr 1958
- (e) MIL-STD-721B, Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety
- (f) OPNAV INSTRUCTION 8020.9A, 8 Dec 1961 Safety Studies and Reviews Involving Nuclear Weapon Systems; Procedures for
- (g) BUORE ltr Re2b-JJSD:b:m S 78-1 (26) Ser 52079 of 8 Jun 1953 to NOL
- (h) Hazard Analysis I, G. S. Watson and M. R. Leadbetter, Biometrika, Vol 51, pp 175-184, Jun 1964
- (i) AFSC Design Handbook DH 1-6 System Safety, Series 1-0 General, Second Edition, 20 Jan 1969
- (j) NAVWEPS Report 8163, Explosive - System Safety, A Review of Bureau of Naval Weapons Policy (U), 1 Dec 1963
- (k) NOLC Report 666, Experimental Methods for Determining the Effectiveness of Interruption of a Fuze Explosive Train, 1 Jul 1966
- (l) Proceedings, Fourth Symposium (International) on Detonation, ACR-126, Office of Naval Research, Department of the Navy
- (m) MIL-S-23069 Safety Requirements, Minimum for Air Launched Guided Missiles, 31 Oct 1961
- (n) AFSCM 122-1, Nuclear Weapon System Safety Design Manual, Air Force Systems Command, USAF
- (o) NAVORD Report 4135, Relative Accident Probability Analysis, 1 Nov 1955
- (p) MIL-SID-331, Fuze and Fuze Components, Environmental and Performance Tests for, 10 Jan 1966
- (q) MIL-STD-882, System Safety Program for Systems and Associated Subsystems and Equipment; Requirements for, 15 Jul 1969
- (r) MIL-STD-1316 (Navy), Fuzes, Navy, Design Safety Criteria for, 16 Jun 1967
- (s) MIL-STD-785A, Reliability Program for Systems and Equipment Development and Production, 28 Mar 1969

APPENDIX A
MEASUREMENT OF UNSAFETY

A-1. Unsafey must first be defined before its measurement can be discussed. Further, it must be defined in terms which permit measurement. For this purpose the following definition will be used.

"Unsafey is the probability of experiencing the destructive forces of one's own weapon resulting from any conditions before intended launch and safe separation."

Like the accepted general definition of reliability, given in reference (a)¹ unsafey is defined as a probability associated with sets of conditions and periods of time. But unlike reliability it is not possible to define one set of conditions. The conditions are any conditions occurring during assembly, handling, transportation, storage, check-out, and launch-to-safe separation. These can be normal or abnormal conditions. A definable set of conditions, such as an accidental drop during handling, will be called a situation. This is consistent with terminology used in reference (b), the Relative Accident Probability (RAP) Analysis.

A-2. Assume that a situation has been defined and is identified as 'situation "1".' Then the probability of experiencing the destructive forces of one's own weapon (frequently hereafter called accident, to use a shorter term) associated with this situation is the probability that the weapon will experience 'situation "1"' times the probability that this experiencing of 'situation "1"' will result in an accident. The probability of experiencing 'situation "1"' will be expressed as E_1 ². The probability that an accident will result from experiencing 'situation "1"' will be expressed as P_1 . Then the probability of an accident caused by 'situation "1"' is:

$$P(A) = E_1 P_1$$

A-3. The probability of accident in 'situation "1"' is only one small part of the overall probability which is unsafey. There are many situations and each contributes a little to the overall probability. Therefore, the overall probability of accident when each term is small, is approximated by:

$$P(A) = E_1 P_1 + E_2 P_2 + E_3 P_3 + \dots + E_n P_n$$

¹MIL-STD-721B defines reliability as "the probability that an item will perform its intended function for a specified interval under stated conditions."

²In the Relative Accident Probability Analysis, (reference (b)), E is the Exposure Factor. There it was expressed as a dimensionless number which could be greater than one if there were repeated exposures to the same situation. Its expression as a probability is therefore a departure from the RAP Analysis.

A-4. The direct way to obtain a measure of P_1 is to set up the conditions of 'situation "1"' and conduct enough tests to obtain a numerical estimate. The same is true for P_2 , P_3 , and so on. Many of these probabilities will be very small. Therefore to obtain any kind of accuracy from these test measurements would require a fantastic number of tests. This is the reason that a numerical measure of safety has been considered impractical.

A-5. Occasionally safety failure rates are quoted for certain weapons. This seems to contradict what has been said. On the other hand, when these quoted safety failure rates are considered carefully they will be found to apply to specific situations. Muzzle bursts of gun or mortar projectiles are the most common when it comes to quoted accident rates. In these cases the situation is gun or mortar firing. The probability of encountering the situation is normal. So the accident rate quoted is a measure of P_1 where in this case 'situation "1"' is projectile firing. To say that this estimate of P_1 is the full measure of unsafety as defined above is incorrect. The fused projectiles encounter many other situations which contribute to the probability of accident. But experience shows that the firing situation is the greatest contributor to unsafety and that a number obtained in this situation is a pretty substantial part of the probability which is unsafety.

A-6. The fact that one or more specific situations contribute predominantly to the unsafety of certain weapons is indication that there is some hope of obtaining approximate measures of unsafety for these weapons before accidents in use take their toll. At least there is a reasonable number of sets of conditions. Perhaps one or two situations are all that need be considered. If either of these is a normal situation, the problem is difficult because a large number of tests would be required to obtain a measure of a small probability, P . If the situation is abnormal, a much larger value of P could be acceptable and the number of tests could be reasonable. For example, if 1×10^{-6} is an acceptable value for $P(A)_1$ and 'situation "1"' is a normal situation where $E_1 = 1.0$, then the acceptable value of P_1 is 1×10^{-6} . But if 'situation "1"' is abnormal with $E = 1 \times 10^{-2}$, then a value of 1×10^{-2} for P_1 is acceptable. This would not require an excessive number of tests. Is there some way the conditions of a normal situation could be related to the conditions of an abnormal situation so that the measure of P obtained in tests at the abnormal levels could be used to predict the value of P at the normal levels? This question cannot be answered here. The answer undoubtedly depends on the nature of the environments which make up the conditions of the situation. It depends on whether or not these environments can be scaled for test purposes. It appears to be a fruitful area for study in the search for means for obtaining measurements of unsafety.

A-7. The probability of encountering a situation must come from experience. The best estimate of the chance of dropping a weapon during a moving operation is obtained by consulting the records

to find out what fraction of weapons were dropped during the operation. The probability that the weapon will be engulfed in a fire is best obtained from the records of fires related to total numbers of weapons. Extracting such information from the records is a problem. Data banks of accident statistics have been set up by various agencies. But each has its special purpose and it is not possible to obtain like statistics from all. Consequently the lack of central accident data storage and retrieval system is a great handicap to obtaining good estimates of the probability of encountering accident situations.

A-8. The definition of unsafety used in this report refers to the destructive forces of one's own weapon. This is important as a guide to how much safety is needed in particular weapons. A bore burst of a mortar projectile is a serious accident. It frequently kills the entire gun crew. But isn't detonation of a stockpile one megaton nuclear weapon a more disastrous accident? The consequences of an accident cannot be independent of the needed safety. The design and control of nuclear weapons must provide them with more safety than the mortar projectile. The probability of experiencing the destructive effects of our own nuclear weapons must be smaller than that of our own small conventional weapons.

A-9. When the safety needed is related to the destructive potential of a weapon a cost factor is introduced.³ The purpose of this factor is to weight the importance of safety provisions according to the consequences of accidents. A large accident hurts more than a small one. So greater importance must be attached to prevention of large accidents than small ones. This is logical. The same logic applies to anything involving risks or gains and losses. Military information is classified according to the damage which would result from its divulgence. The top secret document must be guarded more closely than the confidential document. In the same manner, the provisions to prevent large accidents, whether they be design features or mandatory procedures, must be more effective than those preventing small accidents.

A-10. If $P(A)$ is the probability that the weapon will encounter and be involved in an accident in 'situation "1"', then the expected cost of accident per weapon in 'situation "1"' is:

$$P(A)S_1 = E_1 P_1 S_1$$

If E_1 is small, a small expected cost per weapon results because most weapons will never encounter 'situation "1"'. For weapons which never experience 'situation "1"' the cost of accidents in 'situation "1"' will be zero. Occasionally a weapon will encounter 'situation "1"' but if P_1 is small an accident is not likely. For these weapons which experience 'situation "1"' but this does not result in an accident

³The S is the RAP Analysis Severity Factor (reference (b)). It was expressed as dollar loss per weapon due to the accident. However, any scale will do which gives proper weighting of importance of safety.

the cost of accidents in 'situation "1"' is also zero. If enough weapons encounter 'situation "1"', eventually an accident will result. This will be very costly. It is this cost averaged over all weapons which gives the expected cost per weapon. This is a reasonable approach. Compare it to flight insurance. For example, a man pays three dollars for flight insurance. If the plane crashes and he is killed, his heirs will receive one hundred fifty thousand dollars. The insurance company can afford to sell him this insurance because the planes seldom crash. The insurance company is saying there is less than one chance in fifty thousand that the plane will crash. On this basis the man should not pay a great deal to protect his family. Similarly, if a situation is very unlikely to occur, a large investment to protect the weapon, if it gets in the situation, is not warranted.

A-11. The expected cost of accidents per weapon in all situations is approximated by:

$$\sum_1^n E_1 P_1 S_1 = E_1 P_1 S_1 + E_2 P_2 S_2 + E_3 P_3 S_3 + \dots E_n P_n S_n$$

This is now a series of individual problems. Each situation must be considered individually because the conditions of each situation are unique. Also, the cost of an accident in each situation may be different. An average cost has no meaning. In one situation the cost of an accident might be very high because of a concentration of men and material. In another, men and material might be dispersed and the cost of an accident would be much less. Provisions for safety must be greater in the first situation and not based on an average of the two.

A-12. One possible way to use the weighting of cost of accident is to place an upper tolerable limit on cost of accident per situation. This upper limit should be the same for every situation. It would not make sense to accept more cost in one situation than another. The upper limit will be designated L. This gives:

$$L \geq E_1 P_1 S_1; L \geq E_2 P_2 S_2; L \geq E_3 P_3 S_3; \dots; L \geq E_n P_n S_n$$

Since L is fixed arbitrarily, and E and S are fixed by the situation, the one factor which is capable of adjustment is P. Solving for P gives

$$P_1 \leq \frac{L}{E_1 S_1}; P_2 \leq \frac{L}{E_2 S_2}; P_3 \leq \frac{L}{E_3 S_3}; \dots P_n \leq \frac{L}{E_n S_n}$$

This sets an upper limit for P for each situation. It shows that P must be made small if E and S are large. It shows that P need not be small if E and S are small.

A-13. P is the factor which can be controlled by safety devices. It is the probability of an accident when the weapon experiences the

conditions of the situation. When the conditions of the situation are known, it is usually possible to equip the weapon with safety devices for the express purpose of preventing an accident in these conditions. This is a design problem. Setting an upper limit for P shows how much effort must go into solving the design problem. When P must be very small a better safety device is required than when P can be relatively large.

A-14. Sometimes the conditions of a situation are such that there is no known way to obtain protection from safety devices. In these cases it is necessary to look for ways to avoid the situation. E is the factor which can sometimes be controlled by safety procedures. When E can be made small, a larger P is tolerable. Safety precautions and warnings are standard practice with weapons. They are intended to reduce exposure of the weapon to such things as fire, rough handling, and careless drops. The problem with precautions and warnings is that when they become too numerous the likelihood of strict compliance with each becomes less. Even though each precaution is issued with good intent, it may have the effect of reducing the importance attached to other precautions. A means for identifying the most important precautions is needed. The relation of P to E, S, and the arbitrary number L offers this means. When the satisfactory reduction of P by the design of safety devices is not possible it is important to search for means to reduce E. Reducing E in situations where P is acceptably small is desirable too as long as it does not divert from the importance of precautions or procedures needed to compensate for too large a P.

A-15. Considering probability of accident on a per weapon basis or average cost of accident on a per weapon basis is not entirely satisfactory. Some weapons are used in much greater quantities than others. Unless these weapons are safer they contribute more accidents. They may or may not contribute more to cost of accidents depending on how costly each accident is. However, this does raise the question of whether or not weapons used in great quantities need to be safer than weapons used in small quantities.

A-16. Since the expected cost of accidents per weapon in all situations is,

$$\sum_1^n E_i P_i S_i$$

the cost of accidents for N_a weapons is,

$$N_a \sum_1^n E_i P_i S_i$$

Now if an upper tolerable limit, L, is placed on cost of accidents per situation with all weapon a's, and N_a is the number of weapon a's,

$$L \geq N_{a1} E_1 P_1 S_1; L \geq N_{a2} E_2 P_2 S_2; L \geq N_{a3} E_3 P_3 S_3; \dots; L \geq N_{an} E_n P_n S_n$$

solving for P gives

$$P_1 \leq \frac{L}{N_a E_1 S_1}; P_2 \leq \frac{L}{N_a E_2 S_2}; P_3 \leq \frac{L}{N_a E_3 S_3}; \dots P_n \leq \frac{L}{N_a E_n S_n}$$

It is apparent that the larger N is the smaller P must be.

A-17. Introducing a N factor for number of weapons creates new problems. If the N factor is to influence the tolerable size of P, it must be known before the safety features of the weapon are designed. To some extent it is known. Certain types of weapons are used in much greater quantities than other types. Antiaircraft ammunition was used in great quantities during World War II. Rockets were used in much smaller quantities. But since World War II there have been many new weapon developments. The large quantity weapons of the past are not the large quantity weapons of today. And today's large quantity weapons will not necessarily be the large quantity weapons of the future.

A-18. Another problem with quantities of weapons arises with the so-called interim weapons. Here it is common to decide that only a certain number of weapons will be made to fill an immediate need. Subsequent needs will be filled by a more advanced weapon to be developed. But frequently the interim weapon becomes the final weapon and the advanced weapon development is cancelled. Or the advanced weapon development is delayed and many times the originally planned numbers of the interim weapon are procured. Consequently numbers of weapons based on planning of this type are not a sound basis for decisions regarding needed safety.

A-19. The measurements described above require that data be available for determining the probabilities of encountering accident situations and the probabilities that safety features will be defeated by the conditions of the situations. These data are not available and are not easily obtained. Consequently, other approaches for obtaining a safety index have been suggested. Reference (c) is the final report of a study of safety measurement concepts. It discusses a probabilistic approach, two weighted factors approaches (one for ordnance components and one for all variables) and a checklist rating method. The probabilistic approach would be the most accurate, and therefore the most desirable method for quantifying safety but it is subject to the difficulties described above; i.e. data not available are needed. The weighted factors approach is a less exact method because the weighted factors are in essence approximations of true probabilities. The checklist rating method is the least accurate and depends on opinions and judgment which may vary considerably between individuals.

A-20. The dilemma in safety measurement is whether to shoot for a probabilistic method which can bear fruit only if an adequate bank of safety technical data becomes available, or settle for a checklist rating method which includes the disadvantages of personal bias, non-repeatability of results and lack of sensitivity to the effects of changes. Reference (c) suggests that these extreme choices are

not the only ones available. Intermediate between these extremes, and therefore more easily realized, is the weighted factors approach. As long as the weighted factors are obtained in a logical and repeatable manner, this may well be the best goal for the present. Furthermore it has the advantage of employing the methods of the probabilistic approach and therefore does not preclude continued effort toward the desired goal. As part of the study reported by reference (c), a phase-state model was developed which can depict success states, hazard states, and hazard state paths for weapons or components. Either true probabilistic numerics or weighted factors numerics can be applied to the model. Although this model needs further development, it is a type of model which adapts equally well to the present and the hoped for applicable safety statistics of the future. Whether or not a truly probabilistic approach can ever be achieved will depend on the effort required to obtain valid safety data. If the present consensus that these data are lacking is more a case that the data are not now retrievable, there is hope that increased interest will bring data to light from the hidden depths of uncoordinated files. In this case the costs might not be prohibitive. But if the data simply do not exist and can be obtained only by many extensive test programs, the cost of obtaining a complete data bank may be prohibitive.

A-21. To be most useful, safety should be expressed as a probability. Measurement of safety is then a matter of obtaining a measure of this probability. This is difficult because the conditions in which safety is required are so numerous, which leads to the consensus that safety data are lacking. Steps which might help to reduce the problem to manageable size are:

a. Advance identification of one or two situations as the predominant contributors to unsafety.

b. Determination of means to scale the conditions of normal situations to abnormal conditions to permit fewer tests.

c. Advancing methods for estimating failure probabilities (weighted factors) without conducting extensive testing.

A-22. How much safety is needed depends on the cost of unsafety. Cost is influenced by the destructive effects of the weapon and the number of weapons in circulation.

A-23. A truly probabilistic approach to safety measurement should be a goal but may be prohibited by the high cost of obtaining a complete safety data bank.

APPENDIX A

REFERENCES

- (a) MIL-STD-721B, Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety
- (b) NAVORD Report 4135, Relative Accident Probability Analysis, 1 Nov 1955
- (c) CR 68-566-1, Safety Measurement Concepts for Naval Weapon Systems, 29 Feb 1968 by S. Canale, RCA, Defense Electronic Products, Defense Communication Systems Division, Camden, New Jersey (Contract NOO:178-67-C-0036)

DISTRIBUTION

	Copies
Commanding Officer U. S. Naval Weapons Evaluation Facility Kirtland Air Force Base Albuquerque, New Mexico 87117 Technical Library	2
Commanding Officer U. S. Naval Air Development Center Johnsville, Pennsylvania 15000 Technical Library	2
Commanding Officer U. S. Naval Underwater Weapons Research and Engineering Station Newport, Rhode Island 02844 Technical Library	2
Commanding Officer Picatinny Arsenal Dover, New Jersey 07801	
Mr. W. J. Ryan (SMUPA-DK)	1
Mr. R. Nitzsche (SMUPA-DF6)	1
Mr. B. Frey (SMUPA-LW2)	1
Mr. R. J. DeKleine (SMUPA-ND7)	1
Mr. R. E. Todd (SMUPA-ND)	1
Mr. R. A. Hogan (SMUPA-ND)	1
Mr. W. F. Larsen (SMUPA-ND)	1
Technical Library	2
Commanding General U. S. Army Munitions Command Dover, New Jersey 07801 AMSMU-RE-F	2
The Franklin Institute Benjamin Franklin Parkway Philadelphia, Pennsylvania 19103 Technical Library	2
Mr. Gunther Cohn	1
Chief of Naval Material Strategic Systems Project Office Washington, D. C. 20360	
SP-2720	1
SP-2721	1
SP-2731	1
SP-2012	1
SP-2730	1

NOLTR 70-94

DISTRIBUTION

	Copies
Director Defense Atomic Support Agency Washington, D. C. 20301	2
NASA Scientific and Technical Information Facility P. O. Box 5700 Bethesda, Maryland 20546	1
R. H. Stresau Laboratory Star Route Spooner, Wisconsin 54081	1
Department of the Army Harry Diamond Laboratories Washington, D. C. 20438	
Att: AMXDO-TI (Dr. B. Altmann)	1
AMXDO-ED (R. S. Hoff)	1
AMXDO-DAB (D. L. Overman)	1
AMXDO-RD (Mr. VanTrump)	1
AMXDO-TD (Dr. Apstein)	1
Commanding Officer Edgewood Arsenal, Maryland 21040	
SMUEA-WGM (A. S. Berlin)	1
SMUEA-WDEL	1
Commanding Officer Frankford Arsenal Philadelphia, Pennsylvania 19137	
SMUFA J6100 (B. Nabreski)	1
SMUFA J6200 (C. McKnight)	1
Technical Library	2
Armed Services Explosives Safety Board Department of Defense 5616 Columbia Pike Arlington, Virginia 22204	2
Director Applied Physics Laboratory John Hopkins University 8621 Georgia Ave Silver Spring, Maryland 20910	2

NOLTR 70-94

DISTRIBUTION

	Copies
Assistant Chief of Naval Operations (Op-98) Room BD778 Pentagon Washington, D. C. 20350 Attn: LCDR D. J. O'Toole, USN	1
Sandia Corporation Albuquerque, New Mexico 87115 Technical Library	2
C. Winters	1
S. Love	1
E. E. Ives	1
Sandia Corporation Livermore, California 94550 Technical Library	2
A. D. Ford	1
Superintendent Naval Post Graduate School Monterey, California 93940	1
NASA Scientific and Technical Information Facility P. O. Box 33 College Park, Maryland 20740	1
Sylvania Electric Products, Inc. 63 Second Avenue Waltham, Massachusetts 02154 Mr. Paul E. Radtke	2
Program Manager, System Safety Analysis	
Director Naval Research Laboratory Washington, D. C. 20390 Technical Information Section	2
NASA Manned Spacecraft Center P. O. Box 1537 Houston, Texas 77001 Library	2

DISTRIBUTION

	Copies
Commander Air Force Armament Laboratory Eglin Air Force Base, Florida 32542	
ATWB	1
ADFC	1
Library	2
Commander Naval Safety Center Naval Air Station Norfolk, Virginia 23511	1
Test and Evaluation Coordinator Naval Air Test Center Patuxent River, Maryland 20670	1
Defense Documentation Center Cameron Station Alexandria, Virginia 22314	20
Office of Naval Research Washington, D. C. 20360 Code ONR-460	2
Commanding Officer Naval Ordnance Station Indian Head, Maryland 20640 Attn: Code FS6	1
Commanding Officer Hill Air Force Base Ogden, Utah 84401 Attn OONECB	1

UNCLASSIFIED

Security Classification

DOCUMENT CONTROL DATA - R & D

See entry classification of title, body, of abstract and indexing annotation - to be entered when the overall report is classified.

1. ORIGINATOR'S ACTIVITY (Corporate author) U. S. Naval Ordnance Laboratory White Oak, Silver Spring, Maryland		2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	
		2b. GROUP NONE	
3. REPORT TITLE FUZE SAFETY CONCEPTS			
4. DESCRIPTIVE NOTES (Type of report and inclusive dates)			
5. AUTHOR(S) (First name, middle initial, last name) Allen M. Corbin			
6. REPORT DATE 18 May 1970		7a. TOTAL NO. OF PAGES 89	7b. NO. OF REFS 22
8a. CONTRACT OR GRANT NO.		8b. ORIGINATOR'S REPORT NUMBER(S) NOLTR 70-94	
b. PROJECT NO. A532-5323/292-5/0245-0000-03 Work Unit A53233A-2		9c. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)	
10. DISTRIBUTION STATEMENT Each transmittal of this document outside the agencies of the U. S. Government must have prior approval of NOL.			
11. SUPPLEMENTARY NOTES		12. SPONSORING MILITARY ACTIVITY Naval Air Systems Command Washington, D. C. 20360	
13. ABSTRACT This report discusses the achievement of better weapon and fuze safety by employing methods and techniques used in formal reliability programs. Some of the safety counterparts of the reliability tools are less developed. Most notable is safety's counterpart of reliability's environmental criteria. The potential hazards analysis is proposed as a technique for improving this situation by developing a list of abnormal environments. This gives the designer engineering goals for his safety components. Other aspects of the formal design safety program which are discussed are the series safety redundancy, safety analyses, tests, design reviews, and failure reporting and corrective actions.			

UNCLASSIFIED

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Safety Safety Design Reliability Safety-Reliability Balance Safety System Safety Program Conceptual Safety Safety Analysis Safety Objectives RAP Analysis Fault Tree Analysis Potential Hazards Analysis						