NAWCWD TP 8504

DESIGN METHODOLOGY FOR SAFE AND ARM DEVICES

by

Friedrich Sauerlaender
Ordnance Systems Division

AUGUST 2001

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

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 2001	Summary

4. TITLE AND SUBTITLE

Design Methodology for Safe and Arm Devices (U)

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)

Friedrich Sauerlaender

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

NAWCWD TP 8504

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

Steven E. Fowler, Code 478000D
Naval Air Warfare Center Weapons Division
1 Administrations Circle
China Lake, CA 93555-6100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. **ABSTRACT** (Maximum 200 words)

(U) This document provides some design process guidance, to both inexperienced and veteran fuze developers, for the most critical part of a fuze, the safe and arm (S&A) device. It, along with its appendixes, provides a basic overview and some general guidance for the most important aspects in this area from a U.S. Navy perspective.

(U) Included is information about the elements to S&A safety, the Navy's fuze development process, and the approach and process for a successful S&A design.

14. SUBJECT TERMS

Weapon Systems Explosives Safety Review Board (WSESRB), Safety and Arming (S&A) Device, Arming Environment, Signal Processing, Weapon Specification, Fuze Development Specification, Program Requirements Review (PRR), Preliminary Design Review (PDR), Critical Design Review (CDR), Safety and Suitability for Service (S^3), Adverse Environment, Standardization Agreement (STANAG), Military Standard (MIL-STD), Department of Defense Standard (DOD-STD), Credible Accidents, Electromagnetic Interference, (Preliminary) Hazards Analysis (P)HA, Fault Tree Analysis (FTA), Failure Mode Effects (and Criticality) Analysis (FME[C]A), Integrated Design Analysis (IDA), Sneak Circuit Analysis (SCA), Preliminary FTA, Unique Environment, Electronic Safe-Arm Device (ESAD), Mean Time Between Failures, Failure Rate, Probability of Failure.

15. NUMBER OF PAGES

76

16. PRICE CODE

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

Naval Air Warfare Center Weapons Division

FOREWORD

This document provides some design process guidance, to both inexperienced and veteran fuze developers, for the most critical part of a fuze, the safe and arm (S&A) device. It, along with its appendixes, provides a basic overview and some general guidance for the most important aspects in this area from a U.S. Navy perspective. Included is information about the elements to S&A safety, the Navy's fuze development process, and the approach and process for a successful S&A design.

This effort was sponsored by the Ordnance Systems Division of the Naval Air Warfare Center Weapons Division, China Lake, California.

Approved by
S. O'NEIL, *Head*
Weapons/Targets Department
24 August 2001

Under authority of
C. H. JOHNSTON
RDML, U.S. Navy
Commander

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

NAWCWD Technical Publication 8504

Published by..... Technical Information Division
Collation..... Cover, 39 leaves
First printing..... 80 copies

CONTENTS

ACKNOWLEDGMENTS

The author wishes to acknowledge the individuals from both the Ordnance Systems and System Safety Engineering Divisions of the Naval Air Warfare Center Weapons Division, China Lake, California, who contributed to this document by sharing their thoughts and expertise or by supplying the documents and tools needed in its preparation. In addition, special thanks go to the following:

1. Steven Fowler, who made this document possible by hosting the author, a German exchange scientist, and by providing valuable input and comments.
2. Jack Waller and David Riggs, who gave the author an understanding of the U.S. Navy's fuze development process and commented on the end product.
3. Ken Chirkis, who provided valuable guidance concerning the general aspects of the safety analyses.

Finally, much gratitude goes to Erhard Knebel and Werner Gehrke from the Fuze Group *WF I 5* at the *Bundesamt für Wehrtechnik und Beschaffung* in Germany. As Mr. Sauerlaender's mentors when he initially became involved in fuze safety, they provided the basic skills and general concepts that form the foundation for this document.

INTRODUCTION

Fuze development is a very complex process. For example, not only must the fuze initiate the warhead at the appropriate time (reliability considerations), the weapon must be safe to store, transport, and handle prior to that point (safety considerations). The safety criterion, as derived from MIL-STD 1316 (U.S.) (Reference 1) and STANAG 4187 (North Atlantic Treaty Organization [NATO]) (Reference 2), is as follows:

> The risk of premature arming must not exceed one in a million (10^{-6}).

In other words, throughout its lifetime, the fuze must be 99.9999% safe—an accomplishment that is quite difficult to achieve and even harder to substantiate.

Because safety is of vital importance and the risk standards are so stringent, numerous regulations, guidelines, and standards exist, all of which must be followed. The Weapon Systems Explosives Safety Review Board (WSESRB) of the U.S. Navy (the Army and the Air Force have similar review boards) examines each design closely to ensure that it meets all criteria. For example, does it comply with the regulations, standards, and guidelines? Is all the necessary documentation available? Were all the analyses performed and were the appropriate results achieved? In effect, is it safe for U.S. Navy use?

As such, to an inexperienced fuze developer, the process is difficult to understand; the regulations are quite complex; and, in general, the most appropriate starting point is difficult to determine.

This document, in conjunction with Appendixes A through I, provides some design process guidance, to both inexperienced and veteran fuze developers, for the most critical part of a fuze, the safe and arm (S&A) device. The reader should keep in mind that this publication is not, as no single document can be, a complete guide to achieve the requisite safety. For example, it cannot replace a knowledge and understanding of all the important regulations and helpful guidance documents. However, it does provide a basic overview and some general guidance for the most important aspects from a U.S. Navy perspective.

ELEMENTS TO S&A SAFETY

The S&A device is the most important weapon component in achieving warhead safety. Figures 1 and 2 show the two key elements of the design's safety—material and signal processing, respectively. These are further subdivided to provide additional details. Because every part is essential and interacts with the others, the design becomes very complex.

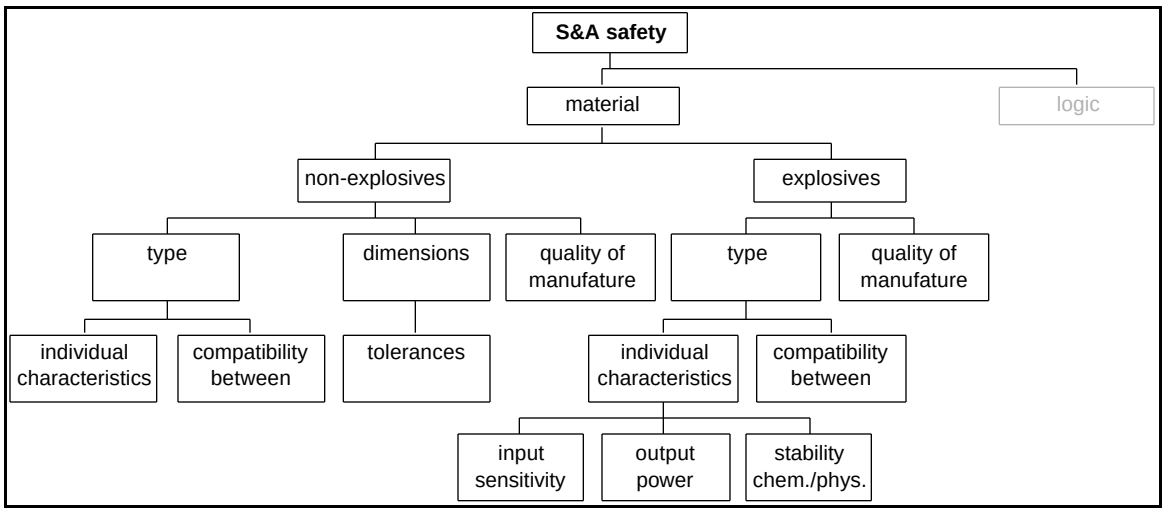

FIGURE 1. Material Elements to Safety.

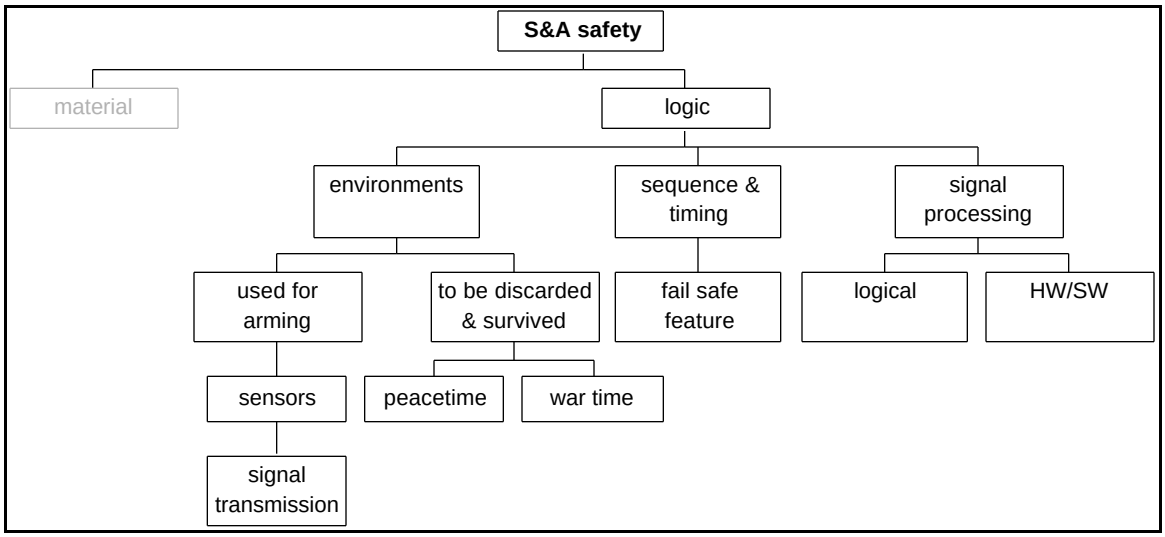

FIGURE 2. Logic Elements to Safety.

Most of the subelements for the material aspect of the S&A device safety (Figure 1) are self-explanatory. However, pertinent information about some of them, as well as for all the items of the signal processing portion (Figure 2), is provided in this document and its appendixes.

Figure 1 pertains only to those items that relate to the material characteristics and dimensions, such as the choice of material and electronic parts. Figure 2 shows the three major contributors to the logic element of the S&A device safety:

1. The structure and inherent logic of S&A device, which is considered to be "signal processing."
2. The environments, which are the inputs to the S&A device. (Some of these are chosen as arming environments—an arming environment is a condition or a set of conditions that indicates the proper launch of a munition.)

3. The required sequence and timing of these inputs, the subelement that is the basis for the subsequent "processing" of the input in the S&A device.

For example, an event like acceleration (input) is "processed" by the inherent logic of the S&A design to result in proper arming (output). First, this event is compared to the expected arming environments and their levels and then is checked for the appropriate sequence and timing. If the event is verified as the correct environment, the device reacts appropriately. This action may occur electronically or mechanically. A lock removed by a setback weight against a spring is considered (mechanical) signal processing of the acceleration. In other words, the logic segment contains all the design features, such as layout, sequencing, and type of sensor (acceleration or piezoelectric as opposed to mechanical setback), that are not material but primarily logic characteristics.

NAVY FUZE DEVELOPMENT PROCESS

Figures 3 and 4 are flowcharts of the Navy fuze development process, which generally begins with the weapon specification. The fuze requirements are then derived from this document to create a Fuze Development Specification, which is reviewed and, if satisfactory, approved at a Program Requirements Review (PRR).

The design process starts with the draft of several concepts. Then, by conducting trade-off studies and comparing the findings, cognizant personnel can choose the most promising concept, which must be approved at a Preliminary Design Review (PDR). The design is then introduced to the WSESRB in a courtesy briefing to inform the members and to give them an opportunity to express any concerns at the onset of the development process.

The next step is to build prototypes and test them in the laboratory. Any problems must be corrected and the units retested.

At this point, the design evaluation units are built and subjected to an extended examination in design evaluation tests and ordnance system tests. If necessary, the design is further modified and tested to demonstrate that it fulfills the requirements. The design and the results must be approved at a Critical Design Review (CDR).

Next, the qualification units are built and the design is formally qualified. At this point, it is approved by the WSESRB for operational testing in which the user evaluates the entire weapon system. After any necessary changes, the last step is the final WSESRB approval of the Safety and Suitability for Service (S^3) for the fuze and the weapon system.

During the process, the technical data package must be maintained and updated throughout each step. This effort requires a strict configuration management that incorporates all documents, such as specifications, drawings, and analyses.

In addition, the device’s ultimate manufacturing method should be considered during the development phase. For example, if the fuze is simple to manufacture and assembly can occur only in a safe state, the manufacturing costs will be much lower than those for a design that requires complicated processes, safety precautions, and multiple checks during and after assembly.

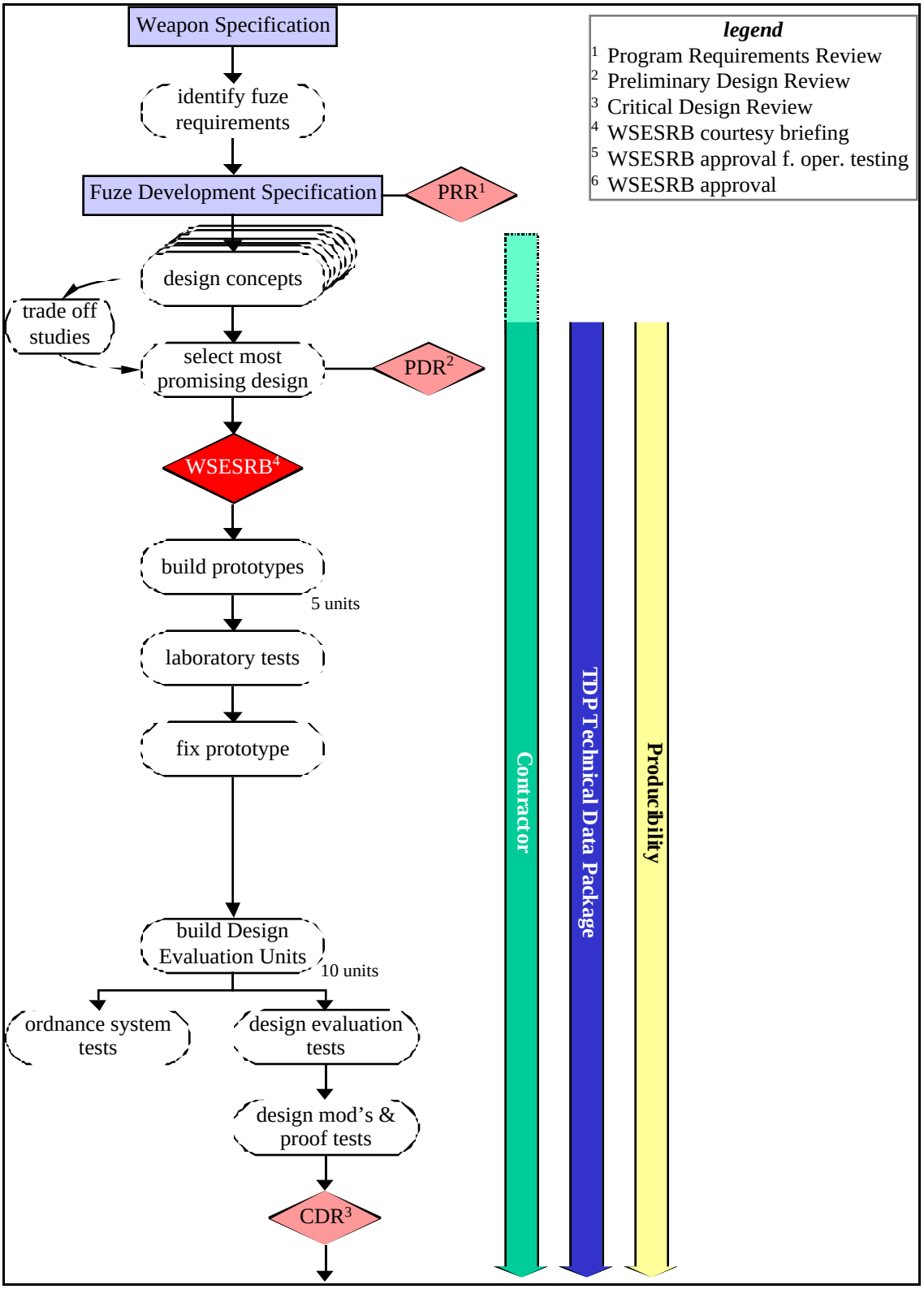

FIGURE 3. Navy Fuze Design Process, Part 1.

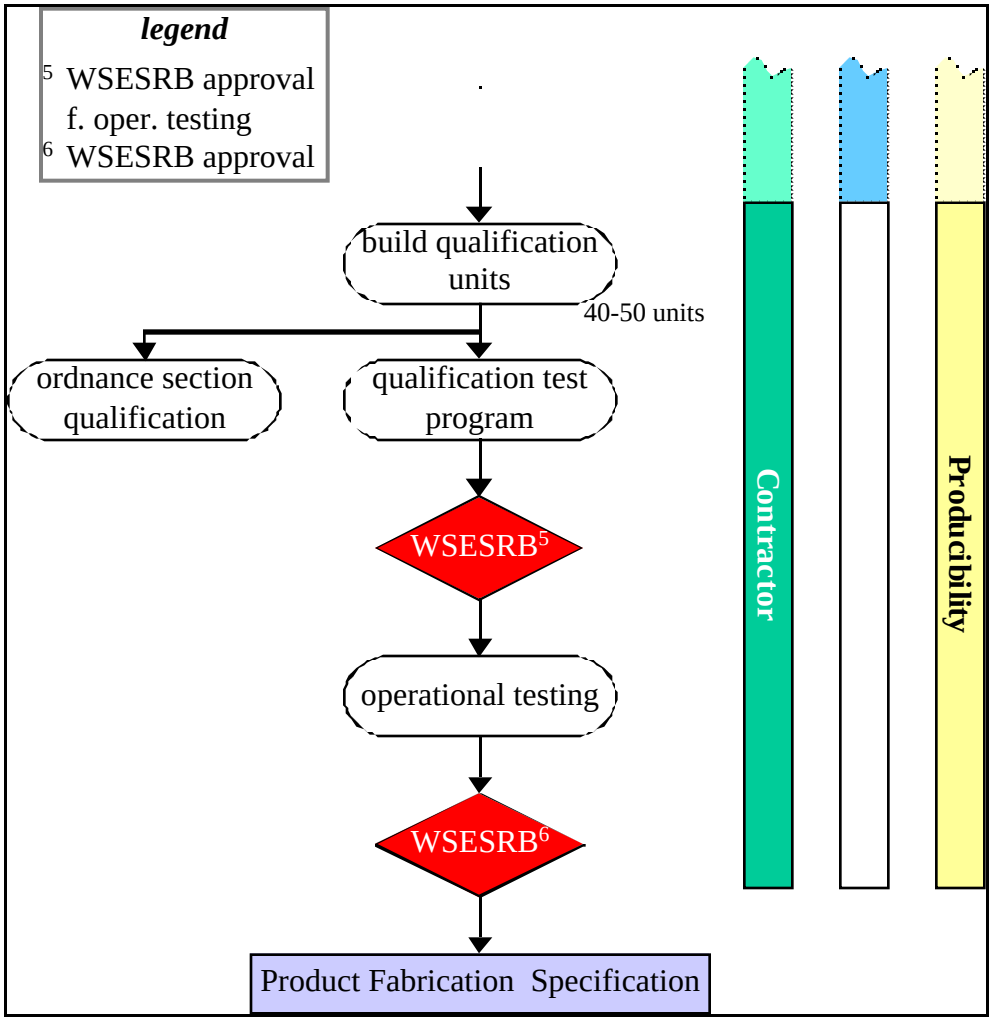

FIGURE 4. Navy Fuze Design Process, Part 2.

S&A DEVICE DESIGN APPROACH

Six major fields influence the S&A device's design (Figure 5). They include (1) fuze and S&A requirements, (2) interfaces, (3) adverse environments, (4) arming environments, (5) analyses, and (6) testing. Many of these are derived from the weapon specification, which contains the information about the actual weapon, such as the interfaces, the user requirements (function), and the weapon's life cycle.

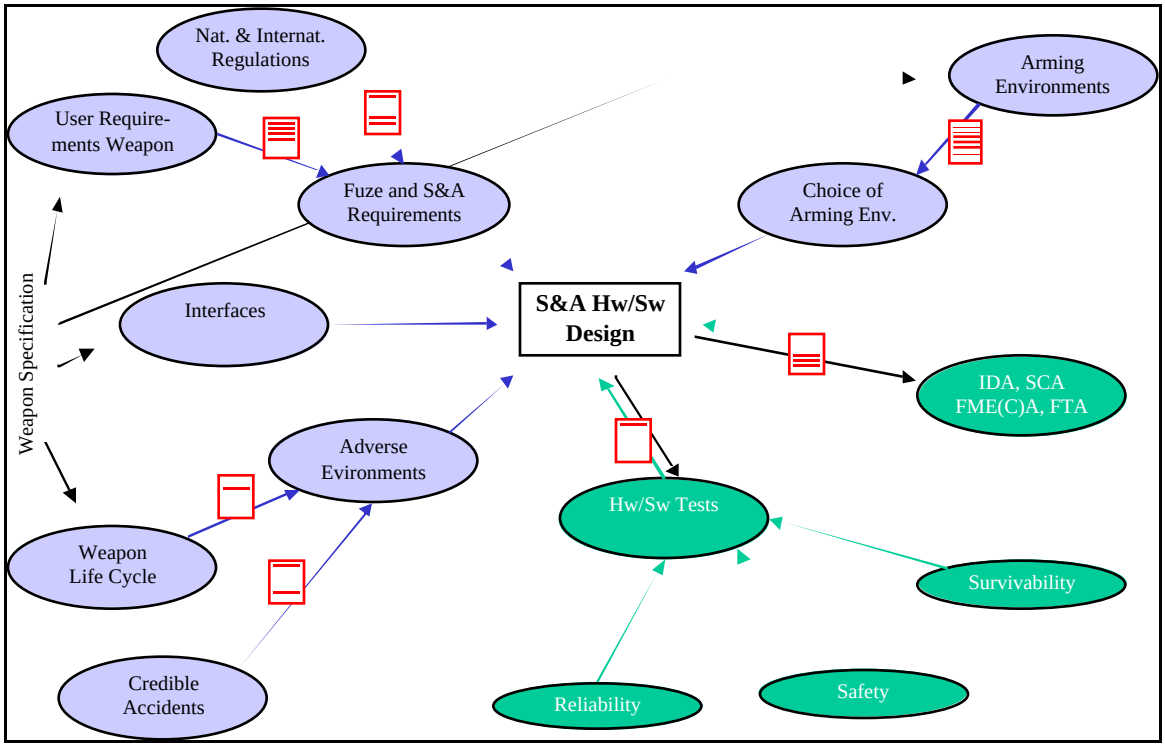

FIGURE 5. Main Areas of Influence on S&A Device Design and Checklists (Red).

The first field incorporates the user requirements and the national and international regulations, which are merged into the fuze and S&A device requirements. To avoid expensive errors caused by overlooking user requirements, it is important to devote great care in extracting them from the weapon specifications because, in many cases, some are not explicitly stated. Appendix C provides a checklist of the requirements in the weapon specification and includes a list of typical areas that are significant.

In addition, the national and international regulations* are important. A list of the most pertinent documents for S&A device development is contained in Appendixes A and B. Generally, many of the necessary documents, including all of the aforementioned regulations and other documents, should be named in the weapon specification or in the contract. Thus, this list is helpful if one must develop a fuze development specification.

At times, the user requirements may contradict some of the regulations, a situation that should be discussed with the customer. Keep in mind that these regulations, which are based on many years of experience, are rooted in legitimate safety concerns. Therefore, the designer should not discard them without prudent deliberation. A very careful examination of the consequences of adopting any compromises or of dropping requirements must be conducted. After the designer has informed the user of the possible negative effects, the decision of how to proceed should be made together. That decision and its justification must be documented for the WSESRB. Another reason for this audit trail is that, many times, those involved are unable to recall why specific choices were made if questions arise later.

* Standards such as Department of Defense Standards (DOD-STDs) (U.S. national documents), Standardization Agreements (STANAGs) (NATO standards, which are often used in combination with additional documents, such as Allied Ordnance Publications [AOPs]), and other documents, such as the Military Handbook (MIL-HDBK) (a U.S. national document).

The second major field of influence entails all the interfaces between the fuze (S&A device) and the weapon. These are also included in the weapon specification. Besides the obvious mechanical and electrical interfaces, explosive, chemical, thermal, and other types must be considered.

The third field consists of the adverse environments that the weapon must withstand. While these conditions are partially derived from the weapon life cycle, as described in the weapons specification, they also include credible accidents. Either, the S&A device must survive all adverse phenomena fully functional and safe or it must fail in a safe state, depending on the weapon specification and the regulations. Appendix D provides some assistance in creating the list of adverse environments.

The fourth field of influence is that of the arming environments, phenomena that are utilized to arm the device. The decision as to which ones (at least two or more) to use is one of the most important during the design. In fact, the fuze community understands that the right choice of arming environments is the most significant contributor to S&A device safety. This decision also affects several other fields, such as the costs, the difficulty and extent of the required analyses, and the manufacturing. Appendix E provides some guidance for this process.

At best, the arming environments should be unique, which means that they occur only during or after launch. Unfortunately, very few usable environments are unique. So, the selected environments must be absolutely discernable from *any* other occurrence during the weapon life cycle, for example, in terms of strength and/or duration. The more discernable the environments are and the more directly they can be applied, the simpler and more cost effective the design will be. At least one of the arming environments should occur after the proper launch.

As mentioned, the arming environment should be used as directly as possible. For example, an acceleration should be applied directly to remove a lock mechanically, in contrast to the following to remove the lock:

1. Sensing and converting it into electrical energy, for example, by a piezoelectric accelerometer.
2. Transferring it by a wire to an amplifier.
3. Amplifying it.
4. Transferring it by a wire to the signal processing.
5. Processing the signal (safety check).
6. Amplifying it again.
7. Transferring it by a wire to a “converter.”
8. Converting it from electrical back to mechanical energy, for example, via a motor or pyrotechnic device.

Every transformation of energy and energy transfer increases the possibility of errors and necessitates extra parts, each of which my cause additional errors.

To achieve the extremely low risk acceptable for safety-critical errors (10^{-6} for each fuze), it is wise to use as few parts as reasonably possible. In addition, most modern weapon systems necessitate numerous electrical signals and electromagnetic interference occurs in almost every scenario. For example, because of some kind of failure, even outside the S&A device, an electrical signal could be fed into the system that is sufficiently similar to remove the safety feature. The direct application of the arming environments also helps to keep the design simple.

The aforementioned fields merge into the fuze development specification, the document that provides the S&A device requirements. The final two—(5) analyses, such as the (Preliminary) Hazards Analysis or (P)HA (this effort includes both the Preliminary Hazards Analysis (PHA) and the Hazards Analysis); Fault Tree Analysis or FTA; Failure Mode, Effects (and Criticality) Analysis or FME(C)A; Integrated Design Analysis or IDA; and Sneak Circuit Analysis or SCA, and (6) testing—also directly influence the design. During development, many analyses and tests are performed to determine if the design behaves as expected and meets the requirements. The results indicate if the design needs improvement.

Figure 6 shows the manner in which a S&A device design is derived from the weapon specification and the national and international regulations. The first step is to extract the necessary information from the weapon specification, e.g., the weapon life cycle and adverse environments, possible arming environments, the interfaces (mechanical, electrical, explosive, thermal, and others), and the basic fuzing and S&A device requirements. The next step, before beginning the development process, is to select the arming environments (Appendix E) because that choice must determine the design, not vice versa.

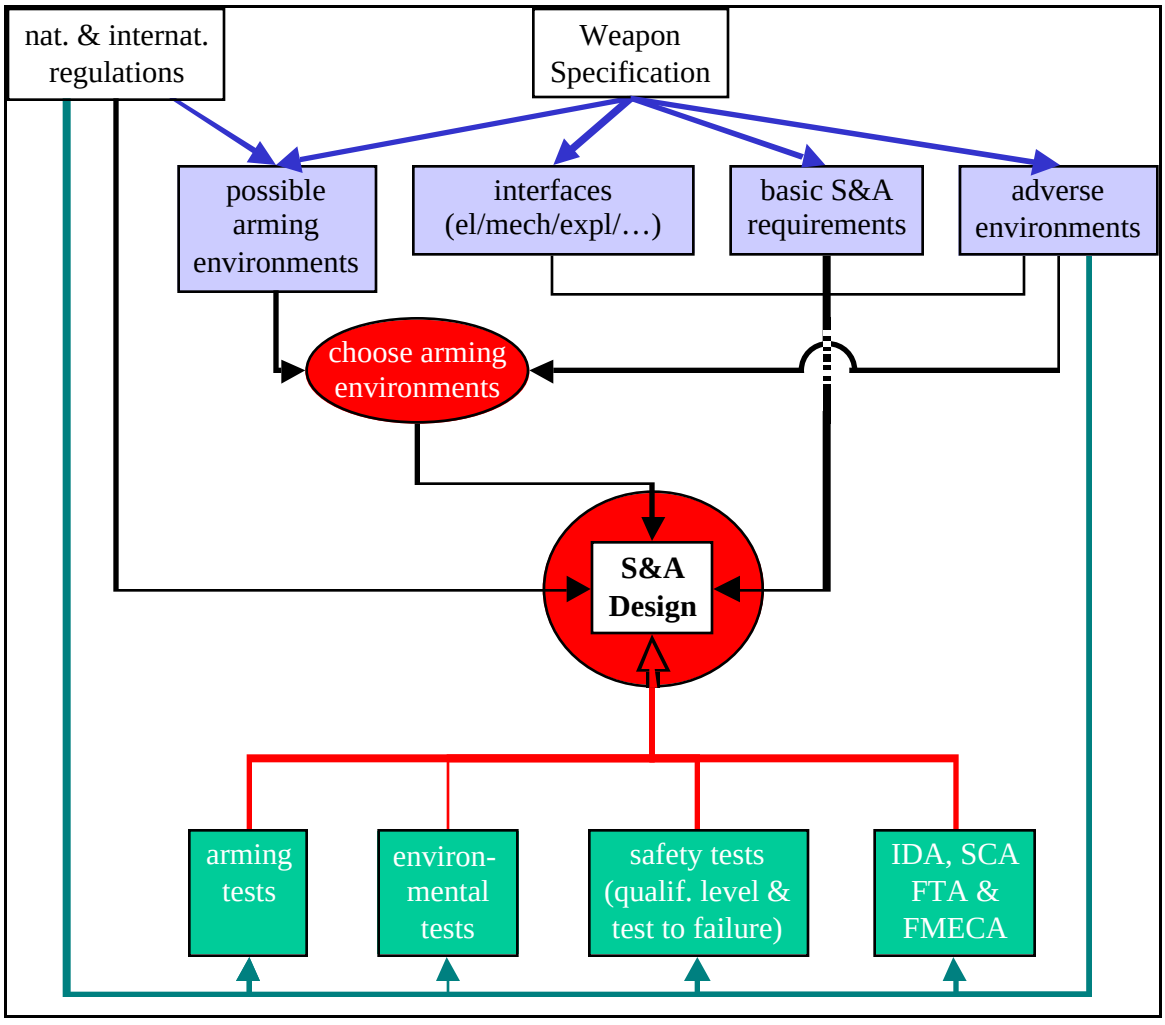

FIGURE 6. Weapon Specification and Requirements (the Starting Points for Every S&A Device Design).

Then, based on the identified requirements (interfaces, weapon life cycle, and others) and the chosen arming environments, the design process for the S&A device hardware and software begins. First, several concepts are devised, analyzed via trade-off studies, and compared; and the most promising design is chosen. Then, to achieve the acceptable level of safety and to ascertain the device's reliability in meeting the requirements, the design is subjected to various types of analyses and tests. The details of this process are explained in the *S&A Device Design Process* section.

Important factors in choosing a design concept for further development are the actual arming environments, the directness of application of the arming environments, the simplicity of the design, the development risk, and the ease of manufacturing. Of course, all safety regulations and user requirements must be met.

S&A DEVICE DESIGN PROCESS

Figure 7 shows the order of the requisite steps for a S&A device design. Keep in mind that this process is not as linear as that shown. In fact, much of the work will be done concurrently, depending on the number of people involved and the evaluation tools available. The order of the steps in Figure 7 applies to the final checks on the specific subjects, all of which need to be considered throughout the design process. For example, if the designer fails to incorporate reliability from the beginning, he will most likely encounter an almost impenetrable barrier after spending hours on the design and the other analyses. In addition, acquiring preliminary results from the various analyses throughout the development helps to uncover design flaws early.

The first step is to perform a PHA, which is based on the given parameters (see upper left corner of Figure 7), such as the basic S&A device requirements, interfaces, and weapon life cycle, derived from the weapon specification and from the national and international regulations. Even the initial design must be based on a careful consideration of this framework, the results from the PHA, and other items listed in the flowchart. The design variables (see upper right corner of Figure 7), which are not only influenced by the PHA but also affect the analysis, include all the parameters that must be optimized during the design process.

As mentioned earlier, two (or more) arming environments must be chosen prior to the design process based on their availability and uniqueness. The utilized arming environments, the arming sequence and logic, the basic S&A device type, the explosive train design, the fail safe features, the materials and parts, and the internal signal processing are subject to optimization during the design process. Normally the arming environments should be the same as those chosen earlier. Yet, in rare occasions, it may be necessary to use different phenomena, which must also fulfill the safety requirements. The reasons may be improved reliability and safety through achieving a simpler design. Appendix F provides a detailed explanation and checklist for the steps shown in Figure 7.

Moreover, for every design or redesign, a preliminary FTA should be conducted. Appendix G furnishes some guidance for the FTA and the quantitative evaluation of the risks because these areas often create problems for and with the WSESRB. However, adherence to the guidelines will facilitate WSESRB review approval. The appendix also highlights the need for the preliminary FTA.

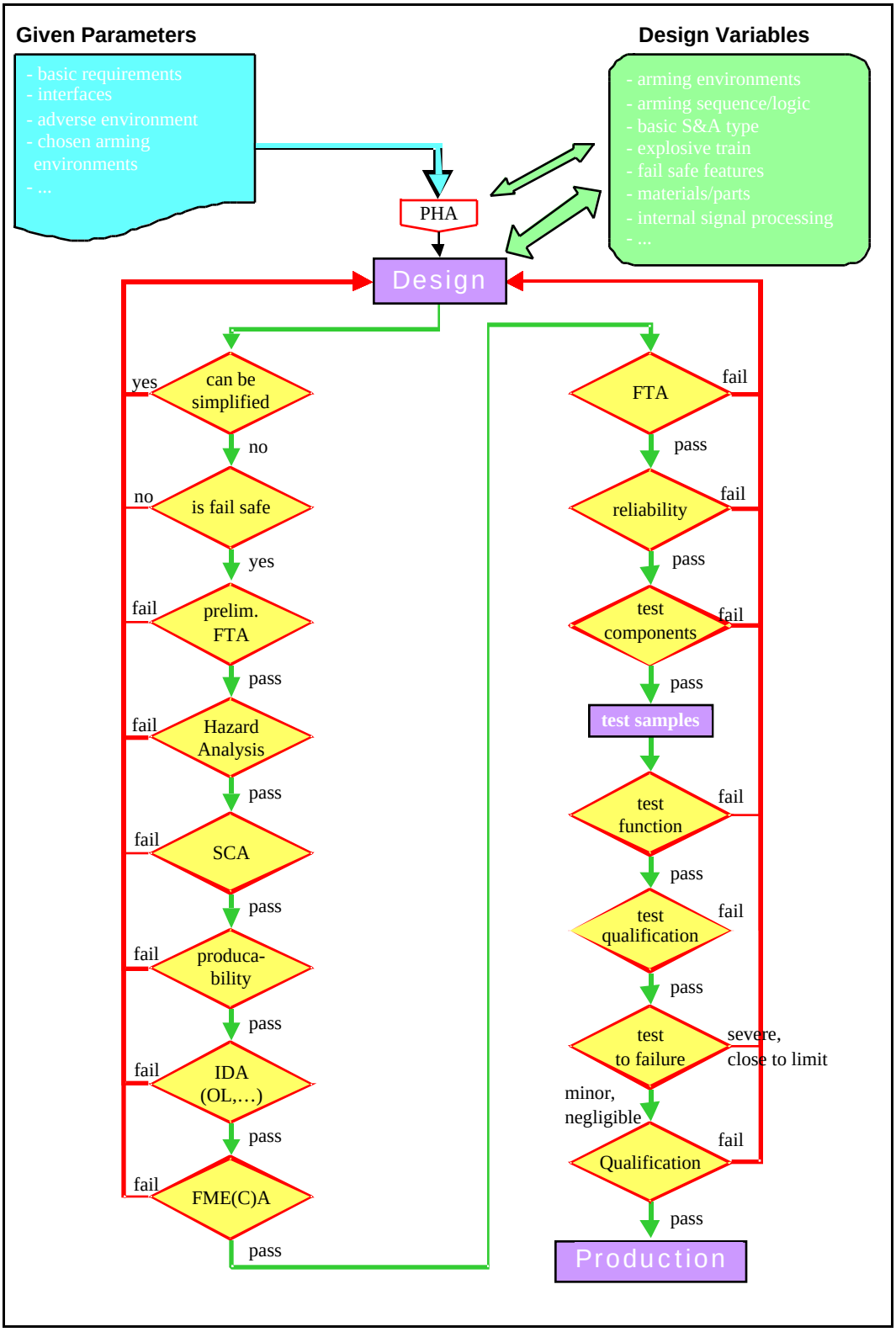

FIGURE 7. S&A Device Design Flowchart.

Appendixes H and I contain checklists for the mechanical S&A devices and ESAD, respectively—checklists that provide factors that must be considered throughout development. Obviously, this document and these lists cannot, without encompassing several volumes, rather than being a short synopsis of the subject, include all the requirements from every regulation and guideline. However, the appendixes are included to emphasize some relevant factors in effective S&A device design—elements that the U.S. Navy considers significant. As such, the intent is that the appendixes be used in conjunction with this document to provide guidance for the successful design of a S&A device.

SUMMARY

In summary, the author has provided some information and guidelines for the design of a safe S&A device. This section included the elements of S&A device safety, which incorporated both material and logic elements. He also described the Navy's fuze development process and the proper S&A device design approach. The latter included a discussion about the six major fields that influence the design. Next, the author explained the design process by supplying the requisite steps to follow in successfully achieving a safe S&A device.

In addition, in Appendixes A through I, the author offers much valuable information about the documents that pertain to S&A device development, guidelines for the compilation of the user requirements and adverse environments, as well as help in selecting the arming environments and conducting the FTA, and checklists to follow in the design process.

As mentioned, the intent is that the appendixes be used in conjunction with this document to provide both inexperienced and veteran fuze developers with some basic information to facilitate the development of safe S&A devices.

REFERENCES

1. Department of Defense. *Department of Defense Design Criteria Standard, Fuze Design, Safety Criteria for*, by Fuze Engineering Standardization Working Group. Washington, DC, DOD, 10 July 1998. (MIL-STD-1316E, publication UNCLASSIFIED.)

2. North Atlantic Treaty Organization. *Standardization Agreement 4187, Edition 3, Fuzing Systems—Safety Design Requirements*, by AC/310. Brussels, Belgium. NATO, 2 November 1999. (STANAG 4187 Edition 3, publication UNCLASSIFIED.)

NOMENCLATURE

AOP	Allied Ordnance Publications
CDR	Critical Design Review
DOD-STD	Department of Defense Standard
FME(C)A	Failure Mode, Effects (and Criticality) Analysis

FTA	Fault Tree Analysis
IDA	Integrated Design Analysis
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
NATO	North Atlantic Treaty Organization
PDR	Preliminary Design Review
PHA	Preliminary Hazards Analysis
(P)HA	(Preliminary) Hazards Analysis
PRR	Program Requirements Review
S^3	Safety and Suitability for Service
S&A	safe and arm
SCA	Sneak Circuit Analysis
STANAG	Standardization Agreement, a NATO standard
WSESRB	Weapon Systems Explosives Safety Review Board

Appendix A
U.S. NATIONAL AND MULTILATERAL DOCUMENTS

(This page intentionally left blank.)

U.S. NATIONAL AND MULTILATERAL DOCUMENTS

The reader should keep in mind that this list, which is in alphabetical order by document number, is not complete because the development of standards is an ongoing process. Moreover, it may include documents that are not applicable to a specific weapon or fuze. Because the publications are continuously updated, the editions are not provided. Therefore, the designer should ensure that he or she is using the most recent version.

AFSC DH 1-6	*Design Handbook, System Safety*
AMC-R 385-100	*Safety Manual*
DOD-STD 1463	*Evaluation of Munitions for Electromagnetic Fields, Requirements for*
DOD-STD 1795	*Lightning Protection of Aerospace Vehicles and Hardware*
DOD-STD 2167	*Software Development Standards for Military Systems*
DOD-STD 2169	*High Altitude Electromagnetic Pulse (HEMP) Environment*
ML-HDBH 217	*Reliability Prediction of Electronic Equipment*
MIL-HDBK 235	*Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment, Subsystems and Systems Part 1B*
MIL-I 23659	*Initiators, Electrical, General Design Specification*
MIL-STD 202	*Lighting Protection of Aerospace Vehicles and Hardware (Controlled Distribution)*
MIL-STD 322	*Explosive Components, Electrically Initiated, Basic Evaluation, Test for*
MIL-STD 331	*Fuze and Fuze Components, Environmental and Performance Tests for*
MIL-STD 444	*Nomenclature and Definitions in the Ammunition Area*
MIL-STD 461	*Electromagnetic Interference Characteristics, Requirements for*
MIL-STD 810	*Test Method Standard for Environmental Engineering Considerations and Laboratory Tests*
MIL-STD 882	*System Safety Program Requirements*

MIL-STD 1316	*Fuze Design, Safety Criteria for*
MIL-STD 1385	*Preclusion of Ordnance Hazards in Electromagnetic Fields, Requirement for*
MIL-STD 1455	*Dispenser and Sub-Munitions, Air Delivered, Safety Design and Safety Qualification Criteria for*
MIL-STD 1512	*Electro-Explosive Subsystems, Electrically Initiated, Design Requirements and Test Methods*
MIL-STD 1670	*Environmental Criteria and Guidelines for Air-Launched Weapons*
MIL-STD 1757	*Lightning Qualification Test Techniques for Aerospace Vehicles and Hardware*
MIL-STD 1901	*Ignition Safety Devices, Safety Design Criteria for*
MIL-STD 1911	*Hand-Emplaced Ordnance Design, Safety Criteria for*
NAVORD OD44811	*Explosive Qualification Criteria*
NAVORD OD44942	*Weapon System Safety Guidelines Handbook*
NAVSEA OP 2165	*Navy Transportation Safety Handbook for Ammunition Explosives and Related Hazardous Materials (Volumes 1 and 2)*
NAVSEA OP 30393	*Design Principles and Practices for Controlling Hazards of Electromagnetic Radiation to Ordnance (HERO Design Guide)*
NAVSEAINST 8020.5B	*Technical Requirements for Insensitive Munitions*
NAVSEANOTE 9310	*Responsibilities and Procedures for the Naval Lithium Battery Safety Program*
NUREG 4493	*Fault Tree Analysis*
RAC EPRD-95	*Reliability Assessment Center, Electronic Parts Reliability Data, 1997*
RAC NPRD-95	*Reliability Assessment Center, Non-Electronic Parts Reliability Data, 1995*
RAC NONOP-1	*Non-operational Parts Reliability Data, 1987*
ITOP 1-2-601	*Laboratory Vibration Schedules - ITOP 1-2-601*
ITOP 4-2-601	*ITOP 4-2-601 - FR/GE/UK/US Drop Test for Munitions*

Appendix B
NORTH ATLANTIC TREATY ORGANIZATION (NATO) DOCUMENTS

(This page intentionally left blank.)

NORTH ATLANTIC TREATY ORGANIZATION (NATO) DOCUMENTS

The reader should keep in mind that this list, which is in alphabetical order by document number, is not complete because the development of standards is an ongoing process. Moreover, it may include documents that are not applicable to a specific weapon or fuze. Because the documents are continuously updated, the editions are not provided. Therefore, the designer should ensure that he or she is using the most recent version.

AECP 1	*Mechanical Environmental Conditions to Which Materiel Intended for Use by NATO Forces Could Be Exposed*
AECTP 100	*Environmental Testing Guidelines on Management Planning*
AECTP 200	*Environmental Testing—Definitions of Environments*
AECTP 300	*Climatic Environmental Tests*
AECTP 400	*Mechanical Environmental Test*
AECTP 500	*Electrical Environmental Test*
AOP 07	*Manual of Tests for the Qualification of Explosive Materials for Military Use*
AOP 08	*NATO Fuse Characteristics Catalogue*
AOP 15	*Guidance on the Assessment of the Safety and Suitability for Service of Non-Nuclear Munitions for NATO Armed Forces—STANAG 4297*
AOP 16	*Fuzing Systems: Guidelines for STANAG 4187*
AOP 20	*Manual of Tests for the Safety Qualification of Fuzing Systems*
AOP 21	*Fuzing Systems: Manual of Development Characterization and Safety Test Methods and Procedures for Lead and Booster for Explosive Components*
AOP 22	*Design Criteria and Test Methods for Inductive Setting of Electronic Projectile Fuzes*
AOP 26	*NATO Catalogue of Explosives*
AOP 42	*Integrated Design Analysis for Safety Critical Systems* [Draft]

STANAG 1307	*Maximum NATO Naval Operational Electro-Magnetic Environment Produced by Radio and Radar*
STANAG 2895	*Extreme Climatic Conditions and Derived Conditions for Use in Defining Design Test Criteria for NATO Forces Materiel (UK)*
STANAG 2914	*Mechanical Environmental Conditions to Which Materiel Intended for Use by NATO Forces Could Be Exposed for AECP-1*
STANAG 2916	*NOSE Fuse Contours and Matching Projectile Cavities for Artillery and Mortar Projectiles*
STANAG 4147	*Chemical Compatibility of Ammunition Components With Explosives (Non-Nuclear Applications)*
STANAG 4157	*Fuzing Systems: Test Requirements for Assessment of Safety and Suitability for Service*
STANAG 4170	*Principles and Methodology for the Qualification of Explosive Materials for Military Use*
STANAG 4187	*Fuzing Systems—Safety Design Requirements*
STANAG 4234	*Electromagnetic Radiation (Radio Frequency) 200 kHz to 40 GHz Environment—Affecting the Design of Materiel for Use by NATO Forces*
STANAG 4235	*Electrostatic Environmental Conditions Affecting the Design of Material for Use by NATO Forces*
STANAG 4236	*Lightning Environmental Conditions Affecting the Design of Materiel for Use by NATO Forces*
STANAG 4238	*Munition Design Principles, Electrical/Electromagnetic Environments*
STANAG 4239	*Electrostatic Discharge, Munitions Test Procedures*
STANAG 4242	*Vibration Tests Methods and Severities for Munitions Carried in Tracked Vehicles—AOP 34*
STANAG 4297	*Guidance on the Assessment of the Safety and Suitability for Service of Munitions for NATO Armed Forces—AOP 15*
STANAG 4324	*Electromagnetic Radiation (Radio Frequency) Test Information To Determine the Safety and Suitability for Service of Electro-Explosive Devices and Associated Electronic Systems in Munitions and Weapons Systems*

STANAG 4325	*Environmental and Safety Tests for the Appraisal of Air-Launched Munitions*
STANAG 4326	*NATO Fuse Characteristics Data—AOP 8*
STANAG 4327	*Lightning, Munition Assessment and Test Procedures*
STANAG 4363	*Fuzing Systems—Development Testing for the Assessment of Lead and Booster Explosive Components*
STANAG 4368	*Electric and Laser Ignition Systems for Rockets and Guided Missile Motors—Design Safety Requirements*
STANAG 4369	*Design Requirements for Inductive Setting of Large Calibre Electronic Projectile Fuzes*
STANAG 4370	*Environmental Testing*
STANAG 4404	*Safety Design Requirements and Guidelines for Munition Related Safety Critical COMPUTING Systems*
STANAG 4416	*Nuclear Electromagnetic Pulse Testing of Munitions Containing Electro-Explosives Devices*
STANAG 4432	*Air-Launched Guided Munitions: Principles for Safe Design*
STANAG 4452	*Safety Assessment of Munition-Related Computing Systems*
STANAG 4497	*Hand-Emplaced Munitions (HEM), Principles for Safe Design*
STANAG 4519	*Gas Generators, Design Safety Principles and Safety and Suitability for Service Evaluation*
STANAG 4547	*Design Requirements for Inductive Setting of Medium Calibre Electronic Projectile Fuzes*
STANAG 4560	*Fuzing Systems, Characteristics of Electro-Explosive Devices*

(This page intentionally left blank.)

Appendix C
USER REQUIREMENTS

(This page intentionally left blank.)

USER REQUIREMENTS

Translating the weapon specification document into a detailed list containing all the requirements that may influence the fuze/safe and arm device (S&A device) design is difficult. Often, the weapon specification includes some requirements that are not explicitly stated or that are not obvious. Therefore, all the criteria must be considered carefully, even when they do not, on the surface, seem pertinent.

For example, the specification for a digital underwater explosive ordnance disposal device may require that the device be programmed on ships. In this case, an unwritten requirement is the need for resistance to strong electromagnetic interference because strong radar signals with peak field strengths of several hundred volts per meter are present. In effect, because these explosive devices must be prepared in the open, no shielding from the ship's superstructure is available. Therefore, this situation must be considered in the design.

By developing a complete list of the S&A device requirements, in addition to those provided by the weapon specification, and discussing the details with the user, the designer ensures that no requirements are overlooked.

To that end, for each requirement, the designer should first list the type, time of occurrence (e.g., logistic handling, storage, combat), number of occurrences, duration, and levels. If applicable, different levels for various situations (e.g., storage versus use) should be specified. From this comprehensive list, a summary of all the requirements can easily be made and the ones pertaining to the fuze and the S&A device can be extracted.

It is important that this list incorporate actual numbers so that the designer can incorporate the proper dimensions in the resultant design. In addition, in those instances in which the requirements are deduced, the reasoning must be included to simplify later reviews. For example, for the scenario provided, one would state: "Use on ships implies strong radio/radar transmitters."

While the list contained in Table C-1 is not complete, it may provide some assistance to the designer.

TABLE C-1. User Requirements.

1. Interfaces · mechanic · electric · explosive · thermal · optical · communication with system
2. Mechanics · weight · size · vibration · shock/drop · acceleration/deceleration · jumble, jolt
3. Arming Environments · first arming environment · second arming environment · other arming environments
4. Climatic Zones and Environments · temperature · temperature changes · humidity · rain/snow/hail · sun · wind · air pressure (e.g., logistics) · sand, dust · salt spray, etc. · logistic transport · conditions at launch (e.g., under water)
5. Electromagnetic Interference · internal electromagnetic compatibility (EMC) · external EMC · electrostatic discharge · lightning · high-frequency fields (frequency, field strength, power) · high-power microwave weapons
6. Nuclear, Biological, and Chemical Requirements

TABLE C-1 (cont.). User Requirements.

7. Other · system requirements · power supply · insensitive munitions · anticipated lifetime · weapon life cycle · handling · maintenance · modularity · multiple impact · ease of manufacturing (cost)

NOMENCLATURE

EMC	electromagnetic compatibility
S&A	safe and arm

(This page intentionally left blank.)

Appendix D
ADVERSE ENVIRONMENTS

(This page intentionally left blank.)

ADVERSE ENVIRONMENTS

Translating the weapon specification into detailed adverse environments is difficult because it usually includes some requirements that are not obvious. For example, the specification for a digital underwater explosive ordnance disposal device may require that the device be programmed on ships. In this case, an unwritten requirement is the need for resistance to strong electromagnetic interference because strong radar signals with peak field strengths of several hundred volts per meter are present. In effect, because these explosive devices must be prepared in the open, no shielding from the ship's superstructure is available. Therefore, this situation must be included in the list of adverse environments.

By developing a complete list of the environments, in addition to those provided by the weapon specification, and discussing the details with the user, the designer ensures that no environment is overlooked.

To that end, for each type of condition, the designer should list the expected situations of occurrence, levels, duration of exposure, and possible effects on the safe and arm (S&A) device. From this comprehensive list, a summary containing all the adverse environments and their worst-case occurrences can easily be made. Credible accidents, such as fire or shock from a drop or a hit, are included in the following list because they are types of the adverse environments. While the list contained in Table D-1 is not complete, it provides some common types of environments to assist the designer.

TABLE D-1. Adverse Environments.

1. Mechanical Stress · shock (hit, drop, jettison, impact/multiple impact) · vibration (transport, aircraft carriage, flight) · acceleration/deceleration · jumble · jolt · static loads · expansion/contraction (caused by temperature or pressure changes)
2. Thermal · thermal expansion/contraction · thermal shock · change of material properties (e.g., chemicals)
3. Weather · climatic zones · temperature ranges and changes · humidity · rain, snow, hail · sun (including ultraviolet exposure) · wind
4. Chemical · corrosion · acids/bases · chemical interaction/compatibility · stability of materials · salt water
5. Biological · bacteria · fungi · animals [a] · plants
6. Electromagnetic Interference [b] · electrostatic discharge · radio/radar transmission · lightning · man-made noise · high-power microwave weapons · internal electromagnetic compatibility (EMC) · external EMC
7. Other · sand, dust (abrasion) · fire (e.g., slow/fast cookoff)

TABLE D-1 (cont.). Adverse Environments.

8. Man-made
· bullet impact
· fragment impact
· mishandling
· credible accidents of different types

[a] For example, a fiber optic that was used as a tripwire lasted no longer than dusk because the rabbits loved the taste of the coating.
[b] Note: List for each: source, frequency range, power, field strength at weapon, likeliness of occurrence, and other characteristics.

NOMENCLATURE

EMC	electromagnetic compatibility
S&A	safe and arm

(This page intentionally left blank.)

Appendix E
SELECTION OF ARMING ENVIRONMENTS

(This page intentionally left blank.)

SELECTION OF ARMING ENVIRONMENTS

An arming environment is a condition or a set of conditions that indicates the proper launch of a munition. Most of the requirements for these environments come from MIL-STD 1316 (Reference E-1) and STANAG 4187 (Reference E-2). The selection of the arming environments is the most important design decision; and many factors, such as safety, reliability, and cost, are based on that choice. Therefore, that determination should be made very carefully.

The following are some of the issues that the designer should consider.

1. What typical environments exist only at launch? Provide the following information for each scenario.
    a. type and reason.
    b. levels and range.
    c. characteristics.
    d. time and duration of occurrence.
    e. circumstances and conditions.
    f. prerequisites.
2. Under what circumstances (any, even unusual ones) might these types of environments occur? Provide the following information for each scenario.
    a. type and reason.
    b. levels and range.
    c. characteristics.
    d. time and duration of occurrence.
    e. circumstances and conditions.
    f. prerequisites.
    g. probability.
3. How accurately can the two selected arming environments be distinguished from any other and with what degree of safety? For example, address the following factors.
    a. type.
    b. differences in levels and range.
    c. differences in characteristics.
    d. differences in time and duration of occurrence.
    e. differences in circumstances and conditions.
    f. differences in prerequisites.
    g. common characteristics.
    h. sensor requirements.

4. If these two phenomena cannot be distinguished in an absolutely safe manner, what conditions might make it possible? Address the following factors.
    a. type and reason.
    b. levels and range.
    c. characteristics.
    d. time and duration of occurrence.
    e. conditions.
    f. prerequisites.
    g. type of connection with original environment.
5. Which of the unique environments are the simplest and most directly applied for arming. For example, which require the least energy transformation and signal processing? Address the following factors
    a. type and reason.
    b. type of arming process (possible sensors, transmission of signal).
    c. used characteristics and required levels.
    d. conditions.
    e. prerequisites.
    f. number of parts and assumed safety/reliability (only relative comparison).
6. What kinds of sensors are available for the different environments? Address the following factors.
    a. type.
    b. levels and range.
    c. characteristics.
    d. kind of output.
    e. conditions for proper operation.
7. Does the selection provide the most discernable and directly applied environment? Consider the following factors.
    a. type and reason.
    b. levels and range.
    c. characteristics.
    d. time and duration of occurrence.
    e. conditions and prerequisites.
    f. useable (and best) sensors.
    g. gap to otherwise occurrence.

Note: The more unusual and directly applied the selected environments are, the simpler the design will be. Thus, the safe and arm device's manufacturing process is easier, a situation that results in a lower price per unit.

REFERENCES

E-1. Department of Defense. *Department of Defense Design Criteria Standard, Fuze Design, Safety Criteria for,* by Fuze Engineering Standardization Working Group. Washington, DC, DOD, 10 July 1998. (MIL-STD-1316E, publication UNCLASSIFIED.)

E-2. North Atlantic Treaty Organization. *Standardization Agreement 4187, Edition 3, Fuzing Systems—Safety Design Requirements,* by AC/310. Brussels, Belgium. NATO, 2 November 1999. (STANAG 4187 Edition 3, publication UNCLASSIFIED.)

(This page intentionally left blank.)

Appendix F
EXPLANATIONS AND CHECKLIST FOR SAFE AND ARM (S&A) DEVICE FLOWCHART

(This page intentionally left blank.)

EXPLANATIONS AND CHECKLIST FOR SAFE AND ARM (S&A) DEVICE FLOWCHART

In developing a S&A device, the designer should follow the steps shown in Figure F-1.

1. **Determine if the design can be simplified; keep the design as simple as possible.**

   It is imperative that it be as uncomplicated as possible. Designs, especially after several improvements, tend to become increasingly complex. Therefore, one should determine if the same goal can be achieved with the following:

   a. a less complex design, for example, one with fewer parts.

   b. simpler or different sensors.

   c. a less complicated or different mechanical assembly or electronic layout.

   d. functions that are less integrated and a design that is more modular.

   Keeping the design simple and well structured provides quite a few advantages. For example, design flaws are more likely to occur in complex designs, but the designer is less likely to detect them. Also, the Failure Mode, Effects (and Criticality) Analysis (FME[C]A); the Fault Tree Analysis (FTA); and other analyses become more complex and difficult. Also, the system could be less reliable.

   While simplifying the design, the engineer could consider different arming environments only if higher reliability or failure rates can be achieved without decreasing safety. This modification must be made with the same high degree of care devoted to the initial selection and be based on a careful evaluation of all the possibilities.

2. **Determine if the design is fail safe.**

   This effort is similar to a Failure Modes and Effects Analysis (FMEA), except that this evaluation is done quickly and in a less formal manner. It provides an initial determination of how good the design is.

   For this phase, the designer must consider the individual parts of the design and determine what happens if one of them misses, breaks, or fails in any way (for electronics, one must also consider electromagnetic interference [EMI]). At this juncture, the input from other cognizant personnel is beneficial to ensure that nothing is overlooked. These findings also provide a sound basis for subsequent analyses.

3. **Perform a Preliminary Fault Tree Analysis.**

   This step provides the first insight of whether the design meets the safety requirements. For this analysis, the complete fault tree structure is required. However, instead of performing the labor-intensive process of researching the actual reliability data, the designer uses generic probabilities for each fault event. For electronic parts, the probability of failure is between 10^{-2} (conservative) and 10^{-4} (very optimistic), depending on the part being examined. While, with today's computers, this study takes very little time, design problems rooted in the design's arming logic or sequence that preclude achieving the required safety are often detected

before starting the more time-consuming analyses. (For additional details about the FTA and the preliminary FTA, see Appendix G.)

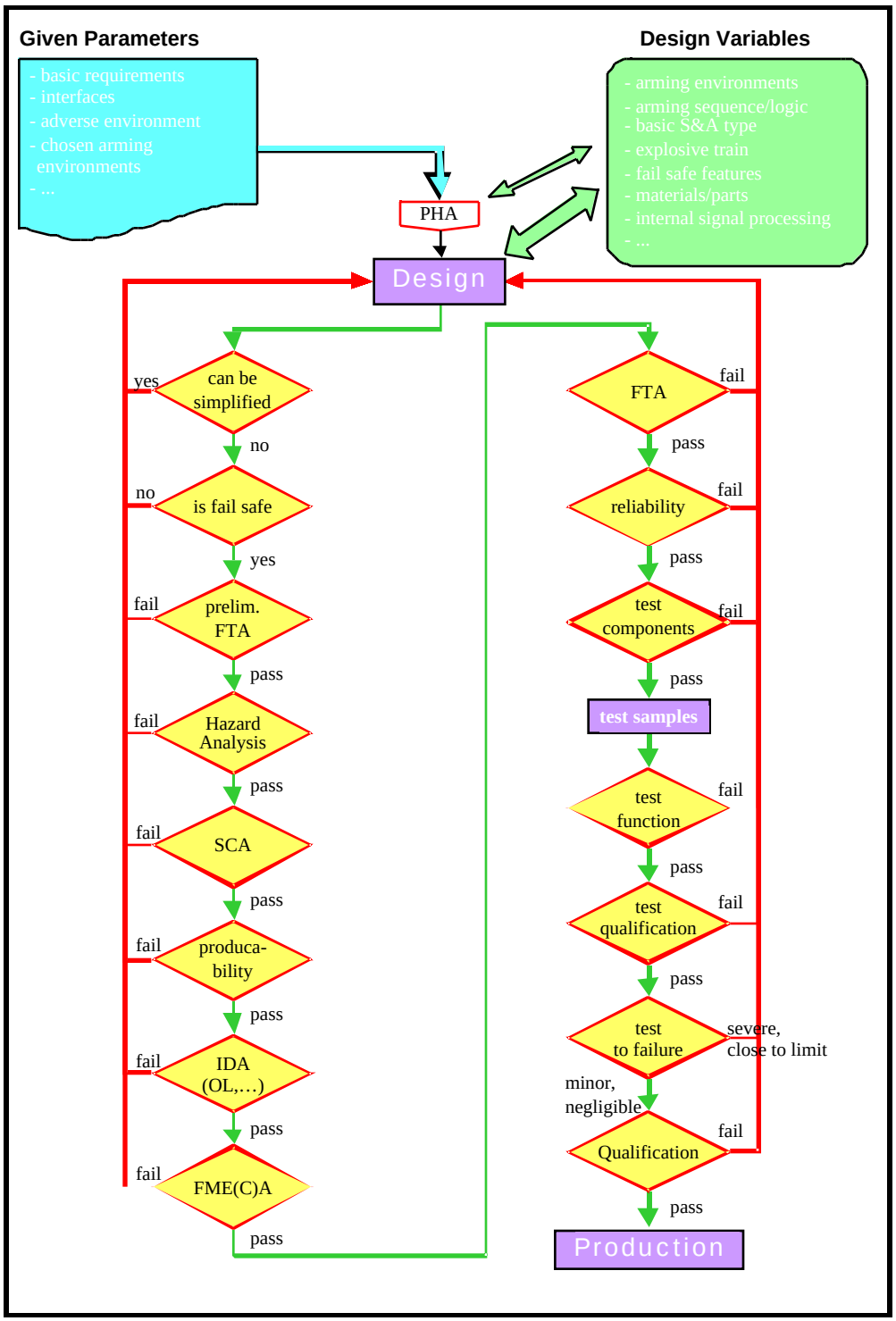

FIGURE F-1. S&A Device Design Flowchart.

4. **Update the (Preliminary) Hazards Analysis, or (P)HA, for the current design.**

   If hazardous states in the fuze can occur during or because of the weapon's life cycle conditions, the design must be modified.

5. **Perform a Sneak Circuit Analysis (SCA).**

   This step is performed to determine if any sneak circuits exist and to ensure that there is only one way in which the S&A device can become armed. Part of this effort is to look for circumstances, other than a proper launch, under which arming or partial arming can occur. If any of these conditions (even unusual ones) exist, it must be determined if they can occur during the life cycle of the weapon. If so, the designer must ensure that there is a wide gap between those environments intended to cause arming or partial arming and any conditions during the weapon life cycle that may inadvertently do so.

6. **Achieve an economically and technically producible design.**

   During development, the designer must keep in mind that the final S&A device must be manufactured in large or very large quantities at a reasonable price. To achieve this goal, the following guidelines should be followed.

   a. Use common, well-known parts of high quality to ensure reliability and safety.

   b. Ensure that the parts are of the proper dimension to guarantee the requisite safety but do not excessively oversize them.

   c. Make the design easy (but fail proof) to assemble.

   d. Create a modular design to facilitate later upgrades and clearly define the interfaces so that the analyses are simplified. The software code or field programmable gate arrays (FPGAs) should be modular, with comprehensive comments and documentation.

7. **Perform an Integrated Design Analysis (IDA).**

   The IDA provides a sound basis for all subsequent analyses. It also furnishes an understanding of how the system works in the absence of failure. At a minimum, the study should address the operation logic, including an operation logic tree. However, the analysis may also include the following areas, called frames:

   a. circuitry.

   b. computing systems.

   c. electrical power supply.

   d. environmental protection.

   e. chemical interaction.

   Part of the IDA is the compilation of a complete list of all S&A device items that must be used as a common basis for the FTA, FME(C)A, and reliability assessment.

   For specific guidance on the IDA, see North Atlantic Treaty Organization (NATO) Document AOP 42, "Integrated Design Analysis for Safety Critical Systems" (Reference F-1). Although this document is not fully developed, it provides the basics of the IDA approach.

8. **Conduct a Failure Mode Effects Analysis (FMEA) or a FME(C)A.**

   To achieve consistency among the various analyses, the designer should utilize the same list of items as that for the IDA.

9. **Conduct a Fault Tree Analysis (FTA).**

   To achieve consistency among the various analyses, the designer should utilize the same list of items as that for the IDA. For additional guidelines on the FTA, see Appendix G.

10. **Perform a reliability assessment.**

    Reliability must be designed into the S&A device from the beginning of the process to avert later problems and eliminate the necessity of having to repeat the entire design effort. Again, to achieve consistency among the various analyses, the designer should utilize the same list of items as that for the IDA.

    The typical failure rate curve over time is shaped like a bathtub (Figure F-2). In Phase I (Infant Mortality), the failure rate is high because of inherent defects in the newly manufactured parts that cause failure after a relatively short time. In Phase II, the rate is almost constant because most of the defective parts have already failed. In Phase III, the rate again increases because of wear and deterioration. Fortunately, the high failure rate experienced during Phase I can be lowered by subjecting all new parts to a burn-in stage prior to use. In addition, incorporating high-quality parts, such as MIL-STD parts, also enhances reliability.

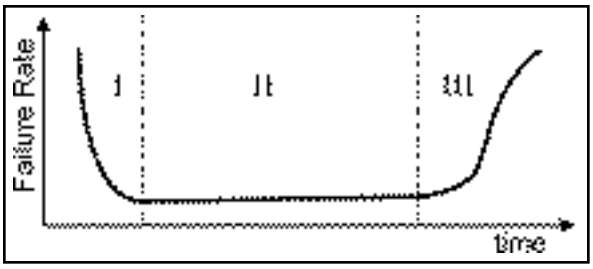

FIGURE F-2. Bathtub Curve for Failure Probability vs. Time.

11. **Perform component tests.**

    Critical components of the design must be tested as single devices first to ensure that they work properly and as intended. This approach is also more economical than testing the S&A device as a whole. In addition, the designer should conduct qualification-level tests and test-to-failure tests. The latter, especially, provide information about weak points in the design and the safety margin beyond the qualification levels. For example, a component that fails shortly after passing the qualification-level tests may require modifications to ensure safety and reliability over the weapon life cycle and to pass the qualification tests.

    It is important to be aware that some components, such as all the explosive items, require individual formal qualification prior to that of the S&A device. The S&A device's qualification is not a substitute for the formal qualification of each of its components.

12. **Manufacture test samples and conduct function tests, qualification-level tests, and tests to failure.**

    All of these show whether the fuze can successfully be qualified. As mentioned earlier, a test to failure provides additional information about weak points in the design and the safety margin beyond that stage. Again, a component that fails shortly after passing the qualification-level tests may require modifications to ensure safety and reliability over the

weapon life cycle. The part may also experience problems in the acceptance or qualification tests during full production because increased tolerances might result in unsafe hardware.

In addition, it is wise, at least at the qualification level, for an impartial agent to perform the tests so that they are conducted in a completely objective fashion. This goal is almost impossible to achieve by the designer, who might avoid thoroughly testing those areas in which known weaknesses exist.

13. **Subject the S&A device to qualification testing.**

    The development effort culminates with the S&A device successfully passing the qualification test.

After successful qualification, the final step before full production is the user's operational testing. This phase is not shown in Figure F-1 because it normally does not apply to the S&A device if properly designed and tested in accordance with this document and its appendixes.

REFERENCES

F-1. North Atlantic Treaty Organization. *Integrated Design Analysis for Safety Critical Systems*, by AC/310. Brussels, Belgium, NATO (in process). (AOP 42, publication UNCLASSIFIED.)

NOMENCLATURE

EMI	electromagnetic interference
FMEA	Failure Mode Effects Analysis
FME(C)A	Failure Mode Effects (and Criticality) Analysis
FPGA	field programmable gate array
FTA	Fault Tree Analysis
IDA	Integrated Design Analysis
NATO	North Atlantic Treaty Organization
(P)HA	(Preliminary) Hazards Analysis
S&A	safe and arm
SCA	Sneak Circuit Analysis

(This page intentionally left blank.)

Appendix G
FAULT TREE ANALYSIS (FTA)

(This page intentionally left blank.)

FAULT TREE ANALYSIS (FTA)

The following guidelines should be adhered to when doing a FTA. In general, the designer should discuss any results and possible faults with independent personnel with no vested interest in the safe and arm (S&A) device development. In this way, all relevant faults are more likely to be identified.

The first task after developing a design or making a change to that design is to do a Preliminary Fault Tree Analysis (PFTA) to determine if the device is likely to meet the 10^{-6} requirement. Each fault is assigned a conservative failure probability between 10^{-2} (conservative) to 10^{-4} (very optimistic), depending on the part, and then scaled with a safety factor of 5. If the result is well below the 10^{-6} requirement, it is likely that the design will fulfill the requirements. While this exercise takes little time, it often saves much time and money—sometimes a large investment—that would otherwise be wasted in further developing a bad design. For example, if the PFTA is omitted and a design's safety value is relatively close to the limit, expensive high-quality parts or additional testing could be required during manufacturing, which increases costs. So, to avoid this situation, companies sometimes adapt the calculation to prevent a redesign. For example, they adopt different or less conservative reliability data or introduce favorable scaling factors. In this case, the experts, who typically detect these palliations, place little confidence in the analysis results. As such, the design may fail the Weapon Systems Explosives Safety Review Board (WSESRB) review.

Note: Whenever additional explanations are required, the FTA author shall provide the necessary detail so that the FTA can be understood, even after several years, by someone who has not previously worked on the specific S&A device for which the FTA is created.

FAULT TREE STRUCTURE

1. Generally, the top events in an FTA for S&A devices are premature arming and early burst. However, if, at times, valid reasons dictate adopting some other incident (for example, a premature arming after normal release), the justification for choosing this alternate approach, the kinds of faults that are omitted and why, and the reasons this option does not affect the analysis must be explained and documented.
2. The fault tree must include primary, secondary, and command faults. If the tree is based on the Failure Mode, Effects (and Criticality) Analysis (FME[C]A) alone, a tendency exists to consider only internal primary fault events. However, other possible failures must also be given a great deal of consideration. These include credible accidents, even though most of them are quite rare. Therefore, typically, they will be deleted later in the process and seldom appear in the final fault tree. As such, they are dealt with in a different place in the FTA.
3. If not prevented by supplementary means, such as a 100% inspection or a functional test of the manufactured S&A/electronic safe-arm device (ESAD), errors during manufacturing must be considered. For example, for an ESAD, besides the possibility of a broken (shorted/open) resistor, one must also consider that the wrong resistor (type or value) might have been used.
4. At a minimum, the fault tree must be based on and verified against the Sneak Circuit Analysis (SCA), the FME(C)A, the drawings and schematics, and the logic tree (from the Integrated Design Analysis [IDA]).

5. Initially, the fault tree should be developed in great detail and to a level at which all the faults from the FME(C)A, as well as from the other analyses, are mentioned, even though, at first glance, the incidents appear minor. As such, this approach ensures that no major faults or cut-sets are overlooked.

6. Any fault event or limb that can be excluded by technical means or because the probability of occurrence for this specific fault is too minimal must be mentioned and its deletion explained in the FTA. (Typically, for a reasonable design, most credible accidents can be eliminated from the fault tree structure in this manner.)

QUANTITATIVE ANALYSIS

1. For the FTA, the designer must include not only the origin of the information but also all the raw data required to duplicate the calculations. Examples include the exact type of component, the failure rate, the quality level (type and factor), and the environments (type and factor). This step is important so that readers will understand and have confidence in the results, especially if using the document some time after it was written.

2. All the expressions, terms, and factors, as well as their origins, must be provided, including an explanation of why they are applicable and the source of supporting data. For example, if a factor is used to derive a dormant mode from an active one, an explanation of the applicability for the specific part should be provided (such as a resistor [probably applicable] or a spark gap [probably not applicable because vibration and gas leakage are largely independent of the spark gap being powered]).

   Note: For ESADs, the designer should use MIL-HDBK 217F (Reference G-1), which contains expressions for the calculation of a "stress" (the ratio of the actual power to rated power) of zero, rather than using artificial factors.

3. For all the analyses, the same data must be used, such as for the FTA and reliability prediction. As of January 2001, the standard sources of data are the following:

   a. Collected reliability data: (1) Reliability Assessment Center (RAC) EPRD-97 (electronic parts) (Reference G-2), (2) RAC NPRD-95 (non-electronic parts) (Reference G-3), and (3) RAC NONOP-1 (non-operational parts) (Reference G-4).

   b. Models: MIL-HDBK 217F (electronic parts) (Reference G-1).

   Only these documents shall be used for the FTA of ESADs.

4. If for valid reasons, a designer feels using other sources of reliability data is appropriate, he or she must prove that, at a minimum, those sources provide the same quality level as the standard sources mentioned earlier. In addition, the customer's approval is required.

5. For the ESAD, to adjust for the statistical imprecision of the reliability data, the deficiency of the models, and the reliability deviations of the individual parts, the value must be increased by a scaling factor of 5. For example, a part with a failure rate of 3×10^{-3} is scaled to 1.5×10^{-2}. Always remember that a FTA is about safety, so common sense dictates a conservative approach. In other words, it is better to be safe than sorry.

   Note: A factor of 5 is considered reasonable, and its use does not negatively affect the analysis of a good design. Moreover, in general, it compensates for all the possible part deviations, for example, those that occur during the manufacturing process. EPRD-97 (Reference G-2) contains the reliability data for the parts in which the same item at ground benign (GB) environment exhibits a failure rate 20 times higher than under much more severe airborne

uninhabited fighter (AUF) conditions. So, under normal circumstances, adopting this factor provides conservative analysis results that are "on the safe side."

The following is an example of this conservative approach. For an ESAD, three independent switches are required. With a safety factor of 5, each switch must have a failure rate of 2×10^{-3} or less. In other words, $[5 \times (2 \times 10^{-3})]^3 = 10^{-6}$ or an average failure rate of 1/500 for each switch.

So, for an ESAD with no additional safety features, under the assumption of ten parts per switch, each of whose failure could cause the switch to fail, the required average failure probability per part is 2×10^{-4} or less. This number appears to be quite low, chiefly because of the overly simplistic calculation. The probability of a static switch failing may be slightly higher 2×10^{-4}, but the chances of a dynamic switch failing in a safety critical way are considerably lower for a good design. However, the use of interlocks, sequences, and time windows further reduces the requirements for the safety-critical reliability of the individual parts.

6. If, for a specific part, the reliability data collections do not specify a well-defined failure rate but stipulate "smaller than" (<) a value, this value or a value from a model or pooled data (see below) should be used. The scaling factor for ESADs still applies.

7. If a reliability data collection shows that a part has been fielded for some time without any failures, the failure rate is usually specified as "smaller than" (<) some value. If the necessary data are available for similar parts, the designer can pool the data with Equation G-1 from EPRD-97 (Reference G-2).

$$\lambda_{pool} = \left(\prod_{i=1}^{n'} \lambda'_i \right)^{\frac{1}{n'}} \times \frac{\sum_{i=1}^{n'} h'_i}{\sum_{i=1}^{n} h_i} \qquad \text{(G-1)}$$

where

λ_{pool}	=	resultant failure rate for pooled data
λ'_i	=	failure rate of component, where failure occurred
h_i	=	time in hours of pooled component *i*
h'_i	=	time in hours of pooled component *i* where failure occurred
n	=	total pooled components
n'	=	number of pooled components where failure occurred

The scaling factor for ESADs also applies here.

8. For an ESAD, if no data are available for a part, the designer should use the pooled data for similar parts with well-defined failure rates or the model in MIL-HDBK 217 (Reference G-1).

9. When human action becomes a factor in the FTA, the probability of an error occurrence is at least 10^{-2} per action (very optimistic). However, when this intervention is required under stressful conditions, that value may increase to several times 10^{-1} per action, depending on the difficulty of the task. Therefore, it is strongly advised that human action be eliminated as much as possible.

10. For the FTA, the designer should always assume a service life of at least 20 years, even if the contractual service life may be shorter (often 10 years). For example, experience indicates that expensive weapons systems often have a shelf life of more than 20 years. So, if the design

fails to pass the FTA based on this increase timeframe, it is an weak design that, in any case, should be modified.

11. A part does not have a probability of failure, per se, but a failure rate (the number of failures per time) or a mean time between failures (MTBF) (the inverse of the failure rate). The probability of failure is the failure rate multiplied by the time frame (or the time divided by MTBF) and is always related to a well-defined time period.

    For example, what is the probability of failure for a car? Depending on the time frame, it may be very low (almost 0% for 1 hour of operation) or very high (almost 100% for 20 years).

    Table G-1 shows the connection among failure rate, MTBF, and probabilities for specific time intervals.

    For the ESAD, the probabilities of failure for a part with a 20-year service life are generally 10^{-2} to 10^{-4} and the failure rates are 10^{-7}/hr to 10^{-9}/hr (the MTBF is 10 to 1000 million hours). Any values lower than those mentioned should be given a great deal of consideration and must be proved, preferably by testing.

TABLE G-1. Failure Rate, MTBF, and Probability.

Failure Rate (λ), hr^{-1}	MTBF, hr	Probability of Failure for a Given Time					
		1 minute = 1/60 hr	1 hour = 1 hr	1 day = 24 hr	1 month = 720 hr	1 year = 8,766 hr	20 years = 175,320 hr
1000×10^{-6}	0.001×10^{6}	1.7×10^{-5}	1×10^{-3}	2.4×10^{-2}	0.74	1	1
100×10^{-6}	0.01×10^{6}	1.7×10^{-6}	1×10^{-4}	2.4×10^{-3}	7.4×10^{-2}	0.88	1
10×10^{-6}	0.1×10^{6}	1.7×10^{-7}	1×10^{-5}	2.4×10^{-4}	7.4×10^{-3}	8.8×10^{-2}	1
1×10^{-6}	1×10^{6}	1.7×10^{-8}	1×10^{-6}	2.4×10^{-5}	7.4×10^{-4}	8.8×10^{-3}	0.18
0.1×10^{-6}	10×10^{6}	1.7×10^{-9}	1×10^{-7}	2.4×10^{-6}	7.4×10^{-5}	8.8×10^{-4}	1.8×10^{-2}
0.01×10^{-6}	100×10^{6}	1.7×10^{-10}	1×10^{-8}	2.4×10^{-7}	7.4×10^{-6}	8.8×10^{-5}	1.8×10^{-3}
0.001×10^{-6}	1×10^{9}	1.7×10^{-11}	1×10^{-9}	2.4×10^{-8}	7.4×10^{-7}	8.8×10^{-6}	1.8×10^{-4}
0.0001×10^{-6}	10×10^{9}	1.7×10^{-12}	1×10^{-10}	2.4×10^{-9}	7.4×10^{-8}	8.8×10^{-7}	1.8×10^{-5}

12. Obviously, for the FTA, all the various failure probabilities over the weapon's life cycle must be accumulated for the different environments, for example:
    a. storage (fixed, mobile, field) (20 years).
    b. transportation (truck, tracked vehicle, aircraft).
    c. carriage (on an aircraft, on a launcher, in a weapon).
    d. handling.
    e. launch, firing, and boost phase.
    f. march, coast phase, and flight.

The applicable expressions for this information are defined in Equations G-2 and G-3.

$$P(\lambda, t) = \sum_i \lambda_i \cdot t_i \tag{G-2}$$

$$P(MTBF, t) = \sum_i \frac{t_i}{MTBF_i} \tag{G-3}$$

where

P = probability of failure
λ_i = failure rate in environment *i*
$MTBF_i$ = MTBF in environment *i* (the inverse failure rate λ_i)
t_i = duration of environment *i*

The following are two examples that show why it is inappropriate to consider the time of operation only. They are based on a part in a missile that has a shelf life of 20 years. Table G-2 shows the time spent in and the failure rate, probability of failure, and percentage contribution to probability of failure experienced for the specified environments.

The first example is that of an extremely reliable part that is quite sensitive to environmental stress. In other words, the failure rates are strongly influenced by and, therefore, increase dramatically with added stress levels. This scenario was chosen to increase the contribution of the launch and flight environment.

TABLE G-2. Typical Probabilities of Failure for Highly Reliable but Stress-sensitive Part.

Environment	Time	λ (10^{-6}/hr)	P(λ,t)	% Contribution to Probability of Failure
Ground storage (GB)	20 years (170,265 hr)	0.001	1.7×10^{-4}	53
Field storage (GF)	6 months (4,383 hr)	0.01	4.4×10^{-5}	14
Transportation (GM)	21 days (504 hr)	0.05	2.5×10^{-5}	8
Aircraft carriage (AUF)	7 days (168 hr)	0.5	8.4×10^{-5}	26
Launch and flight (ML)	120 seconds (1/30 hr)	5	1.7×10^{-7}	0.05
Accumulated probability of failure			3.2×10^{-4}	

GF = ground fixed, GM = ground mobile, ML = missile launch.

As the table clearly indicates, even though the failure rate is high during launch and flight, the probability of failure for this environment is negligible—adding only 0.05% (1 out of 2,000) to the overall total. The most significant contributor is the long period in which the item is in ground storage, even though the part is highly reliable in this environment.

Table G-3 provides the same data but for a less reliable part that is also less sensitive to environmental stress than that in the first example.

TABLE G-3. Typical Probabilities of Failure for Less Reliable and Less Stress-sensitive Part.

Environment	Time	λ [10^{-6}/hr]	$P(\lambda,t)$	% Contribution to Probability of Failure
Ground storage (GB)	20 years (170,265 hr)	0.05	8.5×10^{-3}	92
Field storage (GF)	6 months (4,383 hr)	0.1	4.4×10^{-4}	5
Transportation (GM)	21 days (504 hr)	0.2	1.0×10^{-4}	1.1
Aircraft carriage (AUF)	7 days (168 hr)	0.8	1.3×10^{-4}	1.5
Launch and flight (ML)	120 seconds (1/30 hr)	2	6.7×10^{-8}	0.001
Accumulated probability of failure			9.2×10^{-3}	

In this case, the launch and flight environment contributes only 0.001% (or 1 of 100,000 failures) to the overall probability of failure. In addition, more than 90% of all failures occur during ground storage.

Obviously, the major contributor to these outcomes is the timeframe. The storage time is more than seven orders of magnitude greater than the time for launch and flight while the failure rate usually increases about three or, at a maximum, five orders of magnitude.

So, if storage is omitted from the FTA, with only launch and flight accounted for, the device's safety is overestimated by three to five orders of magnitude.

REFERENCES

G-1. Department of Defense. *Military Handbook, Reliability Prediction of Electronic Equipment.* Washington, DC, 2 December 1991. (MIL-HDBK 217F, publication UNCLASSIFIED.)

G-2. Reliability Analysis Center. *Electronic Parts Reliability Data, A Compendium of Commercial and Military Device Field Failure Rates*, by W. Denson, W. Crowell, P. Jaworski, and D. Mahar. Rome, New York, Reliability Analysis Center, 1997. (RAC EPRD-97, publication UNCLASSIFIED.)

G-3. Reliability Analysis Center. *Nonelectronic Parts Reliability Data*, W. Denson, et al. Rome, New York, Reliability Analysis Center, 1997. (RAC NPRD-95, publication UNCLASSIFIED.)

G-4. Reliability Analysis Center. *Nonoperating Reliability Data*, by M. Rossi. Rome, New York, 1987 (RAC NONOP-1, publication UNCLASSIFIED.)

NOMENCLATURE

AUF	airborne uninhabited fighter
ESAD	electronic safe-arm device
FME(C)A	Failure Mode, Effects (and Criticality) Analysis
FTA	Fault Tree Analysis
GB	ground benign
GF	ground fixed
GM	ground mobile
h'_i	time in hours of pooled component *i* where failure occurred
h_i	time in hours of pooled component *i*
IDA	Integrated Design Analysis
ML	missile launch
MTBF	mean time between failures
$MTBF_i$	mean time between failures in environment *i* (the inverse failure rate λ_i
n	total pooled components
n'	number of pooled components where failure occurred
λ'_i	failure rate of component, where failure occurred
λ_i	failure rate in environment *i*
λ_{pool}	resultant failure rate for pooled data
P	probability of failure
PFTA	Preliminary Fault Tree Analysis
RAC	Reliability Assessment Center
S&A	safe and arm
SCA	Sneak Circuit Analysis
t_i	duration of environment *i*
WSESRB	Weapon Systems Explosives Safety Review Board

(This page intentionally left blank.)

Appendix H
CHECKLIST FOR MECHANICAL SAFE AND ARM (S&A) DEVICE WITH INTERRUPTED EXPLOSIVE TRAIN

(This page intentionally left blank.)

CHECKLIST FOR MECHANICAL SAFE AND ARM (S&A) DEVICE WITH INTERRUPTED EXPLOSIVE TRAIN

The following is a checklist of the guidelines for a mechanical S&A device with an interrupted explosive train. For a general report on S&A device design principles, see Reference H-1.

1. **Materials, non-explosive**
   a. The materials are compatible with each other, even at adverse conditions; and/or
   b. Measures are taken to shield the materials from these adverse conditions.
   c. The materials are durable, in other words, no degradation occurs; and/or
   d. Measures are taken to prevent the degradation of the parts.
   e. No unintentional dangerous ejection of materials can occur, for example, from the battery.
   f. The quality of material is high enough to fulfill the safety requirements.
   g. The supplier has exhibited the ability to deliver high quality parts consistently.
2. **Materials, explosive**
   a. The materials are qualified for the intended use.
   b. The materials are such that their sensitivity does not change (especially increase) over time under any credible circumstances.
   c. At a minimum, the materials are stable over the intended lifetime; and/or
   d. Periodical maintenance will be performed.
   e. No unintentional dangerous ejection of materials can occur, for example, due to a change of state, vibration, abrasion, or temperature changes.
   f. The manufacturer has exhibited the ability to deliver high quality parts consistently.
3. **Dimensions**

   The dimensions of the parts fulfill the safety requirements for handling by humans.
4. **Locks (Safety Features)**

   An explanation of the requirement of "at least two safety features" is provided in a note at the end of this appendix.
   a. At least two locks are present, each directly locking the interrupter. A lock on a lock does not fulfill this requirement.
   b. The locks are independent of each other. In other words, they do not depend on one another to ensure safety/locking; they use different environments and sensors; etc.
   c. The locks are operated by independent environments. For example, spin and acceleration of an artillery shell are considered independent even though they are both connected to firing. In contrast, acceleration and velocity or distance are dependent because velocity and distance are direct results of the acceleration.
   d. The locks are different to avoid common mode failures.

e. The chosen arming environments meet the North Atlantic Treaty Organization (NATO) or U.S. requirements, which are found in STANAG 4187 (Reference H-2) or MIL-STD-1316 (Reference H-3), respectively.

f. The arming environments are selected according to the checklist for arming environments and are independent and fundamentally different from each other.

g. At least one arming environment occurs after the launch of the weapon only; and/or

h. Additional requirements ensure that the S&A device is armed only when proper launched is verified.

i. Each lock by itself can prevent arming.

j. Gears or toothed wheels are not considered locks because of the wear experienced during mechanical stress, such as vibration.

k. A spring on the interrupter that prevents the latter from moving is not considered a lock.

5. **Lock Operation**

a. The locks directly lock the interrupter.

b. The locks are directly operated by the environment. In other words, they do not use any translated energy. An example of translated energy is perceiving the acceleration (mechanic) with a piezoelectric sensor (output electric), converting and amplifying the signal into viable current for an electric device, and then using a rotary magnet to remove the lock (mechanic). In contrast, direct operation is the incorporation of a mechanical setback device that removes the lock by the acceleration alone, or

c. If the locks do operate from translated energy, the signal chosen must be unique, cannot be imitated by any other signal in the system under any conditions, and must occur at no time and under no circumstances during the weapon life cycle, except at the intended launch.

d. If electrical signals are used to remove a lock, the following supplementary requirements must be met.

(1) To be considered valid, the electrical signal possesses unique characteristics and is verified as a valid signal; and/or

(2) The design, as a whole, ensures that, under no circumstances, will a wrongful signal occur.

(3) The lock removal should require a continuous signal instead of a single pulse. For example, a stepped motor is preferred over a normal rotary magnet or a pyrotechnic device because the stepped motor requires a signal with a specific frequency. Such a mechanism is less likely to remove the lock because of some kind of electromagnetic interference (EMI) or electrostatic discharge (ESD), such as lightning. So, the inherent safety is enhanced.

e. No pyrotechnic elements are used to operate the locks unless the following conditions exist.

(1) Use of pyrotechnic devices is unavoidable, a determination that must be proved.

(2) Use is approved by the National Safety Approving Authority (NSAA).

(3) Only the second lock is operated by such a device.

(4) In the case of premature function or operation of the pyrotechnic mechanism, the S&A device is mechanically blocked in a safe status (dudded).

f. No stored energy, such as springs or pyrotechnic devices, should be used to operate the locks, except when unavoidable, a determination that must be proved.

g. The arming environment is verified by its unique characteristics, such as strength, envelopes, direction, or frequency, as valid before the locks are functioned.

6. **Fail-safe Design**

If any part of the S&A device breaks, the S&A device fails in a state that presents no hazard.

7. **Safe Assembly**

a. If any safety-critical part is missing, it is impossible to assemble the S&A device, and/or

b. After assembly, a 100% inspection is conducted according to a different and independent method. These results are then documented and retained. However, this scenario should be avoided because of an enhanced risk of failure and increased costs. Here, a different and independent method is one in which, each time the system is checked, that examination is conducted by different personnel using different tools. For example, the same assembly person performing the same test three times does not significantly lower the probability of an error. In contrast, three different people (independent) utilizing three different methods (independent and different) does lower the probability.

c. It is impossible for the S&A device to be assembled if not in the safe status, and/or

d. After assembly, a 100% inspection is conducted according to a different and independent method (See 7.b). These results are documented and retained.

e. It is impossible for the S&A device to be built into the weapon if not in a safe status, and/or

f. After assembly, a 100% inspection is conducted according to a different and independent method (See 7.b). These results must be documented and retained.

8. **Overall Design**

a. The parts of the S&A device are dedicated to fuzing alone and, preferably, to arming only.

b. The S&A device has its own sensors and does not receive any pre-sensed, processed, or preprocessed signals for arming from the weapon system (it is a stand-alone device).

c. The manufacturing process ensures that only safe S&A devices are assembled and processed further.

d. The tolerances are such that, while safety and reliability are guaranteed, the tolerances do not create undue problems during serial production. The recommendation is to follow the 6-σ (σ = standard deviation) production rule, which is to use the 1-σ value from the design requirements as the 6-σ value for the production of the parts. This approach ensures that virtually all the parts are within the required tolerances; and/or

e. If reliability and safety depend on narrow tolerances, after assembly, a 100% inspection is conducted according to a different and independent method. These results are documented and retained.

f. All the turning parts, such as wheels, are balanced to prevent forces that cause inordinate wear through vibration or shocks.

g. All the parts are balanced, with no possibility of forces being applied to them in the direction of arming prior to that stage.

Note: The requirement for "at least two locks/safety features" is due to the fact that the reliability (or safety) of this lock/safety feature must be proved. Table H-1 provides the number of items that must be included in a go/no-go test (with a maximum of one failure) to prove the specified probability within the required confidence interval (Poisson distribution).

TABLE H-1. Items Needed To Prove Specified Probability at Required Confidence Level.

Confidence Interval, %	Number of Test Items for a Given Probability					
	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
50	5	46	456	4,556	45,563	455,625
60	7	70	705	7,056	70,560	705,600
70	10	107	1,073	10,732	107,329	1,073,295
80	15	163	1,637	16,383	163,839	1,638,399
90	25	268	2,704	27,058	270,600	2,706,023
95	35	381	3,838	38,413	384,157	3,841,597
98	46	498	5,018	50,216	502,204	5,022,076
99	60	657	6,630	66,352	663,571	6,635,770
99.5	71	781	7,872	78,785	787,918	7,879,242
99.9	98	1,073	10,820	108,296	1,083,058	10,830,671
99.99	137	1,499	15,117	151,306	1,513,195	15,132,085
99.999	176	1,931	19,482	194,992	1,950,087	19,501,037

As the reader can see, the items required to substantiate the requisite reliability for probabilities above 10^{-3} and confidence intervals of at least 90% preclude actual testing. Thus, the easiest way to demonstrate that a S&A device has a risk of premature arming below 10^{-6} is to prove it for a device with two locks/safety features each having a risk lower than 10^{-3}.

REFERENCES

H-1. Naval Air Warfare Center Weapons Division. *Safety and Arming Device Design Principle*s, by Steven E. Fowler. China Lake, California, NAWCWD, May 1999. (NAWCWD TP 8431, publication UNCLASSIFIED.)

H-2. North Atlantic Treaty Organization. *Standardization Agreement 4187, Edition 3, Fuzing Systems—Safety Design Requirements,* by AC/310. Brussels, Belgium. NATO, 2 November 1999. (STANAG 4187 Edition 3, publication UNCLASSIFIED.)

H-3. Department of Defense. *Department of Defense Design Criteria Standard, Fuze Design, Safety Criteria for,* by Fuze Engineering Standardization Working Group. Washington, DC, DOD, 10 July 1998. (MIL-STD-1316E, publication UNCLASSIFIED.)

NOMENCLATURE

EMI	electromagnetic interference
ESD	electrostatic discharge
NATO	North Atlantic Treaty Organization
NSAA	National Safety Approving Authority
S&A	safe and arm

(This page intentionally left blank.)

Appendix I
CHECKLIST FOR ELECTRONIC SAFE-ARM DEVICE (ESAD) WITH NON-INTERRUPTED EXPLOSIVE TRAIN

(This page intentionally left blank.)

CHECKLIST FOR ELECTRONIC SAFE-ARM DEVICE (ESAD) WITH NON-INTERRUPTED EXPLOSIVE TRAIN

The following is a checklist of the guidelines for an ESAD with a non-interrupted explosive train. For a general report on safe and arm (S&A) device design principles, see Reference I-1; and, for a detailed report on ESAD design philosophy, see Reference I-2.

1. **Materials, non-explosive**
   a. The materials and parts are durable, in other words, no degradation occurs; and/or
   b. Measures are taken to prevent the degradation of the materials and parts.
   c. Different types of electronic parts (for example, bipolar and CMOS parts) are used wherever possible to avoid common mode failures.
   d. No unintentional dangerous ejection of materials can occur, for example, from the battery.
   e. The quality of material is high enough to fulfill the safety requirements.
   f. The supplier has exhibited the ability to deliver high quality parts consistently.
2. **Materials, explosive**
   a. The materials are qualified for the intended use.
   b. The materials are such that their sensitivity does not change (especially increase) over time under any circumstances.
   c. At a minimum, the materials are stable over the intended lifetime; or
   d. Periodical maintenance will be performed.
   e. No unintentional dangerous ejection of materials can occur, for example, due to a change of state, vibration, or abrasion.
   f. The manufacturer has exhibited the ability to deliver high quality parts consistently.
3. **Dimensions**
   a. The parts' dimensions fulfill the safety requirements for handling by humans.
   b. For analog electronic parts, the derating requirements found in Reference I-3 are followed.
   c. For all the parts that operate relatively close to the maximum load, the design must function at as low a load as reasonably possible (for example, 90% is better than 100% and 88% is better than 90%). In addition, it must be impossible for an overload to be applied to the circuits, even under adverse conditions.
4. **Switches (Safety Features)**

   An explanation of the requirement for "at least two safety features" is provided in a note at the end of this appendix.

   a. At a minimum, the number of safety features is at least as high as that indicated in one of the combinations shown in Table I-1.

TABLE I-1. Types and Numbers of Required Switches/Safety Features.

Safety Feature Type	Combination Options			
	A [a]	B	C	D
Mechanical safety feature	2	1	0	0
Dynamic electrical safety feature	0	1	2	1
Non-dynamic electrical safety feature	0	0	0	2

[a] This may be an ESAD with mechanical switches or a classical ESAD with an interrupted explosive train, in which case, Appendix H applies.

b. Each of the safety features (switches) directly prevents the flow of energy to the firing capacitor or high-voltage converter. A switch on a switch does not fulfill this requirement.

c. Each switch by itself can prevent the accumulation of energy in the firing capacitor (arming).

d. The switches are independent of each other. In other words, they do not depend on one another to ensure safety or interruption of the energy flow; they use different environments and sensors or sensor combinations; etc.

e. The switches are operated by independent environments. For example, spin and acceleration of an artillery shell are considered independent even though they are both connected to firing. In contrast, acceleration and velocity or distance are dependent because velocity and distance are direct results of the acceleration.

f. The chosen arming environments meet the North Atlantic Treaty Organization (NATO) or U.S. requirements, which are found in STANAG 4187 (Reference I-4) or MIL-STD-1316 (Reference I-5), respectively.

g. The arming environments have been selected according to the checklist for arming environments and are independent and fundamentally different from each other.

h. At least one arming environment occurs after the launch of the weapon only.

i. The switches use different technology to avoid common mode failures (for example, one bipolar, one CMOS switch).

j. Each switch has its own dedicated logic or logic device, which is physically separated from the others.

k. Logic devices use different technology and logic to avoid common mode failures (for example, one bipolar, one CMOS device, or some inverse logic).

5. **Operation of Switches (Safety Features)**

a. It is improbable (at least 10^{-6}) for the electrical signals from the sensors to the switches to be imitated by any other signal in the system when defects arise or to occur at any time and under any circumstances during the weapon life cycle, except at the intended launch. For example, the designer must be aware of the harmonics of signals present in the system.

b. The electrical signal possesses unique characteristics and can be verified as a valid signal; and/or

c. The design, as a whole, ensures that, under no circumstances, will a wrongful signal occur.

d. The switches are operated by microprocessors; or

e. The hardware and software for the microprocessors are submitted to a thorough and detailed safety review (a quantitative analysis is required) that includes all possible errors and resulting states.

f. The operation of the dynamic switches requires a continuous signal of fixed frequency.

g. The signal for the dynamic switches is the direct result of a sensor (e.g., alternator of an engine) or of the correct operation of the entire ESAD (e.g., a calculation by a field programmable gate array [FPGA], application-specific integrated circuit [ASIC], or microprocessor). Using a microprocessor to generate, based on the correct input from the sensors, a dynamic signal is acceptable. In contrast, it is not acceptable for the microprocessor to operate all the switches directly. In addition, the dynamic signal must not be generated by any oscillating device (e.g., a quartz or oscillatory circuit) and then be switched directly to the dynamic switch. In fact, merely switching a signal on or off from an oscillating device replaces the dynamic switch with the static one that switches through the oscillator signal. As soon as this static switch is enabled, the dynamic switch will operate, a situation that eliminates the increased safety of a proper dynamic switch.

h. The signal for at least one of the switches is derived from a post-launch environment.

i. The arming environment is verified by its unique characteristics, such as strength, envelopes, direction, or frequency, as valid before the switches are operated.

6. **Fail-safe Design**

If any part of the ESAD breaks or malfunctions, the ESAD fails in a state that presents no hazard.

7. **Safe Assembly**

a. It is impossible for the ESAD to be assembled if not in the safe status; and/or

b. After assembly, a 100% inspection is conducted according to a different and independent method. These results are documented and retained. Here, a different and independent method is one in which, each time the system is checked, that examination is conducted by different personnel using different tools. For example, the same assembly person performing the same test three times does not significantly lower the probability of an error. In contrast, three different people (independent) utilizing three different methods (independent and different) does lower the probability.

c. It is impossible for the ESAD to be built into the weapon if not in a safe status; and/or

d. After assembly, a 100% inspection is conducted according to a different and independent method. These results are documented and retained.

8. **Overall Design**

a. The parts of the ESAD are dedicated to fuzing alone and, preferably, to arming only.

b. The ESAD has its own sensors and does not receive any pre-sensed, processed, or preprocessed signals for arming from the weapon system (it is a stand-alone device).

c. The manufacturing process ensures that only safe ESADs are assembled and processed further.

d. The tolerances are such that, while safety and reliability are guaranteed, the tolerances do not create undue problems during serial production. The recommendation is to follow the 6-σ (σ = standard deviation) production rule, which is to use the 1-σ value from the design requirements as the 6-σ value for the production of the parts. This approach ensures that virtually all the parts are within the required tolerances; and/or

e. If reliability and safety depend on narrow tolerances, after assembly, a 100% inspection is conducted according to a different and independent method. These results are documented and retained.

Note: The requirement for "at least two locks/safety features" is due to the fact that the reliability (or safety) of this lock/safety feature must be proved. Table I-1 provides the number of items that must be included in a go/no-go test (with a maximum of one failure) to prove the specified probability within the required confidence interval (Poisson distribution).

TABLE I-1. Items Needed To Prove Specified Probability at Required Confidence Level.

Confidence Interval, %	Number of Items for a Given Probability					
	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
50	5	46	456	4,556	45,563	455,625
60	7	70	705	7,056	70,560	705,600
70	10	107	1,073	10,732	107,329	1,073,295
80	15	163	1,637	16,383	163,839	1,638,399
90	25	268	2,704	27,058	270,600	2,706,023
95	35	381	3,838	38,413	384,157	3,841,597
98	46	498	5,018	50,216	502,204	5,022,076
99	60	657	6,630	66,352	663,571	6,635,770
99.5	71	781	7,872	78,785	787,918	7,879,242
99.9	98	1,073	10,820	108,296	1,083,058	10,830,671
99.99	137	1,499	15,117	151,306	1,513,195	15,132,085
99.999	176	1,931	19,482	194,992	1,950,087	19,501,037

As the reader can see, the items required to substantiate the requisite reliability for probabilities above 10^{-3} and confidence intervals of at least 90% preclude actual testing. Thus, the easiest way to demonstrate that a S&A device has a risk of premature arming below 10^{-6} is to prove it for a device with two locks/safety features each having a risk lower than 10^{-3}.

REFERENCES

I-1. Naval Air Warfare Center Weapons Division. *Safety and Arming Device Design Principles,* by Steven E. Fowler. China Lake, California, NAWCWD, May 1999. (NAWCWD TR 8431, publication UNCLASSIFIED.)

I-2. Naval Air Warfare Center Weapons Division. *Electronic Safe-Arm Device Design Philosophy,* by R. D. Cope. China Lake, California, NAWCWD, November 1997. (NAWCWD TR 8323, publication UNCLASSIFIED.)

I-3 Naval Sea Systems Command. *Parts Derating Requirements and Application Manual for Navy Electronic Equipment.* Washington, DC, NSSC, 1991. (NSSC TE000-AB-GTP-010, Revision 1, publication UNCLASSIFIED.)

I-4. North Atlantic Treaty Organization. *Standardization Agreement 4187, Edition 3, Fuzing Systems—Safety Design Requirements,* by AC/310. Brussels, Belgium. NATO, 2 November 1999. (STANAG 4187 Edition 3, publication UNCLASSIFIED.)

I-5. Department of Defense. *Department of Defense Design Criteria Standard, Fuze Design, Safety Criteria for,* by Fuze Engineering Standardization Working Group. Washington, DC, DOD, 10 July 1998. (MIL-STD-1316E, publication UNCLASSIFIED.)

DOCUMENTATION

I-1. Weapon System Explosives Safety Review Board. *Technical Manual for Electronic Safety and Arming Devices with Non-Interrupted Explosive Trains.* WSESRB, 31 December 1993. (Publication UNCLASSIFIED.)

NOMENCLATURE

σ	standard deviation
ASIC	application-specific integrated circuit
ESAD	electronic safe-arm device
FPGA	field programmable gate array
S&A	safe and arm

(This page intentionally left blank.)