NOT MEASUREMENT SENSITIVE

MIL-HDBK-504
10 February 2004

DEPARTMENT OF DEFENSE
HANDBOOK

GUIDANCE ON SAFETY CRITERIA FOR INITIATION SYSTEMS

This handbook is for guidance only.
Do not cite this document as a requirement.

AMSC N/A FSC:13GP

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

FOREWORD

1. This handbook is approved for use by all departments and agencies of the Department of Defense.

2. This handbook is for guidance only. This handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.

3. This handbook contains reference comments for the definitions and requirements in the Military Standards MIL-STD-1316, Safety Criteria for Fuze Design and MIL-STD-1911, Safety Criteria for Hand Emplaced Ordnance Design. It should be noted that a large part of the technical content is specific to MIL-STD-1316E and MILSTD-1911A, and that the applicable paragraphs are annotated accordingly. It will be expanded soon to include MIL-STD-1901, Safety Criteria for Munition Rocket and Missile Motor Ignition System Design. The comments are based on lessons learned about initiation safety systems and are intended for use by both contractor and government personnel. The comments further document for readers the historical basis of some requirements, especially where technology advances could require updating of the requirements.

4. The text assumes that the reader is familiar with the differences between an initiator, a detonator, and a squib, and the technology and nomenclature used in the design of initiation systems, such as the term in-line.

5. The following format is used throughout this document: a requirement from the cited reference document is presented and then comments are presented. A reader only need review the requirement(s) of interest. Suggested additions and changes should be limited to comments that would be useful to the entire community. Additions should have concise text, since lengthy comments will reduce usage of the document.

6. Comments suggestions, or questions on this document should be addressed to: Commander, US Army Armament Research Development and Engineering Center, Attn.: AMSRD-AAR-AIC-S, Picatinny Arsenal, NJ 07806-5000 or emailed to vcharles@pica.army.mil. Since contact information can change, you may want to verify the currency of this address information using the ASSIST Online database at www.dodssp.daps.mil.

PARAGRAPH PAGE

1. SCOPE

1.1 Scope. This handbook contains background and guidance information on the intent of the safety standards (MIL-STD-1316 and MIL-STD-1911) that are applied to munition initiation systems. It is intended for use by both government and contractor personnel. This handbook will document historical rationale for a number of requirements, in order to preserve them for future reference. This will allow proper judgement in those cases where technology changes may require tailoring of requirements. This handbook is also intended to provide information for developers to avoid known or common mistakes in the design of initiation systems. This handbook is for guidance only. This handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed below are not necessarily all of the documents referenced herein, but are the ones that are needed in order to fully understand the information provided by this handbook.

2.2 Government documents.

2.2.1 Specifications, standards, and handbooks. The following specifications standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-1316	Fuze Design, Safety Criteria for
MIL-STD-1911	Hand-Emplaced Ordnance Design, Safety Criteria for

(Copies of these documents are available on line at http://assist.dla.mil/quicksearch/ or www.dodssp.daps.mil or from the Standardization Documents Order Desk, Bldg. 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.)

2.2.2 Other Government documents, drawings and publication. The following other Government documents, drawings and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

NAVSEA OD44942	Weapon System Safety Guidelines Handbook
AFSC Design Handbook DH 1-6	System Safety
Nuc Reg 0492	Fault Tree Handbook

(Source for ODs is: Commander, Port Hueneme Division, Naval Surface Warfare Cente;r, Code 6001E, Port Hueneme, CA 93043-4307)

(Source for DH 1-6 is: ASC/ENOI, 2530 Loop Road West, Wright Patterson AFB, OH 45433-7101)

(Copies of Nuc Reg 0492 can be obtained from the following sources: 1)GPO Sales Program, Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555; 2) The NRC Public Document Room, 11555

Rockville Pike, Mail Stop O1F13, Washington, DC 20555-0001 and 3) http;//www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492)

3 DEFINITIONS

3.1 Detent. A mechanical device that directly restrains an explosive train interrupter's motion prior to arming. It is coupled to the interrupter, and is overcome by the force or torque exerted on it by the interrupter through its interaction with the interrupter during arming. An example of a detent is a spring clip or shear pin that retains a rotor or slider in place when subjected to the environments which are normally experienced prior to arming, but is overcome by the energy that moves the rotor or slider to the armed position. It is not to be confused with a lock.

3.2 Lock. A mechanical device that directly restrains the explosive train interrupter(s) in the safe position during all credible environments including the direct application of the arming energy to the interrupter. It releases the interrupter when it senses the proper environment. The proper environment must be one that is unique to the intended initiation of the launch or emplacement sequence. An example of a lock is a spring loaded spin lock, that restrains the interrupter under all environments normally experienced prior to arming, but is overcome by a centrifugal force indicative of spin induced by gun launch. In addition, if the torque derived from the centrifugal force is applied only to the interrupter with the spin lock engaged, the lock will still restrain the interrupter.

4. COMMENTS ON MIL-STD-1316 SAFETY CRITERIA FOR FUZE DESIGN

This section is organized with paragraphs, using the same title as the requirement or definition as quoted in MIL-STD-1316E. The paragraphs are listed alphabetically.

4.1 Analyses: "MIL-STD-1316E, Analyses. The following analyses shall be performed to identify hazardous conditions for the purpose of their elimination or control.

a. A preliminary hazard analysis shall be conducted to identify and classify, hazards of normal and abnormal environments, as well as conditions and personnel actions that may occur in the phases before safe separation distance. This analyses shall be used in the preparation of system design, test and evaluations requirements. (See 6.5)

b. System hazard analyses and detailed analyses, such as fault tree analyses, and failure mode effects and criticality analyses, shall be conducted to arrive at an estimate of the safety system failure rate and to identify any single point or credible failure modes.

c. For fuzing systems containing an embedded microprocessor, controller or other computing device, the analyses shall include a determination of the contribution of the software (see 4.2.4) to the enabling of a safety feature.

d. Where the software is shown to directly control or remove one or more safety features, a detailed analysis and testing of the applicable software shall be performed to assure that no design weakness, credible software failures, or credible hardware failures propagating through the software can result in compromise of the safety features.

4.1.1 Comments on Analyses:

a. An early step in the process of designing of a safety system that is often overlooked is the performance of a hazard analysis. A detailed analysis, such as a Fault Tree Analysis (FTA), is required at the completion of a program for design verification by the safety review authorities. However, other analyses should be performed before the design is so mature that it is difficult to correct. Even when early analyses are conducted, a common mistake is to assume hardware will fail selectively, or to trivialize the evaluation. An example is to assume an internal failure in an IC will be safe because the same IC BIT logic will prevent an unsafe failure. It is a mistake to conclude that a failed hardware component can correctly and safely detect its own fault.

b. There are several analysis tools that could be included in the preliminary hazard analysis before any hardware is built or bread boarded.

1) Credible circumstances. A list of reasonable munition scenarios and environments should be developed. This is not the list of normal life cycle environments; an accident is usually caused by a combination of environments, and the stress from accident environments

often significantly exceed those of normal environments. Some services have baseline lists of environments they use for internal purposes, but there are no complete lists available. Judgment is required to generate this list, based on the characteristics of the system under review, and the anticipated manufacture-to-target sequence of events.

2) Credible circumstance review. A first analysis tool is to systematically predict the behavior of the safety system during and after each credible circumstance. This is similar to a conventional potential hazards review, except it is at the safety and arming device (S&A) level, and must consider combinations of environments that match the circumstance.

c. Once a block diagram of the safety system is proposed:

1) A "broad brush" FTA is especially useful for electronic systems to predict a worst case detailed FTA failure rate. The analysis can be performed when a basic block diagram and possible basic hardware devices have been proposed. Form an FTA based on the block diagram and the location of functions in specific integrated circuits (IC) (and other electronic components). Assign IC failure rates for each output according to the whole IC (for multiple IC outputs use a common mode failure rate of one), rather than attempting to predict the details of the internal circuitry (0.0005 is a common failure rate for high reliability IC's).

2) Another analysis tool that is particularly useful is to perform an analysis of subverted safeties. The evaluator analytically reviews normal operation while intentionally subverting an individual safety feature (locks, individual components of locks, logic, etc.) to the unsafe state. Each safety feature is subverted one at a time in turn. The performance of the design then should be evaluated for response to expected life cycle environments. This procedure is especially effective at exposing single point failure mechanisms and weaknesses.

d. Techniques for conducting the required detailed fault tree analyses are described in NAVSEA OD44942, AFSC Design Handbook DH 1-6, and Nuc Reg 0492.

e. Poor FTA analyses are very common. The most common problem is formulating an analysis that accurately represents the functional logic of the system. It is imperative that undesired events be properly selected and accurately delineated in a systematic, repeatable manner in order for the analysis to be valid. The most controversial part of the FTA is assessing the failure rates of the components. It is recommended that the developers ensure the failure rates used are consistent with rates previously used for similar hardware designs (contact the service safety authority). This analysis typically can only be performed with close coordination between representatives of the service safety authority and the developer.

f. An area of concern for electronic safety and arming devices (ESADs) that are used with in-line explosive trains is when the arming delay was based on a single timer or double integration. This design cannot pass the safety analyses described above. Another area of concern is when the partitioning of safety critical logic and components is inadequate. If safety

depends too much on a single device, the ability of the design to meet requirements becomes questionable.

g. Some safety review authorities may request a sneak circuit analysis of the safety circuitry as part of the detailed analyses. A common misconception is that sneak circuit analysis is a thorough review of the circuitry. A sneak circuit analysis only investigates the potential of a circuit to operate with unexpected circuit behavior independent of component failures; it is not a failure analysis.

4.2 Application: "MIL-STD-1316E, Application. This standard applies to the design of fuzes and S&A devices."

4.2.1 Comments on Application:

a. The safety system design requirements of the referenced military standards are a reflection of the best safety system design implementations and practices developed over the years. On first examination the requirements for the different munition classes (warheads, rocket motors, and hand emplaced ordnance) can appear to be inconsistent. While the required safety system failure rate (not to exceed one failure in one million) remains constant, other requirements as well as what is meant by the term "safety system" varies among the munition classes.

b. In the development of a safety system it is important that the basis for the requirements and the variations, be understood. When comparing requirements for the different types of ordnance systems, the following thought is likely to occur: "If this approach is safe enough for hand emplaced ordnance (HEO) or rocket applications it should be safe enough for warhead applications as the failure of any of these safety systems can be catastrophic." This discussion is intended to present the reasons why this logic is not accepted in the safety community, and why the requirements for warhead, rocket motor, and HEO safety systems should not be, and are not the same.

c. The following illustrates some of the variations;

(1) Warhead applications - the "safety system" is the aggregate of devices included in the fuze/S&A that prevents unintentional arming and functioning. Specifically, for out of line implementations, two independent safety features, enabled by different environments and each locking the interrupter in the safe position are required.

(2) Rocket and missile motor applications - the "safety system" is the aggregate of devices in the ignition safety device (ISD), the munition, the launcher, and the launch platform that prevent unintentional arming or functioning. Only one independent safety feature is required on the interrupter of the ISD.

(3) HEO applications - the "safety system" is the aggregate of safety features and devices of the HEO and the procedures associated with its use, that eliminate, control or mitigate hazards from the HEO throughout its life cycle. Two independent safety features, enabled by different actions in a specific sequence, each capable of preventing unintentional arming are required.

d. The safety system designer's job is different than most designers in that the main objective, providing acceptable safety, is only quantifiable or measurable subjectively. Faced with the potentially catastrophic consequences associated with a safety system failure, the DOD safety community has adopted the approach of establishing a set of minimum requirements, which, when adhered to, provides an acceptable level of safety. Included in these is the requirement that the system safety failure rate be calculated, and that it not exceed one failure in one million. The failure rate, SSFR determined by this calculation is not the ultimate measure of, or deciding factor in determining the acceptability of a given design, but is one important tool to help determine that minimum safety requirements are met. The approach of using design requirements along with a calculated failure rate ensures meeting the overriding objective of providing the safest system possible within the overall system level requirements.

e. In theory, it would be desirable to have one set of minimum requirements applicable to all types of munition explosive initiation systems. This set of preferred requirements would employ the most conservative approach, and would, for example, mandate the use of environmentally derived energy (derived from unique and distinct environments) to remove safety features. However, in reality there are constraints imposed on the safety system designer, such as volume, power, and the availability of unique and distinct environments, which vary tremendously between munition classes. These constraints force designers to deviate from the theoretical set of preferred design guidelines, to a set of implementation options that determine the ultimate level of safety that is achievable. When constraints dictate the use of design options other than the preferred, the resultant degradation of the safety level must be compensated for in the best manner possible. In keeping with the objective of providing the safest system possible, a safety system developed and judged acceptable under a specific set of limitations should not be used as a benchmark for judging the acceptability of safety systems not constrained by the same limitations. This is the reason for the variations in safety requirements for different munition classes that is reflected in this document. It should be noted that reviewing authorities do not accept justifications to reduce safety below acceptable levels based on programmatical constraints, such as cost and schedule.

f. To illustrate the preceding point, consider arming environments, a key design variable for the safety system designer. Generally the more distinct or unique from the normal handling and logistical environments (including potential abnormal environments) the available arming environments are, the easier it is to implement a safety feature that takes advantage of this difference. Consider that it would be easier to design a safety feature which would be removed under the influence of the tens of thousands of g's available during gun launch, as opposed to one that must be removed under tens of g's experienced during a missile launch, and still provide the same level of safety from normal logistical and potential adverse environments. Missile and

projectile warhead applications typically provide the designer with the most unique arming environments. Rocket motor safety systems in general, do not have unique flight environments available for use by safety system designers, and therefore, adjustments are made to the requirements in that other munition or launcher system features are used to provide additional safety. HEO's typically represent a special case, since in most cases unique environmentally derived arming environments are not available. This is compensated for by requiring specific operational procedures and sequencing of actions to provide an acceptable level of safety. This compensation can come with increased risk and costs. The use of operational procedures in place of environmentally derived environments places a much heavier reliance on human interaction in these systems. The safety provided by this approach is more difficult to quantify due to the human element, which in some cases represents an increased risk, i.e., the potential for intentional removal of safety features prior to emplacement. Meeting the requirement for sequencing of safety features may lead to increased complexity of designs. HEO safety system designs may lead to additional indirect costs incurred in the training required to familiarize personnel with these operations and to minimize the potential increased risks.

g. It should be noted that the same type of variations in constraints occurs within munition classes covered by one standard. For instance the characteristics of the arming environments available for an artillery projectile fuze and a free fall bomb fuze are normally considerably different. This leads to a similar situation where bomb fuze safety systems are normally more complicated than projectile fuze safety systems, and are usually considered to involve greater safety risks. Similarly, it may be necessary in some warhead safety system applications to allow a portion of the safety features to be located outside of the basic configuration item usually identified as the S&A or fuze, similar to what is done for rocket motor safety systems. This decision involves additional costs and risks that may not be immediately obvious. In this case, the number of configuration items involved and the number of people responsible for their maintenance over the life of the munition are increased. The procedures used in the documentation and control of critical safety features over the life of the munition, the safety and hazard analysis, and any unique safety related qualification testing of the safety system, would now apply to portions of the munition system designated as part of the safety system. In some applications this type of approach may be justified, but again it is important that exception does not become the rule.

4.3 Approved explosives:

"MIL-STD-1316-E, TABLE I. Approved Explosives

Explosive	Specification
Comp A3	MIL-C-440
Comp A4	MIL-C-440
Comp A5	MIL-E-14970
Comp CH6	MIL-C-21723
PBX 9407	MIL-R-63419
PBXN-5	MIL-E-81111
PBXN-6	WS-12604
DIPAM	WS-4660
HNS Type I or Type 2 Gr A	WS-5003
HNS IV	MIL-E-82903
* Tetryl	MIL-T-339
* Tetryl Pellets	MIL-P-46464

* No longer manufactured, not for use in new developments"

4.3.1 Comments on Approved explosives: New explosives can be accepted for a particular application by one service, but to be certified for general in-line use, the tests need to be accepted by the authoritative experts in all services. Reviews of a material for inclusion in this table can be time consuming, especially if a test characteristic is marginal or a manufacturing process is difficult to document adequately for transfer to another source.

4.4 Armed: "MIL-STD-1316E, Armed. A fuze is considered armed when any firing stimulus can produce fuze function.

a. A fuze employing explosive train interruption (see 5.3.3) is considered armed when the interrupter(s) position is ineffective in preventing propagation of the explosive train at a rate equal to our exceeding 0.5 percent at a confidence level of 95 percent.

b. A fuze employing a non-interrupted explosive train (see 5.3.4) is considered armed when the stimulus available for delivery to the initiator equals or exceeds the initiator's maximum no-fire stimulus (MNFS)."

4.4.1 Comments on Armed:

a. There is more than one possible use for the word "armed". The principal use of the word armed is for establishing the point at which the arming delay ends. When the probability of propagation of the explosive (or firing) train, given a proper stimulus, exceeds a certain level, the device is considered armed. The arming delay is then used to calculate a minimum arming

distance which must be greater than the safe separation distance for the intended application. The safe separation definition of armed as used in MIL-STD-1316 should not be confused with the meaning of "armed" used in a reliably sense (tactically functional at a .99 or greater reliability. This is used to indicate the minimum target engagement distance. As an illustration, consider a progressively armed rotor that starts at 90 degrees out-of-line. By the definition of armed, the system is considered armed at perhaps 40 degrees (or less) out-of-line when the probability of propagation exceeds .005, but the system will not be fully armed (tactically reliable) until the system is perhaps less than 2 degrees out-of-line. Similarly, an ESAD is considered armed for safe separation purposes when the charge on the firing capacitor rises to a level where the probability of firing the initiator reaches .005 at, for example, 600 volts, but the device is not tactically armed until it rises to the operationally reliable level of, for example, 1500 volts.

b. The use of the word "any" is significant where it states: ... "or any firing stimulus can produce fuze function." This wording was used to include firing stimuli that are accidental, or have a form other than the expected firing stimulus, such as a mechanical shock when the expected firing stimulus is electrical in nature.

4.5 Arming delay: "MIL-STD-1316E, Arming delay. The time elapsed, or distance traveled by the munition, from launch to arming (see Definition and Arming Delay requirement of MIL-STD-1316E)."

4.5.1 Comments on Arming delay:

a. A common misconception is that a previously approved fuze is acceptable in a new or upgraded munition without changing the arming delay. In a modified weapon using the same warhead explosives and munition structure, the safe separation distance usually remains constant. However, if the munition flight velocity profile changed, the fuze arming delay may need to change to assure the fuze arms after the munition achieves safe separation. Alternately, if the basic munition structure or the warhead changed, then the safe separation distance probably changed. In this case a new safe separation distance must be established by test, and the arming delay may need to be reset to be compatible with an adjustment to the safe separation distance.

b. Another common misconception is that arming delay is the same as safe separation. Arming delay, normally time, is a performance characteristic of the fuze design. Arming delay should not be confused with safe separation, which is a function of the fragmentation pattern of the munition, (independent of the fuze arming delay) and is usually expressed as a distance.

c. Also see Safe separation distance.

4.6 Common mode failures: "MIL-STD-1316E, Common mode failures. Multiple failures that result from, or are caused by, seemingly unrelated failures or an adverse environment.

Examples include the failure of two gates on a single digital integrated circuit due to loss of the ground lead to the chip or failure of two transistors due to exposure to a high temperature environment."

4.6.1 Comments on Common mode failures:

a. Common mode failures can be induced by personnel actions, through the use of common materials, component location, energy sources, functional actions, etc. Examples: A voltage regulator failure causes over-voltage on safety logic devices, which in turn arm the safety system as they fail. Mechanical logic devices (sequential leafs, G-weights, etc.) that function in the same direction may be vulnerable to common mode failure; an abnormal force sufficient to overcome one safety may defeat all the safeties to the same unsafe condition.

b. Traditional methods to reduce the risk from common mode failures can be physical or functional. Physical techniques can consist of selection of different technology components and their packaging. Functional techniques can consist of processing different types of signals, applying proper power management (to include return/ground references) and systematic signal controls (interrupts, reset circuits).

c. Partitioning is another method commonly used to reduce the risk of common mode failures within electronic safety and arming devices (ESAD) and other electronically controlled fuzes. "Partitioning" here consists of a physical separation, or the use of positioning control of the energy interrupters to avoid susceptibilities from similar environments and conditions.

d. The circuit which controls operation of the arming switches should be physically partitioned into at least two elements, none of which are capable (by virtue of circuit architecture and partitioning, not element design) of independently arming the system. The functional partitioning must be essentially immune to being bypassed by normal or abnormal electrical, mechanical, and thermal environmental hazards. Requiring the S&A control logic to be partitioned into at least two independent arming switch drive elements is comparable to requiring dual safety for a mechanical S&A device. That is not to say that a safe system could not be built with a single circuit element (IC). However, such "single-chip" designs are not being allowed because of the difficulty in proving that a complex single element can give a safety failure rate of less than one in a million units. By having more than one physically independent control element, the safety failure rate of each contributes to the overall safety requirement and each one independently does not have to provide safety to 10^{-6}.

4.7 Credible environment: "MIL-STD-1316E, Credible environment. An environment that a device may be exposed to during its life cycle (manufacturing to tactical employment, or eventual demilitarization). These include extremes of temperature and humidity, electromagnetic effects, line voltages, etc. Combinations of environments that can be reasonably expected to occur must also be considered within the context of credible environments."

4.7.1 Comments on Credible environment: This term was borrowed from the general safety community. Credible environments include those that are believable but not necessarily expected, such as bullet impact, accidental circuit exposure to 120 VAC, or exposure of electronics to maximum source voltage when a voltage regulator fails. An example of a non-credible environment is multiple bullet impacts - all in the same hole.

4.8 Credible failure mode: "MIL-STD-1316E, Credible failure mode. A failure mode resulting from the failure of either a single component or the combination of multiple components, that has a reasonable probability of occurring during a fuzing system's life cycle."

4.8.1 Comments on Credible failure mode: Examples include failure modes in an IC that may not be easily predicted by the schematic, but can occur because of the mechanical layout or method of construction (the dominant storage IC failure mechanism is caused by chemical corrosion).

4.9 Design approval: "MIL-STD-1316E, Design approval. At the inception of engineering development, the developing activity should obtain approval from the cognizant safety authority of both the design concept and the methodology for assuring compliance with safety requirements. At the completion of engineering development, the developing activity shall present a safety assessment to the cognizant safety authority (see 4.9) for review to obtain approval of the design."

4.9.1 Comments on Design approval: For maximum benefit, designs should be reviewed as soon as possible during concept development. Guides to help in the preparation of presentations may be available from the review boards. A widely held misconception is that a previously accepted or waivered design is automatically acceptable in a new application. Whether old or new, each candidate for a new application must be assessed against the current requirements based on its own design merits.

4.10 Design for Quality control, inspection, and maintenance:

"MIL- STD-1316E, Design for Quality control, inspection, and maintenance.

a. Fuzes shall be designed and documented to facilitate application of effective quality control and inspection procedures. Design characteristics critical to fuze safety shall be identified to assure that the designed safety is maintained.

b. The design of the fuze shall facilitate the use of inspection and test equipment for monitoring all characteristics which assure the safety and intended functioning of the fuze at all appropriate stages. The fuze design should facilitate the use of automatic inspection equipment.

c. Embedded computing systems and their associate software (firmware) shall be designed and documented for ease of future maintenance. Software development shall be in

accordance with accepted high quality software development procedures, such as MIL-STD-498."

4.10.1 Comments on Design for Quality control, inspection, and maintenance:

a. The manufacturing data packages must document the entire fuze safety system, normally consisting of a single configuration item. It may be necessary to locate components essential to perform the fuzing safety function, such as a sensor, outside the basic configuration item usually identified as the fuze. Such components must be referenced within the fuze data package so they are documented as part of the fuze.

b. Safety critical design characteristics: In addition to those safety features that directly prevent inadvertent arming, aspects, characteristics, or components of a design that are unique and required to prevent inadvertent subversion of a safety feature should be identified as safety critical, with an associated explanation provided in the appropriate manufacturing and acquisition data packages describing why it should not be altered. Examples of safety critical design characteristics:

1) Microprocessors have dual-use input/output ports, with any port pin capable of being either an input or an output according to the program performed by the microprocessor. Used in safety systems, the inputs are isolated by diodes to prevent an inadvertent output from an input port from influencing the other circuitry.

2) At times the specific materials used in a barrier can be critical to passing the safety tests. If a barrier is made from a special steel, document the critical steel characteristics and the reasons for the material selection.

4.11 Electrical firing energy dissipation: "MIL-STD-1316E, Electrical firing energy dissipation. For electrically initiated fuze explosive trains, the fuze design shall include a provision to dissipate the firing energy within 30 minutes of the expiration of the fuze arming life, or a fuze failure. The dissipation means shall be designed to prevent common mode failures."

4.11.1 Comments on Electrical firing energy dissipation:

a. This is a requirement for both in-line and out-of-line fuzes and applies to the device (usually a capacitor) that stores the firing energy directly used by the initiator. Munition batteries are required to meet this requirement unless they cannot develop a hazardous current in the initiator with the other fuze energy storage devices depleted (eg. firing capacitor). Service safety authorities may exempt the battery from the requirement if closing the firing switch after the fuze arming life cannot develop a current in the initiator exceeding its no-fire level

b. After the firing energy has dissipated (30 minutes) an electrically initiated out-of-line system that was armed during use, is still "armed" and unsafe even though the primary firing mode has been eliminated. Thirty minutes was chosen because it was regarded to be a practical time limitation.

c. An acceptable way to meet this requirement and to prevent common mode failures is as follows. Redundant bleed resistors are mounted on orthogonal axes, as far from each other as practical, and in a manner reducing the probability of damage from corrosion or physical force to both resistors without similarly damaging essential firing circuit components (typically the capacitor & switch). A better technical solution is preferred, but may currently be unavailable.

d. The primary purpose of the energy depleting resistors is to assure that any energy inadvertently developed on the firing circuit is automatically dissipated. This feature may also be used for EOD purposes.

4.12 Electrical initiator sensitivity: "MIL-STD-1316E, Electrical initiator sensitivity. The initiator for electrical fired non-interrupted explosive train shall:

a. Meet appropriate characteristics listed for Class B initiators of MIL-DTL-23659.

b. Not exhibit unsafe degradation when tested in accordance with MIL-STD-1512.

c. Not be capable of being detonated by any electrical potential less than 500 volts.

d. Not be capable of being initiated by any electrical potential of less than 500 volts, when applied to any accessible part of the fuzing system after installation into the munition or any munition subsystem."

4.12.1 Comments on Electrical initiator sensitivity:

a. Just as Tetryl was accepted as a safe standard for explosive sensitivity, a level of insensitivity of 500 volts for initiators was accepted to assure initiators are insensitive to electrical stimuli that might be seen during munition repairs, rework, etc. The establishment of the 500 volt threshold was apparently based on the 440 volt power that is commonly available on military equipment and in test facilities. The 500 volt level is considered to provide an acceptable safety margin while still providing a threshold that could readily be achieved through design.

b. EFIs are accepted as meeting the 500V no-detonate requirement based on the predicted no-fire voltage and unique energy characteristics from the fire set. This is acceptable because, for current designs, the EFI's fire set is tuned for that initiator by optimizing the fire set to reliably fire the initiator at the lowest possible energy. If the no-fire voltage delivered to the initiator by that fire set is above 500V then it is accepted that other 500V wave forms will not create a

detonation. Initiators that do not utilize a tuned fire set may readily detonate at voltages less than 500V, and therefore would be unacceptable to meet "Electrical Initiator Sensitivity" (Not be cable of detonated by any electrical potential of less than 500 volts) requirement of MIL-STD-1316E". All initiators should be reviewed with respect to the intent of the requirement. The initiator must not detonate at any electrical potential less than or equal to 500 volts.

c. Meeting the requirement for "Electical Initiator Sensitivity" (applied potential of less than 500 volts) of MIL-STD-1316E", assures that during or after final installation of the item containing the initiator into the munition (or munition subsystem) will not initiate (either detonate or deflagrate) as a result of an accidental electrical input to any leads that may be accessible to assembly, test or repair personnel. If the initiator leads are directly accessible, then the requirement applies to the initiator itself; generally though, the requirement applies to a fire set, or the S&A as a whole.

4.13 Electromagnetic environments: "MIL-STD-1316E, Electromagnetic environments. Fuzes, in their normal life cycle configurations, shall not inadvertently arm or function during and after exposure to: electromagnetic radiation (EMR), electrostatic discharge (ESD), electromagnetic pulse (EMP), electromagnetic interference (EMI), lightning effects (LE) or power supply transients (PST). In addition, fuzes shall not exhibit unsafe operation during and after exposure to the above environments. Fuzes shall be tested or evaluated for:

a. EMR per MIL-STD-1512 and MIL-STD-464

b. ESD per MIL-STD-331

c. EMP per DOD-STD-2169

d. EMI per MIL-STD-461 and MIL-STD-462

e. LE - per MIL-STD-464

f. PST by appropriate test and analysis

4.13.1 Comments on Electromagnetic environments:

a. Insensitivity to power supply transients is a requirement for electronically controlled safety systems for two reasons. First, electronic devices are exposed to electrical noise, an environment that they may be susceptible to. Second, existing MIL-STD requirements such as MIL-STD 461 and MIL-STD-462 were never intended to address fuzing PST requirements and are considered inadequate for evaluating responses to noise levels. While subsystems are usually required to meet 461 specifications, the overall munition system is not required to be below the 461 conducted susceptibility levels; and such a requirement would usually be a severe design

constraint. It is better to assure that the subsystem has a design margin so it will be safe when exposed to credible voltages and noise levels.

b. Power supply transients (system noise, circuit noise, ground loops & shifts, generators, return/ground line noise, etc.) are known to be capable of causing inadvertent arming and are a source of common mode failure mechanisms. The ARMY requires a special test that exposes any electronically controlled safety and arming system to the known system noise voltage, amplified by 10 dB (or times 3.16). The unit must remain safe during the test.

4.14 Electronic logic functions: "MIL-STD-1316E, Electronic logic functions. Any electronic logic related to safety functions performed by the fuze shall be embedded as firmware or hardware. Firmware devices shall not be erasable, or alterable by credible environments which the fuze would otherwise survive."

4.14.1 Comments on Electronic logic functions: Control of independent safety features by reprogrammable or erasable electronic logic devices or software is not allowed. Any logic used in a safety critical capacity should be implemented in firmware or hardware. Care should be taken with safety logic devices that the integrity of the separate environments used for enabling independent safety features is maintained and common mode failures are avoided. Additionally, when determining safety failure rates, common mode failures in electronic logic devices should be considered so that safety is not over estimated. Certain functions that occur after arming, such as the time delay between two firing signals, are not considered safety critical and may be programmable. Software can require a separate review and developers should contact the service representative for special guidelines or requirements.

4.15 Environment: "MIL-STD-1316E, Environment. A specific physical condition to which the fuze may be exposed."

4.15.1 Comments to Environment:

a. There are two types of environments: arming environments and risk environments.

b. Arming environments are normally selected from specific environments associated with the use of the weapon system (launch acceleration, spin, flight velocity, etc); selecting the appropriate arming environments can significantly simplify the safety system design.

c. Risk environments can include any credible environment; designers should be alert to the effects of induced credible environments such as electrical noise on logic, or vibrations on mechanical devices. Electrical circuit noise is an environment for electronic logic devices.

d. A common misconception concerning launched weapons is that acceleration and velocity form two different environments when velocity is determined by the integration of the acceleration. This process is vulnerable to common mode failure mechanisms that could create

both environmental stimuli simultaneously. To use acceleration and velocity as independent environments, they must be sensed by different sensors, with velocity sensed directly, such as by wind pressure, rather than by an integration (derived via accelerometer).

4.16 Explosive compositions: "MIL-STD-1316E, Explosive compositions. Explosive compositions in fuzes shall be qualified for use in accordance with OD 44811 or MIL-STD-1751 in their intended role in explosive trains."

4.16.1 Comments on Explosive compositions:

a. While it is unusual, primary explosives can auto initiate; that is function without any external firing stimulus at all. This is one reason such explosives must be kept out-of-line. To assure these hazards are controlled, the main explosive in a system is limited to explosives that are known to be stable and acceptably insensitive.

b. The historical basis for evaluating acceptable secondary explosive sensitivity criteria (ESD, shock, temperature, materials compatibility, aging, etc.) is Tetryl - chosen because the explosive had an acceptable safety record. Through time, as individual tests were refined, the pass-fail threshold levels were rounded - conservatively. As a result, Tetryl and some other approved secondary explosives will not pass the current in-line explosive test requirements.

4.17 Explosive ordnance disposal: "MIL-STD-1316E, Explosive ordnance disposal (EOD). Features shall be incorporated in fuzes that facilitate their being rendered safe by EOD tools, equipment and procedures even if sterilization or self-destruction features are incorporated."

4.17.1 Comments on Explosive ordnance disposal:

a. EOD can be a programmatic problem if sufficient planning has not been made. EOD should be considered early in the program and is one of the reasons an early design review is recommended. Additionally, EOD appraisals often require testing of some hardware which requires budgeting. Blow-in-place is not considered an acceptable solution.

b. In accordance with system requirements, munitions which contain self-destruct features should be provided with a positive means of identifying if the self destruct mechanism has not functioned.

4.18 Explosive train interruption: "MIL-STD-1316E, Explosive train interruption.

a. When an element of the explosive train contains explosive material other than allowed by 5.3.2, at least one interrupter (shutter, slider, rotor) shall functionally separate it from the lead and booster explosives until the arming sequence is completed as a consequence of intentional launch. The interrupter(s) shall be directly locked mechanically in the safe position by at least

two independent safety features. These safety features shall not be removed prior to initiation of the launch cycle.

b. If the primary explosive is positioned such that omission of the interrupter will prohibit explosive train transfer, a single interrupter locked by the two independent safety features is acceptable.

c. If the primary explosive is positioned such that safety is dependent upon the presence of an interrupter, the design shall include positive means to prevent the fuze from being assembled without the properly positioned interrupter.

d. The effectiveness of interruption for the fuze explosive train in its configuration prior to initiation of the arming sequence shall be determined numerically in accordance with the Primary Explosive Component Safety Test of MIL-STD-331. If the explosive train interruption is removed progressively after intentional initiation of the launch sequence, the relationship between interrupter position and its effectiveness shall be established by a progressive arming test conducted in accordance with the Primary Explosive Component Safety Test, using a test strategy given by the Projectile Fuze Arming Distance Test of MIL-STD-331. The chosen test strategy and results shall be presented and justified to the appropriate service safety authority."

4.18.1 Comments on Explosive train interruption: Systems that incorporate a delay in the arming process, such as a rotor that is controlled by an escapement, should have the .005 probability-to-fire point defined statistically by a procedure or method such as the Neyer, Langley, Bruceton, etc. Also, see the comments on safety feature, 4.27 of this handbook.

4.19 Launch cycle: "MIL-STD-1316E, Launch cycle. The period between the time the munition is irreversibly committed to launch and the time it leaves the launcher."

4.19.1 Comments on Launch cycle: A launch cycle is considered to be irreversible when a non-restorable launch function occurs and the launch cycle is subsequently out of the gunner's control. For example, when one-shot devices such as thermal batteries in the munition are initiated, it is accepted as an irreversible start of the launch cycle in spite of the fact that the fire control system may interrupt launch if a late error is detected. In addition, a command signal initiating the thermal battery may be acceptable, but not the battery output.

4.20 Main charge: "MIL-STD-1316E, Main charge. The explosive charge which is provided to accomplish the end result in the munition; e.g., bursting a casing to produce blast and fragmentation, splitting a canister to dispense submunitions, or producing other effects for which it may be designed. Main charge explosives are compounds or formulations such as TNT or Composition B, which are used as the final charge in any explosive application. These explosives, because of their relative insensitivity, ordinarily require initiation by a booster explosive."

4.20.1 Comments on Main charge: The term main charge includes the energetic material causing submunition dispersal or that in other dispenser systems.

4.21 Maximum no-fire stimulus: "MIL-STD-1316E, Maximum No-Fire Stimulus (MNFS). The stimulus level at which the initiator will not fire or unsafely degrade with a probability of 0.995 at a confidence level of 95 percent. Stimulus refers to the characteristic(s) such as current, rate of change of current (di/dt), power, voltage, or energy which is (are) most critical in defining the no-fire performance of the initiator."

4.21.1 Comments on Maximum no-fire stimulus: MNFS is used in the definition for armed. The requirement in a previous version of Safety Criteria for Fuze Design (MIL-STD 1316C) was effectively a probability to fire of 10^{-6}. This value was considered unacceptable as being unrealistic, and a design driver for some systems that must arm quickly, since the time to physically complete arming would be very short between arm delay (safe separation distance) and the minimum tactical engagement distance (which determines the minimum arming distance). The value of 0.005 probability to fire was the compromise reached during discussions to develop MIL-STD-1316D that was consistent for both in-line and out of line safety and arming devices.

4.22 Non-armed condition assurance options: "MIL-STD-1316E, Non-armed condition assurance options. Fuzing system designs shall incorporate one or more of the following:

a. A feature that prevents assembly of the fuzing system in the armed condition.

b. A feature that provides a positive means of determining that the fuzing system is not armed during and after its assembly and during installation into the munition. Where the fuzing system is accessible after installation into the munition, the positive means of determination shall also be available.

c. A feature that prevents installation of an armed, assembled fuzing system into a munition.

If arming and reset of the assembled fuzing system in tests is a normal procedure in manufacturing, inspection, or at any time prior to its installation into a munition, subparagraph a is not sufficient and either subparagraph b or c must also be met."

4.22.1 Comments Non-armed condition assurance options: A feature that prevents assembly of the fuzing system in the armed position should not in itself be capable of being omitted or misassembled during fuze assembly unless the omission or misassembly is readily detectable after fuze assembly.

4.23 Non-interrupted explosive train control: "MIL-STD-1316E, Non-interrupted explosive train control. Explosive train interruption is not required when the explosive train contains only explosive materials allowed by 5.3.2. One of the following methods of controlling fuze arming shall be employed:

a. For systems using techniques for accumulating all functioning energy from the post-launch environment, the fuze shall not permit arming until verification, by the fuze, of a proper launch, and attainment of the required arming delay. Accumulation of any functioning energy shall not occur until as late in the arming cycle as operational requirements permit.

b. For systems using techniques that do not accumulate all functioning energy from the post-launch environment, at least two independent energy interrupters, each controlled by an independent safety feature shall prevent arming until proper launch is verified by the fuze and the required arming delay is attained. Additionally, the fuze shall not be capable of arming in cases of the absence, or malfunction, of any and all energy interrupters."

4.23.1 Comments on Non-interrupted explosive train control:

a. There are special Army (see appendix C) and Navy service requirements for non-interrupted systems; the services expect these guidelines to be met in addition to the requirements of MIL-STD-1316. While the Standard requires only two energy interrupters for example, the Army and Navy waiver guidelines are more conservative and require three switches, at least one being dynamic.

b. The last sentence in the requirement (Additionally, the fuze ... all energy interrupters) forms the requirement to have a dynamic switch (a semiconductor such as a field effect transistor, FET) in an ESAD. The term "malfunction" is generally accepted to mean a static failure. Dynamic failure mechanisms are generally unknown in electronic systems, although microprocessors are known to be capable of failing dynamically. There is very little information available about the detailed behavior of electronic components as they fail, and the interpretation of the paragraph could change if components are discovered that can fail dynamically within a bandwidth (or harmonic) close to that used in the DC to DC voltage multiplier.

c. The requirements for a dynamic switch and partitioning are considered to be fundamental design practices in reducing the probability of unsafe static failures (whether single point or common mode), in in-line electronic safety systems.

4.24 Post safe separation safety: "MIL-STD-1316E, Post safe separation distance safety. When operational requirements necessitate protection of friendly forces in addition to the delivery system and its personnel, one of the following options shall be incorporated in the fuze design:

a. Extension of the arming delay.

b. Control of unintentional functioning after the proper arming delay.

The fuze requirements document shall specify for the selected option a minimum quantitative failure rate for the time frame after safe separation distance to attainment of the required protection."

4.24.1 Comments on Post safe separation safety: Post safe separation distance safety is normally expected for munitions that dispense submunitions and can fly over positions occupied by friendly troops. Overhead safety or post safe separation distance safety is more than the reliability of functioning after arming, it is a feature that prevents final arming or the firing signal from occurring before or after a window of intended function. The user should establish a requirement (10-5 has been used in previous applications).

4.25 Safe separation distance : "MIL-STD-1316E, Safe separation distance. The minimum distance between the delivery system (or launcher) and the launched munition beyond which the hazards to the delivery system and its personnel resulting from the functioning of the munition are acceptable."

4.25.1 Comments on Safe separation distance:

a. There are two reference documents on safe separation distance**.** The first in Appendix A is guidelines prepared by the ARMY to cover weapons that are not air launched. The second in Appendix B is a Tri-service agreement for safe separation for air-launched weapons.

b. Safe separation distance is often confused with fuze arming; it is a characteristic of the warhead independent of the fuze. The purpose of establishing a safe separation distance is to provide safety to launch personnel and the launch platform. Safe separation distance is measured in meters (feet) and is the physical distance from the gunner (or gun crew, platform, etc) to a point where part or all of the munition can function without presenting an unacceptable risk. Safe separation distance has two important variables -- the fragmentation characteristics, and environmental effects (wind usually). The gunner should be acceptably safe from any and all explosive products -- whether from the munition warhead or the propulsion system if it sympathetically initiates. Further, he should be safe even if the wind blows a portion of the munition back on him (for example, a submunition or chemicals). Maneuvering of the delivery platform should be considered for safe separation.

c. The procedure to establish safe separation distance for air-launched weapons is based on the vulnerable area of the aircraft, not just the pilot. If the resulting safe separation distance is tactically unacceptable, there is a potential problem. The procedure describes steps to verify safety even while arming at distances that are less than the safe separation distance.

4.26 Safety and arming device: "MIL-STD-1316E, Safety and arming device. A device that prevents fuze arming until an acceptable set of conditions has been achieved and subsequently effects arming and allows functioning."

4.26.1 Comments on safety and arming device:

a. The safety system should be maintained in a single configuration item not distributed or integrated with other functions. The documentation requirements are for the entire safety system, not only for the device commonly referred to as a fuze or S&A. Developing agencies will be expected to provide a documentation package that covers the complete safety system, i.e., all those elements that combine to meet the requirements of the MIL-STD.

b. It is highly desirable for fuze safety systems to be contained in a single device or assembly (the more localized and isolated the better).

c. Integrating safety functions into other munition hardware creates special problems. For example, the safety system hardware will be expected to demonstrate design margin; other than the safety system components, it is abnormal for hardware to be designed to survive credible environments that exceed life cycle environments. Further, hardware costs associated with conducting safety system tests could be prohibitive.

4.27 Safety feature: "MIL-STD-1316E, Safety feature. An element or combination of elements that prevents unintentional arming or functioning."

4.27.1 Comments on Safety feature:

a. There are several terms that are often misused including - safety feature, interrupter, lock, detent, energy interrupter, and energy control feature.

b. A safety feature can be thought of as anything that contributes to the safety of the system; however, in this standard it is used as one or more components that prevent inadvertent arming. A safety feature performs functions required in this standard. In rare cases safety features can be a single component, but normally they have several. An example of an ESAD safety feature could be the energy interrupter coupled with the logic that senses acceleration and controls the energy interrupter. An example for a mechanical system is a spring biased mass which moves under acceleration to release the interrupter. The interface of the mass with the interrupter is considered part of the safety feature.

c. The term interrupter is used in out-of-line systems and is a physical, movable barrier between the sensitive and insensitive explosives. A set of safety features mechanically lock the interrupter to prevent it from moving during any credible environment.

d. A lock is that portion of the safety feature which prevents the interrupter from moving during any credible normal and abnormal environments up to and including the application of the energy level which moves the interrupter to the armed position.

1) A lock should not be confused with a detent. A lock is defined in 3.2 of this handbook. A lock is retracted to release the interrupter, not overcome by the interrupter itself - due to the arming environment. For example, the restraint on an interrupter armed with a piston actuator output is a lock only if it can withstand a force equal to that applied to the interrupter by that piston actuator. Additionally, the restraint on an interrupter armed by environmentally derived energy is a lock only if it can withstand the force equal to that applied to the interrupter by the environmentally derived energy. The maximum achievable level of energy, resultant torque, or force, either measured or calculated, that can be derived from the arming environment must be used when evaluating the effectiveness of the lock. For example, a Belleville spring or a spring loaded ball which would hold a rotor in place during assembly, but would be overcome to allow arming by either the function of a piston actuator or environmentally derived energy as described above is a detent, not a lock, and the same is true for a shear wire. In summary, if application of any credible force including arming force to the interrupter can overcome the restraining feature, that feature is considered a detent, not a lock.

2) In the past, the spring biased levers that lock the rotor in fuzes for artillery projectiles and are used in some submunition fuzes have been referred to as spin detents or rotor detents in the technical data package. The term detent was used to differentiate these safety features from the setback locks. These features are, in fact, true locks as described above and should be considered as such even though the drawings refer to them as detents.

e. The term energy interrupter is used with in-line systems and can be either a direct or indirect means of controlling arming.

1) An energy interrupter as used in MIL-STD-1316C meant a component directly interrupting the energy path to the initiator. The MIL-STD-1316C energy interrupter was similar to a firing switch but it had to be mechanically locked by safety features just like an out-of-line interrupter. Two interrupters were required if the S&A contained stored energy. When MIL-STD-1316D was created, the term energy interrupter was kept, but now it meant either the interpretation used in MIL-STD-1316C or it could mean energy control feature. An energy interrupter could indirectly control the energy to the firing capacitor (or other storage device) or directly mechanically interrupt the energy to the initiator. The direct interruption has not been used in in-line systems to date.

2) One energy interrupter used in current electronic S&A's is referred to as a "dynamic switch". The switch itself is a semiconductor (usually an FET) that is cycled (between states) to provide proper circuit functions for high voltage conversion. Interrupters should be designed or implemented such that any static failure of the device will disable the dynamic (cyclic) operation of the switch. This intent is subverted when commanding the dynamic switch with circuitry that

is susceptible to simple static failures. An example of this is an oscillator driven switch that only requires a discrete input. Developers have met the requirement in several ways such as an oscillator controlled by AND gates in the feedback loop as well as gates in series with the oscillator input and output.

f. When the Army drafted the Army waiver guidelines to MIL-STD-1316C to permit Electronic Safety and Arming Devices, the term energy control feature was created to avoid confusion with energy interrupter that was used in the MIL-STD. An energy control feature was not directly in-line with the initiator, instead it indirectly prevented arming energy from being developed in the firing energy storage device (capacitor).

4.28 Safety redundancy: "MIL-STD-1316E, Safety redundancy. The safety system of fuzes shall contain at least two independent safety features, each of which shall prevent unintentional arming of the fuze. The stimuli enabling a minimum of two safety features shall be derived from different environments. Utilization in the fuze design of environments and levels of environmental stimuli to which the fuze may be exposed prior to initiation of the launch cycle shall be avoided. Operation of at least one of these safety features shall depend on sensing an environment after first motion in the launch cycle or on sensing a post-launch environment. An action taken to initiate launch may be considered an environment if the signal generated by the action irreversibly commits the munition to complete the launch cycle."

4.28.1 Comments on Safety redundancy:

a. The two independent safety features in a mechanical system means that control of the arming interrupter is accomplished directly by two locks. The two independent safety feature requirement is not met by a lock on a lock. Evaluation of a system for subverted safeties usually will expose this design weakness. In a subverted safety evaluation the safety of the unit is evaluated without the presence of each individual lock in turn. If there are two locks on the interrupter, it is not released by the absence of either one of them.

b. Non-interrupted explosive train control requires in-line warhead fuze safety systems to contain two independent safety features to prevent arming until the required arming delay is attained. Since these safety features must be independent, and thereby free of common mode failures, the design aspect that provides the arming delay in each safety feature must be independent. But, the start of the arming delay may be initiated by the same environment.

4.29 Safety system failure rate: "MIL-STD-1316E, Safety system failure rate. The fuze safety system failure rate shall be calculated for all logistic and tactical phases from fuze manufacture to safe separation or to the point at which friendly forces and equipment no longer need protection. The safety system failure rate shall be verified to the extent practical by test and analysis during fuze evaluation and shall not exceed the rates given for the following phases:

a. Prior to intentional initiation of the arming sequence: one failure to prevent arming or functioning (irrespective of arming) in one million fuzes.

b. Prior to the exit (for tube launched munitions): one failure to prevent arming in ten thousand fuzes, and one failure to prevent functioning in one million fuzes.

c. Between initiation of the arming sequence or tube exit, if tube launched, and safe separation: one failure to prevent arming in one thousand fuzes. The rate of fuze functioning during this period shall be as low as practical and consistent with the risk established as acceptable for premature munition functioning."

4.29.1 Comments on Safety system failure rate:

a. The design safety requirement that the safety systems covered by this document have a failure rate that must not exceed one failure in one million is one that is continuously revisited. While there is almost universal agreement that a numerical safety requirement is needed, there have been, and continue to be, varying opinions on what the numerical value should be, and how to apply it. This variation in opinion results for several reasons. One is that the safety system failure rate is not practically measurable or demonstrable due to its extremely small numerical value. Another is that it is applied without variation to munition systems with different natures and potential hazards and produced at different volumes.

b. The exact origin of the "one in a million" numerical value is unknown. It is believed that this was arrived at as a compromise value between what was an acceptably small enough probability for the occurrence of an undesired event, and the degree of safety that could be practically achieved. The popularly accepted remoteness associated with the term "one in a million" is also considered a likely factor in its selection. At this writing the earliest known documented use of the one in a million safety system failure rate is in a US Navy policy letter on Safety and Arming of Fuzes, dated 8 June 1953. In 1967 it was included as an objective in the first version of MIL-STD-1316 (NAVY), and was first stated as a requirement in MIL-STD-1316B, 1977, which was now a tri-service version of the document. Since that time the "one in a million" safety system failure rate has been incorporated in the first editions of MIL-STD-1901, "Design Safety Criteria for Munition Rocket Motor and Missile Motor Ignition System Design", and MIL-STD-1911, " Safety Criteria for Hand-Emplaced Ordnance Design". It is important to note that while the "one in a million" numerical value is identical in all three of the MIL-STD's, what constitutes a safety system, and a safety system failure, do vary as one would expect. The acceptance and continued support of "one in a million" as a valid requirement by the safety community is reflected via its inclusion in all major initiation design safety documents from 1953 to the present.

4.30 Sterilization: "MIL-STD-1316E, Sterilization. Fuzing systems shall incorporate a sterilization feature based on its applicability to system requirements."

4.30.1 Comments on Sterilization:

a. The goal of sterilization is to provide the safest unexploded munition condition possible, which implies that the fuzing system is permanently incapable of functioning either accidentally or intentionally. Sterilization is preferably accomplished by permanently rendering inoperable or removing the sensitive explosives from the explosive train. Another method of sterilizing a munition may be to incorporate one or more self-destruct features.

b. In accordance with system requirements, munitions which contain self-destruct features should be provided with a positive means of identifying if the self destruct mechanism has functioned.

4.31 Stored energy: "MIL-STD-1316E, Stored energy. Stored energy shall not be employed for enabling or arming when environmentally derived energy, after initiation of the launch cycle, can be practically obtained. Examples of stored energy components are:

a. Batteries
b. Charged capacitors
c. Compressed gas devices
d. Explosive actuators
e. Loaded springs"

4.31.1 Comments on Stored energy: The original concerns about stored energy were for spring armed rotors and enabling features, and piston actuator enabled features. Stored energy increases the probability of the safety system failing in an armed condition. To use stored energy, the developer must prove that environmentally derived energy cannot be practically obtained.

4.32 Visual indication: "MIL-STD-1316E, Visual indication. If visual indication of the non-armed or armed condition is employed in the fuze, visible indicators shall be designed to provide a positive, unambiguous indication of condition. Indicator failure shall not result in a false non-armed indication. If color coding is used to represent condition, the colors and coding shall be as follows:

a. Non-armed condition. Fluorescent green background with the letter S or word SAFE superimposed thereon in white. Colors shall be nonspecular.

b. Armed condition. Fluorescent red or fluorescent orange background with the letter A or the word ARMED superimposed thereon in black. Colors shall be nonspecular.

c. Suggested color specifications.

1) Fluorescent green, Color No. 38901 per FED-STD-595

2) Fluorescent red, Color No 38905 per FED-STD-595
3) Fluorescent orange, Color No 38903 per FED-STD-595."

4.32.1 Comments on Visual indication:

a. The purpose of the visual indicator is to show that the S&A Device is not armed up to the point of installation into the munition whether in the field or at a load plant. In several munitions such as bombs, rocket propulsion ISD's, and some warheads the visual indicator may be required to be visible from outside the munition. It is recommended that the developer check with the cognizant service program authority.

b. Why is a visual indicator not required to be accessible in all munitions after installation? Visual indication of the safe or armed condition like most design features is subject to need evaluation. The benefits of being able to verify that a fuze is in the safe position prior to installation in a loaded munition are fairly obvious. Basically it slants the odds greatly in your favor that you are not just one low energy event away from initiating the munition. In this instance you are getting protection from misassembled units and units that may have been armed during testing and not properly reset. Visual indicators at the fuze level are generally very simple devices such as a letter and an access window, and therefore can be implemented very easily. Once a fuze has been installed (in the verified safe condition) into the munition the benefits are not as great for many applications. In most cases, precautions are taken to assure only fuzes in a verified safe condition are installed in a munition, and follow-on processes and procedures are limited to those which will not lead to arming and re-safing of the fuze. Electrical checks such as low voltage continuity checks are acceptable and routine after assembly. In applications with robust safety features, the possibility of being armed inadvertently after installation is very remote, normally much less than the one in million requirement contained in MIL-STD-1316E. At the same time the opportunity for implementing an accessible visual indicator is basically nonexistent. In instances where the benefits don't justify the implementation problems a visual indicator capable of being viewed after installation should not be required. In applications where robust safety features are not available, safety devices that use manually activated safety features that are routinely exercised for instance, visual indicators that are accessible after installation are required.

5. COMMENTS ON MIL-STD-1911 SAFETY CRITERIA FOR HAND-EMPLACED ORDNANCE (HEO) DESIGN

This section is organized with paragraphs, using the same title as the requirement or definition as quoted in MIL-STD-1911. The paragraphs are listed alphabetically.

5.1 Analyses: "MIL-STD-1911A, Analyses. The following analyses shall be conducted to identify hazardous conditions associated with the HEO. The analyses shall be done early enough in the development process to enable elimination or control of the identified hazards by the design of the HEO.

a. A preliminary hazard analysis to identify hazards of normal and abnormal environments, with special emphasis on conditions and personnel actions that may occur throughout the HEO life cycle. This analysis shall be used in the definition of the HEO design, test and evaluation requirements. (see 6.5)

b. System and major component hazard analyses to estimate the HEO safety failure rate and to identify any single point or credible failure modes. Techniques such as fault tree analysis and failure modes, effects and criticality analysis may be used in carrying out hazards analyses.

c. When the HEO contains a computing subsystem, an appropriate analysis shall be conducted to identify all safety-critical functions that are controlled by the computing subsystem. Computing subsystems that control safety-critical functions shall be analyzed in detail and tested for the purpose of verifying that no design weakness, software failure, or credible hardware failure propagating through the computing subsystem will compromise safety."

5.1.1 Comments on Analyses:

a. An early step in the process of designing of a safety system that is often overlooked is the performance of a hazard analysis. A detailed analysis, such as a Fault Tree Analysis (FTA), is required at the completion of a program for design verification by the safety review authorities. However, other analyses should be performed before the design is so mature that it is difficult to correct. Even when early analyses are conducted, a common mistake is to assume hardware will fail selectively, or to trivialize the evaluation. An example is to assume an internal failure in an IC will be safe because the same IC BIT logic will prevent an unsafe failure. It is a mistake to conclude that a failed hardware component can correctly and safely detect its own fault.

b. There are several analysis tools that could be included in the preliminary hazard analysis before any hardware is built or bread boarded.

1) Credible circumstances. A list of reasonable munition scenarios and environments should be developed. This is not the list of normal life cycle environments; an accident is usually caused by a combination of environments, and the stress from accident environments

often significantly exceed those of normal environments. Some services have a baseline list of environments they use for internal purposes, but there are no complete lists available. Judgment is required to generate this list, based on the characteristics of the system under review, and the anticipated manufacture-to-target sequence of events.

2) Credible circumstance review. A first analysis tool is to systematically predict the behavior of the safety system during and after each credible circumstance. This is similar to a conventional potential hazards review, except it is at the safety system level (or S&A level, where appropriate), and must consider combinations of environments that match the circumstance.

c. Once a block diagram of the safety system is proposed:

1) A "broad brush" FTA is especially useful for electronic systems to predict a worst case detailed FTA failure rate. The analysis can be performed when a basic block diagram and possible basic hardware devices have been proposed. Form an FTA based on the block diagram and the location of functions in specific integrated circuits (IC) (and other electronic components). Assign IC failure rates for each output according to the whole IC (for multiple IC outputs use a common mode failure rate of one), rather than attempting to predict the details of the internal circuitry (0.0005 is a common failure rate for high reliability IC's).

2) Another analysis tool that is particularly useful is to perform an analysis of subverted safeties. The evaluator analytically reviews normal operation while intentionally subverting an individual safety feature (locks, individual components of locks, logic, etc.) to the unsafe state. Each safety feature is subverted one at a time in turn. The performance of the design then should be evaluated for response to expected life cycle environments. This procedure is especially effective at exposing single point failure mechanisms and weaknesses.

d. Techniques for conducting the required detailed hazard analyses are described in NAVSEA OD44942, AFSC Design Handbook DH 1-6, and Nuc Reg 0492.

e. Poor FTA analyses are very common. The most common problem is formulating an analysis that accurately represents the functional logic of the system. It is imperative that undesired events be properly selected and accurately delineated in a systematic, repeatable manner in order for the analysis to be valid. The most controversial part of the FTA is assessing the failure rates of the components. It is recommended that the developers ensure the failure rates used are consistent with rates previously used for similar hardware designs (contact the service safety authority). This analysis typically can only be performed with close coordination between representatives of the service safety authority and the developer.

f. An area of concern for electronic safety and arming devices (ESADs) that are used with in-line explosive trains is when the arming delay was based on a single timer or double integration. This design cannot pass the safety analyses described above. Another area of

concern is when the partitioning of safety critical logic and components is inadequate. If safety depends too much on a single device, the ability of the design to meet requirements becomes questionable.

g. Some safety review authorities may request a sneak circuit analysis of the safety circuitry as part of the detailed analyses. A common misconception is that sneak circuit analysis is a thorough review of the circuitry. A sneak circuit analysis only investigates the potential of a circuit to operate with unexpected circuit behavior independent of component failures; it is not a failure analysis.

5.2 Application: "MIL-STD-1911A, Application. This standard applies to the design of hand-emplaced ordnance."

5.2.1 Comments on Application: Hand-emplaced ordnance includes hand grenades.

5.3 Approved explosives:

"MIL-STD-1911A, TABLE I. Approved Explosives

Explosive	Specification
Comp A3	MIL-C-440
Comp A4	MIL-C-440
Comp A5	MIL-E-14970
Comp CH6	MIL-C-21723
PBX 9407	MIL-R-63419
PBXN-5	MIL-E-81111
PBXN-6	WS-12604
DIPAM	WS-4660
HNS Type I or Type 2 Gr A	WS-5003
HNS IV	MIL-E-82903
* Tetryl	MIL-T-339
* Tetryl Pellets	MIL-P-46464

* No longer manufactured, not for use in new developments"

5.3.1 Comments on Approved explosives: New explosives can be accepted for a particular application by one service, but to be certified for general in-line use, the tests need to be accepted by the authoritative experts in all services. Reviews of a material for inclusion in this table (the same table as in MIL-STD-1316E) can be time consuming, especially if a test characteristic is marginal or a manufacturing process is difficult to document adequately for transfer to another source.

5.4 Armed: "MIL-STD-1911A, Armed.

a. An HEO is considered armed when any firing stimulus can produce HEO function.

b. An HEO employing explosive train interruption (see 5.1.1.3) is considered armed when the interrupter(s) position is ineffective in preventing propagation of the explosive train with a probability equal to or exceeding 0.005 at a confidence level of 95 percent.

c. An HEO employing an non-interrupted explosive train (see 5.1.1.4) is considered armed when the stimulus available for delivery to the initiator equals or exceeds the initiator's maximum no-fire stimulus."

5.4.1 Comments on Armed:

a. There is more than one possible use for the word "armed". The principal use of the word armed is for establishing the point at which the arming delay ends. When the probability of propagation of the explosive (or firing) train, given a proper stimulus, exceeds a certain level, the device is considered armed. The arming delay is then used by the HEO designer to evaluate the probability that the user can take the proper steps to move to a position beyond the safe separation distance for the intended application within the prescribed delay. HEO is unique in the sense that in most cases, the user performs some action (i.e., walks away, or takes shelter behind some protective obstruction) to attain a safe separation from the emplaced munition. The definition of armed as used in MIL-STD-1911A is exactly the same as that used for MIL-STD-1316, except that it is given at the munition level. However, it should be noted that the definition of armed for out-of-line systems is based on the effectiveness of the interrupter, not on how close to being physically fully armed the system is. As an illustration, consider a progressively armed rotor that starts at 90 degrees out-of-line. By the definition of armed, the system is considered armed at perhaps 40 degrees (or less) out-of-line when the probability of propagation exceeds .005, but the system will not be fully armed (tactically reliable) until the system is perhaps less than 2 degrees out-of-line. Similarly, an ESAD is considered armed when the charge on the firing capacitor rises to a level where the probability of firing the initiator reaches .005 at, for example, 600 volts, but the device is not tactically armed until it rises to the operationally reliable level of, for example, 1500 volts.

b. The use of the word "any" is significant where it states: ... "or any firing stimulus can produce HEO function." This wording was used to include firing stimuli that are accidental, or have a form other than the expected firing stimulus - such as mechanical shock when the expected firing stimulus is electrical.

c. HEO safety systems that arm slowly, such as a rotor that is controlled by an escapement, should have the .005 probability-to-fire point defined statistically, by a Langley, Bruceton, or similar procedure.

5.5 Arming delay: "MIL-STD-1911A, Arming delay. The time elapsed from the final commitment to the arming process until the armed condition is attained."

5.5.1 Comments on Arming delay: In the definition for HEO arming delay, the term "final commitment" usually refers to the last physical action necessary to start arming.

5.6 Arming or firing-control delay: "MIL-STD-1911A, Arming or firing-control delay. HEOs shall incorporate a method for obtaining safe separation. An arming delay provides the highest level of safety and shall be used wherever feasible. If operational or functional requirements dictate and with prior approval of the cognizant safety authority, a fail safe firing-control delay may be used to obtain safe separation."

5.6.1 Comments on Arming or firing-control delay: Most initiation systems are not allowed to mechanically arm before safe separation; however, many HEO are mechanically armed directly by the user.

a. A firing control delay is an alternative to a fixed HEO arming delay and can be used when operational constraints require arming control or remote arming.

b. State-of-the-art HEO's are electrically initiated; therefore, while the system is mechanically armed by the user, additional safety is provided by electrical controls preventing firing energy from being delivered (and careful handling). This HEO unique safety characteristic is termed firing-control delay. A fail-safe delay is required for the firing control delay to give the user time to reach a safe distance from the HEO. Since the system is armed, fail-safe in this case is relative, and the developer should assure the delay elements are carefully evaluated for expected component failure modes.

5.7 Common mode failures: "MIL-STD-1911A, Common mode failures. Multiple failures that result from the same cause, such as an adverse environment, or a seemingly unrelated failure. Examples of electrical common mode failures include the failure of two gates on a single digital integrated circuit due to loss of the ground lead to the chip, and failure of the two transistors due to exposure to a high temperature environment."

5.7.1 Comments on Common mode failures:

a. Common mode failures can be induced by personnel actions, through the use of common materials, component location, energy sources, functional actions, etc. Examples: A voltage regulator failure causes over-voltage on safety logic devices, which in turn arm the safety system as they fail. Mechanical logic devices (sequential leafs, G-weights, etc.) that function in the same direction may be vulnerable to common mode failure; an abnormal force sufficient to overcome one safety may defeat all the safeties to the same unsafe condition.

b. Traditional methods to reduce the risk from common mode failures can be physical or functional. Physical techniques can consist of selection of different technology components and their packaging. Functional techniques can consist of processing different types of signals, applying proper power management (to include return/ground references) and systematic signal controls (interrupts, reset circuits).

c. Partitioning is another method commonly used to reduce the risk of common mode failures within electronic safety and arming devices (ESAD) and other electronically controlled HEO. "Partitioning" here consists of physical separation, or the use of positioning control of the energy interrupters to avoid susceptibilities from similar environments and conditions.

d. The circuit which controls operation of the arming switches should be physically partitioned into at least two elements, none of which are capable (by virtue of circuit architecture and partitioning, not element design) of independently arming the system. The functional partitioning must be essentially immune to being bypassed by normal or abnormal electrical, mechanical, and thermal environmental hazards. Requiring the S&A control logic to be partitioned into at least two independent arming switch drive elements is comparable to requiring dual safety for a mechanical S&A device. That is not to say that a safe system could not be built with a single circuit element (IC). However, such "single-chip" designs are not being allowed because of the difficulty in proving that a complex single element can give a safety failure rate of less than one in a million units. By having more than one physically independent control element, the safety failure rate of each contributes to the overall safety requirement and each one independently does not have to provide safety to 10^{-6}.

5.8 Credible environment: "MIL-STD-1911A, Credible environment. An environment that a device may be exposed to during its life cycle (manufacturing to tactical employment, or eventual demilitarization). Credible environments include, but are not limited to electromagnetic effects, line voltages, extremes of temperature, humidity, vibration, shock and pressure. Combinations of environments that can be reasonably expected to occur must also be considered within the context of credible environments."

5.8.1 Comments on Credible environment: This term was borrowed from the general safety community. Credible environments include those that are believable but not necessarily expected, such as bullet impact, accidental circuit exposure to 120 VAC, or exposure of electronics to maximum source voltage when a voltage regulator fails. An example of a non-credible environment is multiple bullet impacts - all in the same hole.

5.9 Credible failure mode: "MIL-STD-1911A, Credible failure mode. A failure mode that has a reasonable probability of occurring."

5.9.1 Comments on Credible failure mode: Examples include failure modes in an IC that may not be easily predicted by the schematic, but can occur because of the mechanical

layout or method of construction (the dominant storage IC failure mechanism is caused by chemical corrosion).

5.10 Design for Quality control, inspection, and maintenance: "MIL-STD-1911A, Design for quality control and inspection. HEO shall be designed and documented to facilitate application of effective quality control and inspection procedures. Design characteristics critical to safety shall be identified to assure that designed safety is maintained."

5.10.1 Comments on Design for Quality control, inspection, and maintenance:

a. The manufacturing data packages must document the entire HEO safety system, normally consisting of a single configuration item. If other hardware (or software) is necessary to perform the HEO safety system function, then it must also be documented.

b. Safety critical design characteristics: In addition to those safety features that directly prevent inadvertent arming, aspects, characteristics, or components of a design that are unique and required to prevent inadvertent subversion of a safety feature should be identified as safety critical, with an associated explanation provided in the appropriate manufacturing and acquisition data packages describing why it should not be altered. Examples of safety critical design characteristics:

1) Microprocessors have dual-use input/output ports, with any port pin capable of being either an input or an output according to the program performed by the microprocessor. Used in safety systems, the inputs are isolated by diodes to prevent an inadvertent output from an input port from influencing the other circuitry.

2) At times the specific materials used in a barrier can be critical to passing the safety tests. If a barrier is made from a special steel, document the critical steel characteristics and the reasons for the material selection.

5.11 Electrical firing energy dissipation: "MIL-STD-1911A, Electrical firing energy dissipation. For electrically initiated explosive trains, the design shall include a provision to dissipate the firing energy whenever an armed HEO is returned to the non-armed condition. The dissipation means shall be designed to prevent common-mode failures."

5.11.1 Comments on Electrical firing energy dissipation:

a. This is a requirement for both in-line and out-of-line systems and applies to the device (usually a capacitor) that stores the firing energy directly used by the initiator.

b. The primary purpose of the energy depleting resistors though is not EOD, but to assure energy inadvertently developed is automatically dissipated.

b. After the firing energy has dissipated, an electrically initiated out-of-line system that was armed during use, is still "armed" and unsafe even though the primary firing mode has been eliminated.

c. An acceptable way to meet this requirement and to prevent common mode failures is as follows. Redundant bleed resistors are mounted on orthogonal axes, as far from each other as practical, and in a manner reducing the probability of damage from corrosion or physical force to both resistors without similarly damaging essential firing circuit components (typically the capacitor & switch). A better technical solution is preferred, but may currently be unavailable.

d. The primary purpose of the energy depleting resistors is to assure that any energy inadvertently developed on the firing circuit is automatically dissipated. This feature may also be used for EOD purposes.

5.12 Electrical initiator sensitivity: "MIL-STD-1911A, Electrical initiator sensitivity. The initiator for an electrically fired non-interrupted explosive train shall:

a. Meet the appropriate characteristics listed for Class B initiators of MIL-I-23659.

b. Not exhibit unsafe degradation when tested in accordance with MIL-STD-1512.

c. Not be capable of being detonated by any electrical potential less than 500 volts.

d. Not be capable of being initiated by any electrical potential of less than 500 volts, when applied to any accessible part of the HEO after final assembly."

5.12.1 Comments on Electrical initiator sensitivity:

a. Just as Tetryl was accepted as a safe standard for explosive sensitivity, a level of insensitivity of 500 volts for initiators was accepted to assure initiators are insensitive to electrical stimuli that might be seen during munition repairs, rework, etc. The establishment of the 500 volt threshold was apparently based on the 440 volt power that is commonly available on military equipment and in test facilities. The 500 volt level was considered to provide an acceptable safety margin while still providing a threshold that could readily be achieved through design.

b. EFIs are accepted as meeting the 500V no-detonate requirement based on the predicted no-fire voltage and unique energy characteristics from the fire set. This is acceptable because, for current designs, the EFI's fire set is tuned for that initiator by optimizing the fire set to reliably fire the initiator at the lowest possible energy. If the no-fire voltage delivered to the initiator by that fire set is above 500V then it is accepted that other 500V wave forms will not create a detonation. Initiators that do not utilize a tuned fire set may readily detonate at voltages

less than 500V, and therefore would be unacceptable to meet the "less than 500 volt" requirement of MIL-STD-1911A. All initiators should be reviewed with respect to the intent of the requirement. The initiator must not detonate at any electrical potential less than or equal to 500 volts.

c. Meeting the requirement of "less than 500 volts" of MIL-STD-1911A assures that during or after final installation, the item containing the initiator at the munition level will not initiate (either detonate or deflagrate) as a result of an accidental electrical input to the leads accessible to assembly, test, repair, or user personnel. If the initiator leads are accessible, then the requirement applies to the initiator itself; generally though, the requirement applies to a fire set, or the HEO as a whole.

5.13 Electrical/electromagnetic environments: "MIL-STD-1911A, Electrical/electromagnetic environments. The HEO shall be designed such that, in its normal life cycle configurations, it shall not unintentionally arm, nor shall any explosive component unintentionally function, during or after exposure to: electromagnetic radiation (EMR), electrostatic discharge (ESD), electromagnetic pulse (EMP), electromagnetic interference (EMI) lightning effects (LE) or power supply transients (PST). The HEO shall be tested or evaluated for the following as applicable:

a. EMR - per MIL-STD-1512 and MIL-STD-464

b. ESD - per MIL-STD-331

c. EMP - per DOD-STD-2169

d. EMI - per MIL-STD-461 and MIL-STD-462

e. LE - per MIL-STD-464

f. PST - by appropriate test and analysis"

5.13.1 Comments on Electrical/electromagnetic environments:

a. Insensitivity to power supply transients is a requirement for electronically controlled safety systems for two reasons. First, electronic devices are exposed to electrical noise, an environment that they may be susceptible to. Second, existing MIL-STD requirements such as MIL-STD 461 and MIL-STD-462 were never intended to address PST requirements and are considered inadequate for evaluating responses to noise levels. While subsystems are usually required to meet MIL-STD-461 specifications, the overall munition system is not required to be below the MIL-STD-461 conducted susceptibility levels; and such a requirement would usually be a severe design constraint. It is better to

assure that the subsystem has a design margin so it will be safe when exposed to credible voltages and noise levels.

b.

b. Power supply transients (system noise, circuit noise, ground loops & shifts, generators, return/ground line noise, etc.) are known to be capable of causing inadvertent arming and are a source of common mode failure mechanisms. The ARMY requires a special test that exposes any electronically controlled safety and arming system to the known system noise voltage, amplified by 10 dB (or times 3.16). The unit must remain safe during the test.

5.14 Environment: "MIL-STD-1911A, Environment. A specific physical condition to which the ordnance may be exposed."

5.14.1 Comments on Environment:

a. There are two types of environments: arming environments and risk environments.

b. Arming environments are normally selected from specific environments that may be available during deployment of the munition. For HEO, a man-in-the-loop is common for deployment, and it is acceptable to perform distinct manual operations to arm the munition. Selecting the appropriate arming environments (or manual operations) can significantly simplify the safety system design.

c. Risk environments can include any credible environment; designers should be alert to the effects of induced credible environments such as electrical noise on logic, or vibrations on mechanical devices. Electrical circuit noise is an environment for electronic logic devices.

5.15 Explosive compositions: "MIL-STD-1911A, Explosive compositions. Explosive compositions in fuzes shall be qualified for use in accordance with OD 44811 or MIL-STD-1751 in their intended role in explosive train components."

5.15.1 Comments on Explosive compositions:

a. While it is unusual, primary explosives can auto initiate; that is function without any external firing stimulus at all. This is one reason such explosives must be kept out-of-line. To assure the hazards are controlled, the main explosive in a system is limited to explosives that are known to be stable and acceptably insensitive.

b. The historical basis for evaluating acceptable secondary explosive sensitivity criteria (ESD, shock, temperature, materials compatibility, aging, etc.) is Tetryl - chosen because it had an acceptable safety record. Through time, as individual tests were refined, the pass-fail threshold levels were rounded - conservatively. As a result, Tetryl and some other approved secondary explosives will not pass the current in-line explosive test requirements.

5.16 Explosive ordnance disposal: "MIL-STD-1911A, Explosive ordnance disposal (EOD). Features shall be incorporated that facilitate HEOs being rendered safe by EOD tools, equipment and procedures even if sterilization or self-destruction features are incorporated."

5.16.1 Comments on Explosive ordnance disposal:

a. EOD can be a programmatic problem if sufficient planning has not been made. EOD should be considered early in the program and is one of the reasons an early design review is recommended. Additionally, EOD appraisals often require testing of some hardware which requires budgeting. Blow-in-place is not considered an acceptable solution.

b. In accordance with system requirements, munitions which contain self-destruct features should be provided with a positive means of identifying if the self destruct mechanism has not functioned.

5.17 Explosive train interruption: MIL-STD-1911A: "Explosive train interruption.

a. When an element of the explosive train contains explosive material other than allowed by 5.1.1.2 (e.g., primary explosive), at least one interrupter (shutter, slider, rotor) shall functionally separate it from the lead and booster explosives until the intended arming delay is achieved. The interrupter(s) shall be directly locked mechanically in the non-armed position by at least two independent safety features. The safety features shall not be removed prior to intended initiation of the arming sequence.

b. If the primary explosive is positioned such that omission of the interrupter will allow explosive train transfer to the lead or booster, the design shall include positive means to prevent the HEO form being assembled without the properly positioned interrupter.

c. The effectiveness of interruption for the explosive train in its configuration prior to initiation of the arming sequence shall be determined numerically in accordance with the Primary Explosive Component Safety Test of MIL-STD-331. If the explosive train interruption is removed progressively after intentional initiation of the arming sequence, the relationship between position and its effectiveness shall be established by a progressive arming test conducted in accordance with the Primary Component Safety Test, using a test strategy given by the Projectile Fuze Arming Distance Test of MIL-STD-331. The chosen test strategy, including selection rationale, and results shall be presented to the appropriate service safety reviewing authority."

5.17.1 Comments on Explosive train interruption: Systems that incorporate a delay in the arming process, such as a rotor that is controlled by an escapement, should have the .005 probability-to-fire point defined statistically by a procedure or method such as the Neyer, Langley, Bruceton, etc. Also, see the comments on safety feature, 5.24 of this handbook.

5.18 Explosive trains without interruption: MIL-STD-1911A: "Explosive trains without interruption. When the explosive train contains only explosive materials allowed by 5.1.1.2, no explosive train interruption is required. For non-interrupted explosive train designs, at least two independent energy interrupters, each controlled by an independent safety feature, shall prevent stimulus, equal to or in excess of the initiator's maximum no-fire stimulus (MNFS), from reaching the initiator until the required arming delay is completed. The design of the HEO shall preclude arming if any energy interrupter malfunctions or is absent."

5.18.1 Comments on Explosive trains without interruption:

a. There are special Army (see appendix C) and Navy service requirements for non-interrupted systems; the services expect these guidelines to be met in addition to the requirements of MIL-STD-1911A. While the Standard requires only two energy interrupters for example, the Army and Navy waiver guidelines are more conservative and require three switches, at least one being dynamic.

b. MIL-STD-1911A, Explosive trains without interruption, (The design of the HEO must preclude arming if any or all energy interrupter(s) malfunctions or is absent.) forms the requirement to have a dynamic switch (which is generally a semiconductor such as a field effect transistor, FET) in an ESAD. The term "malfunction" is generally accepted to mean a static failure. Dynamic failure mechanisms are generally unknown in electronic systems, although microprocessors are known to be capable of failing dynamically. There is very little information available about the detailed behavior of electronic components as they fail, and the interpretation of the paragraph could change if components are discovered that can fail dynamically within a bandwidth (or harmonic) close to that used in the DC to DC voltage multiplier.

c. The additional safety authority requirements for a dynamic switch and partitioning are considered fundamental to reducing the probability of unsafe single point or common mode static failures in an in-line electronic safety system.

5.19 HEO safety system failure rate, MIL-STD-1911A, "The HEO safety failure rate shall be predicted for all phases of the HEO's life cycle. The safety failure rate shall be less than one in one million until intentional initiation of arming. The safety failure rate predicted by analysis shall be verified to the extent practical by test during evaluation. The failure rate for a specific HEO design to prevent unintentional functioning during and after arming shall be acceptable to the cognizant safety authority (see 6.4)."

5.19.1 Comments on HEO safety system failure rate:

a. The requirement that the safety systems covered by this document have a failure rate that must not exceed one failure in one million is one of the most frequently discussed requirements

in safety design. While there is almost universal agreement that a numerical safety requirement is needed, there have been, and continue to be, varying opinions on what numerical value to use and how to apply it. This variation in opinion is due to several reasons. One is that the safety system failure rate is not practically measurable or demonstrable due to its extremely small numerical value. Another is that it is applied without variation to munition systems with inherently different natures and potential hazards.

b. The exact origin of the "one in a million" numerical value is unknown. It is believed that this was arrived at as a compromise value between what was considered an acceptably low probability for the occurrence of an undesired event, and the degree of safety that could be practically achieved. The popularly accepted remoteness associated with the term "one in a million" is also considered a likely factor in its selection. At this writing the earliest known documented use of the one in a million safety system failure rate is in a US Navy policy letter on Safety and Arming of Fuzes, dated 8 June 1953. In 1967 it was included as an objective in the first version of MIL-STD-1316 (NAVY), and was first stated as a requirement in a US tri-service agreement in MIL-STD-1316B, 1977. Since that time the "one in a million safety system failure rate" has been incorporated in the first editions of MIL-STD-1901, "Design Safety Criteria for Munition Rocket Motor and Missile Motor Ignition System Design", and MIL-STD-1911, "Safety Criteria for Hand-Emplaced Ordnance Design". It is important to note that while the "one in a million" numerical value is identical in all three of the MIL-STDs, what components of a design constitute a safety system, and what constitutes a safety system failure, do vary as one would expect. The acceptance and continued support of "one in a million" as a valid requirement by the safety community is reflected via its inclusion in all major initiation design safety documents from 1953 to the present.

5.20 Intended use: “MIL-STD-1911A, Intended use. This standard is intended for use by designers and developers of hand-emplaced ordnance and provides criteria by which the safety of such ordnance may be assessed.”

5.20.1 Comments on Intended use:

a. The safety system requirements of this document are a reflection of the best safety system design implementations and practices developed over the years. On first examination the safety system requirements for the different munition classes (warheads, rocket motors, and hand emplaced ordnance) can appear to be inconsistent. While the required safety system failure rate (not to exceed one failure in one million) remains constant, other requirements as well as what is meant by the term "safety system" varies among the munition classes.

b. In the development of a safety system it is important that the basis for the safety system requirements and the variations be understood. When comparing requirements for the different types of ordnance systems, the following thought is likely to occur: "If this approach is safe enough for fuzing or rocket motor applications it should be safe enough for hand emplaced applications as the failure of any of these safety systems can be catastrophic." This discussion is

intended to present the reasons why this logic is not accepted in the safety community, and why the requirements for warhead, rocket motor, and HEO safety systems should not be, and are not the same.

c. The following illustrates some of the variations;

(1) Warhead applications - the "safety system" is the aggregate of devices included in the fuze/S&A that prevents unintentional arming and functioning. Specifically, for out of line implementations, two independent safety features, enabled by different environments and each locking the interrupter in the safe position are required.

(2) Rocket and missile motor applications - the "safety system" is the aggregate of devices in the ignition safety device (ISD), the munition, the launcher, and the launch platform that prevent unintentional arming or functioning. Only one independent safety feature is required on the interrupter of the ISD.

(3) HEO applications - the "safety system" is the aggregate of safety features and devices of the HEO and the procedures associated with its use, that eliminate, control or mitigate hazards from the HEO throughout its life cycle. Two independent safety features, enabled by different actions in a specific sequence, each capable of preventing unintentional arming are required.

d. The safety system designers job is different than most designers in that the main objective, providing acceptable safety, is only quantifiable or measurable subjectively. Faced with the potentially catastrophic consequences associated with a safety system failure, the DOD safety community has adopted the approach of establishing a set of minimum requirements, which, when adhered to, provides an acceptable level of safety. Included in these is the requirement that the system safety failure rate be calculated, and that it must not exceed one failure in one million. The failure rate determined by this calculation is not the ultimate measure of, or deciding factor in determining the acceptability of a given design, but is one important tool to help determine that minimum safety requirements are met. The approach of using design requirements along with a calculated failure rate ensures meeting the overriding objective of providing the safest system possible within the overall system level requirements.

e. In theory, it would be desirable to have one set of minimum requirements applicable to all types of munition explosive initiation systems. This set of preferred requirements would employ the most conservative approach, and would, for example, mandate the use of environmentally derived energy (derived from unique and distinct environments), to remove safety features. However, in reality there are constraints imposed on the safety system designer, such as volume, power, and the availability of unique and distinct environments, which vary tremendously between munition classes. These constraints force designers to deviate from the theoretical set of preferred design guidelines, to a set of implementation options that determine the ultimate level of safety that is achievable. When constraints dictate the use of design options other than the preferred, the resultant degradation of the safety level must be compensated for in

the best manner possible. In keeping with the objective of providing the safest system possible, a safety system developed and judged acceptable under a specific set of limitations should not be used as a benchmark for judging the acceptability of safety systems not constrained by the same limitations. This is the reason for the variations in safety requirements for different munition classes that is reflected in this document. It should be noted that reviewing authorities do not accept justifications to reduce safety below acceptable levels based on programmatical constraints, such as cost and schedule.

f. To illustrate the preceding point, consider arming environments, a key design variable for the safety system designer. Generally the more distinct or unique from the normal handling and logistical environments (including potential abnormal environments) the available arming environments are, the easier it is to implement a safety feature that takes advantage of this difference. Consider that it would be easier to design a safety feature which would be removed under the influence of the tens of thousands of g's available during gun launch, as opposed to one that must be removed under tens of g's experienced during a missile launch, and still provide the same level of safety from normal logistical and potential adverse environments. Missile and projectile warhead applications typically provide the designer with the most unique arming environments. Rocket motor safety systems in general, do not have unique flight environments available for use by safety system designers, and therefore, adjustments are made to the requirements in that other munition or launcher system features are used to provide additional safety. HEO's typically represent a special case, since in most since in most cases unique environmentally derived arming environments are not available. This is compensated for by requiring specific operational procedures and sequencing of actions to provide an acceptable level of safety. This compensation can come with increased risk and costs. The use of operational procedures in place of environmentally derived environments places a much heavier reliance on human interaction in these systems. The safety provided by this approach is more difficult to quantify due to the human element, which in some cases represents an increased risk, i.e., the potential for intentional removal of safety features prior to emplacement. Meeting the requirement for sequencing of safety features may lead to increased complexity of designs. HEO safety system designs may lead to additional indirect costs incurred in the training required to familiarize personnel with these operations and to minimize the potential increased risks.

g. It should be noted that the same type of variations in constraints occur within munition classes covered by one standard. For instance the characteristics of the arming environments available for an artillery projectile fuze and a free fall bomb fuze are normally considerably different. This leads to a similar situation where bomb fuze safety systems are normally more complicated than projectile fuze safety systems, and are usually considered to involve greater safety risks. Similarly, it may be necessary in some warhead safety system applications to allow a portion of the safety features to be located outside of the basic configuration item usually identified as the S&A or fuze S&A or fuze, similar to what is done for rocket motor safety systems. This decision involves additional costs and risks that may not be immediately obvious. In this case, the number of configuration items involved and the number of people responsible for their maintenance over the life of the munition are increased. The procedures used in the

documentation and control of critical safety features over the life of the munition, the safety and hazard analysis, and any unique safety related qualification testing of the safety system, would now apply to portions of the munition system designated as part of the safety system. In some applications this type of approach may be justified, but again it is important that exception does not become the rule.

5.21 Maximum no-fire stimulus (MNFS): "MIL-STD-1911A, Maximum no-fire stimulus (MNFS). The stimulus level at which the initiator will not fire or unsafely degrade with a probability of 0.995 at a confidence level of 95 percent. Stimulus refers to the characteristic(s), such as current, rate of change of current (di/dt), power, voltage, or energy, which is (are) most critical in defining the no-fire performance of the initiator."

5.21.1 Comments on Miximum no-fire stimulus (MNFS): MNFS is used in the definition for armed. The requirement in a previous version of Safety Criteria for Fuze Design (MIL-STD 1316C) was effectively a probability to fire of 10^{-6}. This value was considered unacceptable as being unrealistic, and a design driver for some systems that must arm quickly, since the time to physically complete arming would be very short between arm delay (safe separation distance) and the minimum tactical engagement distance (which determines the minimum arming distance). The value of 0.005 probability to fire was the compromise reached during discussions to develop MIL-STD-1316D that was consistent for both in-line and out of line safety and arming devices. The same approach was considered

5.22 Safety approval: "MIL-STD-1911A, Safety approval. During the HEO's concept development phase, the developing activity should obtain approval from the cognizant safety reviewing authority of the design concept, of the applicability of this document, and of the methodology for assuring compliance with safety requirements. At the completion of engineering and manufacturing development, the developing activity shall present a safety assessment to the cognizant safety reviewing authority. The purpose of such a presentation would be to obtain concurrence that the design of the HEO satisfactorily complies with this document and that the safety risks associated with the in-service use of the HEO are acceptable. All new or altered designs, or new applications of existing designs, shall be presented to the appropriate service safety review authority for a safety evaluation and certification of compliance with this standard. (See 6.4)"

5.22.1 Comments on Safety approval: For maximum benefit, designs should be reviewed as soon as possible during concept development. Preparation guides are available from the review boards. A common misconception is that a previously accepted or waivered design is automatically acceptable in a new application. Safety designs, whether old or new must be assessed for each new application against current requirements based on the design merits.

5.23 Safe separation: "MIL-STD-1911A, Safe separation. A physical condition or state within the space between the HEO and friendly personnel and equipment that provides an acceptable level of risk from the hazards of the ordnance functioning."

5.23.1 Comments on Safe separation: Guidelines on safe separation distance prepared by the ARMY are in AppendixA.

5.24 Safety feature: "MIL-STD-1911A, Safety feature. An element or combination of elements that prevents unintentional arming or functioning."

5.24.1 Comments on Safety feature:

a. There are several terms that are often misused including safety feature, interrupter, lock, detent, energy interrupter, and energy control feature.

b. A safety feature can be thought of as anything that contributes to the safety of the system; however, in this standard it is used as one or more components that prevent inadvertent arming. A safety feature performs functions required in this standard. In rare cases safety features can be a single component, but normally they have several. An example of an ESAD safety feature could be the energy interrupter coupled with the logic that senses acceleration and controls the energy interrupter. An example for a mechanical system is a spring biased mass which moves under acceleration to release the interrupter. The interface of the mass with the interrupter is considered part of the safety feature.

c. The term interrupter is used in out-of-line systems and is a physical, movable barrier between the sensitive and insensitive explosives. A set of safety features mechanically lock the interrupter to prevent it from moving during any credible environment.

d. A lock is that portion of the safety feature which prevents the interrupter from moving during any credible normal and abnormal environment up to and including the application of the energy level which moves the interrupter to the armed position. For some HEO the energy level is provided by hand action.

1) A lock should not be confused with a detent. A lock is defined in 3.2 of this handbook. A lock is retracted to release the interrupter, not overcome by the interrupter itself - due to the arming environment. For example, the restraint on an interrupter armed with a piston actuator output is a lock only if it can withstand a force equal to that applied to the interrupter by that piston actuator. Additionally, the restraint on an interrupter armed by environmentally derived energy is a lock only if it can withstand the force equal to that applied to the interrupter by the environmentally derived energy. The maximum achievable level of energy, resultant torque, or force, either measured or calculated, that can be derived from the arming environment must be used when evaluating the effectiveness of the lock. For example, a Belleville spring or a spring loaded ball which would hold a rotor in place during assembly, but would be overcome to allow arming by either the function of a piston actuator or environmentally derived energy as described above is a detent, not a lock, and the same is true for a shear wire. In summary, if

application of any credible force including arming force to the interrupter can overcome the restraining feature, that feature is considered a detent, not a lock.

e. The term energy interrupter is used with in-line systems and can be either a direct or indirect means of controlling arming.

1) An energy interrupter as used in MIL-STD-1316C meant a component directly interrupting the energy path to the initiator. The MIL-STD-1316C energy interrupter was similar to a firing switch but it had to be mechanically locked by safety features just like an out-of-line interrupter. Two interrupters were required if the S&A contained stored energy. When MIL-STD-1316D was created, the term energy interrupter was kept, but now it meant either the interpretation used in MIL-STD-1316C or it could mean energy control feature. An energy interrupter could indirectly control the energy to the firing capacitor (or other storage device) or directly mechanically interrupt the energy to the initiator. The direct interruption has not been used in in-line systems to date.

2) One energy interrupter used in current electronic S&A's is referred to as a "dynamic switch". The switch itself is a semiconductor (usually an FET) that is cycled (between states) to provide proper circuit functions for high voltage conversion. Interrupters should be designed or implemented such that any static failure of the device will disable the dynamic (cyclic) operation of the switch. This intent is subverted when commanding the dynamic switch with circuitry that is susceptible to simple static failures. An example of this is an oscillator driven switch that only requires a discrete input. Developers have met the requirement in several ways such as an oscillator controlled by AND gates in the feedback loop as well as gates in series with the oscillator input and output.

f. When the Army drafted the Army waiver guidelines to MIL-STD-1316C to permit Electronic Safety and Arming Devices, the term energy control feature was created to avoid confusion with energy interrupter that was used in the MIL-STD. An energy control feature was not directly in-line with the initiator, rather it indirectly prevented arming energy from being developed in the firing energy storage device (i.e., capacitor).

5.25 Safety redundancy: "MIL-STD-1911A, Safety redundancy. The safety system of HEO shall contain at least two independent safety features, each of which shall prevent unintentional arming. Enabling of each safety feature shall require a different action. Those actions must be performed in a specific sequence for arming to be permitted."

5.25.1 Comments on Safety redundancy:

a. The two independent safety features in a mechanical system means that control of the arming interrupter is accomplished directly by two locks. The two independent safety feature requirement is not met by a lock on a lock. Evaluation of a system for subverted safeties usually will expose this design weakness. In a subverted safety evaluation the safety of the unit is

evaluated without the presence of each individual lock in turn. If there are two locks on the interrupter, it is not released by the absence of either one of them.

b. Non-interrupted explosive train control requires in-line warhead fuze safety systems to contain two independent safety features to prevent arming until the required arming delay is attained. Since these safety features must be independent, and thereby free of common mode failures, the design aspect that provides the arming delay in each safety feature must be independent. But, the start of the arming delay may be initiated by the same environment (or in the case of HEO, the same action).

5.26 Sterilization: "MIL-STD-1911A, Sterilization . A planned, programmed process that renders the HEO permanently incapable of activating energetic materials after specific events and time when the munition has served its useful purpose or is no longer capable of functioning as designed."

Or

"MIL-STD-1911A, Sterilization. If the HEO cannot be restored to its predeployed configuration, its design shall provide a sterilization capability. Self destruction is an acceptable alternative to sterilization when the HEO has been properly armed."

5.26.1 Comments on Sterilization:

a. There are several definitions used especially with discussions about unexploded ordnance.

b. The goal of sterilization is to provide the safest unexploded munition condition possible, which implies that the initiation system is permanently incapable of functioning either accidentally or intentionally. Sterilization is preferably accomplished by permanently rendering inoperable or removing the sensitive explosives from the explosive train. Another method of sterilizing a munition may be to incorporate one or more self-destruct features.

c. The next safest condition is a neutralized HEO. A neutralized HEO initiation system is still capable of functioning accidentally but not from the normal target detection sensor. An example is a mine with the firing system disabled so a fire signal cannot be generated. An Electronic Safety and Arming device with an expended battery and discharged capacitor is neutralized (until the battery is replaced - if firing circuit components had been destroyed it would be considered sterilized).

6. NOTES:

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use. This handbook contains lessons learned and background information about initiation safety system requirements specifically, MIL-STD-1316, Safety Criteria for Fuze Design, and MIL-STD-1911, Hand-Emplaced Ordnance Design, Safety Criteria For. These comments by government experts were prepared to aid both contractor and government designers and prime contractors. However, the text assumes the reader has a good general acquaintance with the technology, such as being familiar with the differences between an initiator, detonator, and squib.

6.2 Subject term (key word) listing.

Arming
Arming control
Arming delay
Explosive ordnance disposal
Explosive train
Explosive train interruption
Fail-safe
Fuze
Fuze design, safety criteria for
Fuzing system
Hand emplaced ordnance
Ignition safety device
Ignition system
Manual arming
Munition initiation device or system
Non-interrupted explosive train
Premature function
Pyrotechnic train
Safe separation
Safety and arming device
Safety design requirements
Sterilization

US ARMY FUZE SAFETY REVIEW BOARD
US ARMY GUIDELINES FOR SAFE SEPARATION DISTANCE ANALYSIS
(OCTOBER 28, 1994)

A.1 SCOPE

A.1.1 Scope. This appendix contains a standard procedure for calculating safe separation distance(s) for nonnuclear munitions for presentation to the US Army Fuze Safety Review Board (AFSRB).

A.2. APPLICABLE DOCUMENTS

A.2.1 General. The documents listed below are not necessarily all of the documents referenced herein, but are the ones that are needed to fully understand the information provided by this appendix.

A.2.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation or contract.

AR-385-16 System Safety Engineering and Management

(Copies of AR-385-16 are available from the HQDA (DACS-SF), Washington, DC 20310-0200).

A.3 DEFINITIONS

a. Safe Separation Distance: The minimum distance between the munition crew and the launched (intentionally or accidentally), manually emplaced or hand thrown munition beyond which the hazards to the munition crew resulting from the functioning of the munition are acceptable.

b. Hazards: Hazards to be considered in the calculation of safe separation distance are fragments and/or shock waves resulting from detonation of the munition explosive charge.

c. Fragmentation: All munition or target debris from the detonation of the munition will be considered as fragments and included in the analysis.

d. Hazardous Fragment: A hazardous fragment is one with sufficient residual energy so that upon impact with a member of the munition crew it has a 50% probability of penetrating exposed human skin; also, a fragment that damages the weapon system significantly in a manner likely to cause injury to the crew. The vulnerability characteristics of the launching platform

will be considered in fragment hazard assessment, both for the protection provided the gunner and the vulnerability of the launching system.

A.4 REQUIREMENTS

A.4.1 In establishing the safe separation distance, the following concerns should be addressed:

a. Launch through intentional obstructions, such as glass, windows, or brush, and into unintentional obstructions such as a tree or the ground that may either alter the flight path or inadvertently complete S&A arming and create warhead function.

b. Early dispersal of submunitions.

c. Wind that can blow back submunitions or chemicals.

d. Materials from the munition systems that float in the air presenting risk to a launch aircraft that is diving on the target.

e. All fragments, large or small.

f. Materials that are blown back from target impact.

g. Energetic materials that are not part of the warhead such as propulsion system propellants.

h. Abnormal flight conditions, such as a lost missile fin, corkscrewing in flight, etc.

i. The possibility of the munition carrier (such as aircraft) to be damaged significantly or in a manner that is likely to cause injury to the crew.

A.4.2 Additional conditions to be included in the computation of the safe separation distance are:

a. The possibility that some systems (especially dispensed submunitions) are safer close than they are at a distance. Thus the analysis may need to be extended beyond the closest point of predicted safety.

b. Some warheads are safe to stand behind, but increase in lethality dramatically as the incident angle approaches the side. Thus, it is necessary to evaluate any credible warhead position that would significantly influence the risks.

A.4.3 Safe separation distance fragmentation/debris data: To provide data for determining the safe separation distance, detonation fragmentation/debris will be obtained from

the detonation of at least three "all up" munitions. The data must be sufficient to define the velocity and size distributions of all fragments and debris and all blast effects along the entire center axis (nose to tail) of the munition using traditional fragmentation projection techniques.

A.4.4 The computation of the risk to the munition crew: The computation of the risk to the munition crew from a launched, manually emplaced or hand thrown munition is based on the probability of a warhead event multiplied by the probability of the munition crew impact by a hazardous fragment (given a warhead event has occurred). In equation form:

RISK TO MUNITION CREW = PROB OF WARHEAD EVENT *
PROB OF IMPACT BY HAZARDOUS FRAGMENT (GIVEN WARHEAD EVENT)

The maximum total risk to the munition crew at safe separation distance is generally accepted as 10^{-6}. The probability of a warhead event at safe separation distance is an assigned value of 10^{-2}, which has been selected on the basis of experience independent of the fuze or warhead design. These two values then combine to provide a numerical criterion for safe separation distance, i.e. the shortest distance at which the probability of a hazardous fragment from the functioning of a munition is 10^{-4} (This value is generally accepted by the AFSRB, but other organizations often require the lower value of 10^{-6} instead. A value of one must be used for the probability of warhead event at the minimum tactical engagement distance.).

A.4.5 Designing the arming distance to be less than the conventional safe separation distance: Designing the arming distance to be less than the conventional safe separation distance, when required for tactical effectiveness, is acceptable in extreme cases, with the approval of the proper authorities. For example,

a. Where the risk to the munition crew from the target is high, as with aircraft in a dogfight, an operator switch has been allowed to reduce the normal safe separation provisions of the S&A for self defense.

b. The target may be unavoidably closer to the gunner than the safe separation distance, such as when a gunner fires from one building to another across a street. It can be acceptable to provide a switch that reduces the munition arming distance below the safe separation distance. The gunner would be instructed of the risk and trained to fire only from a protected position such as behind a wall. The acceptability of damage to the munition crew in such a short range target situation is still 10^{-6}, but it can be based on tests/evaluations that include protected munition crew positions used in training.

The usage of an arming distance which is less than the safe separation distance requires a formal acknowledgment by the User Command in accordance with standard ARMY Risk Acceptance Procedures in AR 385-16 that minimum target engagement requirements conflict with and take precedence over safe separation distance requirements.

A.4.6 Reports: Safe separation distance analysis reports should list the risks that were considered and the rationale why each is not a concern at safe separation distance. Usually more than one situation has to be reviewed. The procedure will vary according to the risk and the system. It is practical to measure the fragmentation from some warheads and use a computer simulation to predict the fragmentation densities for various flight profiles. Usually a safe separation distance is predicted, then shown by analysis and test to be acceptable. In other cases, where testing is impractical, as with a chemical warhead or smart submunition, only analysis is sensible. Occasionally, it is necessary to conduct some tests before making an initial prediction of the safe separation distance. For example, this has been required in some weapons to determine if the propulsion system can sympathetically detonate from the warhead function - usually significantly increasing the accidental explosive output.

A.5 NOTES

(The information contained herein is intended for guidance only.)

A.5.1 Intended Use. These notes are intended to provide general and explanatory information that may be helpful in the computation of safe separation distance.

a. Safe separation distance is not:

1) an assigned point of desired safety
2) a point where an existing fuze arms
3) limited to sympathetic function of the entire warhead
4) related to the fuze probability to function where the fuze arms

b. The minimum fuze arming distance must exceed safe separation distance (unless otherwise approved, as per A.4.5).

c. Damage to the munition system from a premature warhead function that would not directly or indirectly lead to gunner injury is not a safety issue; therefore, is not considered in the safe separation distance calculation. If warhead function beyond safe separation distance has a probability to damage the system it should be included in the reliability assessment for the system.

FUZE MANAGEMENT BOARD JOINT AGREEMENT ON SAFE SEPARATION DISTANCE ANALYSIS FOR AIR-LAUNCHED MUNITIONS (FEBRUARY 1978)

B.1 SCOPE

B.1.1 Scope. This appendix is a copy of a tri service agreement to establish a procedure for insuring that the calculated safe separation distance(s) for nonnuclear air-launched munitions is acceptable to all using Services. The objective is to preclude a potential barrier to inter-Service commonality or inter-Service operability of air-launched munitions due to differing safe separation distance analysis procedures. The family of nose-mounted fuzes for 20-40mm automatic cannon, HE ammunition, as outlined in the approved Joint Service Operational Requirement (JSOR), dated 23 Aug 76, is excluded from this agreement. This appendix is not a mandatory part of this standard. The information contained herein is intended for guidance only.

B.2 APPLICABLE DOCUMENTS:

This section is not applicable to this Appendix.

B.3 DEFINITIONS

For the purpose of this agreement the following definitions apply:

a. Safe Separation Distance. A minimum distance between the launching system (AIRCRAFT & PILOT) and its launched munitions at which hazards associated with munitions functioning are acceptable. This distance may be achieved by providing arming delay(s) (time or distance).

b. Hazards. Hazards to be considered in the calculation of safe separation distance are fragments and/or shock waves resulting from detonation of the munition explosive charge. All munition vehicle debris from the detonation of the munition must be considered as fragments and included in the analysis. Detonation fragmentation/debris data must be obtained from the detonation of at least three "all up" munitions. The data must be sufficient to define the velocity and size distribution of all fragments and debris and all blast effects along the entire center axis (nose-to-tail) of the munition.

c. Fragment Hit. A fragment which contains sufficient kinetic energy to penetrate the launch aircraft skin which is exposed to the hazard. Caution must be exercised not to eliminate from the calculations those low relative velocity fragments which may cause serious damage if ingested by the engine(s).

B.4 REQUIREMENTS

B.4.1 The Fuze Management Board (FMB) policy for defining the safe separation distance(s) for air launched munitions in an engineering development or product improvement program.

a. Fuzes must be designed to arm at or after the safe separation distance. For munitions in which the primary kill mechanism is fragmentation, the safe separation distance will be established such that the probability of a fragment hit is no greater than one in ten thousand assuming a detonation occurs at the minimum calculated safe separation distance. If for tactical effectiveness reasons, the fuze must be designed to arm at a distance where the hazard level exceeds a probability of hit of one in ten thousand, the hazard level computed for the selected arming point must be included in the formal Tri-Service coordination procedures described below. In those cases where the probability of detonation at arming is known, or can be calculated with a high degree of confidence, (e.g., mechanical impact bomb fuzes) this factor can be considered in calculating the fuze arming point. When this factor is used, the values acceptable in calculations are from one to one in one-hundred. The allowable probability of hit is still one in ten thousand.

b. The developing Service will be responsible for conducting the required safe separation distance analysis as early as possible in the developing cycle, and for keeping using Services informed regarding status of the analysis. Immediately upon completion, the results of the analysis, along with the proposed analysis conditions, assumptions, and specific methodology employed, will be sent to the using Services for review and comment. It will then be mandatory for using Services to provide a formal response to the developing Service within 45 days, indication concurrence or nonconcurrence with reasons therefore. If the analysis is for a single Service munition, the safe separation distance analysis will be provided to the other Services without necessity for a response.

c. Any problems which are surfaced by the information exchange described above and which cannot be resolved between the using Services, will be presented to the FMB for resolution. Development may proceed pending the FMB resolution. The FMB resolution will be immediately provided to the program sponsor (SYSCOM, PM, etc.) for appropriate action.

d. The minimum acceptable safe separation distance analysis must be sufficiently comprehensive in scope that operational and design decisions can be made with knowledge of the accuracy and limitations of the supporting analysis. The minimum content is a prediction of the hazard level, and a discussion concerning the limitations of the analysis. In particular, the effects of (1) uncertainties in assumptions, (2) mathematical approximations, (3) data, and (4) numerical computations should be identified and estimated.

e. The analysis procedure and the acceptable hazard level for munitions which utilize a different kill mechanism (other than fragmentation) will be provided immediately to the using Services for mandatory review and formal comment within a 45 day time frame prior to being adopted as a tri-Service procedure and criterion. The Joint Fuze Task Group (JFTG) or successor, will be provided copies (when issued) of all correspondence in this connection. In the case of nonconcurrence, procedures outlines in B.4.1.c. will be followed.

B.4.2 The FMB procedure for calculating the safe separation distance(s) for air-launched munitions.

a. The minimum safe separation distance will be calculated using the definition of fragment hit in B.3.c and considering the presented area of the entire launch system. In this analysis assume that the probability of detonation at arming is one.

b. If the minimum safe separation distance resulting from the above procedure restricts tactical delivery conditions, the probability of a fragment hit may be further qualified by considering only the presented area of critical systems or components rather than the area of the complete launching system.

c. If the minimum safe separation distance resulting from procedure B.4.2.b will restrict tactical delivery conditions, a minimum probability of detonation at arming of one in one hundred can be used in the calculations, provided the probability of detonation at arming is known or can be calculated with a high degree of confidence.

d. If the above procedures still result in restricting tactical delivery conditions, then selected fuze arming conditions which are such that a safe separation distance is not achieved, must be justified by a thorough analysis. This analysis should consider probability of a specific type of damage, decreased risk from enemy ordnance, and tactical advantage gained by use of the recommended fuze arming characteristics. This analysis, and justification, will be sent to using services with requirements for response and resolution as specified in B.4.1.b. and B.4.1.c. The results of this analysis will be in the final safe separation analysis report and the tactical manuals will identify those fuze arming conditions which, for given delivery conditions result in specified hazards to the launching system.

ARMY FUZE SAFETY REVIEW BOARD GUIDELINES FOR EVALUATION OF ELECTRONIC SAFETY & ARMING (S&A) SYSTEMS THAT REQUIRE A WAIVER FROM MIL-STD-1316C August 1988 REVISION

C.1 SCOPE

C.1.1 Scope. This appendix contains guidelines developed by the ARMY Fuze Safety Review Board. These guidelines provide the U.S. Army Fuze Safety Review Board with a consistent set of conservative criteria for use in considering requests for waiver from MIL-STD-1316C for fuzes and their S&A systems that utilize electrical or electronic energy interrupters within the above scope. Waivers, within the scope of these guidelines, are being considered because technology is overtaking current standards. In general, these guidelines deal with overall circuit architecture rather than more detailed material such as component design and selection. They embody the spirit of MIL-STD-1316 and are intended to supplement applicable requirements rather than substitute for them. For example, providing an arming delay, incorporating EOD features, etc., will still be required. The information contained herein is intended for guidance only.

C.1.2 Application. These guidelines have been created based on the knowledge and experience gained in the development of a recent electronic S&A systems. They apply to systems that utilize all-solid-state (semiconductor, no moving parts) energy interrupters. Candidate systems are expected to be configured as a relatively low voltage power source (such as a munitions thermal battery), an electronic S&A circuit, a DC to DC converter to produce high voltage (>500v), and either a high voltage slapper detonator initiation system or a high voltage laser initiation system to generate explosive output. The developing activity, when submitting a candidate design for approval, will provide a written description of how each guideline is satisfied.

C.2. APPLICABLE DOCUMENTS

C.2.1 General. The documents listed below are not necessarily all of the documents referenced herein, but are the ones that are needed to fully understand the information provided by this appendix.

C.2.2 Government Documents.

C.2.2.1 Specifications, standards, and handbooks.

DEPARTMENT OF DEFENSE HANDBOOKS

MIL-HDBK-814 Ionizing Dose and Netron Hardness Assurance Guidelines for Microcircuits and Semiconductor Devices

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-331 Fuze and Fuze Components, Environmental and Performance Tests for

MIL-STD-461 Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

MIL-STD-883 Test Methods and Procedures For Microelectronics.

MIL-STD-1385 - Preclusion of Ordnance Hazards in Electromagnetic Fields, General Requirements for

(Copies of these documents are available online at http://assist.dla.mil/quicksearch/ or www.dodssp.daps.mil or from Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094.)

C.2.2.2 Other Government Documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein.

PUBLICATIONS

Technical Report Electromagnetic Environmental

RD-TE-87-1 Criteria For US ARMY Missile Systems: EMC, EMR, EMI, EMP, ESD, And Lightning.

(Copies of this report are available from Redstone Technical Test Center, STERT-TE-E-EM, Redstone Arsenal, 35898-5250.)

C.2.3 Order of precedence. In the event of a conflict between this document and the references cited herein, the text of this document takes precedence. Nothing in this document,

however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

C.3 DEFINITIONS

This section is not applicable.

C.4 GUIDELINES

C.4.1 Independent arming switches. There must be at least three independent arming switches (at a functional block diagram level) that serve as arming energy interrupters in the low voltage side of the S&A system. Each of these switches may contain (at a detail level) more than one component or element, and associated interconnections. System architecture will require that all arming switches operate normally before system arming can occur. For purposes of these safety guidelines, the armed condition is considered to be achieved when the high voltage firing capacitor is charged to a voltage greater than the minimum no-fire voltage for the detonator (see C.5.1.j).

C.4.2 System arming.

a. System arming must require at least two environmental signatures uniquely associated with "launch" of the munition. No single signature will be capable of directly operating more than one arming switch. Signatures may be combined to operate arming switches, and a single signature may contribute to the arming of more than one switch. Arming must not occur prior to safe separation distance of the munition from the launcher.

b. System arming must not occur if the low voltage power source is directly connected to any point in the circuit or if any point in the circuit is connected to or removed from electrical ground.

c. System arming must not occur if any or all of the arming switches (at a functional block diagram level) have static failures (failed either closed, or opened, or any static combination thereof) and the system's low-voltage power source is applied to the circuit in a normal manner. This includes switch failure before, after, or at the time of the application ofelectrical power. This requires at least one of the arming switches to be dynamic in its operation (continuously cycling between two or more states) during the arming process.

d. Dynamic arming switches will be driven by a signal that is unlikely to be produced inadvertently in the circuit. For example: be driven for a "lengthy" period to open and close at a specific frequency and/or duty cycle. The switch drive will be designed to be relatively immune from initiating the proper signal inadvertently. For example: a free-running oscillator simply switched to an "on" condition would be undesirable.

e. The circuit which controls operation of the arming switches will be physically partitioned into at least two elements, none of which are capable (by virtue of circuit architecture and partitioning, not element design) of independently arming the system. The functional partitioning will be essentially immune to being bypassed by electrical, mechanical, and thermal environmental hazards, as determined by engineering judgement and ordinary ruggedness testing used to develop conventional ammunition.

C.4.3 Safety Analysis. The usual safety analysis required by MIL-STD-1316 to show that the S&A system has no single point failure modes and that it will have no more than one safety failure per million units, will be conducted by at least two independent establishments (Government or commercial). The Board reserves the right to challenge the independence of the sources of such analyses and to require additional analysis if deemed appropriate. The independent safety analysis will also show that the fuze design complies with the safety aspects of its system requirements documents, especially in regard to improper functioning after launch. (Analyses are to show how the requirements for safe arming distance, overhead safety, reliability of self-destruct and sterilization, etc., will be met.) For systems using an embedded microcontroller, the safety analyses will include evaluation of its program for potential safety faults and weaknesses in design.

C.4.4 Immunity of system safety to electrical hazards. Immunity of system safety to electrical hazards will be demonstrated with both analysis and test data. Evaluation will consider exposure to all credible environments such as those listed below, and it will consider the powered state as appropriate to insure that safe separation distance will be achieved under EMR conditions.

(a) Electrostatic discharge including lightning
(b) Electromagnetic pulse
(c) Nuclear radiation (ionizing dose rate, total dose, neutron fluence)
(d) Electromagnetic radiation susceptibility including HPM
(e) Munition system generated noise and transient conditions such as power supply noise and rise rates, intermittent signal and ground connections, and improper input levels and sequences

C.4.5 The product fabrication specification. The product fabrication specification for the S&A device will specify as acceptance requirements, the safety-critical design and construction features of the device, including any associated software/firmware. Documentation of any safety

system software must be in a Government approved standard format. These specification items will be part of the safety review process, and they will remain mandatory during production acceptance inspection unless changed as a result of future safety board proceedings.

C.5 NOTES

(The information contained herein is intended for guidance only.)

C.5.1 Intended Use. These notes are intended to provide general and explanatory information that may be helpful for evaluation of electronic safety & arming (s&a) systems that require a waiver from.

C.5.2 General. The Army's current electronic S&A devices are very safe and relatively simple systems. It seems prudent to require newer S&A designs to match or improve on this established technology whenever practical. Designs which incorporate the above guidelines can be expected to provide a level of safety equivalent to that achieved by existing systems. Rationales for each of the above guidelines follow.

a. Having at least two arming switches is consistent with the current practice of having two independent locks on an explosive train interrupter. The use of three arming switches rather than only two is intentionally conservative and is the specified approach until this infant technology matures. The definition of independence here, means that any one switch (energy interrupter) will prevent arming assuming the other two switches have gone to an armed condition.

b. The requirement for two independent signatures uniquely associated with munition deployment is again consistent with current practice. Care must be exercised in selecting the best method to use the signatures in the arming control system (see C.5.2.k).

c. Protection from shorts of inadvertent application of power to the most critical spot in the circuit is a direct application of the "no single point failure mode" principle. It suggests that the dynamic arming switch be configured as an integral part of the high voltage converter such that any static failure would disable the converter. Placing the static arming switches on both sides of the voltage converter insures that a power bypass of these switches will also bypass the converter.

d. Requiring a safe system in spite of any static arming switch failures provides a great margin of safety compared to other circuit designs. A well-designed dynamic arming system is relatively simple to implement as illustrated by existing designs.

e. Requiring a "unique" signal to control critical safety functions is an established principle having much merit. Safety enhancements are obtained from limiting the conditions that result in this unique signal. System clocks operating at frequencies that may satisfy the dynamic switching requirement are to be avoided. Minimum functional requirements to be met prior to

intentionally producing the signal may include checks for proper operation and conditions of other parts of the circuit, and creation of needed information as a result of proper inputs and sequences.

f. Requiring the S&A control logic to be partitioned into at least two independent arming switch drive elements is comparable to requiring dual safety for a mechanical S&A device. That is not to say that a safe system could not be built with a single circuit element (IC). However, such "single-chip" designs are not being allowed because of the difficulty in proving that a complex single element can give a safety failure rate of less than one in a million units. By having two physically independent control elements, the safety failure rate of each needs to be established only to a lower level, such as one potential failure per thousand units. (Independent "chips" could be put in a suitable single package.)

g. The requirement for two independent safety analyses is made because of the newness and complexity of electronic S&A systems and the desire to be conservative. Safety analysis of embeded computer software has been shown to be essential on numerous occasions, and this should be done by using established methods where practical.

h. Dependence of the S&A function on electronic energy interrupters requires serious consideration of test environments for which electronics are most susceptible. Normal shock, vibration, thermal stress, etc., tests are naturally still required to fully establish safety. As with mechanical safety tests, the electrical test environments should be set at the highest levels expected to be encountered, and no gross safety failures allowed. Test specifications for some of the listed environments have not yet been fully developed, but test and analysis techniques adequate to support an evaluation do exist. Documents related to tests for some of the environments are: MIL-STD-331 (electro-static discharge & EMP-draft), MIL-STD-883 & MIL-HDBKS 279 & 280 (nuclear radiation), MIL-STD-461, MIL-STD-462 & MIL-STD-1385 and MICOM Technical Report RD-TE-87-1 (electromagnetic radiation susceptibility/hazards).

i. The purpose of this requirement is to try to prevent well-intentioned design changes or product improvements in production from deleting design, construction, or configuration features of the device that are critical to its safety. For example, by converting two integrated circuits (IC's) to a single IC for cost savings, etc. By having this information specified in writing and
by having the Government inspection aware of and checking for such safety features during production, it will be less likely that important safety features will be "designed out" of the system.

j. Reference Guidelines for C.4.1. Arming begins when the firing capacitor begins to be charged. This is similar to releasing an explosive train interrupter in a conventional out-of-line S&A device. For most designs, it is preferred to start arming after the safe separation distance is reached. However, for some applications where a short arming distance is required, it will be necessary to start arming before safe separation distance is achieved. In these designs, the

charge on the firing capacitor must not exceed the minimum (worst cast temperature and component tolerance) no-fire voltage prior to safe separation distance. This is similar to the conventional case of a slowly moving interrupter that allows propagation of the explosive train at some point before full alignment. Full arming is achieved when the firing capacitor reaches the maximum all-fire voltage for the detonator. For many applications, a safety advantage can be gained by designing to limit HV charging current so as to establish a minimum arming time commensurate with safe separation.

k. Reference rationale for Guideline C.4.2.a. There are many possibilities to consider in the design of an arming control system. The following are noted: requiring switches to operate in a proper sequence; defaulting to a locked safe mode in the event of abnormal operation; using down-range events such as "good-guidance" or "target recognition" signals for an arming signature; incorporating an anti-runaway feature against fast clocking of safety critical events; insuring automatic discharge of stored electrical energy at a reasonably rapid rate; and monitoring of the safe condition prior to launch where applicable.

CONCLUDING MATERIAL

Custodians:
Army-AR
Navy-OS
Air Force-99

Preparing activity:
Army-AR

Reviewing activities:
Army-MI
Navy-AS
Air Force-10, 11, 70

(Project 13GP-0078)

NOTE: The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the ASSIST Online database at www.dodssp.daps.mil.