NATO STANDARD

AOP-4187

FUZING SYSTEMS – SAFETY DESIGN REQUIREMENTS

Edition A, Version 1

JUNE 2022

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ORDNANCE PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

21 June 2022

1. The enclosed Allied Ordnance Publication AOP-4187, Edition A, Version 1, FUZING SYSTEMS - SAFETY DESIGN REQUIREMENTS, which has been approved by the nations in the CNAD AMMUNITION SAFETY GROUP (CASG – AC/326), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4187.

2. AOP-4187, Edition A, Version 1, is effective upon receipt and supersedes AOP-16 , Edition 4, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Major General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
CZE	CZE Armed Forces do not use cluster munitions according to the Act No. 213/2011 Coll., in valid statues at large.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. AIM

The aim of this document is to standardize safety design requirements for Fuzing Systems for operational and training munitions used by NATO.

1.2. APPLICABILITY

This standard applies as follows:

a. This standard is applicable to the design of new Fuzing Systems, commenced after promulgation of STANAG 4187 and this AOP, for all munitions except those listed in the Exclusions paragraph below. Application of this standard to modifications or new uses of an existing fuzing system shall be determined by the National Safety Approving Authority (NSAA) (see Annex A).

b. The requirements of this standard shall apply to Mission Termination Systems (MTS) where such systems are part of the final tactical weapon configuration. For systems where MTS are part of a test configuration only, nations may use this document or other National approved standards applicable to MTS.

For Hand Emplaced Munitions (HEM), the applicable standard is STANAG 4497. For demolition systems, the applicable standard is STANAG 2818.

1.3. SCOPE

Fuzing Systems include all components (hardware and software), that fulfil the following functions in munitions or weapon systems:

a. Isolate sensitive energetic materials in the explosive train, or the energy required to function them, or both
b. Arm the fuzing system
c. Initiate one or several energetic materials in a munition.

1.4. EXCLUSIONS

The following munitions are excluded from this standard:

a. Nuclear weapon systems and their associated training aids.
b. Flares and Signals dispersed only by hand.

c. Pyrotechnic Countermeasure Devices.
d. Munitions which the NSAA agree do not require a compliant fuzing system.

1.5. DEFINITIONS

Definitions of terms used in this standard are contained in the NATOTerm database. Other recognized International sources may be used to complement but not replace the NATO agreed definitions.
The term Safety, Arming and Functioning (SAF) system (defined in NATOTerm) is the generic term that covers different types of applications such as fuzing systems, HEMs, demolition systems, ignition systems, etc. Therefore, when a requirement is applicable to all these systems, the term SAF system is used instead of a specific term (e.g. fuzing system, HEM, ignition system).

Annex B can be referenced to obtain descriptions of fuzing system states for clarifications if needed.

1.6. GUIDANCE

Guidance on the interpretation of the requirements stated in this standard is given in Annex D.

1.7. WORDING CONVENTIONS

1. “Shall” indicates the application of a procedure or specification is mandatory.

2. “Should” indicates the application of a procedure or specification is recommended.

1.8. ABBREVIATIONS

Abbreviation	Description
AECTP	Allied Environmental Conditions and Tests Publication
AOP	Allied Ordnance Publication
ASIC	Application Specific Integrated Circuits

BIT	Built-In Test
C3	Command, Control and Communications
COTS	Commercial Off The Shelf
DRACAS	Data Reporting, Analysis and Corrective Action System
EBW	Exploding Bridge-wire
ECWGT	Explosive Component Water Gap Test
EED	Electro-Explosive Device
EID	Electrically Initiated Device
EOD	Explosive Ordnance Disposal
EPRD	Electronic Part Reliability Data
ESAD	Electronic Safe and Arm Device
FCE	Firing Capacitor Energy
FET	Field Effect Transistor
FMECA	Failure Modes, Effects and Criticality Analysis
FPGA	Field-Programmable Gate Array
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FTA	Fault Tree Analysis

HEM	Hand Emplaced Munition
HERO	Hazards of Electromagnetic Radiation to Ordnance
IC	Integrating Circuit
LCEP	Life Cycle Environmental Profile
MASS	Maximum Allowable Safe Stimulus
MOTS	Military Off The Shelf
MTS	Mission Termination System
NATO	North Atlantic Treaty Organization
NSAA	National Safety Approving Authority
NPRD	Non-Electronic Part Reliability Data
NSO	NATO Standardization Office
PHA	Preliminary Hazard Analysis
RF	Radio Frequency
RIAC	Reliability Information Analysis Center
SAD	Safety and Arming Device
SAF	Safety, Arming and Functioning
UXO	Unexploded Ordnance

CHAPTER 2 COMMON REQUIREMENTS FOR ALL SAFETY, ARMING AND FUNCTIONING (SAF) SYSTEMS

2.1. DESIGN SAFETY TASKS

2.1.1. System Safety Program Plan

A system safety program plan based on the guidance of AOP-15 shall be implemented at the start of the design and development phase.
The intent of that safety program shall be to identify and minimize hazards through all lifecycle phases.

2.1.2. Hazard analyses

1. A lifecycle environmental profile (LCEP), consistent with AOP-15 and/or AECTP-100, shall be defined for each SAF System. This profile shall be used in assessing hazards encountered by the SAF system.

2. Hazard analyses shall be conducted during the development process to permit control of identified hazards by the most effective means.

Hazard analysis techniques include (but are not limited to) the following:

3. Preliminary Hazard Analysis (PHA). An analysis of the munition (including the SAF System) and its interaction with the weapon system, platform and users shall be conducted. The hazards of normal and credible abnormal environments, conditions and actions of personnel, which may occur during its lifecycle including demilitarization, disposal and/or Explosive Ordnance Disposal (EOD) shall be identified.

4. Hazard Analyses. Analyses (Failure Modes, Effects and Criticality Analysis, Fault Tree Analysis, etc.) shall be conducted and documented as soon as detailed design information is available.

5. Hazard Analysis Revision. Any change in the configuration or application shall be assessed and documented to determine if there is an effect on the existing safety analyses. If required, hazard analyses shall be updated.

6. Safety Critical Components and Characteristics. Components of the SAF System with characteristics that have been determined to be safety critical shall be identified and addressed in the safety assessment report (see annex E). The applicable documentation shall be annotated to show that the component is safety critical together with the safety critical characteristics.

7. Programmable Electronic(s) and software(s).

a. Safety analyses for SAF Systems containing Programmable Electronic(s) and/or software(s) shall include an assessment of their contribution to the SAF system safety.

b. Programmable Electronic(s) and software(s) that control one or more safety features shall be designed in accordance with an appropriate development process, including analysis and tests (e.g. STANAG 4452/AOP-52, RTCA DO-178C, IEC 61508, RTCA DO-254, etc.). The selection of the development standards or guidelines and applicable requirements shall be acceptable to the NSAA. A safety plan applicable to Programmable Electronic(s) and software(s) shall be established.

2.2. SAFETY ASSESSMENT REVIEW AND APPROVAL

1. During the concept stage of a new design, modification of existing design, or new applications of existing design, the design and its safety assessment shall obtain approval from the NSAA for both the design concept and the methodology for assuring compliance with safety requirements. At the completion of the development stage, the design safety assessment including design, analyses, and qualification testing shall be presented to the NSAA for review, approval and compliance with this standard. Results from tests conducted for purposes other than safety can be considered for the design safety assessment. An example of Safety Assessment documentation summary for SAF systems is given in annex E.

2. For any non-compliance with this standard, an associated mitigation case and application for waiver shall be provided to the NSAA to demonstrate that an acceptable level of safety is met.

2.3. WAIVED REQUIREMENTS

If a design and/or test program do not comply with one or more requirements of this standard but is approved for use in the proposed application by the NSAA, the details of the waived requirements and the rationale on which the waivers are based shall be recorded by the NSAA. The reasons for the waivers shall be made known to other NATO nations justifiably requiring information on that design.

2.4. ENVIRONMENTAL CONDITIONS

The SAF System shall be designed to maintain the required degree of safety in credible accident situations and under specified natural and induced environmental conditions in its lifecycle.

2.5. ENERGETIC MATERIALS

Energetic materials shall be selected as follows:

a. Assessment and Qualification. All Energetic materials shall be assessed and qualified for their intended role (e.g. primary explosive, booster explosive, high explosive, etc.) in accordance with the requirements of STANAG 4170 and AOP-7.

a.1. Only those energetic materials qualified as an acceptable booster explosive are permitted to be in a position leading to the initiation of a high-explosive charge without interruption.

a.2. For other energetic train elements, only those energetic materials qualified and approved by the NSAA for non-interrupted use are permitted to be in a position leading to the initiation of a payload without interruption.

b. Lifecycle Safety. Energetic materials shall be chosen so that the system is safe and remains so under the specified lifecycle conditions.

c. Sensitiveness. The sensitiveness of the energetic materials shall not increase beyond the range for which the materials were approved in the specified life cycle conditions.

d. Assessment of Explosive Components. In a fuzing system, detonating components in a position without interruption with the main charge shall be assessed in accordance with the requirements of, and pass the tests specified in, STANAG 4363/AOP-21.

2.6. MATERIAL COMPATIBILITY

All materials used in the SAF System shall be chosen to be compatible and stable under all specified natural and induced environmental conditions in its lifecycle. Assessment of compatibility shall be conducted in compliance with STANAG 4147. The following shall not occur in an unarmed SAF System:

a. Premature arming or functioning.

b. Hazardous ejection or exudation of material.

c. Burning, deflagration or detonation of energetic materials.

d. Formation of volatile or sensitive compounds

e. Production of unacceptable levels of toxic or other hazardous materials.

f. A compromise of the safety, disarming, sterilization or self-destruct features, e.g., by electro-chemical reaction.

2.7. INSENSITIVE MUNITION (IM) SAF SYSTEM

AOP-39 guidelines should be considered for the SAF system design.

2.8. ELECTRO-EXPLOSIVE DEVICES (EEDS).

1. EEDs shall be characterized in accordance with STANAG 4560 and that information shall be made available to the NSAA.

2. EEDs shall be qualified to specific test procedures and pass/fail criteria established or approved by the NSAA.

3. EED Safety Margins. In any SAF system in which safety is dependent on preventing the unintentional functioning of an EED, a minimum safety margin between the Non-Initiation Stimulus and the stimulus that could be induced by electrical or electromagnetic interference shall be demonstrated to be compliant with HERO test standards and accepted by the NSAA.

4. EEDs used in non-interrupted explosive trains shall:

    a. Not be capable of being detonated by any electrical potential of less than 500 V applied directly to the EED as demonstrated by Maximum Allowable Safe Stimulus (MASS) and Non-Initiation Stimulus.

    b. Not be capable of being initiated by any electrical potential of less than 500 V when applied to any accessible part of the SAF System during and after installation into the munition or any munition sub-system.

    c. Not be capable of being detonated by any voltage greater than 500 V found in the munition aside from the EED functioning voltage in the SAF. In these instances, evidence shall be presented to the NSAA that demonstrates the SAF system and EED are insensitive to or sufficiently isolated from these other munition voltages.

Note: for other Electrically Initiated Devices (EID) (such as laser initiators) these systems shall comply with interrupted firing energy path requirements (see STANAG 4368) and the NSAA shall be consulted.

2.9. COMMUNICATION

Any communication with the SAF system shall not compromise the safety of the SAF system.

2.10. BATTERY

If a battery is used in or by SAF systems (as stored energy), it shall be compliant with international or national standards and regulations as agreed by NSAA.

2.11. DEMONSTRATION OF NON-ARMED ASSURANCE DURING ASSEMBLY AND INSTALLATION

1. To provide non-armed assurance, SAF System designs shall incorporate one or more of the following:

    a. A feature which prevents assembly in an armed state.

    b. For SAF Systems with interrupted explosive trains: Positive, direct and unambiguous means of determining that the SAF System is not armed during and after assembly and when installing the SAF System into a munition. Where the SAF System is accessible after assembly into the munition, the positive means of determination shall also be available. Any means employed in compliance of this paragraph shall not degrade safety.

    c. For SAF Systems with non-interrupted explosive trains, the method used shall positively prevent the accumulation of arming/firing energy in the SAF System prior to installation in the munition. Any means employed in compliance of this paragraph shall not degrade safety.

    d. A feature which prevents installation of an armed SAF System into a munition.

2. If arming and disarming of the SAF System is a normal procedure in manufacturing, inspection, or at any time prior to its installation into a munition, the adoption of paragraph 2.11.1.a alone is not sufficient and either paragraph 2.11.1.b, 2.11.1.c. or 2.11.1.d shall also be met.

3. If it is necessary to check individual safety features during or after assembly, the method used shall be unambiguous and positive and shall not degrade safety.

4. Designs in which the safety is dependent upon the presence of an interrupter shall include positive means to prevent the SAF System from being assembled if the interrupter is omitted or if the interrupter is in the unsafe position.

2.12. DESIGN FOR QUALITY CONTROL, INSPECTION

1. SAF systems shall be designed and documented to facilitate the application of effective quality control and inspection and test procedures in accordance with STANAG 4107.

2. Appropriate quality controls in accordance with STANAG 4107 shall be applied to all critical design characteristics (for example: dimensions, material properties, heat treatments, and fabrication operations) identified by the design safety assessment (see annex E) of the SAF system.

3. The design of the SAF system shall incorporate features that will facilitate the use of inspection procedures and test equipment to ensure that no critical design characteristics have been compromised.

4. Incorporation of these features shall not degrade safety.

5. The design should facilitate the use of automatic inspection equipment.

2.13. TEST PROCEDURES

Testing of the SAF system shall be conducted in accordance with STANAG 4157, AOP-4157 using test procedures described in AOP-20 and/or national test procedures as approved by NSAA.

2.14. MAINTENANCE

a. SAF systems should be designed to require no maintenance.

b. If maintenance is required, the safety of the SAF System shall not be degraded by any maintenance activities and SAF system safety assessment shall include those activities.

2.15. UNARMED/ARMED STATUS VISUAL INDICATION

If visual indication of the unarmed or armed state is employed in the SAF system, visible indicators shall be designed to provide a positive, unambiguous indication of state. Indicator failure shall not result in a false non-armed indication. If colour coding is used to represent state, the colours and coding shall be as follows:

a. Unarmed state. Fluorescent green background with the letter S or word SAFE superimposed thereon in white. Colours shall be non-specular.

b. Armed state. Fluorescent red or fluorescent orange background with the letter A or the word ARMED superimposed thereon in black. Colours shall be non-specular.

2.16. DEMILITARISATION AND EXPLOSIVE ORDNANCE DISPOSAL

1. SAF Systems shall meet the requirements of STANAG 4518.

2. Features should be incorporated in SAF Systems in accordance with national policies that facilitate their being rendered safe by EOD tools, equipment and procedures even if disarming, sterilisation or self-destruction features are incorporated.

INTENTIONALLY BLANK

CHAPTER 3 SPECIFIC REQUIREMENTS FOR FUZING SYSTEM

3.1. FUNDAMENTAL SAFETY DESIGN REQUIREMENTS

3.1.1. Inclusion of Safety Features.

a. Fuzing Systems shall include at least two safety features, each of which shall prevent unintentional arming of the Fuzing System. These safety features shall be independent of each other and designed to minimize the potential for common cause failure.

b The control and operation of these safety features shall be functionally and physically isolated from other processes within the munition system.

c. Where it is not technically possible to functionally isolate the safety features from other processes, those non-isolated components, including software, used to enable the safety features shall be considered part of the Fuzing System and shall meet the requirements of this standard.

d. The design of the safety features shall be robust enough to permit exposure of the Fuzing System to the environments anticipated in its lifecycle and remain safe. The robustness of each safety feature and its contribution to the overall safety of the Fuzing System shall be assessed through analysis and/or testing to the satisfaction of the NSAA.

3.1.2. Operation of Safety Features Using Environmental Stimuli

a. The stimuli which enable the independent safety features to operate shall be derived from different environments or different combinations of environments or both; where combinations are used each combination shall be different.

b. The environments selected and sensed by the Fuzing System to remove safety features during arming shall avoid any environment or levels of environmental stimulus that may be experienced by the Fuzing System prior to the commencement of the launch cycle.

c. Any signal used to enable safety features shall be unique and robust.

d. Operation of at least one of the independent safety features shall depend on sensing an environment after first motion in the launch cycle or on sensing a post launch environment.

e. Any action taken to launch a munition may be considered an environmental stimulus if it irreversibly commits the munition to complete the launch cycle.

f. The fuzing system of munitions that are designed to be jettisoned shall be in an unarmed state and shall not function due to the impact from such a release.

3.1.3. Prevention of Unintentional Arming

a. Fuzing Systems shall not be capable of being armed manually.

b. Fuzing Systems shall not rely solely upon defined operating drills or procedures to provide safety.

c. Fuzing Systems shall be designed so that no Single Point failure, single credible circumstance or common-cause failure can result in arming or functioning before launch or deployment.

d. After launch, the probability and quantity of single point or common cause failures of the arming cycle shall be reduced to a minimum. The time window associated with these failures shall be reduced to a minimum and shall exist only at or near expiration of the intended arming delay/distance.

e. Fuzing systems shall be capable of arming only as a consequence of a sequence of actions resulting from the sensing of environments that occur during or after launch or deployment.

f. Fuzing systems shall use environmentally derived energy generated after commencement of the launch or deployment cycle in preference to pre-launch stored energy to enable, arm or function the system. If this cannot be practically achieved and stored energy is used, then the system safety hazard assessment (analyses and tests) of the design shall demonstrate that both the operation and failure modes for that source of energy do not compromise the safety of the fuzing system. Additionally, the same stored energy source shall not be used to both remove a lock and arm the safety and arming device in a single action.

g. Fuzing system features which control arming shall be dedicated solely to the control of arming.

h. At least one of the independent safety features of the fuzing system shall prevent arming after launch or deployment until the specified safe separation distance or equivalent arming delay has been achieved.

3.1.4. Application of Requirements to Multiple Safety and Arming Devices (SADs).

The requirements of paragraph 3.1.1 to 3.1.3 apply to all carrier munitions, including sub-munitions, having a single safety and arming device.

For munitions with multiple safety and arming devices compliance shall be as follows:

a. Independent Safety and Arming Devices. When a Fuzing System incorporates multiple safety and arming devices for which the functions of Arming and Functioning are independent, the requirements of paragraph 3.1.1 to 3.1.3 shall apply to each safety and arming device.

b. Interrelated Safety and Arming Devices. When a Fuzing System incorporates multiple safety and arming devices, which share common functions of Arming, Functioning or both, the requirements of paragraph 3.1.1 to 3.1.3 shall apply overall to the interrelated safety and arming devices.

c. Unintended Launch. The system shall be designed so that no sub-munition Fuzing System can arm solely as a result of leaving the carrier munition during a credible accident before intended launch of the carrier munition.

3.1.5. Fuze setting

If fuzing system setting is safety critical, uncontrolled alteration shall be prevented.

3.1.6. Fail-Safe Design.

Fuzing Systems shall incorporate fail-safe design features based on their applicability to system requirements.

3.1.7. Self-Destruction, Sterilization, Disarming.

Self-Destruction may take one of two forms: self-functioning or self-disruption.

The contribution of self-destruction, sterilization and/or disarming function, if any are required, shall be included in the fuzing system probabilities of failure as defined in Paragraph 3.2 below.

3.1.8. Single device

Safety and Arming in a Single Device. The elements of the fuzing system that prevent arming until valid launch environments have been sensed and either the Safe Separation distance or Arming Delay/distance has been achieved, should be located in a single safety and arming device.

3.1.9 Munition with retargeting capability

Based on system requirements, for designs requiring a re-targeting capability after Arming or Partial Arming, the Fuzing System should not be in the armed state between target engagements.
Arming status during mission profile and between target engagements shall be presented for acceptance to the NSAA early in the design phase.

3.2. PROBABILITY

1. Probabilities of fuzing system failure shall not exceed the following rates:

   a. Prior to Commencement of the Arming Sequence. The probability of arming, or functioning irrespective of arming, between manufacture and the intended commencement of the arming sequence shall not exceed 1E-6.

   b. For Gun, mortar and tube Launched Projectiles, Prior to Tube Exit. The probability of arming between the intended commencement of the arming sequence and tube exit shall not exceed 1E-4 and the probability of functioning between the intended commencement of the arming sequence and tube exit shall not exceed 1E-6.

   c. Between Commencement of the Arming Sequence and Safe Separation Distance or Equivalent Delay. The probability of arming between the intended commencement of the arming sequence and achieving the safe separation distance or equivalent delay shall not exceed 1E-3. The rate of Fuzing System functioning during this period shall be as low as is practical and consistent with the risk established by the NSAA as acceptable for premature munition function.

   d. Post Safe Separation distance or equivalent delay. The probability of unintended functioning after safe separation distance or equivalent delay shall not exceed that specified in the requirement document for the system.

   e. After Intended Function. The design of the fuzing system shall be compliant with User, NSAA or other Authorities' requirements concerning duds.

2. Munitions Including Sub-Munitions. For carrier munitions which include sub-munitions, the following shall apply:

a. Probabilities and conditions given at Paragraph 3.2.1 of this chapter shall apply to the fuzing system of the carrier munition.

b. Probabilities and conditions given at Paragraphs 3.2.1.a and 3.2.1.e shall apply to the fuzing system of the sub-munition. Probabilities and conditions given at Paragraphs 3.2.1.b to 3.2.1.d shall also apply to the fuzing system of the sub-munition unless this is provided for in the carrier munition fuzing system.

c. The probabilities of unintended arming and/or functioning associated with the total number of sub-munitions shall be determined and be acceptable to the NSAA.

d. The system hazard analysis shall demonstrate the requirements of Paragraph 3.1.4.c.

3.3. CONTROL OF EXPLOSIVE TRAIN

3.3.1. Use of Interrupted Explosive Trains

When the explosive train contains qualified energetic materials which do not meet the requirements of paragraph 2.5.a.1 and 2.5.d or paragraph 2.5.a.2, the train is to be interrupted and the following requirements shall apply:

a. At least one interrupter (e.g. barrier, shutter, slider or rotor) shall isolate the energetic materials that do not meet the requirements of paragraph 2.5.a.1 and 2.5.d or paragraph 2.5.a.2, from subsequent elements of the explosive train. The interrupter(s) shall be directly locked mechanically in the safe position by at least two independent safety features of the Fuzing System until the start of the arming sequence.

b. The interrupter shall prevent propagation of an energetic reaction until the required safe separation distance has been achieved or equivalent arming delay has elapsed. The explosive train interruption shall be evaluated by the Primary Explosive Component Safety Test as given in AOP-20 test D1.

3.3.2. Use of Non-Interrupted Explosive Trains

Explosive train interruption is not required when only those qualified energetic materials that meet the requirements of paragraph 2.5.a.1 and 2.5.d or paragraph 2.5.a.2 are used in the train. In these circumstances one of the following methods of controlling arming shall be used:

a. For Fuzing Systems using techniques for accumulating all functioning energy from the post-launch environment, the system shall prevent arming until verification, by the system, 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 Fuzing Systems using techniques that do not accumulate all functioning energy from the post-launch environment, the following shall apply:

(1) At least two safety features (that meet the requirements of paragraph 3.1.1) shall enable at least three energy breaks.

(2) At least one energy break shall be capable of preventing arming in a static mode if any or all of the energy breaks are left out or malfunction. This requires at least one energy break to function in a dynamic mode.
a) The energy break functioning in dynamic mode shall be driven by a specific signal. This signal shall not be unintentionally generated by the effects of system or lifecycle environmental stimuli.

(3) Validation of a post launch environment shall contribute to the enabling of the dynamic energy break.

(4) At least one energy break shall function in a static mode.

(5) Independent control of energy breaks shall be exercised to the maximum extent practical; a minimum of two separate Programmable Electronics or circuits shall be used to validate the arming events, the sequence and time window to control the energy breaks.

Note: An example of a possible architecture is shown in Annex D Figure 2.

3.4. ADDITIONAL REQUIREMENTS FOR FUZING SYSTEMS CONTAINING ELECTROMECHANICS & ELECTRONICS

The following safety design requirements are applicable to electromechanical and electronic Fuzing Systems in addition to those given elsewhere in this standard:

a. Arming and Functioning. Designs shall ensure that:

(1) Independent safety feature controls (e.g. logic) are physically separated and implemented using different component types to minimize the potential for common cause failures.

(2) Where Built-In Test (BIT), other in-service or maintenance tests on the integrity of the Fuzing System are required, the safety of the Fuzing System shall not be degraded.

b. Electrical Firing Energy Dissipation. For electrically initiated Fuzing Systems, the design shall include a provision to dissipate the firing energy after the operating lifetime of the Fuzing System has expired. The time required to dissipate the firing energy shall be reduced to the minimum allowed by the operational requirements for the Fuzing System and the requirements on UXO prevention. The dissipation means shall be designed to prevent single point and common cause failure. The means of dissipation shall be designed so that it does not degrade the overall safety of the Fuzing System before the system is armed.

c. Requirements of safety data are as follows:

(1) Information Transfer. Information passed between an environmental sensor and a Safety and Arming Device shall be unprocessed and transferred by a defined and isolated logic route dedicated to that transfer only.

(2) Interpretation of Information. Information received by the Safety and Arming Device shall be capable of being verified as a valid command to begin a sequence of events resulting in the removal of a safety feature. False or corrupted data shall not cause the removal of a safety feature.

d. Software. Non-embedded software shall not be used.

e. Discrete electronic. Where the logic function is performed by dedicated hardware to give unequivocal interpretation, the hardware systems shall use components in which all the logic states can be identified, verified and validated.

Programmable Electronics

f. Use of Programmable Electronics in the Implementation of Safety Features. To minimize the subversion of Safety Features due to unintentional and/or unrecognized modes of operation, including failure modes, each Safety Feature implemented with Programmable Electronic shall use the least complex device that can practically perform the required functionality.

g. Fixed-in-structure devices should be used and are acceptable. If this is not feasible, a mitigation case shall be provided. To avoid degradation of a safety feature, any Programmable Electronics used in the implementation of that feature:

(1) Shall not be re-programmable or re-programming shall only be possible during manufacture of the fuzing system.

(2) Shall not be alterable by credible environments.

(3) Shall include for devices relying on charged-based non-volatile memory in support of a safety feature, a method that validates the integrity of the data in the memory prior to executing the safety function.

(4) Should be rated to meet or exceed the LCEP of the system. For Programmable Electronics which are not rated to meet or exceed the LCEP of the system, engineering rationale and associated risk(s) shall be provided.

h. To minimize the potential for common cause failures, where all Safety Features are implemented with Programmable Electronics, at least two Safety Features shall be implemented with dissimilar Programmable Electronics. The degree of dissimilarity shall be sufficient to ensure that any credible common cause failure mode susceptibility will not result in unsafe operation of all Programmable Electronics. Where practical, at least one Safety Feature shall be implemented with discrete component(s).

i. To ensure the device operates as intended, Safety Feature logic shall be implemented in accordance with the device manufacturer’s latest specifications and notes. In addition, all programming functionality, testing functionality, unused pins, and any other normally non-operational functionality of the Safety Feature logic shall be appropriately disabled and terminated, according to the device manufacturer’s latest specifications and notes. Non-compliance shall be subject to review and approval by the NSAA.

j. During and after exposure to power transfers, transitions, and/or transients, Programmable Electronics shall not operate in a manner that results in the degradation of the Safety Feature(s).

k. Safety Feature timing functions, excluding arming delay, implemented within logic shall not be susceptible to single point or common cause failures resulting in unintended arming. Single point or common cause failures of the arming delay device shall be reduced to a minimum during the arming cycle. The time window associated with these failures shall be reduced to a minimum and shall exist only at or near expiration of the intended arming delay.

l. The actual logic implementation shall replicate the documented design.

m. Where all Safety Features are implemented with Programmable Electronics, the Safety Feature logic shall be physically and functionally partitioned from each other. This minimizes the potential for inadvertent subversion such as sneak paths or Single Event Upsets.

n. To minimize the potential for unknown failure modes, all logic and/or functionality available within a device shall be disclosed, documented, and assessed in safety analyses and evaluations.

o. Safety Feature documentation shall include the complete logic flow with all inputs and outputs defined, along with timing and interdependence of events.

p. Manufacturing documentation and processes shall ensure that Programmable Electronics within a design approved by the NSAA are produced with an identical configuration.

q. Development tools shall be documented and controlled via configuration management procedures.

r. Power for Safety Feature logic should be partitioned from other power such as communication or platform power. If this is not achievable, it shall be demonstrated that there is no effect on safety.

s. Power for Safety Feature logic should be applied as late in the launch sequence or operational deployment as practical, and justified.

INTENTIONALLY BLANK

ANNEX A List of NSAA or point of contact

Country	Name
ALB - ALBANIA	
BEL - BELGIUM	Directorate General Material Resources Section Management – Risk – Ammunition Queen Elisabeth Barracks Eversestraat 1 1140 Brussels Belgium
BGR - BULGARIA	
CAN - CANADA	Directorate Ammunition & Explosive Management & Engineering (DAEME) National Defence Headquarters 101 Colonel By Drive Ottawa, Canada K1A 0K2
CZE – CZECH REPUBLIC	Military Technical Institute, s.e. Mladoboleslavska 944 197 06 Praha 9 – Kbely Czech Republic
DEU - GERMANY	Bundesamt für Ausruestung, Informationstechnologie und Nutzung der Bundeswehr K1.3 Ferdinand-Sauerbruch-Str. 1 56073 Koblenz Germany
DNK - DENMARK	Danish Acquisition and Logistics Organisation, Lauptrupbjerg 1-5 DK-2750 Ballerup Denmark
ESP - SPAIN	
EST - ESTONIA	
FRA - FRANCE	DGA Techniques terrestre Rocade Est – échangeur de guerry 18021 Bourges Cedex DGA/INSP/IPE 60, boulevard du général Martial Valin 75509 Paris Cedex 15
GBR – THE UNITED KINGDOM	Defence Ordnance Safety Group Science and Technology Division Fir 3a #4304 MOD Abbey Wood South Bristol BS34 8JH
GRC - GREECE	
HRV - CROATIA	
HUN - HUNGARY	
ITA - ITALY	Ministero della Difesa Segretariato Generale della Difesa e DNA Direzione degli Armamenti Terrestri Via Marsala n. 104 00185 ROMA
LTU - LITHUANIA	

LUX - LUXEMBOURG	
LVA - LATVIA	
NLD - NETHERLANDS	Chairperson of the Defence Safety Board on Dangerous Goods PO-box 20701 2500 ES The Hague Netherlands
NOR - NORWAY	Norwegian Defence Material Agency Ammunition division P.O. Box 800, Postmottak N-2617 Lillehammer, Norway
POL - POLAND	
PRT - PORTUGAL	
ROU - ROMANIA	
SGP - SINGAPORE	Defence Science and Technology Agency 1 Depot Road Singapore 109679
SVK - SLOVAKIA	
SVN - SLOVENIA	
TUR - TURKEY	Ministry of National Defence of Republic of Turkey Department of Technical Services 06100 Bakanlıklar / Ankara / TURKEY
USA – THE UNITED STATES	Army US Army Fuze Management Office Attn: FCDD-ACE-Z Picatinny Arsenal, NJ 07806-5000 United States of America Naval Ordnance Safety & Security Activity Attn: WSESRB Chairman, C/O Code N00ED 3817 Strauss Avenue Bldg D323 Suite 108 Indian Head, MD 20640-5151 USA USAF Non-nuclear Munitions Safety Board Attn: 96TW/SES 1001 North 2nd Street, Suite 366 Eglin Air Force Base FL 32542-6838 United States of America

ANNEX B Fuzing system & target sensor terms and descriptions

B.1. INTRODUCTION

a. It has proven necessary to clarify the wide spectrum of possible states that both a Target Sensor and a Safety and Arming Device (SAD) can adopt within a Fuzing System. Table 1 below describes the situation regarding the status of both the sensor and either an interrupted or non-interrupted SAD with the labels assigned for the status of the Target Sensor and the SAD. These terms are then described in Tables 2 and 3. This table was originally developed to describe the various states that an intelligent mine (one that could be turned "on" and "off" for safe passage) might be in. It was decided to include this as it describes one or more states that all Fuzing Systems in munitions can be expected to be in during their lifecycle and use, whether they contain target sensors or not.

b. It is emphasized that the terms and descriptions apply to the states that can be adopted within all types of Fuzing System. For most Fuzing Systems, not all states are either possible or relevant.

c. When referring to a target sensor, “Off” means that the target sensor cannot produce an output (e.g., firing signal, target detection signal).

d. When referring to a target sensor, “On” means that the target sensor can produce an output (e.g., firing signal, target detection signal).

e. Where charging circuitry is working, the firing capacitor can be expected to have a charge less than the Armed Stimulus for only a very short time.

f. Where a firing capacitor has a charge greater than the Armed Stimulus, even in the absence of a working charging circuitry, the Electronic Safety and Arming Device (ESAD) is still armed.

g. A disarmed Safety and Arming Device (SAD) is one which is returned to an unarmed condition having previously been armed.

Table 1 - Examples of Description of Fuzing System status

Ser	Target Sensor	SAD State	Interrupted Safety and Arming Device	Non-Interrupted Safety and Arming Device				Term for system status	
				Power Supply (SAD only)	Static Switches	Dynamic Switch	Firing Capacitor	Target Sensor	Fuzing system
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1	Off	Unarmed	Interrupter locked, by at least 2 independent locking devices, in the position designed to prevent initiation of the main charge by the detonator.	Off or not available	Open	Not Oscillating	Not Charged	Inactive	Unarmed
2	On	Unarmed	As Above	On or off	Open	Not Oscillating	Not Charged	Active	Unarmed
3	On	Partially Armed	Interrupter in the position designed to prevent initiation of the main charge by the detonator but not fully locked in place as in serial 1.	On On	Closed Closed	Not Oscillating Oscillating	Not Charged Charged < Armed Stimulus	Active	Partially Armed
4	On	Armed	Interrupter in the position designed to allow initiation of the main charge by the detonator.	On	Closed	Oscillating	Charged > Armed Stimulus	Active	Armed
5	Functioned	Fired	Fired	Fired				Functioned	Functioned
6	Off	Armed	Interrupter in the position designed to allow initiation of main charge ready to fire. Note: the status of the fuzing system will always be considered armed regardless of the state of the power source, firing capacitor or sensor.	On Off	Closed Closed or open	Oscillating Not oscillating	Charged > Armed Stimulus Charged > Armed Stimulus	De-Activated	Armed
7	Off	Partially Disarmed	Interrupter returned or progressed to a position designed to prevent initiation of the main charge but not fully locked in place. The SAD can be rearmed.	On or Off On or Off	Closed Open	Not Oscillating Not Oscillating	Charged < Armed Stimulus Charged < Armed Stimulus	De-Activated	Partially Disarmed
8	Off	Disarmed	Interrupter returned or progressed to an unarmed position and fully locked in place in such a manner that it can be rearmed.	Off	Open	Not Oscillating	Safely Discharged	De-Activated	Disarmed
9	NA	Sterilized	Interrupter moved from the armed position and returned to the position at which detonator function will not initiate the main charge and is permanently disabled. This may be achieved by functioning the detonator in that position.	Rendered permanently inoperable				NA	Sterilized

Ser	Target Sensor	SAD State	Interrupted Safety and Arming Device	Non-Interrupted Safety and Arming Device				Term for system status	
				Power Supply (SAD only)	Static Switches	Dynamic Switch	Firing Capacitor	Target Sensor	Fuzing system
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
10	NA	Destroyed	SA mechanism armed and main charge functioned after a period of time or environmental condition has been sensed with the purpose of demolishing the munition and leaving no explosive hazard.	Fired and irreparably damaged				NA	Self-Functioned
11	NA	Destroyed	SA mechanism (or secondary SA mechanism) armed and subsidiary charge functioned after a period of time or environmental condition has been sensed with the purpose of disrupting the munition without functioning the main charge.	Disrupted	Disrupted	Disrupted	Fired	NA	Self-Disrupted

B.2. DESCRIPTION OF TERMS RELATED TO TARGET SENSORS

a. Shown in the table below are the descriptions related to the possible states that a Target Sensor for a Fuzing System may adopt.

Table 2 - Description of Terms Related to Sensors:

Ser	Term	Description
(a)	(b)	(c)
1	Inactive	The state in which the target sensor has not yet been turned on.
2	Active	The state in which the target sensor is turned on, making the fuzing system capable of responding to a target and producing an output.
3	Deactivated	The state in which the target sensor is turned off, but still capable of being returned to the active state.

B.3 DESCRIPTION OF TERMS RELATED TO SAFETY AND ARMING DEVICES

a. Shown in the table below are the descriptions related to the possible states that a SAD for a Fuzing System may adopt.

b. Safety and Arming Device (SAD). A subsystem of the fuzing system which controls arming.

c. Firing Capacitor Energy (FCE). The energy stored in the firing capacitor intended to be applied to the initiator by closure of the firing switch.

Note: This energy is not to be confused with that which is stored on any other capacitor used to close a firing switch.

Table 3 - Descriptions Related to Safety and Arming Devices

Ser	**Term**	**Description**	
		Interrupted Explosive Train SAD	**Non-Interrupted Explosive Train SAD**
(a)	(b)	(c)	(d)
1	Unarmed	Interrupter locked, by all safety features, in the original position designed to prevent initiation of the main charge by the detonator.	Firing Capacitor Energy (FCE) shall not be present. All safety features in their original unpowered condition shall prevent accumulation of FCE (power supply to the SAD is off).
2	Partially Armed	The interrupter is in any position where the probability of initiation of the main charge by the detonator is less than 0.005 at the 95% single sided lower level of confidence, but with the safety features not fully applied as in the unarmed state.	FCE is greater than in the unarmed state and/or the Safety Features are not all fully applied. The FCE is less than the Armed Stimulus of the Electro Explosive Device.
3	Armed	The interrupter position is such that the probability of propagation of the explosive train is ≥ 0.005 at the 95% single sided lower level of confidence.	The FCE is greater than or equal to the Armed Stimulus of the Electro Explosive Device.
4	Partially Disarmed	A state in which the SAD, having been armed, is in any configuration where the probability of initiation of the main charge by the detonator is less than 0.005 at the 95% single sided lower level of confidence, but with the safety features not fully applied as in the disarmed state.	After having been armed, the FCE is greater than in the unarmed state and/or not all the Safety Features are fully applied. The FCE is less than the Armed Stimulus of the Electro Explosive Device.
5	Disarmed	A state in which the SAD, having been armed meets all of the following: a. Is rendered incapable of functioning the main charge. b. Meets the safety requirements of Paragraph 3.3.1. c. Can be rearmed.	A state in which the SAD, having been armed meets all of the following: a. Firing capacitor energy shall not be present. b. Meets the safety requirement of Paragraph 3.3.2. c. Can be rearmed.

Ser	Term	Description	
		Interrupted Explosive Train SAD	**Non-Interrupted Explosive Train SAD**
(a)	(b)	(c)	(d)
6	Sterilized	A state in which the SAD is rendered permanently incapable of functioning the main charge. This shall be accomplished by either removal of the detonator or permanent interruption of the explosive train, or similar means.	A state in which the SAD is rendered permanently incapable of functioning the main charge.
7	Self-functioned	The SAD is armed and functioned deliberately, without necessarily sensing a target, with the purpose of functioning the main charge.	The SAD is armed and functioned deliberately, without necessarily sensing a target, with the purpose of functioning the main charge.
8	Self-disrupted	The SAD (or Secondary SAD) is functioned deliberately, without necessarily sensing a target, to operate a specific mechanism with the purpose of breaking up the munition without functioning the main charge.	The SAD (or Secondary SAD) is functioned deliberately, without necessarily sensing a target, to operate a specific mechanism with the purpose of breaking up the munition without functioning the main charge.

INTENTIONALLY BLANK

ANNEX C Additional Safety Design Requirements for Mine Fuzing Systems

C.1. The design of safety and arming systems of all mine systems shall comply with the safety design requirements of this standard. There are additional requirements for mine Fuzing Systems, for example recovery and redeployment, and these are described in this Annex.

C.2. The mines referred to in this Annex may fire either a direct lethal mechanism or consist of a deployed launcher and sub-munition(s). The safety and arming mechanism in either the deployed launcher or the direct lethal mechanism is referred to as the SAD (Safety and Arming Device) throughout this Annex. The SAD of a deployed launcher controls the firing of the expelling charge, whereas the SAD of a direct lethal mechanism controls the firing of the warhead. The SAD of any sub-munition shall be designed in accordance with the requirements of the main body of this standard.

C.3. Within this Annex, mine Fuzing Systems are divided into two functional parts:

a. The Target Sensor. The Target Sensor is a component or series of components designed to detect and respond to a target.

b. The Safety and Arming Device (SAD). A device that prevents the Fuzing System from arming until an acceptable set of conditions has been achieved and subsequently effects arming and allows functioning of the payload.

C.4. Some mine systems also include a command, control and communications (C3) subsystem. In such cases the C3 sub-system shall be included in the munition design safety assessment (Design Safety Assessment paragraph of the standard) to decide if any of its functions are safety critical, e.g., remote control of arming. The C3 sub-system shall be able to validate the status of the mine at any stage of its operational deployment. If the assessment shows that the C3 sub-system is safety critical, the design authority shall demonstrate that the requirements of this standard are not adversely affected.

C.5. Descriptions. Those descriptions set out in the Tables 1, 2 and 3 of Annex B are used to describe the states which may be adopted by the Target Sensor and the SAD.

C.6. Deployment. The target sensor should not be activated until the arming sequence of the SAD has been completed. Where this is not the case the design authority shall demonstrate to the NSAA how the Arming distance or Delay safety requirements of this standard are met.

C.7. Passage of Friendly Forces.

a. A system, designed to allow the passage of friendly forces, is recognized to be inherently less safe when set to this operational scenario. For this reason, operational requirements shall justify such use and commanders shall be made aware of this hazard. Live munitions should not be used in this scenario during training. The design safety assessment shall demonstrate that the level of this hazard is acceptable to the User and the NSAA.

b. To allow the operational passage of friendly forces (operational passage mode):

(1) The SAD shall be in the unarmed or disarmed state.

(2) The target sensor shall be deactivated.

(3) The firing circuit of a direct lethal mechanism or the launcher, in the case of a deployed launcher and sub-munition, shall be disabled.

(4) The remote command to re-arm shall require the operator to perform at least two different actions in a specific sequence, to generate and send a unique signal. If an external command is used to initiate reactivation, the Fuzing System shall validate the command before re-arming and shall not react to an invalid or corrupted command.

(5) Command and control of deactivation and activation of the target sensor shall be independent of the command and control of the SAD so that no common mode failure shall be able to affect the target sensor and the SAD. This shall be demonstrated to the NSAA.

(6) No failure of any part of the Fuzing System related solely to re-arming may inhibit future partial disarming, disarming, sterilization, self-function or self-disrupt.

C.8. Approaching a Mine. If there is a User requirement to approach a mine, the design authority shall demonstrate how this could be achieved with the required safety.

C.9. Field Maintenance. To perform maintenance on a mine, the fuzing system shall be at the unarmed or disarmed state with the target sensor deactivated.

C.10. Recovery. For a mine to be recovered, the Fuzing System shall be in the unarmed state with the target sensor deactivated, or in the sterilized state.

C.11. Re-deployment. For a mine to be re-deployed the fuzing system must be in an unarmed or disarmed state with the target sensor deactivated.

C.12. Self-Destruction. Self-destruction of a mine may be accomplished either by Self-Functioning or by Self-Disruption.

C.13. Where it is intended to use a mine Fuzing System which incorporates a Non-Interrupted Explosive Train SAD, the accumulation of FCE shall be prevented until, and as late as possible, in the engagement sequence.

C.14. Fail-Safe. The failure of any component of the Fuzing System which is not directly involved with disarming, sterilization, self-function or self-disrupt shall not compromise these capabilities.

C.15. End Of Deployed Life. Mines shall either self-destruct or sterilize themselves at the end of their planned life. These actions are intended to minimize the hazard of an unexploded mine. This function shall be included in the design safety assessment to ensure that the incidence of unexploded ordnance is at a level acceptable to the User and/or the NSAA.

C.16. Anti-Tamper. The use of anti-tamper features shall not reduce the safety to the user. Anti-tamper features that pose a potential unintentional hazard shall be deactivated after expiration of the munition’s armed life.

INTENTIONALLY BLANK

ANNEX D Guidelines for AOP-4187

D.1. AIM

1. The aim of this annex is to guide designers in the application of the safety design requirements for Fuzing Systems given in the body of this AOP-4187.

D.2. GENERAL

1. Related Documents. The list of related documents identified in STANAG 4187 is not exhaustive and designers should be aware that other relevant STANAGs may apply.

2. Comments given in the table below follow the order of their applicability to the body of this AOP-4187.

D.3. COMMENTS ON AOP-4187 EDITION A Version 1

Paragraph N°	Paragraph Title	Comments
CHAPTER 1 INTRODUCTION		
1.1.	Aim	none
1.2.	Applicability	none
1.2.a.		none
1.2.b.		Specifically included in the agreement are Mission Termination Systems (MTS) where such systems initiate the munition, sub-munition warhead(s) or other Break-Up unit.
1.3.	Scope	A fuzing system may include power sources, electronic/electromechanical switches, environmental sensors, target sensors, fire command circuits and an explosive train. It may also incorporate self-destruction or sterilization mechanisms. Fuzing system elements may be physically distributed within the munition. Sensitive energetic materials: The potential hazard of all energetic materials should be considered in the assessment of their position.
1.4.	Exclusions	A nation may use this STANAG in whole or in part for munitions excluded in this Paragraph. Application of an exclusion should be justified to the NSAA.
1.4.a.		There are specific national standards and regulations for nuclear weapons systems.
1.4.b.		Examples of munitions excluded by this sub-paragraph are those for items such as hand held signal flares (colours or smoke), thunder-flashes, etc,
1.4.c.		Examples of munitions excluded by this sub-paragraph are those for aircraft decoy flares and land service visual or IR flares or decoys.
1.4.d.		Before determining if a munition doesn't require a compliant fuzing system, it is necessary to assess the severity and probability of occurrence of potential hazards by analysis and/or tests.
1.5.	Definitions	see https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en
1.6.	Guidance	none
1.7.	Wording	none
1.8	Abbreviations	none
CHAPTER 2 COMMON REQUIREMENTS FOR ALL SAF SYSTEMS		
Common requirements of AOP-4187, STANAG 4497 and STANAG 4368 have been consolidated in chapter 2 and the term SAF system is used to cover all. The goal is to have same common requirements between SGA IST standards in the future.		

2.1.	design safety tasks	none
2.1.1.	System Safety Program Plan	The following is a non-exhaustive list of what a system safety program plan may include: - Summary of safety requirements, tasks and required documents, - Schedule of tasks to perform and contents for each milestone, - Organisation description, responsibilities, link between safety tasks and with other development activities, sub-contractor or co-contractor activities and integration of their analysis/tests results, - Standards, methods (functional analysis, PHA, FMECA, FTA, predicted assessment for electronic parts, sneak path analysis if required by NSAA, etc.) and tools used to satisfy requirements, - Meeting, audit, review, working group with sub-contractor and/or customer, - Applicable Severity scale, - Applicable Probability scale, - Applicable Criticality matrix and hazard acceptance, - Critical item list and/or safety item list with critical design characteristics for safety, - Design rationale and engineering change proposals, - Forms and detailed levels used for analysis, - Safety Software development assurance level (and for Programmable Electronics) (see 2.1.2.7 too), - Feedback process (FRACAS/DRACAS), - Safety test and other tests. MIL-STD-882E task 102, AOP-15, or other acceptable standards (especially for software and Programmable Electronics) may be used for information about the safety plan. The plan should be acceptable to NSAA or its representative.
2.1.2.	Hazard analyses	It is not exhaustive because the supplier can perform additional tasks or may use other methods for safety assessment.
2.1.2.1.	Life Cycle Environmental Profile (LCEP)	This task is necessary for the design but also for assessment of dependability, safety, ageing and the establishment of the test program.
2.1.2.2.		For an efficient safety process, the goal is to take actions to improve the safety early in the program. If safety analysis is conducted too late, it is very difficult to change the design which may impact the cost and schedule of the program.

		An efficient approach may be to perform a preliminary safety analysis based on the functional description before the preliminary design review and a detailed safety analysis based on the detailed design before the critical design review.
2.1.2.3.	Preliminary Hazard Analysis (PHA)	The PHA should be performed at the beginning of the design phase. Information to perform a PHA could be derived from lifecycle description (phases), system description and limits, external interface, usage description, macroscopic functional/organic description, technology used, etc. It is also useful to have a generic list of hazards and scenarios to perform a PHA that is as exhaustive as possible. This list should be continuously updated by experience and should consider human errors and accidental events. Information from in service munitions may also be useful (e.g. in service surveillance, technical defects). A credible situation is one that is feasible but not necessarily expected. An example of a credible situation is bullet attack; an example of a non-credible situation is multiple bullet impacts that all penetrate through the same hole.
2.1.2.4.	Hazard Analyses	These analyses evaluate the SAF System design to estimate the probabilities of failure over its anticipated lifecycle for the purpose of their elimination or control, including those due to human error and software failure. The analysis should be performed from the SAF system level down to component level once the design is finalised. Standards such as IEC 60812 are applicable for FMECA. Standards such as IEC 61025 are applicable for FTA. Other standards (from IEC or other standardization organisation) cover other analysis methods (see IEC 60300-2 or STANREC 4174).

		The description of the architecture by a model (static and/or dynamic), diagram, state chart, etc. is useful to improve understanding of the functionality and the propagation of effect in case of failure through the model. The important point is also to have consistency between analyses (PHA, FTA, FMECA, etc.) and with the design. Therefore, configuration management and traceability are essential. Hazard analysis may be qualitative and/or quantitative depending of the design phase. Probabilities used should be justified especially if the event is a cut set of order one in FTA (use of a data base such as NPRD/EPRD (RIAC) is not recommended in this case). For electronic components, standards such as UTE C80-811, MIL HDBK 217, etc. can be used. If necessary, testability may be taken into account in hazard analysis. Another useful method is analysis of subverted safeties.
2.1.2.5.	Hazard Analysis Revision	The design authority should have involvement in the configuration management process. Change in the manufacturing process or location may also influence the performance of the design. In general, when there is a change in design or process the validity of justification previously obtained (by analyse, inspection, test or demonstration) should be checked.
2.1.2.6.	Safety Critical Components and Characteristics	Safety Critical components should be specifically under control during all development, manufacturing and maintenance activities/processes. The rationale for identifying critical components and characteristics is also to prevent future modifications to these elements without detailed analysis which may degrade the level of safety below that which is acceptable. Examples of safety critical design characteristics are: - Sensors such as accelerometers when used in safety systems have certain critical performance values used to sense the environmental forces. The safety critical characteristic list should reflect the specific component for the critical performance values.

		- The specific materials used in an interrupter can be critical to passing the safety tests. If an interrupter is made from special steel, the critical steel characteristics should be in the list. - Safety critical processes: The assembly of components may also be safety critical (e.g. torque, position, spacing, riveting...). To summarize, critical components have critical characteristics. Therefore, both should be documented and under control during manufacturing.
2.1.2.7.	Programmable Electronic(s) and software(s).	Engineering activities and quality assurance level should be described in the system safety program plan or in a dedicated safety plan for Programmable Electronics and software. A safety plan is used to define all activities, standards, tools, organization etc. to conduct during the program. Specific rules, activities, methods, tools, responsibilities, etc. should be defined based on criticality. E.g. : - Software/hardware specification, - Software/hardware interface, - Software/hardware design, - Language and rules associated, - Quality measurement of the code, - Quality assurance, - Configuration management, - Change proposal, - Test procedure, - Traceability, - Review, - Technical event, - Customer audit, - Programmable Electronic and software summary report for each version, - Etc. Note: safety activities should be conducted with appropriate timeliness. This plan should be acceptable to NSAA or its representative.

		Programmable Electronic (definition extracted from https://www.iso.org/obp/ui#search) : based on computer technology which can be composed of hardware, software, and of input and/or output units Note 1 to entry: This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc. EXAMPLE: The following are all programmable electronic devices: — microprocessors; — micro-controllers; — programmable controllers; — field programmable gate array (FPGA); — application specific integrated circuits (ASICs); — programmable logic controllers (PLCs); — other computer-based devices (for example smart sensors, transmitters, actuators).
2.1.2.7.a.		FTA should address contributions of human operators, software and hardware. Minimal cut set, common mode/cause analysis and sensitivity analysis should be performed based on FTA.
2.1.2.7.b.		Several international or national standards are available. See also Paragraph 3.4. Even if Programmable electronic and software are not safety critical, it is important they are reliable. If this is not the case, the consequences may be UXO, lack of operational efficiency and may result in vulnerability of the platform or users.
2.2.	Safety assessment review and approval	none
2.2.1.		If the SAF system is COTS/MOTS sourced, it is important to obtain information from the country of design origin and/or the supplier concerning the compliance early in the acquisition cycle (e.g. at request for proposal). In this case, the NSAA may require an independent safety assessment based on the compliance certification and/or safety assessment documentation (from the original country). A detailed impact analysis of modifications or the use in a new application should be performed.

		New safety assessment documentation should be produced or the existing safety assessment should be updated.
2.2.2.		none
2.3.	Waived requirements	It should be noted that the NSAA may not accept justifications to reduce safety below acceptable levels based on program constraints, such as cost and schedule. Modification(s) of a non-compliant existing design may improve safety even though all previously waived requirements are still not satisfied/resolved. NSAA may require a mitigation plan to resolve non-compliances.
2.4.	Environmental conditions	This requirement is related to Design Safety Tasks such as LCEP (see 2.1.2.1), PHA (see 2.1.2.3) and test procedures (see 2.13). “Induced environment” may be induced by various sources (e.g. vibration during transportation, storage conditions in a container). For example, AOP-20 requires that after the 12m drop test, the fuzing system shall stay Safe for Disposal .
2.5.	Energetic materials	none
2.5.a.	Assessment and qualification	The energetic material may be qualified for general use or a specific use. A list of qualified material may already be established by official National services. A list of qualified energetic material for NATO nations can be found in AOP-26. A payload may be an explosive filling or other configurations. IM tests in accordance with STANAG 4439/AOP-39 may also be considered to assess the reaction of energetic materials. Qualification of an energetic material from another country may be possible based on a certificate and/or qualification assessment report. Qualification of an energetic material may be limited in duration (e.g. duration only 5 years in France). It is useful for identification of evolution.

		For energetic materials, any modification of the design, process or change in supplier of ingredients may have a safety critical impact. Therefore, each evolution should be analysed and if necessary, a new qualification should be done.
2.5.a.1		While it is unusual, sensitive energetic materials can initiate outside their design mode. This is one reason such explosives must be used with interruption. Application for detonating main charge (e.g. high explosive shell)
2.5.a.2		They may be used for example in expulsion applications; BKNO3 has been used as a standard in the qualification of other pyrotechnic compositions used without interruption. But there are different types of BKNO3 and the sensitiveness may vary. Therefore, criteria, methods and threshold identified in AOP-07 may be used as a reference. Application for main charge with other effect (e.g. smoke, illuminating, carrier munitions, propellant…).
2.5.b.	Lifecycle safety	none
2.5.c.	Sensitiveness	Characteristics of energetic materials may change during lifecycle. Specific ageing tests at munition and/or component level should be performed. If necessary, in service surveillance may be applied with pre-defined criteria.
2.5.d.	Assessment of explosive components	none
2.6.	Material compatibility	STANAG 4147 will be used: - During the assessment and qualification of standalone energetic material, - When the energetic material is introduced in the SAF system, - Any change of material affecting the SAF system. Compatibility will be checked with material which are in contact (physical or vapour) or which may come into contact (e.g. glue migration during assembling process). Products used during the manufacturing process should also be analysed under the responsibility of the design authority. A compatibility matrix is useful for identification of all interfaces to check. Special attention should be given when there is a modification of material (or surface treatments) in a SAF system and compatibility tests repeated if necessary.

		Composition of materials, e.g. glue, may also vary without notification from suppliers.
2.6.a.		none
2.6.b.		none
2.6.c.		none
2.6.d.		If used, then the materials should be treated, located or contained to prevent the formation of a hazardous compound.
2.6.e.		none
2.6.f.		Compatibility between inert materials should also be assessed (glue, non-metallic part, oil, grease, etc.). Electro-chemical reaction between metallic parts in physical contact should be assessed as well. A matrix may also be useful for identification of all interfaces to check.
2.7.	Insensitive Munition (IM) SAF system	The technical specification may prescribe IM requirements (threat/type reaction and configuration) and define if they are applicable to the standalone SAF System, in the packaging, and/or installed in the munition. When using a non-IM compliant SAF system with an IM compliant munition, IM response may be compromised.
2.8.	Electro explosive devices (EEDs)	The note, at the end of this Paragraph, applies for laser diode or other EID. As known today, this technology is not used for initiation of explosive main charge. Therefore, if this technology is used in a new design, NSAA should establish specific requirements based on this AOP-4187 and STANAG 4368.
2.8.1.		This characterization is at the EED level.
2.8.2.		Specific additional tests may be performed to qualify the EED for the specific usage at the SAF or munition level.
2.8.3		For an interrupted explosive train, the use of an electro explosive device with an Non Initiation Stimulus of 1A/1W or greater is recommended.
2.8.4.		none
2.8.4.a.		An insensitivity of 500V for EED has been accepted as a safe standard to ensure that EED are insensitive to stray voltages that may be experienced during munition lifecycle.

		For example, EFIs are accepted as meeting the 500V no-detonate requirement based on the predicted Non-Initiation Stimulus, MASS and MAES using the AOP-43 standard fireset unless the NSAA determines that use of the intended fireset is appropriate. The energetic materials of the EED should also be compliant with Paragraph 2.5.
2.8.4.b.		Meeting this requirement assures that during or after final installation of the subsystem containing EED into the munition (or subsystem), it will not initiate as a result of an accidental electrical input to any leads that may be accessible during assembly, test or repair. If the EED leads are directly accessible, the requirement then applies to the EED itself; generally though, the requirement applies to the SAF System as a whole.
2.8.4.c.		The voltage could be provided inside the munition or outside the munition by the weapon system, by military equipments or by test or maintenance facilities interfacing with the munition.
2.9.	Communication	For this requirement, all phases, all functioning modes and all communication should be considered. Security, integrity and susceptibility of communication should be checked (in compliance with national regulations) especially if safety may be compromised. This requirement covers communication between the SAF system and a platform or a remote control. All types of communication is considered in this requirement (e.g. wire, wireless, optical, acoustic…)
2.10.	Battery	The potential hazards from the use of batteries should be assessed in each lifecycle phase and should not compromise safety. E.g., hazards arising from physical and chemical effects of battery activation or failure. The intent of the requirement is to have a minimum level of safety proven by standard tests at cell and battery level. After that, the design of the SAF system and tests at the SAF system or munition level should demonstrate that safety is not compromised by the battery (e.g. by leakage, burning, explosion, hot venting, etc.). Ageing of battery should be considered too. In case of leakage the effect on energetic materials and safety features should be analysed.

2.11.	Demonstration of non-armed assurance during assembly and installation	none
2.11.1.		For an interrupted explosive train, non-armed assurance is based on safe interrupter position and locked by all safety features. For a non-interrupted explosive train, non-armed assurance is based on the absence of energy for arming.
2.11.1.a.		A feature that prevents assembly of the SAF System in the armed state should not, in itself, be capable of being omitted or misassembled.
2.11.1.b.		X-Ray and tomography are acceptable means because it is positive and direct. It should be demonstrated it is non-ambiguous (safety features position visible) in the specific application. X-Ray or tomography could be used with all munitions without unarmed/armed visual indication.
2.11.1.c.		The means required in Paragraph 3.4.b concerning Electrical Firing Energy Dissipation may be used to comply with this requirement. For non-interrupted explosive train, arming and firing energy may be the same.
2.11.1.d.		none
2.11.2.		none
2.11.3.		none
2.11.4.		none
2.12.	Design for quality control, inspection	none
2.12.1.		none
2.12.2.		See Paragraph 2.1.2.6
2.12.3.		It is also applicable for simple features to be added into the design in order to perform quality control or maintenance.
2.12.4.		none
2.12.5.		none

2.13.	Test procedures	Additional test may be necessary, for example wear barrel and high-pressure tests. For logistic transportation regulations (dangerous good transportation regulation) and loading on board a ship, the drop test (12 m or higher) should be conducted (see STANAG 4375, UN orange book (see reference below), AOP-20 test A3 or specific requirements). UNO regulations on transportation of dangerous goods: ST/SG/AC.10/11/ 1 Recommendations on the transport of dangerous goods – manual of tests and criteria ST/SG/AC.10/1/ (volume 1 & 2) Recommendations on the Transport of Dangerous Goods – Model Regulations
2.14.	Maintenance	none
2.15.	Unarmed/armed status visual indication	The purpose of the visual indicator is to show that the SAF System is not armed up to the point of installation into the munition whether in the field or at a depot. 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 appropriate authority. If colours are created or generated by reflected light, they should be glare free and daylight fluorescent protected to ensure they do not decay. Non-specular colours to avoid reflection when exposed to a natural or artificial light. For LCD and LED displays, the colour coding should be acceptable to the National Safety Approving Authority and based on ergonomic standards. Failure of the indication should be assessed. For SAF system with non-interrupted explosive train a dual redundant discharge path is an acceptable alternative to providing a visual indicator (see 3.4.b). But, in some cases, the voltage in the firing capacitor may also be measured and provided to the platform and the user by a dedicated circuit. Such a circuit should not degrade safety.

2.16.	Demilitarisation and Explosive Ordnance Disposal (EOD)	none
2.16.1.		Depending on the munition, may be performed at the munition level instead of the SAF system level.
2.16.2.		EOD should be considered early in the program and is one of the reasons an early design review is recommended. Additionally, EOD assessments often require testing of some hardware which requires budgeting. In situ disposal is not considered an acceptable design solution.
3.1.	Fundamental Safety Design Requirement	
3.1.1.	Inclusion of Safety Features	Fuzing systems include Safety and Arming devices which incorporate safety features. A safety feature is a combination of elements normally comprising a sensor, logic and either a mechanical or electronic means of directly preventing arming. The sensors provide information on the environmental stimuli experienced by the munition. This information is evaluated by the logic system to ensure that the environments representative of a valid launch or deployment have been attained and that enabling of safety features may proceed. If environment sensed are not valid launch or deployment conditions any safety features should be enabled. These combinations of sensors and logic can vary from simple mechanical devices which sense the environment and perform a logic function, to an array of sensors which pass information to the electronic logic.
3.1.1.a.		In an interrupted explosive train a minimum of two independent safety features control the interrupter directly by two locks. A mechanical lock is a device that directly restrains the explosive train interrupter in the safe position during all credible environments. The requirement for two independent safety features is not met by a lock on a lock. In a non-interrupted explosive train a minimum of two independent safety features controlling three independent energy breaks controls the supply of arming energy. An energy break is a device which directly prevents the transfer of energy through the circuit.

		A safety feature can be thought of as anything that contributes to the safety of the system; however, in this standard the term is used to describe one or more components that prevent inadvertent arming. Examples of single safety features could be an energy interrupter coupled with logic that senses acceleration and controls the energy interrupter, or 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. The term interrupter or shutter is used to describe 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 outside of its design intent. Locks release the interrupter when subjected to the correct arming environments only and should not be overcome by the interrupter itself. Safety features should be independent and common cause failures minimized. Therefore the design should take into account for each safety feature: - independence of arming stimulus, - independence of components and functions, Independence indicates no common part or function between arming stimulus treatment and with other functions in the fuzing system or in the munition.
3.1.1.b.		none
3.1.1.c.		none
3.1.1.d.		Credible environments include normal, abnormal and accidental environments.
3.1.2.	Operation of Safety Features Using Environmental Stimuli	The environments below (Paragraph 3.1.2.a), sensed directly, are recommended for use as activating stimuli for safety features; all should be considered before selecting the most suitable. Locks which operate independently of each other but use the same environment are not independent and are therefore unacceptable. Designers need to pay particular attention to the orders of magnitude of the environmental stimuli which munitions may encounter so as to ensure that all systems are suitably constructed. Stimuli selected for use should have an acceptable safety margin or time duration significantly above those expected during the lifecycle up to intentional launch.

		Designs that combine such environments occurring in the correct sequence and within the time duration prescribed by the operational requirement provide additional safety.
3.1.2.a.		Use of environments depends on the nature of the munition and its functioning sequence. Platform factors may also influence the choice. Environments may be: - Launcher chamber pressure. - Propulsion unit operating pressure. - Axial (Launch) acceleration (Setback). - Angular velocity/ radial acceleration (Spin). - Flight acceleration (Powered). - Dynamic air pressure or flow (Velocity). - Hydrodynamic and hydrostatic pressure. - Flight deceleration (Drag). - Barometric pressure. - Absence of gravity force (Zero 'g'). - Stimulus related to irreversible commitment to launch. Other environments may be used if they are representative of munition launch. It is very important to assess the choice and the usage of stimulus during the review of the preliminary design. Environmental sensors contributing to the arming process should be considered part of the fuzing System.
3.1.2.b.		For example, safety features using setback and/or angular velocity stimulus should not be removed in case of accidental drop.
3.1.2.c.		none
3.1.2.d.		none
3.1.2.e.		A launch cycle is considered to be irreversible when a non-restorable launch function occurs and the launch cycle is subsequently out of the user's control. Examples of an action taken to launch a missile that may be considered an environmental stimulus if it irreversibly commits the munition to complete the launch cycle are: - An air launched munition that makes use of a lanyard or solenoid. - A launch signal to a propulsion EED or a thermal battery

		In the absence of a robust launch environment, launch events may be used if such events irreversibly commit the munition to complete the launch cycle. The events should be time windowed and sequenced
3.1.2.f.		none
3.1.3.	Prevention of Unintentional Arming	none
3.1.3.a.		none
3.1.3.b.		none
3.1.3.c.		There is a distinction between a common-cause failure and a common-mode failure. Refer to definitions for clarification (see electropedia.org). Minimal cut set analysis on FTA is one method used to demonstrate compliance (single point failure). The robustness of the design to environmental conditions should be demonstrated. If not, it is a common cause failure, and in this case it may be a systematic failure. Common cause analysis should be performed. Guidance may be found in ARP 4761, IEC 61025. Example of common cause: loss of power, identical component or technology, environmental conditions (e.g. electromagnetic, climatic, mechanical…), etc. Redundancy is imposed by this requirement. But redundancy is not always possible especially for structural components (e.g. body of the fuzing system). Traditional methods to reduce the risk from common cause failures can be physical or functional: - Physical techniques can consist of selection of different technology components, suppliers and/or their packaging (dissimilarity). - 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).

		Partitioning is another method commonly used to reduce the risk of common cause failures within electronic safe and arm devices (ESAD) and other electronically controlled fuzing systems. “Partitioning” here consists of a physical separation, or the selection of different location of the energy interrupters to avoid susceptibilities from similar environments and conditions. To assess the SAD alone is not sufficient. It is necessary to assess the SAD integrated at its place in the fuzing system with respect of interface and confinement.
3.1.3.d		none
3.1.3.e		It is important to check the sequence, time window and the validity of arming stimulus.
3.1.3.f.		Stored energy is: Latent energy within a system, subsystem or component, that, when triggered, is released to perform a function. Stored energy increases the probability of the safety system failing in an armed condition or functioning. Some examples of stored energy are: - Batteries. - Charged capacitors. - Compressed gas devices. - Explosive actuators. - Loaded springs. Stored energy should be analysed in two manners: - Failure of the stored energy itself. - Failure of another item and the energy that is then released
3.1.3.g.		none
3.1.3.h.		none
3.1.4.	Application of Requirements to Multiple Safety and Arming Devices (SADs)	When demonstrating the safety of fuzing systems on sub-munitions, the Design Authority should demonstrate that: - Sub-munition fuzing systems cannot arm as a result of expulsion from the carrier munition except after a verified launch and achievement of the necessary arming delay by the carrier munition.

		- Within the overall system, the inadvertent arming and functioning of any sub-munition fuzing systems is less likely than the inadvertent arming and functioning of the carrier munition fuzing system. - That it is impossible to inadvertently assemble an armed sub-munition fuzing system onto a sub-munition. - That it is impossible to incorporate a sub-munition with an armed fuzing system into a carrier munition. That sub-munition fuzing systems cannot arm as the result of a credible accident, including rupture of the carrier munition as the result of a mechanical handling, traffic accident or as a result of the expulsion charge firing as the result of a fast or slow cook-off.
3.1.4.a.		none
3.1.4.b.		In an interrelated system, there is some form of communication between the multiple Safety & Arming Devices and the action of one directly affects the operation of another. An example of interrelated Safety & Arming Devices would be a device which uses the output of another as an input.
3.1.4.c.		none
3.1.5.	Fuze Setting	The setting of the fuzing system arming delay/distance should not be less than the safe separation distance. Validation of the set parameters used should be considered. The hazard analysis should address setting failures and the effect on safety.
3.1.6.	Fail-Safe Design	The meaning of fail-safe is “a design property of an item which aims to prevent its failures from resulting in critical faults”. For safety, arming and functioning systems, an example would be design features that render the munition incapable of arming and/or functioning upon malfunction of a safety feature or exposure to out-of-sequence arming stimuli or operation of components Adequate testing should be performed in order to demonstrate the ability to fail-safe. .
3.1.7.	Self-destruction, Sterilization, Disarming	It is not always feasible or necessary to incorporate a self-destruction, sterilization, or disarming feature in a fuzing system and therefore the requirement will be specified. The inclusion of this functionality inevitably increases the complexity of a design. Measures must be taken to ensure that this does not have a detrimental effect on the safety of the system.

		Adequate testing should be done to demonstrate the performance and the safety of these functions.
3.1.7.		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. It is not always possible to determine if this function has failed or not, especially when there are no external effects. In this case, and in accordance with system requirements, munitions which contain these features should have a means of establishing if these features have functioned correctly.
3.1.8.	Single Device	The safety and arming device should be maintained in a single configuration item which is not distributed or integrated with other functions. The requirements of this AOP are for the entire fuzing system, not only for the device commonly referred to as a fuze or safe and arming device. Developing agencies will be expected to provide a documentation package that covers the complete fuzing system, (i.e. all those elements that combine to meet the requirements of this standard and parts related to fuzing system functioning). The design should be as simple as possible for safety purposes.
3.1.9	Munition with retargeting capability	Ideally, a “disarmed state” should be attained between target engagements.
3.2.	Probability	The fuzing system is designed for a no-arm distance and an all-arm distance. These distances are different from the safe separation distance. Tests of AOP-20 annex D should be used for the assessment of these distances. If the AOP-20 test procedure is not applicable for a specific munition other test procedures may be required to establish these distances. It is important to check that the no-armed distance is greater than the safe separation distance (determined by specific test and simulation). If it is not the case, users should be informed of this hazard and specific operational procedure should be applied.

		This point should also be checked when a previously designed fuzing system is used on a new munition or when there are modifications of an existing fuzing system or munition. The safe separation distance may also change with the platform (e.g. mid calibre on a land armour vehicle vs aircraft). Probabilities below are the minimum required and are applicable to all lifecycle and associated conditions. Other tests in AOP-20 should be performed to justify robustness of the fuzing system. See figure 1 for illustration of probabilities.
3.2.1.		The probabilities should be justified in hazard analysis (e.g. FTA, FMECA, …) based on knowledge, analysis and test results.
3.2.1.a.		None
3.2.1.b.		The rationale for this requirement is the hazard severity of functioning inside the tube. Arming environments are sensed inside the tube (e.g. spin, setback) for many tube launch munition, therefore it is necessary to delay the arming sequence.
3.2.1.c.		none
3.2.1.d.		This requirement is normally expected for munitions which can fly over positions occupied by friendly troops. Overhead 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 specific requirement (e.g., 1E-4 or 1E-5 has been used in previous applications) at the beginning of the program. The requirement should be considered when the weapon danger area is discontinuous.
3.2.1.e.		It is recommended to check during the specification phase if a specific requirement to address UXO/dud rate is necessary (e.g. Protocol V on Certain conventional weapons of UNO, …). Dud rate should be assessed in all credible firing conditions (e.g. graze impact, soft soil, temperature….). Self-destruction may contribute to the reduction of UXO rate.
3.2.2.		none
3.2.2.a.		none
3.2.2.b.		none
3.2.2.c.		The number of duds per round should be assessed in all credible firing conditions.

3.2.2.d.		none
3.3.	Control of Explosive Train	Figure 3 below shows examples of explosive train architectures.
3.3.1.	Use of Interrupted Explosive Trains	none
3.3.1.a.		Incorporating 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. The safety features which directly lock the interrupter in the safe position until arming begins should require ordered sequential removal. A lock is a device which directly prevents the movement of the interrupter even if arming energy is applied on the interrupter. Testing and evaluation of a system with subverted safeties will demonstrate the robustness of each safety feature. 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 should not be released by the absence of either one of them (See AOP-20 test A1 & A2).
3.3.1.b.		It is imperative that the effectiveness of the interrupter design is assessed by carrying out the AOP-20 test D1 (5 rounds per temperature and severe test for assessment of the failure probability of the interrupter). All explosive components, regardless of location within the SAF System, should be considered. The Progressive Arming Test (AOP-20 test D8) may also be required. Probability in paragraph 3.2 should be justified whatever the architecture may be.
3.3.2.	Use of Non-interrupted Explosive Trains	none
3.3.2.a.		For systems complying with the requirement, the logic should ensure that environments that operate the safety features are sensed in a defined sequential order.
3.3.2.b.		none

3.3.2.b.1.		An energy break is not directly in line with the initiator but indirectly prevents arming energy being developed in the firing energy storage device (i.e., capacitor). Examples are Field Effect Transistors (FETs), bipolar transistors and mechanical switches. An Energy break should be designed or implemented such that any static failure of the device will disable the dynamic (cyclic) operation of the switch. This design is subverted when commanding the dynamic switch with circuitry that is susceptible to simple static failures. Example of safety feature: - Accelerometer sensor + logic circuit for stimulus validation + energy break (MOSFET type) - Aerodynamic sensor + logic circuit for treatment and stimulus validation + bipolar energy break.
3.3.2.b.2.		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 cause failure), in non-interrupted explosive train with electronic fuzing systems. The only known method of achieving the requirement of a fuzing system that is not capable of arming if any or all of the energy breaks are left out is by means of a dynamic switch. If a novel and viable design is made which does not employ a dynamic switch then it should be submitted to the NSAA for scrutiny at the earliest opportunity. Frequency of the dynamic switch should be unique within the system.
3.3.2.b.3.		none
3.3.2.b.4.		none
3.3.2.b.5.		none
3.4.	Additional requirements for fuzing systems containing electromechanics & electronics	The selection of environmental test conditions (mechanical, climatic, electrical or electromagnetic, chemical …) is based on the LCEP and fuzing system configuration. Electro-mechanical and electronic fuzing systems should follow the design principles of STANAG 4238. Furthermore, Electro-mechanical and electronic fuzing systems should be tested at the fuzing system level in all intended operating modes while exposed to environments required in AOP-20 and complimented by AECTP 250/500 which provide the minimum system level electromagnetic environment tests. Designers should be alerted to the effects of induced credible environments such as electrical noise on Programmable Electronics, or vibrations on mechanical devices.
3.4.a.1		Programmable Electronics or logic circuits used as independent safety features may be on the same PCB but physically and functionally separated on that PCB. Common cause failure analysis

		should be conducted if the Programmable Electronics share components/resources (e.g. memory…). Use of a microcontroller and a FPGA is better than using two FPGAs or two microcontrollers. Usage of the same power source is possible if its failure modes don't compromise safety due to common cause failure.
3.4.a.2		The fuzing system must be safe during any test (during BIT or by external tool) where energetic materials are resident/present. The software/hardware compatibility between the fuzing system and external tools should be checked before connecting them together.
3.4.b.		The primary purpose of the energy depleting resistors is to assure that any energy developed on the firing circuit is automatically dissipated. This feature may also be used for EOD purposes and for manufacturing testing and control. This is a requirement for both a non-interrupted and interrupted explosive train in a fuzing system 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 fuzing system's energy storage devices depleted (e.g. firing capacitor). The appropriate NSAA may exempt the battery from this requirement if it can be demonstrated that it poses no hazard of unintended initiation. This requirement could be met by implementation of redundant bleed resistors that are designed to minimise common cause failures (technology, supplier, emplacement, orientation, etc.)
3.4.c.		none
3.4.c.1.		Consideration should be given to a uniquely configured/coded signal to enable the fuzing system to discriminate between spurious sources of electrical energy. The probability of an accident causing the generation and application of continuous or coded signals is less than that of one causing the generation and application of non-coded pulse signals.
3.4.c.2.		Tolerance to invalid, corrupted or out of range data should be analysed and tested during development. The validation of data received is essential before utilisation.

3.4.d.		Non-embedded software may still be used in non-safety critical applications such as mission management software (e.g. target detection when inadvertent function does not result in a hazard to the delivery system, personnel, or friendly forces, etc.).
3.4.e		none
3.4.f.		The preferred design approach is to use the simplest Programmable Electronic that can perform the required functionality. For example, a simple “AND” function does not need to be implemented using an FPGA. A complex device will require more analysis, documentation, testing and more scrutiny by the NSAA E.g., for a Programmable Electronic it is recommended to choose a simple device dedicated to functions required and no other functions in the munition. Therefore, it is easier to justify compliance with requirements of this standard.
3.4.g.		Since, any changes to the safety feature hardware can adversely compromise the safety of the design, it is critical to establish and maintain a stable configuration throughout the lifecycle of the safety feature. A Programmable Electronic, including associated memory devices, may be considered as satisfying the requirements of paragraph 3.4.e if, once programmed or configured during manufacturing, the configuration of its internal logic cannot be changed. Additionally, for devices relying on charged-based memory to implement a safety feature, a method of validating the integrity of the memory should be performed prior to executing the safety function. The memory should be validated with the rigor equivalent to, or better than, that of a 16 bit Cyclic Redundant Check (CRC16). This computed result should be externally compared against a known value that is stored externally. The external device(s) should (1) be fixed-in-structure, (2) be dedicated circuitry, (3) not contain and be exclusive from any other functions, and, (4) when feasible, not be implemented as part of any other safety feature. Consult with the appropriate NSAA. A national example of an internal and external memory validation is provided below in figure 4 below: For use of flash based Programmable Electronics, the following best practices should be followed and if not should be justified: 1. Avoid utilizing technology nodes below 65nm or technologies with a gate oxide thickness below 7nm.

		2. Use technologies which utilize an Oxide-Nitride-Oxide (ONO) dielectric. 3. Avoid technologies which utilize large area floating gate capacitor structures as a data storage node. For the purposes of this recommendation large area is defined as >4 μm^2. 4. Limit the number of program/erase cycling operations to 10 for Flash or EEPROM devices utilized in safety critical applications. 5. Minimize exposure to elevated temperatures for a prolonged duration. For the purposes of this recommendation, elevated temperature is defined as temperatures exceeding 70 degrees Celsius. 6. Mitigate exposure of Flash memory to low field energy (e.g., cell phone emissions, etc.) during long-term storage. Example mitigations could include RF shielding by the housing, packaging, etc.
3.4.h.		It is recognized that all Programmable Electronics can be susceptible to unpredictable operating states in the presence of certain environmental stresses/conditions as well as non-optimal and/or undesired design or manufacturing implementations. For this reason, at least two safety features should be implemented with dissimilar Programmable Electronics resulting in safety features that have dissimilar failure modes. Dissimilar logic refers to distinct methods and/or materials used to develop a particular device that result in devices with minimal, but known and assessed, common cause failures. Some examples would be a Full Custom ASIC, discrete components, Metal-to-Metal Antifuse FPGA, Oxide/Nitride/Oxide Antifuse FPGA, microcontroller, etc.
3.4.i.		An agreement between SAF system design authority and NSAA should be reach in order to focus on main characteristics in the manufacturer's documentation of the Programmable Electronics. A compliance matrix is an acceptable format for recording that the design and programming procedure are in accordance with the device manufacturer's specifications and notes. This includes programming, power up, power down, timing, operational, etc. Appropriately disabled means that the failure of the disabling method will not result in an unsafe failure of the device. If a conflict between the manufacturer's specifications (including notes) and other requirements (safety or otherwise) exists, then the justification for the deviation from the manufacturers specifications should be reviewed and approved by the cognizant safety authority. If a design deviates from the

		manufacturer's specifications then it should be shown that this deviation does not negatively impact safety.
3.4.j.		Power transfer refers to switching from one power source to another. Transition of power refers to the expected power-up and power-down voltage/current profiles (including rise/fall times) that the Programmable Electronic power/ground inputs could be subjected to during its lifecycle. Power transients include any noise, voltage/current spikes or surges, brown outs, etc., to which the Programmable Electronics power/ground inputs could be subjected during its lifecycle. One approach to mitigate the negative effects of power transfers, transitions, and/or transients is for each SF to utilize multiple independent resets logically OR'd together. Multiple SFs, given adequate isolation, could employ these same resets. Prior to intended arming, SF logic should initialize in a safe state and reset to a safe state. Test defined in AOP-20 annex F should also be applied.
3.4.k.		Any safety critical clocks should have a method of verification. The preferred method would be independent clocks or verification of the safety critical clock(s) with a known timed event. Multiple SFs could employ the same time basis for verification. The intent of this requirement is to ensure arming events/environments are correctly validated and invalid environments are not recognized as valid due to clock skew or failure. Some methods to mitigate the potential for single point or common cause failures of the arming delay include: (1) The use of independent timers is preferred. (2) The shortest arm delay set in hardware should be set to the maximum practical value. (3) Any transmission and validation of arm times must be as robust as practical (checksum, parity, CRC, etc.).
3.4.l.		This requirement is to ensure the intended design (Programmable Electronic schematics, software code, etc.) is actually what is in hardware/software. For example: (a) in VHDL, if the design has a binary state machine, the hardware does not have a one-hot state machine, which is functionally equivalent but physically different, (b) a synthesizer's optimizer should not adversely affect the approved design (the preferred approach is for the designer to disable any optimizers), and (c) a Programmable Electronic vendor should not optimize/change/make additions to the approved design.
3.4.m.		The preferred partitioning method is to use distinct components with separate electrical paths. Electronic circuits controlling independent SFs should be physically partitioned into functionally dissimilar elements, neither of which can, during normal operation or upon failure, independently

		arm the system. Additionally, functional and physical partitioning of the SF logic and non-safety logic is encouraged. SFs may be on the same circuit board, but components should be independent. The lack of common cause failures related to inadvertent arming should be justified.
3.4.n.		Undocumented functions or logic within a SF can compromise the safety of the design and is unacceptable. All the logic and functionality within a Programmable Electronic used in the SF should be documented. This includes any programming functionality, testing functionality, JTAG, SCAN, MODE, etc. See also comments on paragraph 2.1.2.7.
3.4.o.		A description of data flow between Programmable Electronics on the integrated circuit (and not inside the Programmable Electronics) should be detailed in the safety assessment documentation. The goal is to be able to establish and/or verify the specification for the Programmable Electronic and for its test procedures. More detailed information should be available on demand to the manufacturer.
3.4.p.		The documentation is intended as a record to assure that Programmable Electronics, developed for the fuzing system, within an approved design are reproduced consistently throughout production. The manufacturer should maintain configuration control on the manufacturing tool suite to include version numbers and manufacturer's datasheets for the computers, operating systems, compilers, synthesizers, analysis tools, testing tools, and other tools used to manufacture, analyse, test, document, and maintain the Programmable Electronic application. The documentation should include all the files generated during this process. Subsequent optimization of an approved design is unacceptable. This guidance doesn't require detailed information from the manufacturer of the Programmable Electronic component itself (i.e. from the manufacturer of the microprocessor or FPGA itself).
3.4.q.		The documentation is intended as a record to assure the Programmable Electronic configuration matches the intended design. These tools can be, but are not limited to: support software/compilers, storage devices, and any other intermediate entity that poses the potential to alter the final intended "as embedded" design. The configuration management practices should be commensurate with the criticality of the end product produced. Activities should be in compliance with requirements and applicable standards. See also comments on paragraph 2.1.2.7.
3.4.r.		The partitioning of power for SF logic from other power sources should be detailed in the safety assessment documentation.

		If there is not partitioning, the consequence on safety should be also assess in the safety assessment documentation.
3.4.s.		Timing for the application of power to the SF logic during the launch sequence or operational deployment should be defined in the safety assessment documentation. The time schedule of all arming event should be described in the safety assessment documentation via chronological diagram for example.

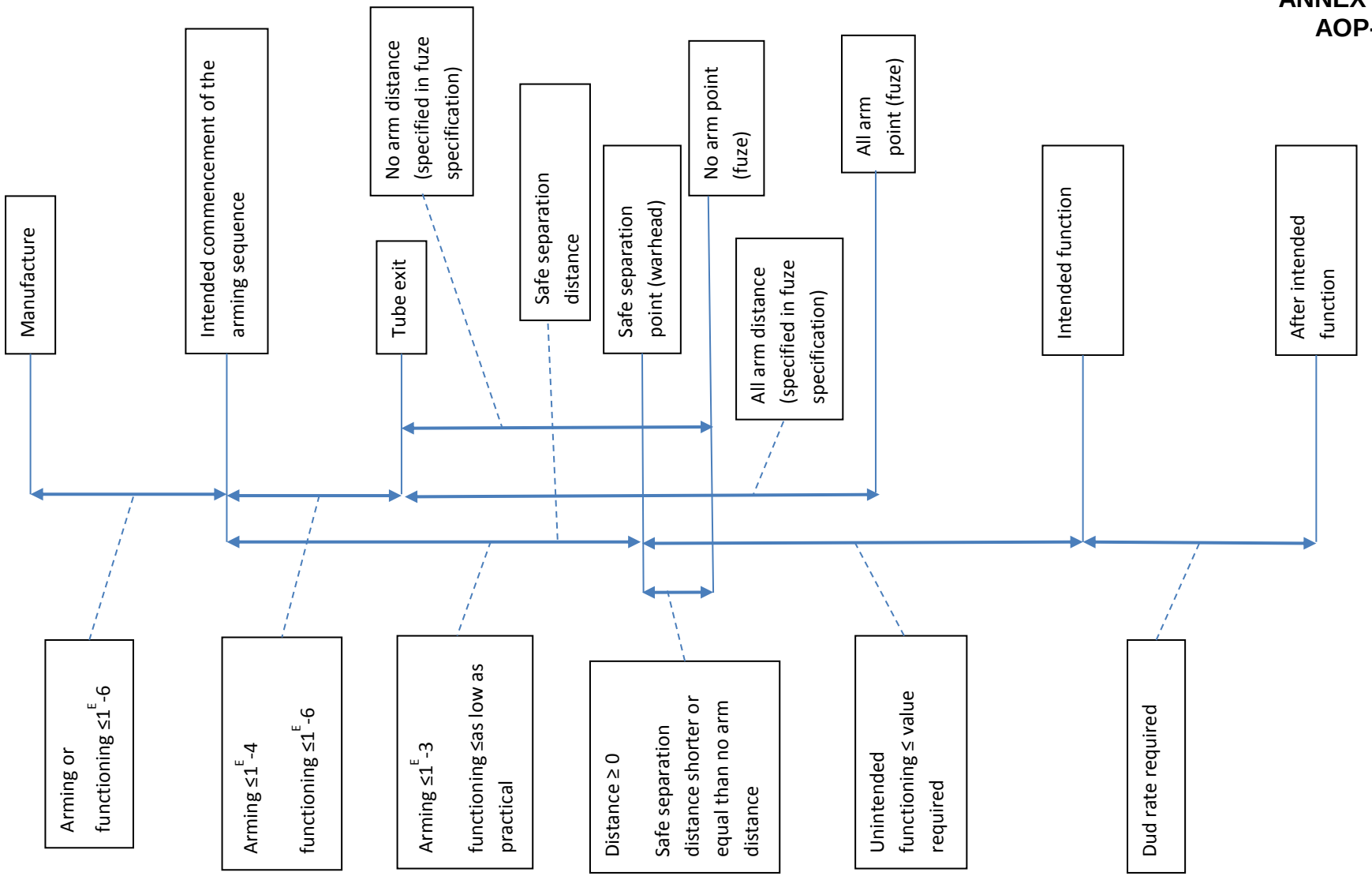
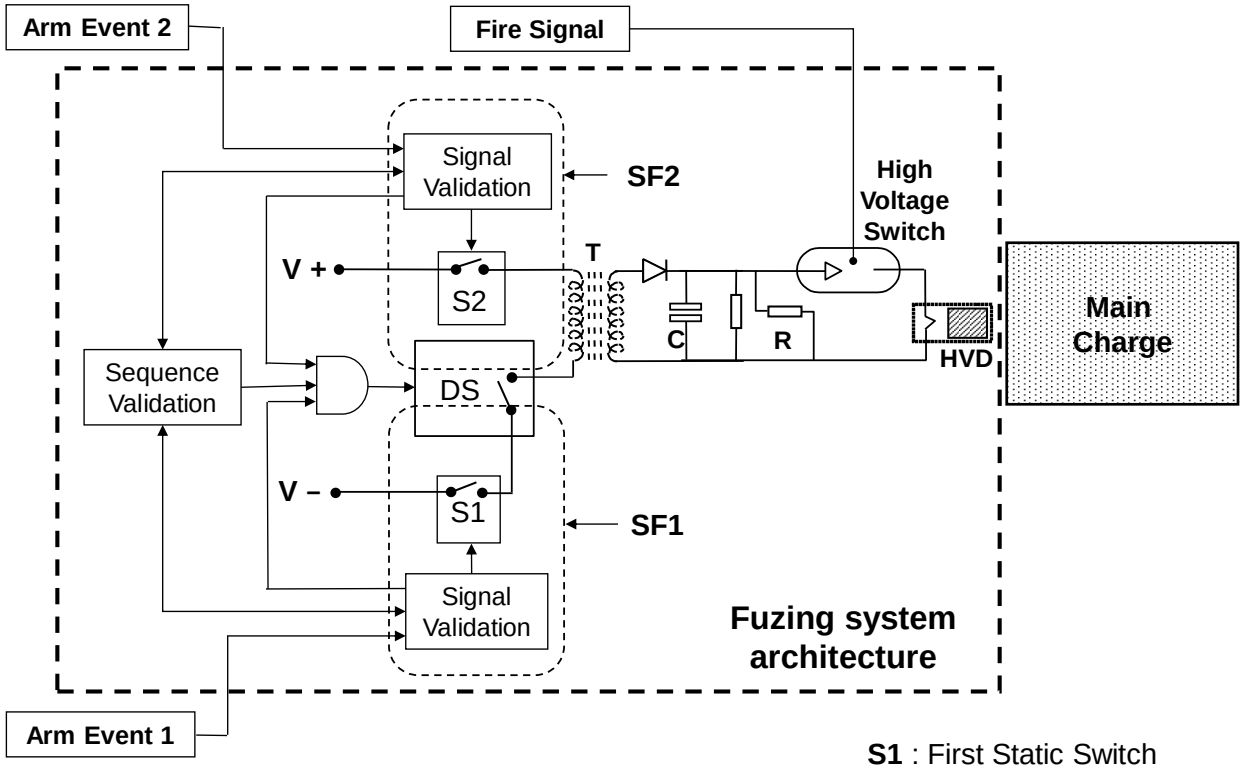


Figure 1: Probabilities and time/space (linked with Paragraph 3.2)



S1 : First Static Switch
S2 : Second Static Switch
DS : Dynamic Switch
SF1: First Safety Feature
SF2: Second Safety Feature
HVD: High Voltage Device

Figure 2: Arming Energy Accumulation Control for non-interrupted explosive train (linked with Paragraph 3.3.2).

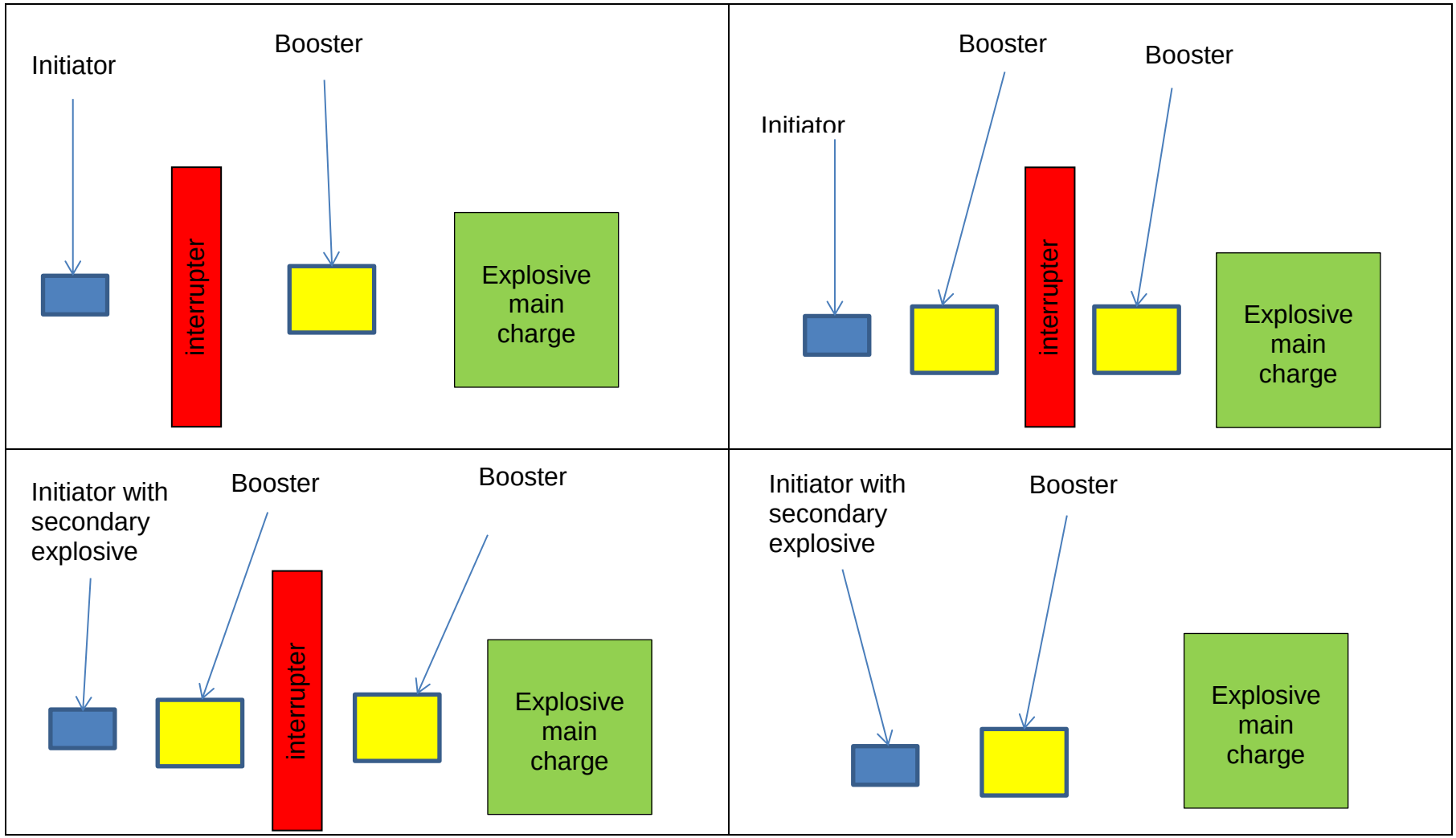


Figure 3: Examples of explosive train architecture – Explosives components beyond the interrupter shall be compliant with Paragraph 2.5.a.1 and 2.5.d or 2.5.a.2

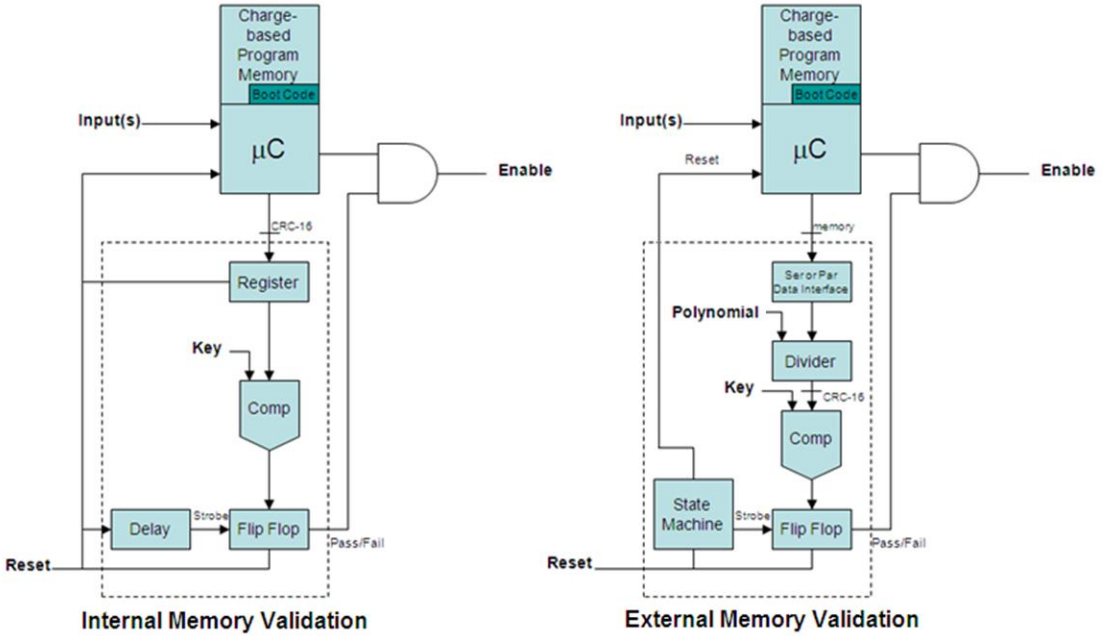


Figure 4: Example of internal and external memory validation

INTENTIONALLY BLANK

ANNEX E Example of a safety design assessment documentation for a SAF system

The safety design assessment documentation for a SAF system should address at minimum the following:

- Lifecycle: phases, environment (climatic, mechanical, electromagnetic, etc.), duration, shelf life, maintenance,
- Design reference,
- Usage description: munition, weapon system,
- Description of the SAF system:
    - Description of the function (i.e. arming, performance, no-arm, all-arm and safe separation distances),
    - Description with drawing of the different state of the safe & arming device,
    - Description of all energetic components/material:
        - their position inside the SAF system,
        - their supplier,
        - part number of the component,
        - nature of material,
        - quantity of material (NEQ),
        - reference of homologation/qualification of energetic material (STANAG 4170),
        - compatibility test reports (STANAG 4147),
        - …
- compliance matrix with applicable standard (STANAG 4187, STANAG 4368, STANAG 4497 or other),
- justifications for non-compliance with requirements,
- Safety analysis and assessment: e.g. PHA, FMECA, fault tree analysis, etc.,
- Safety critical design characteristics,
- Safety critical Programmable Electronic(s) and software(s) activities,
- Battery,
- Compliance matrix with safety requirements in the technical specification,
- Summary of all tests (at SAF system and munition level) performed on the SAF system with the description of the test, the results obtained and the reference of the report,
- Demilitarization and disposal procedure (STANAG 4518),
- Explosive Ordnance Disposal procedure (EOD).

Note: Documentation from another nation NSAA may be used to support compliance.

AOP-4187(A)(1)