NATO STANDARD

AEP-62
Volume VI

PROCEDURES FOR THE ASSESSMENT OF DEFENSIVE AID SUITES (DAS) FOR LAND VEHICLES - ASSESSMENT OF DAS SAFETY

Edition A Version 1
NOVEMBER 2021

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

17 November 2021

1. The enclosed Allied Engineering Publication AEP-62, Volume VI, Edition A, Version 1, " PROCEDURES FOR THE ASSESSMENT OF DEFENSIVE AID SUITES (DAS) FOR LAND VEHICLES – ASSESSMENT OF DAS SAFETY", which has been approved by the nations in the NATO Army Armaments Group, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4686.

2. AEP-62, Volume VI, Edition A, Version 1, is effective upon receipt.

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

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

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AECTP	Allied Environmental Conditions and Test Publication
AEP	Allied Engineering Publication
ALARP	As Low As Reasonably Practicable
ASIC	Application Specific Integrated Circuit
ATGM	Anti Tank Guided Missile
ATR	Anti Tank Rocket
BMS	Battlefield Management System
CDZ	Complete Dangerous Zone
c. f.	check for
CM	Countermeasure
CONOPS	Concept of Operations
DAS	Defensive Aid Suite
E^3	Electromagnetic Environmental Effects
EHA	Environmental Hazard Analysis
e. g.	*exempli gratia* (for example)
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EOD	Explosive Ordnance Disposal
ESD	Electrostatic Discharge
EUC	Equipment Under Control
FA	False Alarm
FD	False Detection
FDR	False Detection Rate
FHA	Functional Hazard Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FMR	Full Material Release
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
H&R	Hazard and Risk

HHA	Health Hazard Analysis
HK-DAS	Hard Kill Defensive Aid Suite
HMI	Human Machine Interface
HMP	Hazard Management Plan
HTS	Hazard Tracking System
HW	Hardware
ICD	Interface Control Document
i. e.	*id est* (that is to say)
IEC	International Electrotechnical Commission
ILS	Integrated Logistic Support
IP	Intercept Point
IR	Infrared
NA	National Authority
O&SHA	Operating and Support Hazard Analysis
PE	Programmable Element
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PLD	Programmable Logic Device
RF	Radio Frequency
RQMT	Requirement
SAF	Safety, Arming and Functioning
SAR	Safety Assessment Report
SDZ	Surface Danger Zone
SHA	System Hazard Analysis
SIL	Safety Integrity Level
SoSHA	System-of-Systems Hazard Analysis
SRHA	System Requirements Hazard Analysis
SSHA	Subsystem Hazard Analysis
SSPP	System Safety Program Plan
STANAG	Standardization Agreement
SW	Software
SwCI	Software Criticality Index
TTP	Tactics, Techniques and Procedures
UMR	Urgent Material Release

UXO	Unexploded Ordnance
VHA	Valid Hit Area
WDZ	Weapon Danger Zone

1 SCOPE

This AEP-62 Edition C Volume VI (Version 1) is part of a document series, as laid down in AEP-62 Edition C from STANAG 4686 Edition 3 “PROCEDURES FOR THE ASSESSMENT OF DEFENSIVE AID SUITES (DAS) FOR LAND VEHICLES”.

AEP-62 Volume I[1] provides the definition of DAS and the Security Classification Guide (SCG).

Volume VI informs DAS safety incrementally from generic to fully integrated platform; it also covers safety aspects for the use of DAS at a test range.

2 SIGNIFICANCE OF USE

The National Authority (NA) may at its discretion accept any deviation from the assessment procedures and requirements outlined in this document, provided the procedures used are judged equivalent, the decisions for deviation are well-founded and both are well documented.

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable national laws and regulations unless a specific exemption has been obtained.

The DAS safety assessment methodology defined in Volume VI enables the understanding of hazards and risks related to the use of DAS in different configurations, or “use cases”. This AEP does not limit the NA to require additional risk mitigation measures for DAS when national regulations are not met. Instead, the NA is encouraged to make use of additional precautions for safety at any level.

This volume may be updated by means of recorded changes as further data becomes available.

Where stated in this document, the NA is an appointed expert or group of experts.

3 PURPOSE

Volume VI provides procedures for the analysis, evaluation and assessment of DAS safety in a standardized way, thereby enhancing interoperability and ensuring that nations can develop and upgrade their equipment to match given threats.

The overriding objectives of this provision are; first, to adequately mitigate risks of unintended events, i. e. inadvertent incidents, with DAS systems, in particular those with critical or catastrophic personal injury; second, to minimize investment risks, that is to say, time and cost risks arising from the testing of DAS systems which are not mature for the respective usage or application.

The objective of Volume VI of the AEP-62 is to:

[1] Here and in the following text “Volume *N*” stands for “AEP-62 Edition C Volume *N* (newest version)”.

1. Provide a uniform guide for the assessment of the safety of Defensive Aid Suites (DAS) for use by NATO armed forces.
2. Present a common methodology to identify risks related to DAS testing and operation, and refer to analysis methods to demonstrate that the residual risks related to DAS are quantified, and are eventually acceptable.
3. Produce reports that increase the confidence in the DAS for safety, starting with common test range information to detail hazard probabilities of key safety aspects, including a safety statement concerning the investigated DAS, if compliance to the safety requirements comprised in this document and sufficient risk mitigation can be shown.[2]

[2] Where possible, safety requirements that could restrict innovative technology or direct to particular solutions are avoided in Volume VI.

4 METHODOLOGY

Against the background of seven use cases that are specified later in this document a general methodology allows for an assessment of DAS safety with regard to those use cases. This methodology, when applied to a specific DAS, is particularly useful to support the safety case for that DAS as required by the NA.

4.1 General

DAS are defensive systems aimed at countering incoming threats. Typically, the core functionality of a DAS is built upon electrical and electronic (programmable) components, such as sensors, countermeasures and their respective interfaces. A common feature of all known DAS is a (central) fire control unit that – based on sensor information – activates one or several countermeasures to engage a threat, see Figure 1. The countermeasure(s) of a DAS is/are designed to destroy certain threats, to minimize residual damage on the platform and/or to the environment, or to avoid a hit from a threat, entirely. How well a DAS satisfies this task is subject to experimental methodologies, defined in Volume II and Volume III of AEP-62; accordingly, these volumes deal with the assessment of the performance of a DAS from an experimental setup.

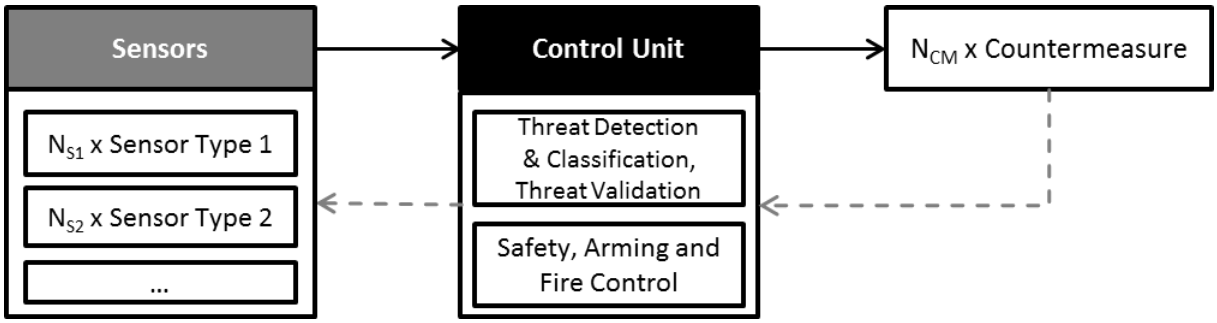

Figure 1: Abstract functional depiction of a DAS

Collateral damage and its assessment, subject to Volume V, are defined as the harmful and unintended effect to civilian and military persons and/or structures due to the normal use of DAS, i. e. in case of justified, and intended countermeasure activation. The methodology described in Volume V "*focuses on the delivery of the countermeasure until it interacts with the threat, the interaction process itself and the residual effects of countermeasure and defeated threat.*" (source: AEP-62 vol. V)

It is important to note that the evaluation rules defined here are based on the assumption that the system and safety functions of a DAS are most certainly both automatic and continuous, as soon as the protective function, i. e. the monitoring of the environment for incoming threats, is activated by the user. This holds true until the user disables the defensive function manually. The assumption of continual operation of DAS functions is the reason why, with regard to the risks of DAS, the terminology of mishap "frequencies", or "rates", (in units "per hour"; [h^{-1}]) is often applied for risk calculations and the assessment of systems. Mishap frequency is then

defined as the actual or expected average number of mishaps in relation to a specified period of time; this time span is usually given by the expected life of one item, duration of a mission; or, as indicated above, one operational hour. In this document the term “probability per hour” is uniformly used. Where necessary to account for failure rates of continuously operated (safety) systems, subsection 7.3 gives guidance on the conversion of failure rates to probabilities.

4.2 Aspects of DAS Safety

DAS Safety of Volume VI is a discipline of system safety, as well as munitions and fuzing systems safety; it complements the other aspects of the performance assessment. Especially in the case of the absence of any threat, a DAS must not entail any unacceptable risks to the user, uninvolved persons or the nearby environment. For instance, countermeasure control has to be taken into account when examining DAS safety, for an unintended activation of a countermeasure is always considered unacceptable. This might happen due to component failure, software error, false detection, or other sources of hazard within the DAS.

Inadvertent countermeasure activation might be regarded the single most critical hazard of a DAS. However, DAS safety assessment is not limited to this hazard. In fact, all hazards specific to a particular DAS that have a potential to become critical to users, uninvolved personnel and/or the environment have to be considered. In this respect all risks resulting from any unwanted, catastrophic or critical effects on persons, environment or material, have to be considered and mitigated to an acceptable level, apart from a situation of a justified and functionally correct reaction of the DAS to an approaching validated threat.

In contrast, if a DAS fails to counter a valid threat and harm from such a threat due to its normal, undisturbed operation occurs, this situation generally is not considered a safety issue of the DAS, unless it is about hazards associated with valid threats as listed in subsection 4.9.2. Rather, this situation is a performance issue of the DAS to be investigated by Volume II and Volume III methodology. Therefore, failure of a DAS to engage a threat is not a hazard being considered during Volume VI safety assessment.

4.3 Levels of DAS Safety Assessment

Generally, many state-of-the-art system safety standards and regulations exist that are well established in the defence industry. These standards are applied to the development of weapon systems; they can be (and are already) applied to the development and safety validation of DAS. Hence, it is the expectation that any DAS, being assessed according to the methodology of Volume VI, has been developed in a manner to be operated safely by the user during training, testing, combat operation or other uses. Volume VI relies on those state-of-the-art system safety standards and the adequate application of applicable requirements during DAS development by the contractor. However, this volume seeks to provide a level of general safety requirements with respect to the testing and operation of DAS.

Volume VI specifies basic, yet mandatory sets of safety requirements as well as recommended practice for a selected set of use cases; it describes procedures to analyse, evaluate and assess DAS for land vehicles in a standardized way with respect to safety. Thereby, Volume VI enhances interoperability and ensures that nations can develop and upgrade their equipment to match given threats. This volume defines seven typical DAS configurations: *Generic; Initial (test range); Generic with platform specific information; Interim with platform specific information (test range); Urgent installation / applique (stand-alone); Final installation / applique (stand-alone);* and a *Fully integrated solution*. These DAS configurations represent seven use cases that are described in detail in section 4.8.

Moreover, Volume VI introduces seven levels of DAS safety assessment: 6A; 6AT; 6B; 6BT; 6C; 6D; and 6E. Each level comprises a set of safety requirements for a specific use case; it directly corresponds to one of the seven DAS configurations so that a minimum set of safety requirements are specified for each use case. The methodology described here allows for testing and assessing a particular DAS configuration with respect to these safety requirements. In case of compliance it offers the frame for a safety approval statement by the NA conducting the assessment.

It should be emphasized that only the *Generic* and *Initial* configurations can be handled without platform specific information. Lack of platform usage information (profiles) may make risk assessment difficult, or speculative. More advanced configurations, up to the integrated solutions, need successively more detailed platform and usage data to provide for higher levels of vehicle integration. This reduces uncertainties and ensures greater confidence in the results of the safety assessment process.

For the assessment of a specific DAS, in order to test and possibly prove a particular level of DAS safety, certain safety requirements have to be met by the DAS. The verification of the fulfilment of those safety requirements is based on additional information and data about the DAS. This is usually provided by the manufacturer. To enable the methodology of Volume VI, those so called artefacts are consulted, and the information and data taken from those artefacts may give reason to support the decision to declare compliance to a safety level.

Thus, in contrast to the methodology described in other volumes of this AEP, Volume VI methodology relies on theoretical considerations based on the thorough study of safety artefacts. No experimental test setups, e. g. for testing technical safety functions, nor the carrying out of shots are required, nor are other “measurements” to practically prove DAS safety pursued in this volume. In a rigorous approach the safety assessment of DAS according to the paperwork of Volume VI is a precondition for performance level testing of other volumes of AEP-62.

However, when a situation with impact on safety occurs, e. g. during a range test, that has not been foreseen in this volume, or a technical DAS safety function deviates from its specification, or a DAS gets into an indeterminate, possibly safety-critical interim state, or shows other safety-critical behaviour which has not been foreseen, such a safety-critical incident must be clarified by investigations which the NA accepts responsibility for.

4.4 Procedures and Design Standards

The procedures described in Volume VI are simple, yet robust and workable to build confidence in the safety reports that can be generated by applying the methods of assessment proposed here. The discipline of DAS safety addresses both system safety and aspects of munitions safety. In general, the methodology presented here is closely related to the state-of-the-art methodologies defined in MIL-STD-882 [1] and STANAG 4297 [2] (AOP-15 [3]). However, giving guidance on DAS safety design is not intended, as it is assumed that already existing DAS are being presented for a safety assessment according to Volume VI; this allows for a simplified safety assessment process, which is proposed in this document. Secondly, the As Low As Reasonably Practicable (ALARP) principle is not applicable in all participating nations. Therefore, an alternative “mechanism” for demonstrating and accepting residual risks going inherently with DAS testing and operation, based on a unified risk-based approach, is proposed here.

4.5 Safety Terms

Throughout this document the following terms apply:

shall	This is a requirement.
should	This indicates a recommendation.
may	This term indicates a possibility or a suggestion.

4.6 Basic System Safety Requirements

For an effective conduct of the DAS system safety assessment it should be ensured in advance that the following requirements are met by the DAS.

1. The DAS system under assessment will have been developed under adequate consideration of safety requirements by the documented application of a state-of-the-art safety standard, e. g. the latest versions of MIL-STD-882 [1], STANAG 4297 [2] with AOP-15 [3], IEC 61508 [4], DEF-STAN 00-56 [5], or equivalent, or as accepted by the NA.
2. Safety-significant software shall be developed according to a recognized standard[3] (e. g. the latest versions of AOP-52 [6], IEC 61508-3 [7], DEF-STAN 00-55 [8], Joint Software Systems Safety Engineering Handbook [9], or DO-178 [10]).
3. The DAS development process will have been accomplished using configuration management. During assessment the DAS configuration, including all software configuration items, shall be assigned unique and retraceable configuration states.

[3] The concept of Safety Integrity Levels (SIL) for SW-based safety functions according to IEC 61508-3 provides methods for the development of safety-significant software components and the safety-proof. The SIL concept harmonizes well with the risk-based approach to safety assessment. Therefore, IEC 61508-3 is the preferred development standard for safety-significant and safety-critical software.

4. A system safety program plan in compliance with MIL-STD-882E Task 102 (System Safety Program Plan) shall be provided that shows how DAS system safety has been managed during development, system integration and realization accordingly. This system safety program plan, or equivalent document, among other data and information required by Task 102, shall explicitly specify the risk acceptance levels that have been applied as a requirement for DAS development.
5. The safety goals and the subsequent safety requirements, including how they have been met by the design of the DAS, shall be documented and made available for evaluation and assessment.
6. DAS safety-significant documentation shall be available for safety analysis, evaluation and assessment. This includes, but is not limited to, a hazard and risk analysis, and a safety assessment report.
7. A document, or several documents, shall be available, which show how munitions and fuzing systems safety according to STANAG 4297, STANAG 4187 [11] (or equivalent regulations), and downstream regulations, with respect to the countermeasure component, of the DAS has been achieved.
8. A detailed elaboration shall be presented which shows how the risk of an unintended countermeasure event during the operational and non-operational phases for the intended use case of the DAS has been reduced effectively to an acceptable level. As technical safety functions can be expected to be applied to mitigate this risk, a quantitative analysis of the residual risk shall be provided, e. g. by Failure Mode, Effects, and Criticality Analyses (FMECA), and Fault Tree Analyses (FTA).

Failure to comply with this set of basic system safety requirements may compromise safety. Therefore, a DAS failing to fulfil these basic system safety requirements should not be considered for assessments according to AEP-62.

4.7 Principles of the Safety Assessment

In general, system safety, i. e. the absence of unacceptable risks during a system's intended use, is a prerequisite for a system to be released into service. DAS safety is assumed to prevail if it can be demonstrated that (a) all risks associated with identified hazards of the DAS have been sufficiently reduced, and (b) all safety requirements are met. Thus, the risk-based approach of Volume VI starts from hazard identification, followed by hazard evaluation and risk assessment with the final step being the safety assessment. This step-wise process is specific for each DAS and its technologies. By means of this safety assessment it may be decided whether the particular DAS configuration is safe to be used in certain use cases, or applications.

On the one hand, learning from abstract functional principles of DAS (see Figure 1) as well as from the technologies of known soft-kill and hard-kill systems, sources of hazard typical of DAS can be delimited; the hazards listed in section 4.9 serve as a starting point for individual hazard identification.

On the other hand, the need exists to generate standardized reports on the safety of DAS for selected, yet typical use cases. With a defined usage profile for a DAS equipped land vehicle and with the experience of DAS safety backed by the robust processes of a risk-based approach, a set of seven use cases, or configurations, have been put together. This set, together with additional, specific safety requirements, constitutes seven increasingly complex levels for DAS safety assessment. See sections 4.8 and 7.4 for details.

When the risk-based approach is followed, standard procedure with standard documentation ("artefacts") is presumed. The verification and validation of system safety is strongly coupled with these artefacts. Therefore, to declare compliance of a DAS configuration with the safety requirements and the necessary risk mitigation that is mandatory for that use case, it has to be proven that the artefacts of this DAS configuration support the claimed safety case, and that they also satisfy national safety requirements as well as national risk acceptance criteria.

4.8 DAS Use Cases

The methodology described in this volume is to assess the compliance of DAS with the NA safety requirements and national risk acceptance criteria, and with the safety requirements and recommendations of seven different use cases specified in this document.

- **Generic**
  The *Generic* use case details DAS specification including safety architecture description of the DAS. Hardware (HW) and Software (SW) configuration items up to full system demonstrator may exist. The *Generic* use case is intended for safety assessment of a DAS when a platform is not or cannot be defined. It primarily serves for project risk mitigation purposes; safety assessment results in the course of the *Generic* use case may be considered for future DAS platform integration decisions.

- **Initial (test range)**
  For the *Initial (test range)* use case the DAS is used in a generic configuration, not specific to a platform. It is used in conjunction with a test rig. DAS functions are self-contained within the DAS. When a DAS in the *Initial (test range)* configuration is subject to performance levelling the system may be set up, e. g. for calibration, over a proprietary maintenance interface.

  DAS is operated (build up and tune test scenario, prepare, calibrate and perform the test, shut-down the DAS after test) by instructed test range personnel, vendor staff, trained personnel by industry, or other specialized persons. Limited HMI capability: DAS might employ special (obscure) servicing modes that are only obvious to persons familiar with the DAS. State of DAS, e. g. arming mode, or countermeasure state might not be displayed.

  DAS is operated on a test range. It is possible to set up and enforce a defined and limited zone, fully covering the surface danger zone (SDZ). Range control is in service to supervise this zone, which is only accessible for trained staff. The primary aims of

this use case are carrying out performance tests on different threats, or collateral damage tests; however, dedicated testing of safety functions is also possible.

- **Generic with Platform Specific Information**
  Use case identical to *Generic*, but with integration information available with respect to the numbers of sensors and countermeasures on a specific platform (vehicle); electrical connections between platform and DAS; estimation of DAS power consumption, weight and claimed volume; possibly discrete and/or digital electronic interfaces between vehicle and DAS with regard to state of movement (speed, orientation, etc.); vehicle state of operation and positions of hatches, turrets, etc.

- **Interim with Platform Specific Information (test range)**
  Use case identical to *Initial (test range)*, except that the DAS is used in a configuration to fit an extended test rig with platform specific appliances, with a vehicle simulator (e. g. geometrical mock-up) with platform specific numbers of sensors and countermeasures in original positions, or a vehicle demonstrator. Specific platform data, e. g. vehicle geometry, platform power, or sensor frequency ranges, are utilized for planning the DAS adaptation to the platform and for customization purposes.

  DAS is operated (build up and tune test scenario, prepare, calibrate and perform the test, shut-down the DAS after test) by instructed test range personnel, vendor staff, trained personnel by industry, or other specialized persons.

- **Urgent Installation / Applique (stand-alone)**
  A platform specific DAS configuration that is minimally connected to the vehicle's electronic architecture, typically only requiring power from the platform.

  Control and HMI functions are self-contained within the DAS. The intended use of the *Urgent Installation / Applique (stand-alone)* configuration is training and operational use with full featured defensive capability. Operation of the DAS is controlled by vehicle command. The safety case for the *Urgent Installation / Applique (stand-alone)* use case may be based on a reduced safety analysis; however, interactions (EMC, EMI) of the DAS electronics with platform electronics, as well as interactions between (different) DAS equipped platforms of a DAS equipped fleet will be taken into account. Additional safety requirements might apply to a turreted vehicle. A comprehensive safety case with the intention to show that this configuration is able to meet the full set of safety requirements, i. e. those that apply to a *Final Installation / Applique (stand-alone)* configuration, is started and carried out in parallel to operational use.

  An exception (waiver) may be required for fielding an *Urgent Installation / Applique (stand-alone)* configuration.

  DAS is operated by trained personnel.

- **Final Installation / Applique (stand-alone)**
  Use case identical to *Urgent Installation / Applique (stand-alone)*, except that all safety requirements are met without restriction.

DAS is operated by trained personnel.

- **Fully Integrated Solution**
  A platform specific configuration that is robustly connected to the vehicles electronic architecture and typically implies battlefield management system, communication, fire control system integration and consumes platform specific data: velocity, rotation rates, GPS, orientation, position, etc. The safety case considers DAS electronic interfaces to the platform and implications of safety on the fleet. Safety analysis is conducted by an independent organization with the final safety case showing full conformity with all safety requirements. Technical documentation is integrated with platform technical data and documentation. The *Fully Integrated Solution* is ready for in-service use.

  DAS is operated by trained personnel.

The seven use cases, or configurations, are tightly coupled, by a 1-to-1 relationship, to seven levels of DAS safety assessment; each level specifies a "level of ambition" for the safety assessment, and it defines a set of safety requirements that are specific for this use case.

Table 1: Use cases (configurations), artefacts, and intent of safety assessment

Level / Use Case		Artefacts	Intent	Comment
6A	Generic	Functional and safety concepts of the DAS	Report required to support pre-selection of DAS	In case of positive result system may be considered for further development activities
6AT	Initial (test range)	Range testing safety artefacts; safety information linked w/ vol. 2, 3 and 5	Report required to test the system on a test range	In case of positive result system may be considered for the range test.
6B	Generic with Platform Specific Information	Valuation of vehicle integration actions; impact on safety architectures (DAS, vehicle)	Report required to support pre-selection of DAS	Pre-selection candidate for platform installation or integration
6BT	Interim with Platform Specific Information (test range)	Interim safety artefacts for testing on a platform; safety information linked w/ vol. 2, 3, 5	Report required for testing on a platform in a controlled environment	In case of positive result system may be considered for the range test; anticipate software changes
6C	Urgent Installation / Applique (standalone)	Baseline safety artefacts for Urgent Material Release	Report required for initial integration on a vehicle	Procedural design (develop TTPs); In case of positive result system may be considered for UMR

6D	Final Installation / Applique (stand-alone)	Baseline safety artefacts for Full Material Release; safety information linked w/ vol. 7	Report required for Full Material Release	Review safety measures developed at final design
6E	Fully Integrated Solution	Baseline safety artefacts for FMR; Safety information linked w/ vol. 7	Report required for Full Material Release	Review safety measures developed at final design

Configurations 6B and 6BT may especially be helpful in aiding the pre-selection of a specific DAS for UMR or FMR; 6C, 6D, and 6E support the safety qualification of the overall DAS vehicle integration.

Figure 2 shows the hierarchy and the sequence of the seven use cases of Volume VI.

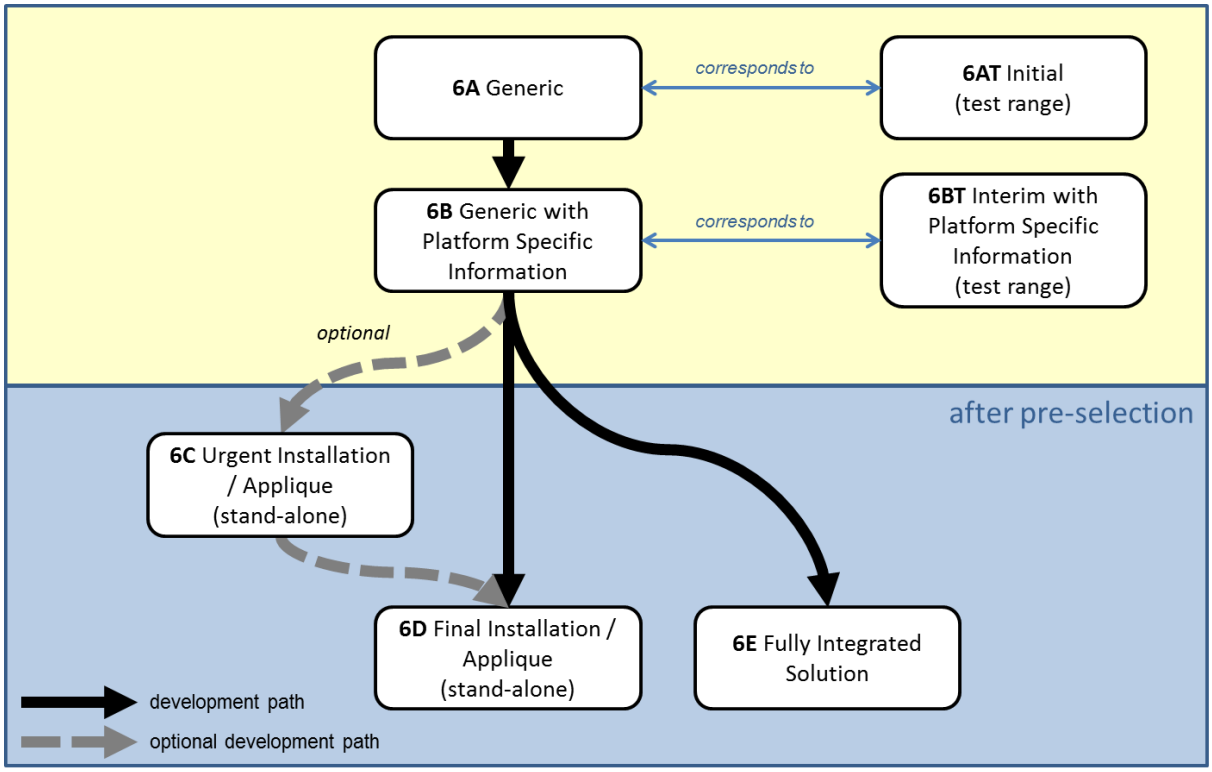

Figure 2: Evolution of seven DAS configurations

The intention of a Volume VI safety assessment is to give evidence that all residual risks of a DAS are mitigated to an acceptable risk level, and that the safety requirements associated with the respective use case are met. From a national perspective, NA enforced additional requirements may be necessary for the safety assessments of specific use cases as listed in Table 1. Particularly, this implies that all inherent hazards of DAS are actually taken into account

during the risk assessment. It is the task of the assessor, or the safety working group to demonstrate that the corresponding safety requirements are met. It is the task of the manufacturer to provide the necessary safety analyses, information and data ("artefacts", see section 7.5). A valid proof that the safety requirements associated with the respective use case are met satisfactorily, and that all residual risks are mitigated to an acceptable level may result in a declaration of compliance.

4.9 Hazard Sources and Typical DAS Hazards

4.9.1 Hazard Sources

All sources of energy contained within a DAS are potential hazard sources. During the safety assessment process only those hazard sources that exist in the DAS have to be taken into account. Typical hazard sources are:

- Electrical energy
  - e. g. batteries, electrical power generators
- Chemical energy
  - e. g. batteries, propellants, explosives in countermeasures and effectors
- Mechanical energy
  - e. g. rotating turret, springs
- Electromagnetic radiation
  - e. g. radio frequency radiation, optical radiation
- Pressure
  - e. g. pressure vessel
- other sources of energy with physical impact on the human body
  - vibration
  - noise
  - extreme temperatures
  - acceleration
  - shock
  - dangerous surfaces

Furthermore, material hazards:

- Toxic substances, e. g.
  - Explosives
  - Toxic gases produced by CM activation
  - Emission of gaseous toxic substances from components, e. g. batteries, propellants, etc.
  - Obscurants and smoke
  - Varnishes and paints

The safety assessor and/or the members of the safety working group have to make sure and finally decide whether the list of hazard sources is complete with regard to a specific DAS.

4.9.2 Typical High Level DAS Hazards

The hazards of a DAS originate from its hazard sources. Inadequate design, poor integration, or neglect of the safety-related interaction of the DAS with other active systems can pose direct hazards to personnel, or (operational) materials even during normal operation of a fully functional DAS. In the case of such direct hazards the substitution of hazard sources or an alternative risk mitigation have to be investigated and taken into account. However, a different set of hazards requires a malfunction of a hardware or software configuration item, the false detection by a sensor (sub-) system, or the faulty action of a user to trigger a critical condition; extreme environmental conditions could cause a component failure resulting in a safety-critical DAS malfunction. Depending on built-in system diagnosis functions or user intervention, a safety-critical DAS interim state will either lead to an inadvertent incident with risk of a mishap, or a controlled safe state of the DAS. External circumstances, e. g. the actual exposure of persons to a countermeasure effect in the Complete Dangerous Zone, are decisive for the outcome of such a dangerous situation. For hazard and risk analyses, those external factors may be estimated using probabilities p_{ext} from reasonable assumptions about the usage of a DAS, its application and surroundings (see Figure 3). Each hazard of a DAS has at least one associated mishap scenario that has to be considered during hazard evaluation.

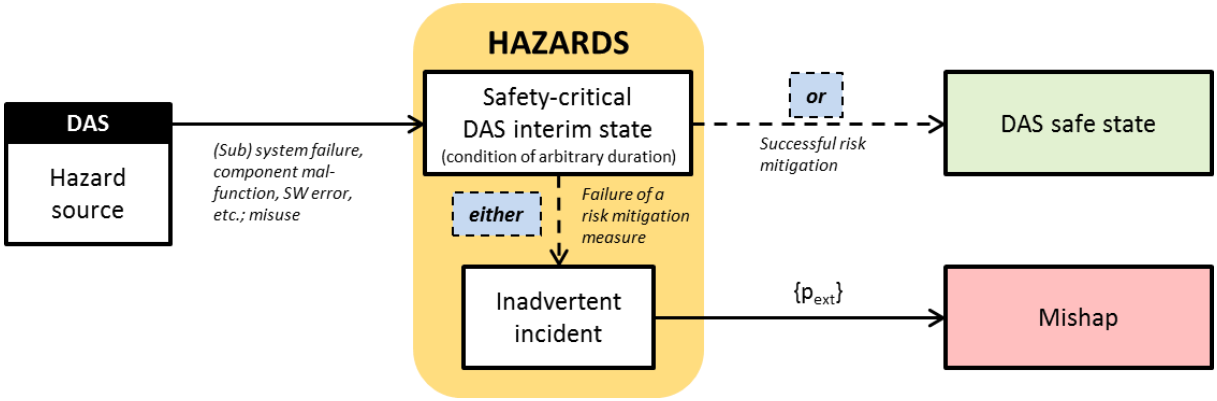

Figure 3: DAS hazards due to malfunction, or misuse potentially leading to mishaps

The following list comprises high level hazards of a DAS. The hazards list serves as a comprehensive example; it is the task of an assessor, or of the safety working group to ensure that a complete list of hazards for an actual DAS is created during the assessment process. Some hazards are open to interpretation during safety assessment process.

1. Unintended countermeasure activation, launch, or release.
2. Hazards associated with valid threats in operational or test scenarios:
    a. Selection and activation/release of wrong countermeasure.
    b. Incorrect activation/release of a countermeasure.

i. Mistimed CM initiation.

ii. Misdirected launch of a countermeasure.

c. Misfire / Hangfire.

3. Hazards associated with arming, and failure of disarming:
    a. Unintended arming of the DAS system.
    b. Unintended (partial) arming of the safety arming and functioning (SAF) (sub-) systems of fuzing components of the DAS, e. g. by accumulation of functioning energy.
    c. Failure of disarming, when arming is a reversible function of the DAS.
4. Radiation, i. e. activation of sensors, e. g. active laser sensors, radar.
5. False detection (see section 7.6).
6. Unintended/uncontrolled movement of turret or CM launcher.
7. Hazards resulting from software error (see section 7.7).
8. Hazards associated with human factors:
    a. Inappropriate or wrong operation of the DAS system, e. g. violation of health and safety regulations.
    b. Inability to distinguish between operational DAS states, e. g. armed DAS.
    c. Unstable interface control.
9. Electrical hazards, e. g. high voltage.
10. Mechanical and physical hazards, e. g. overstressing of material, hot surfaces.
11. Release of toxic substances.
12. Hazards associated with integration of a DAS on a specific platform (e. g. falling from a platform, HMI, electrical/electronic interfaces, toxic substances, EMC; c. f. vol. 7), especially:
    a. Failure to lock CM activation/release during open hatch operation (where this is considered safety-critical).
    b. Exceeding limitations (due to vehicle geometry) while directing a CM launcher.

The list of suggested hazards has to be tailored and possibly expanded during a safety assessment by the assessor, or the safety working group. As the countermeasure is considered the primary hazard source, special consideration should be given to the explosive components of a DAS:

Inherent DAS hazards related to explosive components can be classified into four groups, namely:

a. Intrinsic hazards. Those hazards presented by the explosive material in its quiescent state, such as toxicity, composition breakdown, gas / heat generation, material incompatibility, etc.
b. External and internal hazards. Which could initiate the explosive component or have an adverse effect on the firing chain, such as spurious fire commands, E^3 (Environmental Electromagnetic Effects including Electromagnetic Interference EMI), temperature / drop / shock / vibration, firing chain failure, aerodynamic heating, fragment and bullet attack, etc.
c. Hazardous consequences of initiation. Including partial initiation (whether intentional or unintentional) of the explosive component, such as blast, fragment, noise, toxic efflux, heat, etc.
d. Post launch and dynamic safety hazards. Such as loss of guidance control, unintended launch, ricochet, early burst, etc.

(adopted from: UK Joint Service Publication (JSP) 520 Part 1 Issue 4.2 [12])

4.10 Hazard Identification

What are the hazards of the DAS?

What are the sequences leading to potential mishaps?

The process of hazard identification is necessary to eliminate or mitigate potential causes of death, injury, damage or destruction of personnel, material or the environment in the intended use or application of a DAS. It should begin early in the development of a DAS and continue throughout its life-cycle. Hazards are identified through a systematic analysis process.

The hazard identification process of Volume VI is based on an independent analysis process by the safety assessor as well as on the evaluation of systematic hazard and risk analyses prepared by the manufacturers of DAS. Only by combining both sources of information can it be verified that the list of identified hazards for a specific DAS is complete.

By thorough comprehension of the technical details of the DAS and through application of hazard analyses, the assessor (or the tasked safety working group) for the DAS independently identifies its hazards. For this purpose the assessor evaluates system hardware and software, system interfaces (to include human interfaces), the operational or testing environments and the intended use or application. All historical hazards, mishap data and lessons learned from similar systems are taken into account. The same goes for relevant environmental and occupational health data, user physical characteristics, user knowledge, skills and abilities.

To consider hazards that have been found by the manufacturer of DAS, prior hazard and risk analyses, safety assessment reports and the hazard log, i. e. the hazard tracking system, are relevant sources of information for an assessor.

The result of this process is a list of all identified hazards specific to the particular DAS in the intended application (see 7.4.6.1).

4.11 Hazard Evaluation and Risk Assessment

How severe are the DAS hazards and mishaps?

How serious are the risks in the specific use case?

Although the goal should always be to eliminate a hazard, it is unlikely that the potential for safety-critical failures will ever be completely abolished. Therefore, eliminating all hazards of a DAS is usually impractical for any manufacturer. Thus, hazard evaluation involves a categorization of hazards, which allows for decisions with regard to appropriate hazard mitigation actions to be taken. In the course of this evaluation the assessor will require the manufacturer to have taken all necessary measures to eliminate hazards or mitigate the risks to an acceptable level. It is up to the assessor to take note of the measures aimed at achieving risk mitigation. The processes of hazard evaluation and risk assessment involve the investigation and evaluation of those measures taking into account their effectiveness.

As computing systems are generally considered an important element in DAS, regarding both, functionality and safety, utmost attention should be given to the risk assessment of safety-significant software; see section 7.7 for guidelines.

4.11.1 Hazard Evaluation

On the basis of a sound understanding of DAS system functions, and of how the DAS is operated in its anticipated environments, the assessor records, evaluates and documents all sequences of events that can be reasonably assumed to provoke mishaps. Identified hazards are tested with the intended uses, which are specified in, or may be derived from usage profiles; for every hazard its associated mishap severity is categorized.

Starting from available hazard and risk analyses supplied by the contractor, the assignments of the mishap severity categorisation for each mishap are retraced; the final assignments made by the assessor have to be reasonable and comprehensible to be acceptable. It must be ensured that for each identified DAS hazard the mishap severities of all associated mishaps are being established; this is also true in the case of hazards merely representing a safety-critical DAS interim state (see Figure 3); those hazards should be evaluated, and an adequate severity category should be assigned. An example for a safety-critical interim state is the unintended arming of a DAS.

For hazard evaluation it is recommended to use the mishap severity categorisation depicted in section 7.2.

4.11.2 Risk Assessment

Risk assessment crucially means to assess the likelihood of occurrence of a particular mishap scenario for a given hazard, and to determine the appropriate probability level as defined in

Table 4 in section 7.3. Appropriate techniques for the combination of probabilities exist to estimate, or even calculate, mishap probabilities where unfortunate coincidence of several unwanted events is causally responsible for the occurrence of an incident, referred to as “mishap” throughout the document. Risk assessment leads to assess the probabilities of all inadvertent incidents to result in a particular mishap (see Figure 3).

Systematic risk assessment addresses all identified hazards associated with DAS as well as their corresponding risk mitigation measures, including proof of their effectiveness. To evaluate the risk there are several methods available, e. g. expert judgment, numerical analysis, Failure Mode Effects and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA). Mishap frequency estimation may be based on qualitative and – where appropriate, preferably – quantitative assessment. The result of this process is documented by the assessor (or tasked safety working group).

To estimate the risk of every DAS hazard, the frequencies, or the appropriate mishap frequency levels, respectively, of occurrence for all mishaps are assessed, taking into account the conditions as well as all credible circumstances of actual or intended use; the determination may be based on reasonable assumptions, tests or other qualitative or quantitative methods.

Therefore, the technical safety functions implemented within the DAS have to be allocated. The adequacy of those safety functions, and, in addition, of the proposed organizational or personnel risk mitigation measures as well as their effectiveness to reduce the risks have to be assessed; where it is reasonably understandable those measures may be accepted for the purpose of the risk assessment.

Table 2: Risk assessment matrix showing risk classes

RISK ASSESSMENT MATRIX				
Severity / Mishap probability	Catastrophic (I)	Critical (II)	Marginal (III)	Negligible (IV)
Frequent (A)	A-I	A-II	A-III	A-IV
Probable (B)	B-I	B-II	B-III	B-IV
Occasional (C)	C-I	C-II	C-III	C-IV
Remote (D)	D-I	D-II	D-III	D-IV
Improbable (E)	E-I	E-II	E-III	E-IV

Very improbable (F)	F-I	F-II	F-III	F-IV
Extremely improbable (G)	G-I	G-II	G-III	G-IV
Eliminated (H)	H			

Furthermore, external factors that can reasonably be derived from usage scenarios should be used to evaluate the occurrence (probabilities) of dangerous mishaps in the course of inadvertent incidents; those factors will give a probability of $p_{ext} < 1$, which means that under particular conditions an inadvertent incident does not inevitably lead to a mishap including personal injury, environmental damage, material or monetary loss.

In case of a quantitative analysis appropriate techniques for the mathematical combination of the different occurrence probabilities (or frequencies) of events that are causally related to each inadvertent incident should be used. Among other methods, FTA in combination with FMECA is the preferred method to conduct these analyses.

As above, the estimation and/or the calculation of the mishap probabilities are to be reasonable and comprehensible. The assessor will document the rationale. It is recommended to use the mishap probability levels defined in section 7.3.

As a result of the hazard evaluation and the risk assessment process, for each DAS hazard a well-founded estimation of the residual risk is specified: According to the scheme of Table 2 then at least one of the risk classes[4] in the risk assessment matrix is assigned to each hazard. This risk classifications may be further categorised into more abstract risk levels (e. g. high risk, serious risk, medium risk, low risk; c. f. MIL-STD-882E; c. f. section 7.4.6.2).

4.12 Safety Assessment

Are the DAS's residual risks mitigated to an acceptable level?

Are all safety requirements met?

Before exposing people, equipment, or the environment to known system-related hazards, the final step in the assessment process is a comparison of the DAS specific results of risk assessment according to 4.11.2 to nationally accepted risk thresholds. Any other additional safety requirements should be taken into account for judgment, if appropriate.

[4] The risk classes are: A-I, B-I, C-I, D-I, E-I, F-I, G-I, A-II, B-II, C-II, D-II, E-II, F-II, G-II, A-III, B-III, C-III, D-III, E-III, F-III, G-III, A-IV, B-IV, C-IV, D-IV, E-IV, F-IV, G-IV, and H.

The establishment of user-acceptable risk thresholds is the single most important decision of the user. Normally, these thresholds are a fundamental requirement for the manufacturer, and a precondition for the development of the product.

For this purpose the assessor compares, for each hazard, whether the involved risk is below, or equal to the national maximum permissible risk: With regard to the risk classes that have been assigned to each hazard in accordance with the risk assessment matrix, and by the comparison to national guidelines, the assessor decides whether all risks have been sufficiently minimized and are therefore acceptable. The result of this comparison, and the decision-making bases have to be documented. Should restrictions result with permissible exceptions, then they also have to be documented.

As a second aspect of the safety analysis process, and with reference to the intended use of the DAS, the realization of further, additional safety requirements concerning the respective user is given consideration.[5] It is up to the assessor to identify such – potentially purely national – safety requirements and to either validate their technical and/or organizational realization, or to verify their effective implementation by means of artefacts, e. g. test documents.

The final decision of the assessor is then to declare the safety assessment of the DAS. A DAS is to be declared “all risks assessed” for a certain configuration, when a legitimate risk class for each identified hazard can be justified. If, in a second step, and on the basis of the risk assessment, all prerequisites and safety requirements are met satisfactorily, then safety compliance may be declared, and the risk mitigation of residual risks of all identified hazards is acceptable to the NA. The DAS Safety Assessment Summary (see section 7.4), especially the detailed assessment summary as at subsection 7.4.7, may be used to report the results. If necessary, any restrictions on the respective use should be expressed in addition to this safety compliance declaration.

The following Figure 4 shows the elements of the proposed DAS safety assessment. A brief example of the safety assessment process including the assignment of example risk thresholds (the “colouring of the matrix”) can be found in section 7.8.

[5] Examples of additional safety requirements could be: *a display for the armed status of the DAS shall be available to the user, showing additional system self-diagnosis information; in an operational mode, after arming, the probability for failure of intended DAS disarming shall not exceed one in a million; DAS countermeasure activation shall be controlled by consensus of two or more independent control authorities (i.e. computing systems); etc.*

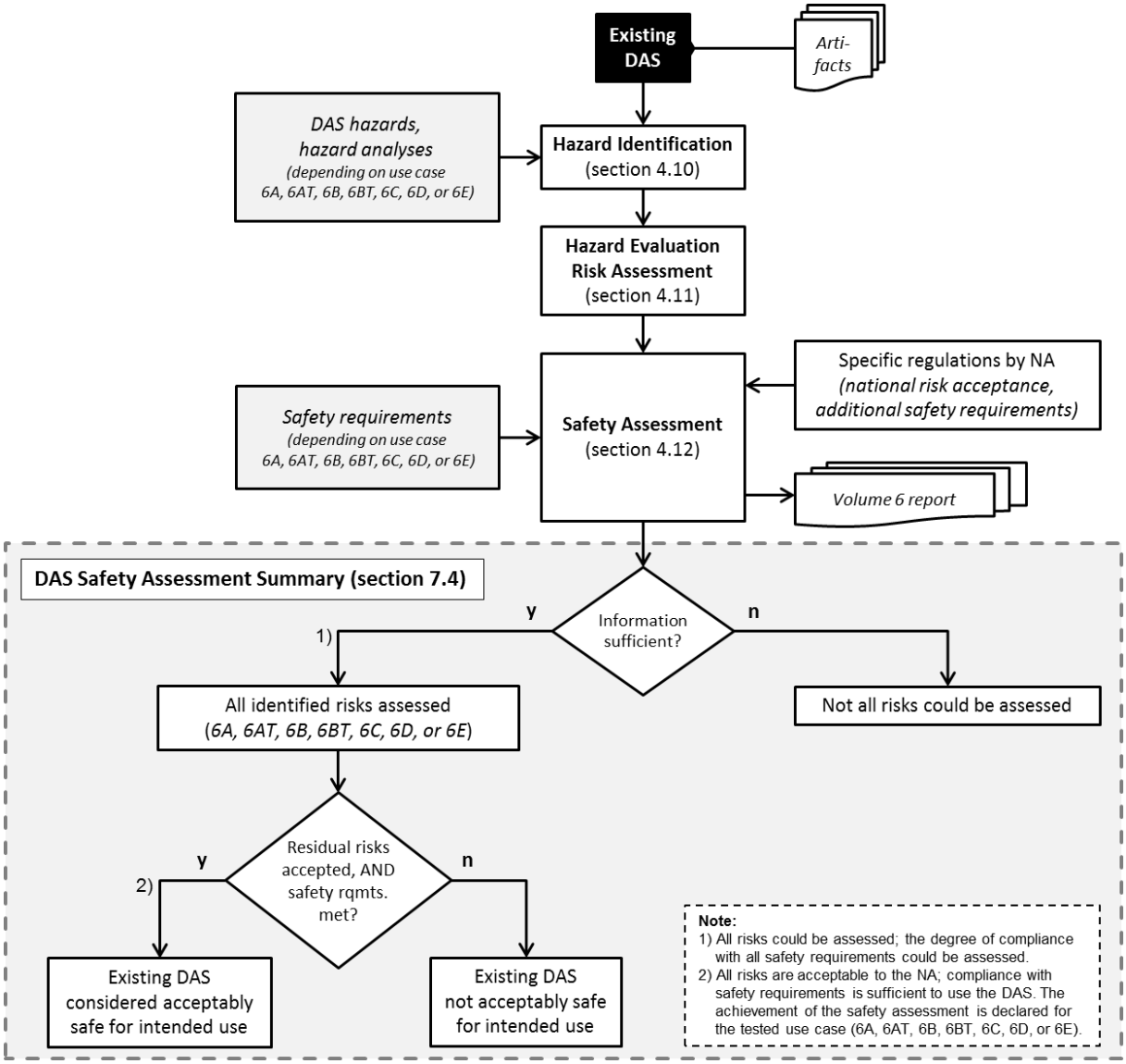

Figure 4: Flow chart of DAS safety assessment process and standard report decisions

5 EVALUATION AND ASSESSMENT

5.1 Generic

This section describes required information and the processes to achieve compliance with the 6A safety requirements for the *Generic* configuration of a DAS. Subsection 5.1.1 lists the information that should be made available for the safety assessment process.

5.1.1 Recommended Information for the *Generic* Configuration:

- Definition of risk acceptance levels (as part of the overall safety requirements, see section 4.6, Basic Requirement No. 4);
- Statement of technical configuration (versions from configuration management);
- DAS definition: concept, functions, specification, and intended use;
- DAS limitations and restrictions;
- Description of the safety architecture of the DAS;
- Specification of DAS functional states including a definition of safe state(s);
- Description of DAS user interface and user accessible functions;
- Hazard and risk analysis including a comprehensive list of hazards;
- Specification of DAS risk mitigation measures, safety features & functions, and measures of control for all hazards associated with the *Generic* use case, e. g. emergency stop capability; personal protective equipment for demonstrator servicing, or calibration, or testing;
- Verification and validation documentation on software safety;
- Hazard area estimation; estimation of surface danger zones (SDZ), including the Complete Dangerous Zone (CDZ) according to AEP-62 vol. 5, or other methods;
- Characterisation of explosives according to STANAG 4170 [13], if applicable;
- Characterisation of fuzing system according to STANAG 4187 [11], STANAG 4497 [14], if applicable;
- Characterisation of the munitions, according to AOP-15 [3], if applicable;
- Characterisation of the transmitting RF sensors according to relevant standards, if applicable;
- Characterisation of weapon systems according to AAS3P-1 [15] (STANAG 4758 [16]), if applicable;
- Characterisation of lasers according to ANSI Z136.1 [17], STANAG 3606 [18] and STANAG 3733 [19], if applicable.

Section 7.5 contains a guideline list of supporting artefacts.

5.1.2 Hazard Identification

The hazard identification for the *Generic* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9. Special emphasis should be given to the sensor technology applied in the DAS, and the operating principle of the countermeasure.

The result of these activities is a list of all hazards specific for the DAS *Generic* configuration.

5.1.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Generic* configuration complies with the procedures described in section 4.11. The requirements of a risk assessment can be satisfied by a qualitative or quantitative risk estimation of all identified hazards.

With respect to the hazard of false detections (i. e. false positives) this includes, but is not limited to, a thorough review of DAS sensor technology:

- Exploitation of unequivocal physical threat features for threat detection and validation;
- Sensor/sensor interaction;
- Interference of sensor radiation, reflected signals, etc., in all credible environments.

The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Generic* configuration.

5.1.4 Safety Assessment

To achieve compliance with a level 6A safety assessment for the *Generic* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for the *Generic* configuration follows the procedure outlined in section 4.12.

In accordance with NA regulations a DAS in the *Generic* configuration shall meet the *Basic Safety Requirements* of section 4.6. Moreover, the DAS shall be shown to at least fulfil the following additional safety requirements:

- DAS shall rely on two or more different sensor types, exploiting dissimilar physical properties of threats, for threat detection and threat validation;
- False detection rates, or false detection probabilities, that are claimed in safety analyses of DAS shall have credible evidence either by theoretical analysis, or by experimental tests, conducted under conditions reflecting the projected environments of planned DAS use;
- Data transmissions of safety-significant information within the DAS shall be safeguarded against communication errors by appropriate measures. The frequencies of such errors shall be reduced to an acceptable level;

Note:
Typical communication errors are: data corruption, unintended repetition of messages, incorrect sequence, loss, unacceptable delay, insertion, masking, and wrong addressing of data messages; high bus load conditions, possibly bus overload.
Note:
IEC 61784-3:2016 [20] defines profiles of safety fieldbuses for industrial communication networks and describes general rules for implementation.

- SAF devices of DAS shall comply with STANAG 4187 Edition 4, or equivalent safety criteria for fuzing system design; they shall be tested according to the requirements of STANAG 4157 [21] and related AECTP;
- If computing systems that perform or support threat detection and/or threat validation functionality are considered safety-critical, or safety-related then they shall be designed to facilitate a safety assessment to the satisfaction of the NA (see section 7.5.12);
- SAF features of DAS controlling (cyclic) arming, disarming and re-arming processes in a reversible manner during powered modes of operation shall facilitate to re-establish a level of safety as is required prior to use in order to enter DAS safe state (e. g. the unpowered mode).

If national regulations or specific safety requirements exist for the *Generic* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for *Generic* use.

5.2 Initial (test range)

This section describes the required information and processes to achieve compliance with the 6AT safety requirements for the *Initial (test range)* configuration of a DAS. Subsection 5.2.1 lists the information that should be made available for the safety assessment process.

5.2.1 Recommended Information for the *Initial (test range)* Configuration:

- DAS configuration (version/revision identification of all configuration items, including firmware and software);
- Hazard and risk analysis regarding DAS adapted for the test setup scenario;
- Hazard and risk analysis for the live and surrogate threats (the NA would apply national range safety requirements);
- Operating and support hazard analysis (for test setup);
- Special requirements, or precautions for the test setup, also for pre-tests; measures to establish inner and outer test range safety;
- DAS description: DAS functions, controls, operator interface and displays; technical specification, intended use; working principle of the countermeasure including environmental impact; limitations and restrictions; special modes, functions and processes for testing (calibration, special test set ups, controls/switches used for manual pre-arming, and disarming, etc.);
- Description of DAS modifications for test, and possible deviations from operational DAS configuration;
- Specification of additional work equipment for DAS installation, operation, measurement, and dismantling;
- Specification of DAS risk mitigation measures, including remotely controllable safety features and accessible functions (e. g. for testing), measures of control, e.g. emergency stop(s), for all hazard scenarios associated with the *Initial (test range)* use case;
- Description of DAS functional states, including safe states; methods of determining DAS state during test; operational concept including applicable procedures to reach safe state;
- Hazard area estimation; estimation of surface danger zones (SDZ), including the Complete Dangerous Zone (CDZ) according to AEP-62 vol. 5, or other methods;
- Maximum exposure/safe distances (for maximum noise levels see reference [22]);
- UXO: Regulations pertaining to the disposal of armed/launched/triggered/activated, however unexploded CMs; also for remnants of fired threats;
- Mishap management plan for inadvertent events, e. g. misfire, hangfire;
- Characterisation of explosives according to STANAG 4170 (CM and/or threat);
- Characterisation of fuzing system according to STANAG 4187, STANAG 4497, if applicable;
- Characterisation of the munitions, according to AOP-15 (CM and/or threat);
- Recommended, or required safety equipment, personal protection equipment and procedures for servicing personnel.

For a list of artefacts aiding the collection of information see section 7.5.

5.2.2 Hazard Identification

The hazard identification for the *Initial (test range)* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9. Special emphasis should be given to the operating principle of the countermeasure, and to procedures for installation and calibration, where applicable, performed in the field.

The result of these activities is a list of all hazards specific for the DAS *Initial (test range)* configuration.

5.2.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Initial (test range)* configuration complies with the procedures described in section 4.11. The requirements of a risk assessment can be satisfied by a qualitative risk estimation of all identified hazards. Necessary risk mitigation measures might include measures of inner and outer range safety, which might not be acceptable to the user for operational use scenarios.

The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Initial (test range)* configuration.

5.2.4 Safety Assessment

To achieve compliance with a level 6AT safety assessment for the *Initial (test range)* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for the *Initial (test range)* configuration follows the procedure outlined in section 4.12.

In accordance with the NA regulations a DAS in the *Initial (test range)* configuration shall meet the *Basic Safety Requirements* of section 4.6. Moreover, the DAS shall be shown to at least fulfil the following additional safety requirements:

- The DAS shall provide a remotely operated emergency-off feature, to transfer the DAS into a safe state, e. g. currentless or de-energized, in case of an inadvertent incident during testing. To provide the necessary level of safety the feature shall be operated outside of the Complete Dangerous Zone (CDZ) of the DAS as well as outside of the weapon danger zone (WDZ) of the threat(s); it shall provide a degree of reliability sufficiently high to operate a safety-critical function.
- Persons who carry out calibration work on dangerous sensor devices shall be obliged to use appropriate personal and site protective equipment, e. g. alarming dosimeters when working on dangerous radiation-emitting sensors; set up barriers and warning signs.

If national regulations or specific safety requirements exist for the *Initial (test range)* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for *Initial (test range)* use.

5.3 Generic with Platform Specific Information

This section describes required information and the processes to achieve compliance with the 6B safety requirements for the *Generic with Platform Specific Information* configuration of a DAS. Subsection 5.3.1 lists the information that should be made available for the safety assessment process in addition to the *Generic* configuration.

5.3.1 Recommended Information for the *Generic with Platform Specific Information* Configuration

Extras in comparison to the *Generic* (6A) configuration:

- Information on extended configuration:
  - Regarding actual number of components (sensors, central processing units, countermeasures and/or effectors).
  - Regarding no fire zones.
  - Limitations, for example from test readiness reviews.
- Proposed platform/DAS interfaces (physical, electric/electronic, logical, etc.).
- Physical properties of the DAS for installation/integration on a vehicle (dimensions, weight, electrical power supply requirements, etc.).
- Bands/frequencies of electromagnetic radiation, including laser, electro-optical and/or infrared radiation sources, occupied by DAS.
- Human Machine Interface (HMI, see [23]): processes and operation of the DAS by the user; state information (diagnosis and built-in tests), displays and information on the arming state.
- Human Factors: use of the system, special requirements for the user when operating the DAS.
- Possible requirements for blast shields (at hatches).
- Safety features (switches) on hatches, doors, etc. to (partially) disable the DAS function.

For a list of supporting artefacts see section 7.5. Supporting artefacts might be a part of the overall system (vehicle) safety installation, or integration documentation.

5.3.2 Hazard Identification

The hazard identification for the *Generic with Platform Specific Information* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9, and possible supplements to the list of hazards from an earlier *Generic* safety assessment. Again, special consideration should be given to the operating principle of the countermeasure.

The result of these activities is a list of all hazards specific for the DAS *Generic with Platform Specific Information* configuration.

5.3.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Generic with Platform Specific Information* configuration complies with the procedures described in section 4.11. The requirements of a risk assessment can be satisfied by a qualitative or quantitative risk estimate of all identified hazards. This includes, but is not limited to, a thorough review of the interfaces between platform and DAS. Moreover, this includes:

- consideration of sequences leading to possible inadvertent arming of the DAS;
- displays for indicating the actual armed state of the DAS;
- an assessment of the measures to avoid displaying ambiguously, or incorrectly the actual state or operational mode, respectively, of the DAS to the user, or measures to avoid displaying the safe state erroneously;
- guards (switch cover, physical barrier, etc.);
- multi step switches;
- mutual influencing of DAS subsystem components and platform devices.

The risk assessment should consider a possibly increased risk for arming, for CM activation, and/or for other hazards due to the expected larger number of configuration items (sensors, CMs, etc.) on a platform.

The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Generic with Platform Specific Information* configuration.

5.3.4 Safety Assessment

To achieve compliance with a level 6B safety assessment for the *Generic with Platform Specific Information* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for the *Generic with Platform Specific Information* follows the procedure outlined in section 4.12.

In addition to the safety requirements as of section 5.1 the DAS shall be shown to at least fulfil the following additional safety requirements:

- DAS shall not negatively influence the safety of the platform, or limit risk mitigation measures, e. g. technical safety functions, of the platform;
- Danger zones, mainly by virtue of sensors (dangerous sensor radiation), as well as of countermeasures (blast, noise, fragments, etc., after CM activation) shall be assessable on the basis of the available DAS documentation;
- Safety criticality of interfaces (physical, electrical, logical) between platform and DAS shall be assessable on the basis of the available DAS documentation;

If national regulations or specific safety requirements exist for the *Generic with Platform Specific Information* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for the purpose of *Generic with Platform Specific Information* use.

5.4 Interim with Platform Specific Information (test range)

This section describes required information and the processes to achieve compliance with the 6BT safety requirements for the *Interim with Platform Specific Information (test range)* configuration of a DAS. Subsection 5.4.1 lists the information that should be made available for the safety assessment in addition to the *Initial (test range)* configuration.

5.4.1 Recommended Information for the *Interim with Platform Specific Information (test range)* Configuration

Extras in comparison to the *Initial (test range)* (6AT) and *Generic with Platform Specific Information* (6B) configurations:

- Interfaces with platform; safety-significant DAS functions and features that need to be supplied with correct and reliable signalling from the platform to perform safely;
- Human Machine Interface (HMI): operation of the DAS by the user; state information (diagnosis), arming of the DAS, information of the armed state; possibly modified for test setup;
- Specification of DAS risk mitigation measures, including remotely controllable safety functions (for testing), measures of control for all hazards associated with the *Interim* use case, e.g. emergency stop for DAS and a separate emergency stop for vehicle power.

For a list of recommended supporting artefacts see section 7.5. Supporting artefacts might be a part of the overall system (vehicle) safety installation, or integration documentation.

5.4.2 Hazard Identification

The hazard identification for the *Interim with Platform Specific Information (test range)* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9, and supplements to the list of hazards from an earlier *Initial (test range)* safety assessment. Again, special emphasis should be given to the operating principle of the countermeasure.

The result of these activities is a list of all hazards specific for the DAS *Interim with Platform Specific Information (test range)* configuration.

5.4.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Interim with Platform Specific Information (test range)* configuration complies with the procedures described in section 4.11. The requirements of a risk assessment can be satisfied by a qualitative risk estimate of all identified hazards. Necessary risk mitigation measures for the purpose of performance levelling of a DAS on a test range might include measures of inner and outer range safety, which are not be acceptable for operational use scenarios.

A qualitative risk assessment should give evidence that an increased number (compared to simple test rig configurations) of DAS subsystem components, e. g. sensors and countermeasures, does not adversely affect DAS safety, or exceed risk acceptance thresholds. Such investigation should take into account effective directions of active sensors, coverage areas for DAS movable parts, and effective directions of countermeasure activation, or launches; CDZ and weapon(s) danger zone(s). The influence of interferences on the defined interfaces between the platform and DAS should also be taken into consideration.

The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Interim with Platform Specific Information (test range)* configuration.

5.4.4 Safety Assessment

To achieve compliance with a level 6BT safety assessment for the *Interim with Platform Specific Information (test range)* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for the *Interim with Platform Specific Information (test range)* configuration follows the procedures described in section 4.12.

In addition to the safety requirements as of sections 5.2 and 5.3 DAS shall be shown to at least fulfil the following additional safety requirements:

- Safety features and safety functions of the DAS relying on the supply of external power, or on the functioning of interfaces with the platform shall be covered by DAS documentation. The commissioning of the proper operation of such features shall be demonstrated prior to any active protection tests (firings);
- Failure to supply platform power to the DAS shall not degrade safety of the test setup, nor render the installation to an unknown or unsafe state;
- DAS, and each of its subsystems, shall show electromagnetic compatibility with the fittings of the integrating platform (intended vehicle) and the test setup; c. f. vol. 7.

If national regulations or specific safety requirements exist for the *Interim with Platform Specific Information (test range)* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for *Interim with Platform Specific Information (test range)* use.

5.5 Urgent Installation / Applique (stand-alone)

This section describes required information and the processes to achieve compliance with the 6C safety requirements for the optional *Urgent Installation / Applique (stand-alone)* configuration of a DAS. Subsection 5.5.1 lists information that should be made available for the safety assessment in addition to the *Generic with Platform Specific Information* configuration.

5.5.1 Recommended Information for the *Urgent Installation / Applique (stand-alone)* Configuration

Extras in comparison to the *Generic with Platform Specific Information* (6B) configuration:

- Specification of the applique (stand-alone) installation;
- Documentation of safety-significant mutual dependencies of the interfaces between platform and DAS;
- Hazard and risk analysis; update from earlier H&R with special focus on DAS installation and interface connections between platform and DAS;
- Safety assessment of DAS installation according to the requirements of MIL-STD-882E Task 301 (Safety Assessment Report), including description of implemented risk mitigation measures (technical features; organizational and personal measures);
- Validation of EMC (platform/DAS; also c. f. AEP-62 vol. 7);
- Instructions manual for all modes of operation, including HMI and maintenance specification;
- Specification of failure modes, including troubleshooting procedures;
- Information to facilitate the estimation of DAS danger zone(s) according to national methodology;
- Safety declaration, or safety statement (c. f. MIL-STD-882E Task 401 Safety Verification).

For a list of recommended supporting artefacts see section 7.5.

5.5.2 Hazard Identification

The hazard identification for the *Urgent Installation / Applique (stand-alone)* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9, and possible supplements to the list of hazards from an earlier safety assessment.

The result of these activities is a list of all hazards specific for the DAS *Urgent Installation / Applique (stand-alone)* configuration.

5.5.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Urgent Installation / Applique (stand-alone)* configuration complies with the procedures described in section 4.11. Risk assessment should be supported by a quantitative risk estimation of all identified hazards in all operational scenarios. The result of these activities is an extended list of hazards, with a risk class as of Table 2 assigned to each hazard for the *Urgent Installation / Applique (stand-alone)* configuration.

5.5.4 Safety Assessment

To achieve compliance with a level 6C safety assessment for the *Urgent Installation / Applique (stand-alone)* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for this configuration follows the procedures described in section 4.12.

In addition to the safety requirements as of section 5.3, DAS shall be shown to at least fulfil the following additional safety requirements:

- DAS shall meet all risk acceptance criteria (thresholds) in its anticipated operating environments (for guidelines on environmental testing see STANAG 4370 [24] and related AECTP-500 [25]).
- For safety assessment, reasonable assumptions about the influence of external factors (p_{ext}, see 4.9.2 for details) derived from usage profiles on residual risk may be made.

  Note:
  The risk-based approach allows for the consideration of external factors during risk assessment. Those factors should be based on assignable information from usage profiles, and/or CONOPS documentation. An example for an external factor is the average probability (or frequency) and duration of stay (“exposure”) of persons in the DAS Complete Dangerous Zone (CDZ).
- DAS shall not negatively influence the safety of the vehicle, limit or impede platform risk mitigation measures, e. g. technical safety functions, displays to the user, etc.
- Failure of the carrying platform to continuously supply power to the DAS during any stage of operation shall not put the DAS in an unsafe state, or raise risks to an unacceptable level; the same applies for communication errors at digital interfaces, or discrete signals between platform and DAS (see note in section 5.1.4).
- Electromagnetic compatibility between DAS, including each of its subsystems, with the fittings of the integrating platform (vehicle) shall be demonstrated. AECTP-501, -504 and -507 (see [26], [27], [28]) provide detailed procedures. AECTP-508 [29] provides ordnance test and verification procedures for E^3 hazards (including electromagnetic radiation, Electrostatic Discharge (ESD), Electromagnetic Pulse (EMP) and lightning).
- The effectiveness of risk mitigation measures of the applique (stand-alone) installation shall be validated.

- It shall be demonstrated (by training and education) that the user may control DAS operation, and that the user is able to transfer the DAS applique (stand-alone) system to a safe state manually under all credible emergency or mishap situations.

If national regulations or specific safety requirements exist for the *Urgent Installation / Applique (stand-alone)* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. An *Urgent Installation / Applique (stand-alone)* system configuration may be considered for Urgent Material Release, thereby accepting reasonable residual risks, if necessary.

5.6 Final Installation / Applique (stand-alone)

This section describes the required information and the processes to achieve compliance with the 6D safety requirements for the *Final Installation / Applique (stand-alone)* configuration of a DAS. Subsection 5.6.1 lists information that should be made available for the safety assessment in addition to the required information for the *Generic with Platform Specific Information* and the *Urgent Installation / Applique (stand-alone)* configurations.

5.6.1 Recommended Information for the *Final Installation / Applique (stand-alone)* Configuration

Extras in comparison to the *Generic with Platform Specific Information* (6B) and the *Urgent Installation / Applique (stand-alone)* (6C) configurations:

- System-of-systems hazard analysis, including human/system interaction considerations;
- Interface control documentation with respect to physical and electric installation of the DAS;
- Maintenance procedures for DAS;
- Calibration procedures for DAS sensors (component level, system level);
- Procedures for loading, unloading and on-board stowage of CMs;
- Emergency procedures, e. g. in case of vehicle incidents;
- Installation and operational manual, including operator failure diagnosis procedures;
- Logistical concept;
- Training documentation;
- Human Factors: operational use of the system, special requirements for the user when operating the DAS;
- Concept of operations (CONOPS), including:
    - Reloading of CM with respect to launcher elevation and on-board stowage;
    - Checking the DAS for readiness;
    - Procedures to follow when executing vehicle maintenance with regard to active DAS modes;
- Specification of danger zones;
- Security concept, cyber threat vulnerability analysis, evaluation of impact on safety;
- Disposal.

For a list of supporting artefacts see section 7.5.

5.6.2 Hazard Identification

The hazard identification for the *Final Installation / Applique (stand-alone)* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9, and possible supplements to the list of hazards. Special consideration should be given to all documented modifications, or change proposals of the DAS to meet system integration requirements that could affect system safety and risk mitigation measures; to all platform/DAS connections and interfaces, where safety requirements of a sub-system (DAS) are imposed on the integrating system (vehicle), or vice versa. Moreover, special attention should be given to the identification of unique system-of-systems hazards, which otherwise would not exist.

The result of these activities is a complete list of hazards specific for the DAS *Final Installation / Applique (stand-alone)* configuration.

5.6.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Final Installation / Applique (stand-alone)* configuration complies with the procedures described in section 4.11. Risk assessment should be supported by a quantitative risk estimate of all identified hazards. The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Final Installation / Applique (stand-alone)* configuration.

5.6.4 Safety Assessment

To achieve compliance with a level 6D safety assessment for the *Final Installation / Applique (stand-alone)* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met without restrictions. The safety assessment for this configuration follows the procedures described in section 4.12.

In addition to the safety requirements as of sections 5.3 and 5.5, the following safety requirements apply:

- Based on the analysis of the results of MIL-STD-882E Task 209 (System-of-Systems Hazard Analysis) the compliance of the applique (stand-alone) to the overall platform risk acceptance criteria shall be evident;
- DAS shall not negatively influence the safety of the vehicle, or limit risk mitigation measures, e. g. technical safety functions, of the platform.

In the case that the *Final Installation / Applique (stand-alone)* configuration being assessed has been subject to an earlier Urgent Material Release then it is expected that MIL-STD-882E Task 304 (Review of Engineering Change Proposals, Change Notices, Deficiency Reports, Mishaps, and Requests for Deviation/Waiver) be imposed on the DAS contractor. As a result, a report of this task shall be available for the safety assessment of this configuration.

- The assessor shall analyze and assess the results of Task 304 with regard to compliance of DAS to the overall risk acceptance criteria.

- All requests for deviations, waivers and related change documentation should be reviewed and questioned.

If national regulations or specific safety requirements exist for the *Final Installation / Applique (stand-alone)* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for *Final Installation / Applique (stand-alone)* use.

5.7 Fully Integrated Solution

This section describes required information and the processes to achieve compliance with the 6E safety requirements for the *Fully Integrated Solution* configuration of a DAS. Subsection 5.7.1 lists the information that should be made available for the safety assessment in addition to the *Generic with Platform Specific Information* configuration.

5.7.1 Recommended Information for the *Fully Integrated Solution* Configuration

Extras in comparison to the *Final Installation / Applique (stand-alone)* (6D) configuration, this implicitly includes the *Generic with Platform Specific Information (6B)* configuration:

- Interface control documentation (ICD) of all electronic and discrete interfaces between DAS and vehicle electronics; specification of (possibly bi-directional) data exchange between platform control computers and DAS fire control, including sensor data; data transmitted may include, but are not limited to: vehicle identification, vehicle dynamic state (e. g. speed, orientation, turret azimuth, hatch position, operational status information from BMS); DAS operational state and diagnosis information, DAS sensor data, or battlefield management data, e. g. threat shooter location(s).

See section 7.5 Artefacts for covering documentation.

5.7.2 Hazard Identification

The hazard identification for the *Fully Integrated Solution* configuration complies with the procedures described in section 4.10, taking into account typical DAS hazards as of section 4.9, possible supplements to the list of hazards from an earlier *Generic with Platform Specific Information* safety assessment, or related integrated solutions. See also 5.6.2.

The result of these activities is a list of all hazards specific for the DAS *Fully Integrated Solution* configuration.

5.7.3 Hazard Evaluation and Risk Assessment

The hazard evaluation for the *Fully Integrated Solution* configuration complies with the procedures described in section 4.11. Risk assessment should be supported by a quantitative risk estimate of all identified hazards. This comprises a thorough review of recommended modifications to either the platform, or the DAS due to integration needs, and possible effects on established and accepted risk mitigation measures. Aspects to consider:

- Hazards resulting from the physical and logical connections of vehicles and weapon station controls to DAS controls (e. g. through a bidirectional link to a BMS);
- Consideration of sequences leading to possible inadvertent arming of the DAS;
- Displays for indicating the actual armed state of the DAS;
- Assessment of the measures to avoid ambiguously displaying the state or operational mode of the DAS to the user, or measures to avoid displaying the safe state erroneously;

- Guards (switch cover, physical barrier, etc.);
- Multi step switches;
- Influence on emergency exits, hatch, etc.;
- Influence of the state (open, closed) of hatches on DAS operation;
- Sharing of displays, impact on system state (vehicle, and/or DAS) visibility;
- Vehicle road and off-road stability;
- Sensor interaction/radiation interference with the platform and different environments, including neighbour vehicles; electromagnetic compatibility and interference within a fleet;
- Danger zones;
- Minimal distances for dismounted soldiers, neighbouring vehicles, and uninvolved third parties.

The result of these activities is an extended list of hazards, with at least one risk class as of Table 2 assigned to each hazard for the DAS *Fully Integrated Solution* configuration.

5.7.4 Safety Assessment

To achieve compliance with a level 6E safety assessment for the *Fully Integrated Solution* configuration it has to be shown that DAS risks are sufficiently reduced to be acceptable for the user; all safety requirements have to be met. The safety assessment for the *Fully Integrated Solution* follows the procedure outlined in section 4.12.

In addition to the safety requirements as of sections 5.3 and 5.6 the DAS shall be shown to at least fulfil the following additional safety requirements:

- Based on the analysis of the results of MIL-STD-882E Task 209 (System-of-Systems Hazard Analysis) the compliance of the fully integrated DAS to the overall platform risk acceptance criteria shall be evident;
- Data transmissions of safety-significant information between the platform and the DAS shall be safeguarded against communication errors by appropriate measures. In case that corrupted data are received by DAS from an external platform (sub-) system, then they shall not negatively impact the safety of the DAS (see note on page 23).

If national regulations or specific safety requirements exist for the *Fully Integrated Solution* configuration, these additional safety requirements may be applied to the safety assessment at the discretion of the assessor.

If, on the basis of the risk assessment and the safety assessment all prerequisites are met satisfactorily, compliance can be attested in a safety statement. The DAS may be considered acceptably safe for the purpose of *Fully Integrated Solution* use.

6 REFERENCES

All references need to be evaluated prior to use to ensure most up to date versions are utilized.

[1] Department of Defense, "MIL-STD-882E - System Safety (Standard Practice)," 2012.

[2] NATO, “STANAG 4297 - Guidance on the Assessment of the Safety and Suitability for Service of non-nuclear Munitions for Nato Armed Forces,” 2001.

[3] NATO, “AOP-15 (Ed. 3) - Guidance on the Assessment of the Safety and Suitability for Service of non-nuclear Munitions for Nato Armed Forces,” 2008.

[4] International Electrotechnical Commission, „IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic safety-related Systems,“ 2010.

[5] Ministry of Defence, „DEF-STAN 00-56 - Safety Management Requirements for Defence Systems, Part 1 and 2,“ 2007.

[6] NATO, „AOP-52 - Guidance on Software Safety Design and Assessment of munition-related Computing Systems,“ 2009.

[7] International Electrotechnical Commission, „IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements,“ 2010.

[8] Ministry of Defence, „DEF-STAN 00-055 - Requirements for Safety of Programmable Elements (PE) in Defence Systems,“ 2016.

[9] Department of Defense, „Joint Software Systems Safety Engineering Handbook,“ 2010.

[10] Radio Technical Commission for Aeronautics (RTCA), „DO-178C, Software Considerations in Airborne Systems and Equipment Certification,“ 2012.

[11] NATO, "STANAG 4187 - Fuzing Systems - Safety Design Requirements," 2007.

[12] Ministry of Defence, „JSP 520 - Safety and Environmental Management of Ordnance, Munitions and Explosives over the Equipment Acquisition Cycle (Pt. 1: Directive),“ 2015.

[13] NATO, "STANAG 4170 - Principles and Methodology for the Qualification of Explosive Materials for Military Use," 2008.

[14] NATO, "STANAG 4497 - Hand-Emplaced Munitions (HEM), Principles for safe Design," 2016.

[15] NATO, "AAS3P-1 - Allied Munitions Safety and Suitability for Service Assessment Testing Publication - Guidance," 2011.

[16] NATO, "STANAG 4758 - Safety and Suitability for Service Assessment Testing for Surface and Underwater Launched Munitions," 2017.

[17] ANSI, "American National Standard for Safe Use of LASERS," 2014.

[18] NATO, "STANAG 3606 - Laser Safety for Military Use," 2016.

[19] NATO, "STANAG 3733 - (RESTRICTED) Laser Pulse Repetition Frequencies (PRF) Used for Target Designation and Weapon Guidance," 2005.

[20] International Electrotechnical Commission, „IEC 61784-3: Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions,“ 2016.

[21] NATO, "STANAG 4157 - Safety, Arming and Functioning Systems (SAF Systems) Testing Requirements," 2017.

[22] Department of Defense, „MIL-STD-1474E - Design Criteria Standard Noise Levels,“ 2015.

[23] Department of Defense, „MIL-STD-1472G - Design Criteria Standard Human Engineering,“ 2012.

[24] NATO, "STANAG 4370 - Environmental Testing," 2016.

[25] NATO, "AECTP 500 - Electrical/Electromagnetic Environmental Tests," 2016.

[26] NATO, "AECTP 501 - Equipment and Subsystem EMI Testing".

[27] NATO, "AECTP 504 - Introduction to Platform and System Verification and Testing".

[28] NATO, "AECTP 507 - Land Platform and System Verification and Testing Verification".
[29] NATO, "AECTP 508 - Ordnance Test and Verification Procedures".

6.1 Related Documents

AEP-62 Edition C *Procedures for the Assessment of Defensive Aid Suites (DAS) for Land Vehicles*
Volume I: DAS Threat Classification
Volume I Hard Kill DAS Performance
Volume III: Soft Kill DAS Performance
Volume V: DAS Event Collateral Damage
Volume VII: DAS Integration Considerations

7 APPENDICES

7.1 Glossary

7.1.1 Acceptable Risk

Risk that the National Authority (NA) is willing to accept without additional mitigation.

7.1.2 Accident

See: “mishap” (subsection 7.1.21)

7.1.3 ALARP

A risk is considered to be “As Low As Reasonably Practicable” when the cost of any further risk reduction is demonstrated grossly disproportionate to the benefit obtained from that risk reduction. This cost includes the loss of defense capability as well as financial or other resource costs. (AOP-15 Ed. 3)

7.1.4 Armed DAS

State of a DAS when at least one of the following conditions applies:

1. The state of any Safety, Arming and Functioning (SAF) System[6] controlling the function of a countermeasure is “armed” according to STANAG 4187 Edition 4, or
2. any firing stimulus, e. g. a fire command, can activate one or more countermeasures (derived from: MIL-STD-1316E).

7.1.5 Assessor

Person, persons or organization that performs the safety assessment in order to arrive at a judgment on the DAS system safety, including functional safety achieved by the risk mitigation measures implemented and/or established; usually a representative of the NA.

7.1.6 Collateral Damage

Harmful and unintended effects to uninvolved civilian and military persons and/or structures resulting from DAS operation, e. g. from justified, and intended countermeasure activation.

7.1.7 Complete Dangerous Zone (CDZ)

Area where individuals are exposed with a higher probability than $P_{CD,accept}$ to a predefined (or higher) threshold of injury. P_{CD} is the probability that an individual standing at a given distance r from a 360° HK-DAS protected platform is exposed to higher risk than the selected threshold when a single HK-DAS event occurs anywhere around the platform (with equal angular probability). (See AEP-62 vol. 5 for details.)

[6] Safety and Arming Device (SAD) according to STANAG 4187

7.1.8 DAS Safety

Freedom of a DAS from unacceptable risks originating from the DAS or from specific DAS components.

7.1.9 Defensive Aid Suite (DAS)

A system that when integrated on Land Vehicles is capable of detecting, classifying and providing effective warning/cueing and countermeasures for defined imminent or incoming threats. (AEP-62 vol. 1)

7.1.10 Equipment Under Control (EUC)

Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities. (IEC 61508:2010)

In the context of this AEP, the performance-related functional elements of DAS.

7.1.11 Existing DAS

A specific Defensive Aid Suites configuration physically realized together with a set of artefacts supporting a safety case for one or more of the seven use cases specified in this document.

7.1.12 False Detection (FD)

The erroneous declaration, or signaling of a threat condition at an ICD controlled interface between a sensor-related configuration item and a message receiver, e. g. a fire control unit, or an arming device of DAS.

Note: An example of False Detection is described by a situation where – despite the absence of a valid threat – a single sensor subsystem transmits information to DAS fire control which is suitable to initiate or maintain operational sequences of arming or firing one or more countermeasures, or which is suitable to be interpreted as a threat signature by fire control, or both (see also: section 7.6).

Depending on functional requirements of the specific sensor subsystem this definition includes the false classification of a detected non-threat object as a threat object, or the false identification of a specific threat object.

7.1.13 Fielding

Placing the system into operational use with units in the field or fleet. (MIL-STD-882E)

7.1.14 Functional Safety

Part of the overall safety relating to the equipment under control (EUC) and the EUC control system that depends on the correct functioning of the electrical and/or electronic and/or programmable electronic safety-significant systems and other risk reduction measures.

7.1.15 Hangfire

Remaining of a countermeasure, or an effector within a launcher device despite the ignition of the pyrotechnic train, or the activation of an effector ejection device, or similar.

7.1.16 Hazard

A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (MIL-STD-882E)

7.1.17 Inadvertent incident

An undesirable real or potential condition that results from release of incompatible or toxic substances, (sub-) system or component failure, software error, the implementation of inadequate or incorrect requirements, false detection, maloperation, misuse, or disregard of regulations.

7.1.18 Inner Range Safety

State during a firing exercise in which, according to the latest advances in science and technology, personnel, weapons and equipment involved in the firing exercise are not exposed to danger.

7.1.19 Life-cycle

All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal. (MIL-STD-882E)

7.1.20 Misfire

Failure to launch a countermeasure; possible causes: The launch signal from a fire control system is not received by the countermeasure launcher; rocket motor failure, etc.

7.1.21 Mishap

An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (derived from: MIL-STD-882E). Used as a synonym to the word "accident".

7.1.22 Mitigation Measure

Action required to eliminate the hazard or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood that a mishap will occur. (MIL-STD-882E)

7.1.23 Outer Range Safety

State during a firing exercise in which the safety of ground and airspace hazard areas is ensured according to the latest advances in science and technology in such a way that personnel not participating in the firing exercise, livestock as well as ground vehicles, aircraft and vessels are not exposed to danger.

7.1.24 Probability

A real number in the scale 0 to 1 attached to a random event.

7.1.25 Programmable Elements

Products, Services and Systems implemented in software, or programmable hardware, which includes any device that can be customized, e. g. ASICs, PLDs, FPGAs. (derived from: DEF-STAN 00-055)

7.1.26 Risk

A combination of the severity of the mishap and the probability, or frequency that the mishap will occur. (derived from: MIL-STD-882E)

7.1.27 Safe State

State of the DAS when safety is achieved. (derived from: IEC 61508:2010)

Note: In going from a potentially hazardous condition to the final safe state, the DAS may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the DAS is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

7.1.28 Safety

Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (MIL-STD-882E)

7.1.29 Safety-critical

A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either *Catastrophic* or *Critical* (e.g., safety-critical function, safety-critical path, and safety-critical component). (MIL-STD-882E)

7.1.30 Safety-critical function

A function whose failure to operate or incorrect operation will directly result in a mishap of either *Catastrophic* or *Critical* severity. (MIL-STD-882E)

7.1.31 Safety-critical item

A hardware or software item that has been determined through analysis to potentially contribute to a hazard with *Catastrophic* or *Critical* mishap potential, or that may be implemented to mitigate a hazard with *Catastrophic* or *Critical* mishap potential. (MIL-STD-882E)

7.1.32 Safety-related

A term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Marginal or Negligible. (MIL-STD-882E)

7.1.33 Safety-significant

A term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related. (MIL-STD-882E)

7.1.34 Severity

The magnitude of potential consequences of a mishap to include: death, injury, occupational illness, damage to or loss of equipment or property, damage to the environment, or monetary loss. (MIL-STD-882E)

7.1.35 Surface Danger Zone (SDZ)

The ground and airspace designated within the training complex for vertical and lateral containment of projectiles, fragments, debris, and components resulting from the firing, launching, or detonation of weapons systems to include explosives and demolitions.

7.1.36 System

An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective. (AOP-15 Ed. 3)

7.1.37 System Safety

The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle. (MIL-STD-882E)

7.1.38 Valid Threat

In relation to the respective DAS, an object which is classified as a threat and which is expected to hit the DAS bearing vehicle or test rig due to its speed and other measurable physical properties and within the measurement accuracies of DAS sensors.

7.1.39 Weapon Danger Zone (WDZ)

The three dimensional space associated with firing a weapon, or munition where the risk of death or serious injury exceeds some threshold.

7.2 Mishap Severity Categories

The following table defines the recommended severity categories scheme.

Table 3: Severity Categories

MISHAP SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**I**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or significant monetary loss.
Critical	**II**	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss.
Marginal	**III**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss.
Negligible	**IV**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss.

7.3 Mishap Probability Levels

Table 4 defines the mishap probability levels scheme for DAS safety assessments.[7] The table comprises qualitative and quantitative probability definitions. For quantitative descriptions the probability P is the actual or expected probability of mishaps during one hour of operational use of a single DAS. Assuming a constant failure rate of a (sub-) system, to compute the probability P the following computation is used:

$$P = 1 - e^{-\lambda\tau} \text{ , where}$$

λ = failure rate (const.) [1/h]

τ = exposure time [h]

Table 4: Mishap probability levels during the life of an item (qualitative), or 1 hour of use (quantitative) of a single DAS

MISHAP PROBABILITY LEVELS PER SYSTEM			
Description	**Level**	**Qualitative** (reference: in the life of an item)	**Quantitative** (τ = 1 h)
Frequent	A	Likely to occur often	$\geq 10^{-5}$
Probable	B	Will occur several times	$\geq 10^{-6}$ $< 10^{-5}$
Occasional	C	Likely to occur sometime	$\geq 10^{-7}$ $< 10^{-6}$
Remote	D	Unlikely, but possible to occur	$\geq 10^{-8}$ $< 10^{-7}$
Improbable	E	Occurrence cannot be reasonably expected	$\geq 10^{-9}$ $< 10^{-8}$
Very improbable	F	So unlikely, it can be assumed occurrence may not be experienced	$\geq 10^{-10}$ $< 10^{-9}$
Extremely improbable	G	So unlikely, it can be assumed occurrence may almost certainly not be experienced	$< 10^{-10}$
Eliminated	H	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.	

[7] The definition of mishap probability levels is in reference to example quantitative probability levels in MIL-STD-882E. The conversion of the probability values in MIL-STD-882E to the probabilities used here is based on the assumption of 10,000 operating hours during the life of an item. In the course of this conversion, the “Remote” level of MIL-STD-882E is split in three levels, and two new levels are being introduced (“Very Improbable”, “Extremely Improbable”); the “Improbable (E)” probability level of MIL-STD-882E is equivalent to the “Extremely improbable (G)” probability level in this document.

7.4 DAS Safety Assessment Summary

Nation conducting safety assessment: _____ Date: _____

DAS system name: _____ Configuration / System version number: _____

7.4.1 Safety Artefact Assessment

Artefact	Standard used	Supplier assured	Technically independently assured	Organizationally independently assured	Not available
mandatory artefacts (expected artefacts from AEP-62 vol. 6)					
DAS configuration document:					
optional artefacts					

7.4.2 Tested DAS Safety Assessment Use Case

[ ] 6A Generic
[ ] 6AT Initial (test range)
[ ] 6B Generic with Platform Specific Information
[ ] 6BT Interim with Platform Specific Information (test range)
[ ] 6C Urgent Installation / Applique (stand-alone)
[ ] 6D Final Installation / Applique (stand-alone)
[ ] 6E Fully Integrated Solution

7.4.3 Vehicle Installation Description

Vehicle type: _____

Vehicle version: _____

7.4.4 DAS Risk Assessment Result

DAS has been assessed, and *(only one of the following applies)*

[ ] All identified risks could be assessed. [ ] Not all risks could be assessed.

The safety requirements as of AEP-62 vol. 6 for this use case are met: [ ] yes [ ] no

Additional national safety requirements for examined use case apply: [ ] yes [ ] no
→ only if 'yes': Additional national safety requirements are met: [ ] yes [ ] no

Under the supervision of organizational POC:

_____ of nation:

_____ _____

7.4.5 Remarks

Remarks on the DAS Safety Assessment Summary (short form)
▪ *Possible statement on additional national safety requirements* ▪

7.4.6 Detailed DAS Risk Assessment

7.4.6.1 Identified Hazards as of section 4.10

Hazard		**Event description and severity**
ID	Title *(e.g. unintended release of countermeasure; launcher swivel)*	*(e.g. single canister launched 10 m from vehicle/catastrophic; unexpected start-up during inspection/critical)*
#1		
#2		
#3		
#4		
…		

7.4.6.2 Risk assessment results as of section 4.11

(Fill in unique hazard IDs as assigned in section 7.4.6.1!)

RISK ASSESSMENT MATRIX				
Severity / Mishap Probability	Catastrophic (I)	Critical (II)	Marginal (III)	Negligible (IV)
Frequent (A)				
Probable (B)				
Occasional (C)				
Remote (D)				
Improbable (E)				
Very improbable (F)				

Extremely improbable (G)				
Eliminated (H)				

(Give detailed information for each hazard!)

ID	**Hazardous event (short)**	**Life cycle phase, DAS mode**
#		

Risk class (A, …, H – I, II, III, IV)	**Risk (high, serious, medium, low, eliminated)**
	(optional)

Hazard / hazardous event (detailed description including hazard source(s))
Initial conditions
Potential causes
Mishap (hazard effect)
Mishap end effect
Risk mitigation measures and actions (technical / in design, organizational, personal)
Evidence, verification & validation

Further activities

7.4.7 National Authority DAS Safety Assessment as of section 4.12

7.4.7.1 DAS risks and national risk acceptance criteria comparison

(Superimpose national risk acceptance criteria to DAS risk acceptance matrix as of 7.4.6.1!)

NATIONAL RISK ASSESSMENT MATRIX				
Severity / Mishap Probability	Catastrophic (I)	Critical (II)	Marginal (III)	Negligible (IV)
Frequent (A)				
Probable (B)				
Occasional (C)				
Remote (D)				
Improbable (E)				
Very improbable (F)				
Extremely improbable (G)				
Eliminated (H)				

7.4.7.2 Degree of DAS safety requirements fulfillment

(List all DAS safety requirements!)

Requirement (Reference)	**Supplier assured**	**Technically Independently assured**	**Organizationally independently assured**	**Comment**
ID, title, description	Evidence			
Application of a safety standard (→ 4.6)				

Development of safety-significant software (→ *4.6*)				
Configuration management (→ *4.6*)				
System Safety Program Plan → *4.6*)				
DAS safety verification and validation (→ *4.6*)				
Availability of safety documentation (→ *4.6*)				
Munitions and fuzing system safety verification and documentation (→ *4.6*)				
Evidence for adequate risk mitigation for the hazard of unintended activation of a CM (→ *4.6*)				
DAS Safety requirements for specific use case				
ID, title, description	Evidence			
Additional DAS safety requirements on national basis				
ID, title, description	Evidence			
External requirements specification document(s):				

7.4.7.3 Rationale for deployment

(Describe nation's rationale for system deployment!)

Safety standards and regulations used for assessment:
Safety standards and regulations used by manufacturer during development:
Rationale for deployment:

7.4.7.4 DAS Safety Assessment Statement

DAS System _____, of system version number _____ has accomplished a DAS safety assessment.

DAS residual risks from all identified hazards are mitigated to an acceptable level:

[ ] YES

[ ] NO

All safety requirements, including additional safety requirements by NA are met satisfactorily:

[ ] YES

[ ] NO

Use Case / Configuration: 6 **on date:** _____

Under the supervision of organizational POC:

_____ of nation:

_____ _____

7.5 Artefacts

The following table lists supporting artefacts as recommended for DAS safety assessment of different use cases (configurations). For the definitions of the configurations see section 4.8.

P = preliminary artefact (NA definition for preliminary artefact required)

X = document should be available for consultation with respect to hazard identification, hazard evaluation, risk assessment and safety assessment

Table 5: Artefacts assignment

Artefact	6A	6AT	6B	6BT	6C	6D	6E	Ref.
Hazard Identification and Mitigation Effort using the System Safety Methodology	P	P	P	P	P	X	X	[1]/T101 [3]/P2 [3]/B:G [3]/B:H
System Safety Program Plan (SSPP)	P	P	P	P	X	X	X	[1]/T102 [3]/P1
Hazard Management Plan (HMP)	P	P	P	P	X	X	X	[1]/T103
Documentation of system safety program reviews/audits	P	P	P	P	P	X	X	[1]/T104
Hazard Tracking System (HTS)	P	P	P	P	X	X	X	[1]/T106 [3]/P2
Hazard Management Progress Report	P	P	P	P	X	X	X	[1]/T107
Hazardous Materials Management Plan	P	P	P	P	X	X	X	[1]/T108
System Requirements Hazard Analysis (SRHA)	P	P	P	P	X	X	X	[1]/T203
Hazard Analyses	P	P	P	P	X	X	X	[1]/T204 [1]/T205 [3]/B:G5
Operating and Support Hazard Analysis (O&SHA)		P		P	X	X	X	[1]/T206 [3]/B:G4
Health Hazard Analysis (HHA)	P	P	P	P	X	X	X	[1]/T207 [3]/B:G9
Functional Hazard Analysis (FHA)	P	P	P	P	X	X	X	[1]/T208
System-of-Systems Hazard Analysis (SoSHA)					P	X	X	[1]/T209
Environmental Hazard		P		P	P	X	X	[1]/T210

Artefact	6A	6AT	6B	6BT	6C	6D	6E	Ref.
Analysis (EHA)								[3]/B:G8
Safety Assessment Report (SAR)	P	P	P	P	P	X	X	[1]/T301 [3]/P3
Hazard Management Assessment Report		P		P	P	X	X	[1]/T302
Test and Evaluation Participation		P		P	P	X	X	[1]/T303
Review of Engineering Change Proposals, Change Notices, Deficiency Reports, Mishaps, and Requests for Deviation/Waiver					P	X	X	[1]/T304
Safety Verification					X	X	X	[1]/T401
Explosives Hazard Classification Data	P	P	P	P	X	X	X	[1]/T402 [3]/B:G6
Explosive Ordnance Disposal Data	P	P	P	P	X	X	X	[1]/T403 [3]/B:G7
Evaluation Centre Safety Confirmation		P		P	P	X	X	7.5.1
Energetic Material Evaluation Board Certification	P	P	P	P	P	P	P	7.5.2
Fuze Safety Authority Certification	P	P	P	P	P	P	P	7.5.3
CDZ Estimation	P	P	P	P	P			7.5.4
Complete Dangerous Zone (CDZ)						X	X	AEP-62 vol. 5
Test range standard operating procedures	P	P	P	P	P	X	X	7.5.5
CONOPS and TTPs					P	X	X	7.5.6
DAS state transitions analysis	P		P		P	X	X	7.5.7
Electromagnetic Environmental Effects (E3) Supportability Statement					P	X	X	AEP-62 vol. 7
Explosive Ordnance Disposal (EOD) Statement	P	P	P	P	P	X	X	
Failure Mode Effects and Criticality Analysis (FMECA)	P		P		X	X	X	On devices level

Artefact	6A	6AT	6B	6BT	6C	6D	6E	Ref.
								and overall systems level (where applicable) 7.5.8
Fault Tree Analysis (FTA)	P		P		X	X	X	With regard to system integration level, 7.5.9
Hazardous Component Safety Data Statement		P		P	X	X	X	7.5.10
Safety Architecture Description	P		P		X	X	X	7.5.11
Safety-Critical Items List to support Quality of Production						X	X	
Software System Safety Assessment	P		P		X	X	X	7.5.12
Test Rig Configuration		P		P				7.5.13
Workplace health and safety risk assessment		P		P	X	X	X	7.5.14
Human Factors Analysis					P	X	X	[23] MIL-STD-1472G

In Table 5

[1]/T*xxx* refers to MIL-STD-882E Task *xxx,*

[3]/P*x* refers to AOP-15 Ed. 3 System Safety Principles, subsection 5.*x,*

[3]/B:G refers to AOP-15 Ed. 3 Safety and Suitability Assessment Process Block G,

[3]/B:G*x* refers to AOP-15 Ed. 3 Safety and Suitability Assessment Process Block G, subsection 6.2.7.*x,*

[3]/B:H refers to AOP-15 Ed. 3 Safety and Suitability Assessment Process Block H.

7.5.1 Evaluation Centre Safety Confirmation

Confirmation from evaluation centre, test site, proving ground, or the like

7.5.2 Energetic Material Evaluation Board Certification

National Authority responsibility to determine the acceptable energetic material evaluation and certification

7.5.3 Fuze Safety Authority Certification

National fuze safety board

7.5.4 CDZ Estimation

Estimation of Complete Dangerous Zone (CDZ) according to AEP-62 vol. 5; may be derived from theoretical analysis, simulation, tests, historical data, or other methods.

7.5.5 Test range standard operating procedures

Procedures for operating a DAS on a test range: test procedure plan, test scripts, etc.

7.5.6 CONOPS and TTPs

Includes description of tactical use, interaction with own troops and forces, training and maintenance, etc.

7.5.7 DAS state transitions analysis

Analysis for all states and modes capabilities of the DAS and their transitions, for example:

- power-up
- built-in test
- surveillance / sensor only
- armed
- automatic
- fired
- reload
- maintenance
- system fault
- safe state

7.5.8 Failure Mode Effects and Criticality Analysis

Considered an important method for hazard analyses; highly recommended during integration use cases, i. e. 6C, 6D, 6E.

7.5.9 Fault Tree Analysis

Fault tree analysis (FTA) is a top down, deductive failure analysis in which an undesired state of a system is analysed using Boolean logic to combine a series of lower-level events; see for example IEC 61025:2006.

Considered an important method for hazard analyses at early stages of DAS system analysis; highly recommended during integration use cases, i. e. 6C, 6D, 6E.

7.5.10 Hazardous Component Safety Data Statement

Also known as:

- Hazardous Material Safety Data Sheet
- Safety and Health Data Sheet

Document contains information on: toxicity, chemical composition, radioactivity, handling, storage, disposal, transportation, etc.

7.5.11 Safety Architecture Description

Configuration item level functional description, or specification, of DAS including information on interfaces, logical routes, signalling and communication. The Safety Architecture Description should contain information on integration for advanced configurations (6C, 6D, 6E).

7.5.12 Software System Safety Assessment

It is recognized that there are established and accepted state-of-the-art standards for the development and validation of safety-critical systems. Among those are MIL-STD-882E and IEC 61508:2010.

When following MIL-STD-882E, software associated with a safety-significant system function must be evaluated for its Software Control Category, which is related to the software's level of autonomy, its severity and SW Criticality Index (SwCI), which determines the Level of Rigor. The determined Level of Rigor decides which procedures and methods are to be applied to develop and finally accept a safety-significant software component in a specific DAS HW environment.

Equivalently, IEC 61508-3 recommends many activities during software development in accordance with the Software Integrity Level (SIL) determined for each safety-significant software component. The activities are described in Annexes A, B, and C of IEC 61508-3. The concept of SIL for estimating failure probabilities, or failure rates of software components, being part of, or representing safety functions is accepted. The SIL of a SW safety function can be used to establish the probabilities of inadvertent events during risk analysis.

Additionally, there exist many coding standards, like MISRA C, MISRA C++, or programming language standards with a strong focus on safety, e. g. Ada or the SPARK subset of Ada that

enable a high quality of software components and help avoid the most common programming and coding mistakes. The application of those coding standards, or a project or company specific coding standard, ideally derived from an accepted industry standard is highly recommended during software development. The same applies for appropriate choices of programming tools, integrated software development environments and test suites, which have to be well justified.

However, the application of software standards is not a guarantee that a particular SW component is without safety-critical defects, i. e. that the software itself is safe.

Amongst other things, it is imperative to understand the requirements of the software. Also, appropriate measures of tracking of the software related requirements and the validation of the functioning of the established SW safety functions are key to the acceptance of a safety-significant software component.

Mandatory software safety artefacts comprise the following:

- Test plans
- Test procedures
- Test results
- Analysis plans
- Analysis procedures
- Analysis results
- Software defect correction logs or report

7.5.13 Test Rig Configuration

Configuration of the overall system and of all configuration items, including software

7.5.14 Workplace Health and Safety Risk Assessment

Based upon national health and safety laws and regulations

7.6 False Alarms

False alarms (FA) could be considered as being either false positives or false negatives.

False negatives relate to the failure of a sensor and or a control process to declare a genuine threat to the host vehicle. Medium or high frequencies of false negatives are to be considered as a performance degradation of DAS (c. f. section 4.2). The impact of false negatives may be major (e. g. the DAS fails to detect and defeat a threat resulting in loss of life of the crew, and loss or damage of equipment.).

False positives relate to the false detection (FD) by a DAS sensor subsystem, e. g. an IR sensor could “believe” that an IR signature generated from a non-hostile thermal source is an IR source that it would “see” from a threat launch signature (see 7.1.12). The impact of false positives may be minor (e. g. false detection declared at sensor interface but rejected, and therefore not declared as a threat, by the control logic) or major (e. g. the control logic declares a threat condition resulting in the automatic discharge of a hard-kill countermeasure). The latter example can be referred to as a mishap event and creates a significant safety hazard.

Analysis must discriminate between the outcomes of false positives resulting in events equivalent to failure to defeat a threat, and events exhibiting unique hazards not experienced in a failure to defeat scenario.

To reduce the likelihood and impact of false detections, as a minimum the following should be considered:

- Determine types of FD (e. g. caused by flash after CM release) that could occur in the system. Consider the specific vehicle configuration, the DAS activation sequence, the DAS states and modes, etc.
- Determine the consequences of a FD, including DAS action and potential impact on the vehicle.
- Determine the consequences of a FD on the vehicle operator’s cognitive burden during all operational scenarios.
- Determine the false detection rate (FDR) including consideration of the impact of the specific vehicle configuration (i. e. changes to the system FDR due to the influence of the vehicle) as needed for further analyses. The NA should confirm that the FDR remains acceptable following integration onto the vehicle. The following analyses are recommended:
    - The DAS response to small caliber ammunition fire, ATR, and ATGM;
    - The DAS response to ammunition (including small, medium and large caliber, smoke grenades and single shot and automatic weapons) fired from an adjacent position (i. e. blue force position);
    - The DAS response to explosion, optical flash, electric arc welders and other optical stimuli (including those that emanate from the host vehicle systems such

as muzzle flash);

- The DAS response to electromagnetic stimuli, such as signals from active sensors, including reflections of signals originating from sensors of the own vehicle, and radio equipment;
- The DAS response to electronic stimuli such as on-vehicle electronic countermeasures and communications equipment;
- The DAS response to low velocity objects hurled in vehicle direction (e. g. rocks, bottles, slingshot projectiles, fireworks);
- An effects analysis of the environment and battlefield contaminants, such as smoke, fog, puddles, and of precipitation of dust, humidity, or mud at sensor surfaces on performance.

To establish the probabilities, or rates, of false detection for further analyses, e. g. fault tree analysis (FTA), the following methods should be considered:

- Theoretical analysis, calculation and reasoning
- Simulation
- Laboratory tests
- Literature study
- Measurements in representative environments
- Evaluation of actual test data
- Failure modes and effects analysis (FMEA)

The outcome should enable an understanding of the impact of false detection issues on system design, integration and overall system safety.

7.7 Guideline for evaluating hazards related to software

The following design features should be considered when evaluating hazards potentially resulting from safety-significant DAS software.

- Establishment and enforcement of obstruction zones or exclusion zones
    - Countermeasure obstruction zones prevent the release of energy into vehicle features during response to a threat.
    - Sensor obstruction zones prevent release of radiation from active sensors into vehicle features during operation of the DAS.
    - Countermeasure exclusion zones prevent the release of energy into regions surrounding the vehicle to prevent damage or injury to nearby friendly forces or vehicles.
    - Sensor exclusion zones prevent release of energy into regions surrounding the vehicle to prevent injury or damage to friendly forces or vehicle, or to minimize interference with systems on friendly vehicles.
- Analysis of safe and unsafe shutdown states for DAS subsystems or components. For instance, there are portions of munition launching cycles which cannot be safely interrupted.
- Restarting a DAS system after an emergency shutdown. A DAS user control panel may require switches to be set in a certain sequence to transition the DAS system from a safe non-operational state to a fully autonomous protection state. Employment of an emergency shutdown may leave user control panel switches in a state which will immediately cause the DAS system to transition to autonomous protection state upon powering up the system, resulting in inadvertent activation of autonomous behaviors.
- Automatic setting of a DAS system to a safe mode in response to DAS faults may not be able to de-assert analog safety discrete signals, leaving the DAS in an unexpected unsafe condition.
- Hybrid DAS systems containing combinations of hard-kill and/or soft-kill countermeasures may need multiple safety assessments to allow known safe behavior when one or more of the countermeasures are disabled.
    - Each component in a hybrid DAS can be expected to have a safety compliance declaration for single component operation as well as safety compliance declarations for each reasonable combination of components.
    - This will allow failure of one DAS component to cause the system to fail-over to a known, safety compliant configuration using the remaining subset of DAS capabilities.
    - This also allows DAS end-user tailoring to always result in a safety compliant configuration

- A level 6E *Fully Integrated Solution* opens the possibility of unauthorized commanding of a DAS system from an external source.
    - While this is directly a security issue, it also becomes a safety issue if the external source can change DAS behaviors, such as redefinition of exclusion zones, spoofing sensor inputs to cause DAS to respond to phantom targets, or re-calibration of DAS subsystems to disallowed power or temperature levels.

Note:
Most of the requirements and recommendations related to software are applicable to other forms of Programmable Elements (PE), like FPGAs, PLDs, configuration files, etc.

7.8 A Worked Example

For the purpose of demonstration of methodology the *Generic with Platform Specific Information* use case is chosen for an example DAS safety assessment.

An existing, generic DAS system using vehicle information has been created comprising a number (N1, N2) of two different kinds of sensors, a central control unit, an operator panel and several movable CM launchers.

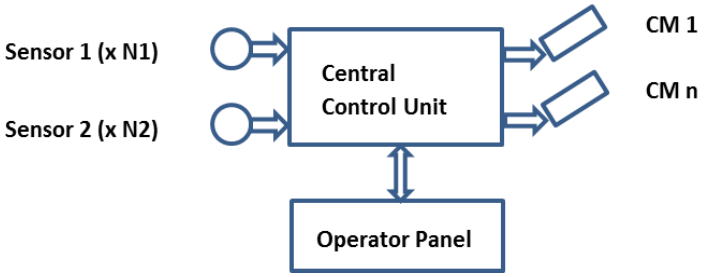

Figure 5: Example Generic DAS with Platform Specific Information

As a prerequisite for the safety assessment the DAS fulfills all basic safety requirements as of section 4.6. Yet, in regard of DAS system architecture NA has one additional (national) safety requirement:

R_1 In the scheduled scenarios the average probability (per sensor) of false detection (i. e. false positives) per hour of operation shall be less than 10^{-4}.

7.8.1 Identified Hazards

After studying supporting artefacts as of section 7.5 the DAS considered here is supposed to show three hazards identified by the methodology described in section 4.10. The following hazards are identified as typical hazards based on the generic system:

#1 Personal injury due to unintended activation of a countermeasure

#2 Personal injury due to unintended movement of turret or launcher

#3 Personal injury due to inadvertent exposure to radiation from sensor

Note:
A complete hazard list would contain many more hazards based on the actual DAS design.

7.8.2 Hazard Evaluation and Risk Assessment

By evaluation of the hazards it can be demonstrated that the mishap severities are estimated to be *catastrophic* (hazard #1), *critical* (#2), and *negligible* (#3). A thorough study of the available safety analyses (deliverables by the manufacturer of the DAS) allows the verification of implemented risk mitigation measures. The assessor independently verifies the residual risks by appropriate techniques for the combination of probabilities (see Figure 6 for an example illustrating an FTA concerning hazard #1; c. f. Figure 1 and Figure 5).

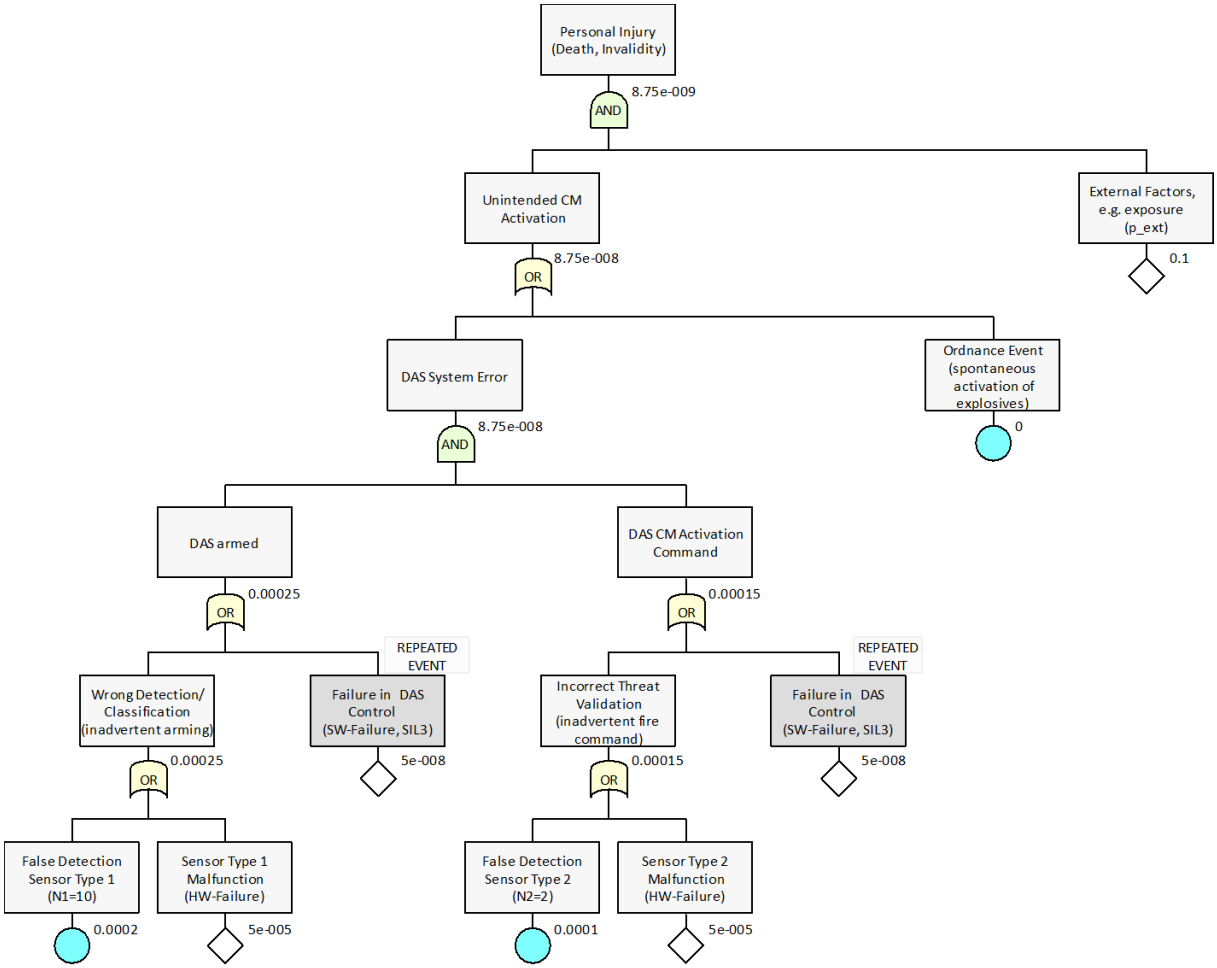

Figure 6: Example FTA for hazard #1 (personal injury due to inadvertent CM activation)

Reasoned assumptions suggest that the probabilities for respective damage events, i. e. the mishaps, are further decreased on average by external factors (e. g. p_{ext} = 0.1). This leads to the following risk classes (c. f. section 4.11):

- hazard #1: risk class **E-I** (improbable – catastrophic)
- hazard #2: risk class **C-II** (occasional – critical)
- hazard #3: risk class **B-IV** (probable – negligible)

7.8.3 Safety Assessment

The fact that all hazards could be evaluated helps to establish a safety rating for the DAS. The last step of the safety assessment is the comparison of nationally accepted risk thresholds with the findings of the risks assessment (see section 4.12). An example risk assessment matrix is shown in Table 6; it reveals that hazards #1 and #3 represent a medium residual risk, whereas hazard #2 represents a serious residual risk. By means of a separate experimental investigation it is shown that the sensors of the system have the required low false detection rates for the projected scenarios of DAS use (R_1 fulfilled).

Based on the decision of the organization conducting the safety assessment it is reported that:

- The DAS has been assessed.
- All risks could be assessed.
- All safety requirements, including additional safety requirements (R_1) by NA are met.
- With regard to operational use, the *Generic with Platform Specific Information* configuration of the DAS is not acceptably safe (6B not achieved):
    - It is desirable to further lower the risk of hazards #1 and #3; medium risks might be considered to be acceptable for DAS use by waiver.
    - Hazard #2 needs additional risk mitigation for the DAS to be considered for future platform integration.

To generate a report the standard forms as shown in section 7.4, *DAS Safety Assessment Summary*, can be used.

Table 6: Example risk assessment matrix

EXAMPLE RISK ASSESSMENT MATRIX				
Severity / Mishap Probability	Catastrophic (I)	Critical (II)	Marginal (III)	Negligible (IV)
Frequent (A)	**High**	**High**	Serious	Medium
Probable (B)	**High**	**High**	Serious	**#3**
Occasional (C)	**High**	**#2**	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	**#1**	Medium	Low	Low
Very improbable (F)	Medium	Low	Low	Low
Extremely improbable (G)	Low	Low	Low	Low
Eliminated (H)	Eliminated			

AEP-62 VOL VI (A) (1)