

NATO STANDARD

AEP-4754

**NATO GENERIC VEHICLE
ARCHITECTURE (NGVA) FOR LAND
SYSTEMS**

VOLUME VI: SAFETY

**Edition A Version 1
FEBRUARY 2018**



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

**Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN**

INTENTIONALLY BLANK

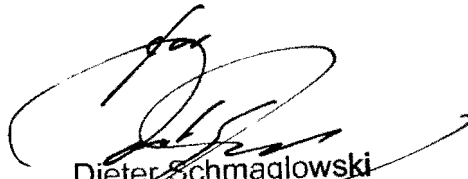
NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

22 February 2018

1. The enclosed Allied Engineering Publication AEP-4754, Volume VI, Edition A, Version 1 NATO GENERIC VEHICLE ARCHITECTURE (NGVA) FOR LAND SYSTEMS VOLUME VI: 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 4754.
2. AEP-4754, Volume VI, Edition A, Version 1 is effective upon receipt.
3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations and Partnership for Peace countries, or NATO commands and bodies.
4. This publication shall be handled in accordance with C-M(2002)60.



Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

[illegible]

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[illegible]

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1	Introduction	1
1.1.	Purpose.....	1
1.2.	Application of the NGVA Standard.....	1
1.3.	Agreement	1
1.4.	Ratification, implementation, and reservations.....	1
1.5.	Feedback	2
CHAPTER 2	Development of NGVA STANDARD	3
2.1.	NGVA Standard Structure.....	3
2.2.	General Notes.....	4
2.2.1.	Scope.....	4
2.2.2.	Warning	4
2.3.	Normative References	4
2.4.	Conventions.....	5
2.5.	Requirements Classifications.....	5
2.5.1.	Compulsory Requirement (CR).....	5
2.5.2.	Optional Enhancement (OE).....	5
2.6.	Abbreviations	5
2.7.	Terms and Definitions	5
2.7.1.	NGVA Definitions.....	5
2.7.2.	AEP Specific Definitions	7
CHAPTER 3	Systems Safety	11
3.1.	Safety Requirements	11
3.2.	Hazard Analysis	11
3.2.1.	Preliminary Hazard Identification	12
3.2.2.	Preliminary Hazard Analysis	12
3.3.	Safety Reviews	12
3.4.	Safety Management Plan.....	12
3.5.	Independent Safety Audit.....	13
3.6.	Safety Risk Analysis	13
3.6.1.	Hazard Severity	13
3.6.2.	Probability of Hazard.....	14
3.6.3.	Risk Classification.....	14
3.6.4.	Acceptability of Risk.....	15
3.7.	Safety Integrity Levels.....	15
CHAPTER 4	Safety Management System	17
4.1.	Safety Management Plan.....	19
4.1.1.	Examples of Safety Management Plan.....	19
CHAPTER 5	Risk Management	21
5.1.	Risk Management Plan.....	21
CHAPTER 6	Safety Requirements and Evidence	23
CHAPTER 7	Interfaces	25
CHAPTER 8	Managing Change and Feedback	27
CHAPTER 9	Safety Audits.....	29
CHAPTER 10	Safety Case	31
10.1.	Safety and Environmental Case Report (SEC Report)	32
CHAPTER 11	NGVA Specific Safety Considerations	33

ANNEX A	Abbreviations	A-1
ANNEX B	Tools Related to Safety Case	B-1
B.1.	SAFETY Case editors	B-1

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. Purpose

The aim of the NGVA Standard AEP-4754 Volumes I through VII is to enable the member nations to realize the benefits of an open architecture approach to Land vehicle platform design and integration, especially in regard to the vehicle platform electronic data and power infrastructure and the associated safety and verification & validation process.

1.2. Application of the NGVA Standard

The NGVA Standard is to be applied to all future land vehicle platforms and vehicle platform sub-system, as well as current vehicle platform refurbishment and upgrade programmes.

This NGVA Standard is applicable to land vehicle platforms, ranging from simple to complex implementations. The requirements for these implementations are determined by the functionality required of the vehicle platform as a whole system including all sub-systems, and not the automotive or power elements alone. The requirements address equipment to be fitted as part of the initial operating capability and equipment likely to be fitted throughout the life of the vehicle platform. These requirements are expressed in the national system requirements documents and/or the sub-system requirements documents for the individual vehicle platforms concerned.

1.3. Agreement

Ratifying nations agree that the NGVA Standard is to be applied to all future land vehicle platforms and vehicle platform sub-systems, as well as current vehicle platform refurbishment and upgrade programmes. Nations may propose changes at any time to the NATO Standardization Office (NSO).

Germany will act as custodian to maintain Configuration Management (CM) and change management of this Standard and its associated AEP Volumes.

Ratifying nations have agreed that national orders, manuals and instructions implementing this Standard will include a reference to the AEP-4754 Volumes I through VII for purposes of identification.

The NGVA Standard and its associated Volumes I through VII shall be considered as the foundation standard for vehicle sub-system integration, and should any conflict arise between this and other extant NATO documentation, this document shall take precedence.

Deviations from the NGVA Standard shall be agreed by the relevant national procurement office.

1.4. Ratification, implementation, and reservations

Ratification, implementation and reservation details are available on request or through the NATO Standardization Office (NSO) (internet: <http://nso.nato.int>).

1.5. Feedback

Any comments concerning this publication should be directed to: NATO/NSO – Bvd Leopold III - 1110 Brussels - Belgium.

Proposals for changes and improvements of the NGVA Standard AEP-4754 volumes I through VII shall be sent to the NSO and then forwarded to the custodian who will collect them and will propose new editions of the NGVA Standard AEP-4754 Volumes I through VII.

The NGVA Standard Point-of-Contact as assigned by the NGVA Standard Custodian is BAAINBw K1.2, Ferdinand-Sauerbruch-Str.1, D-56073 Koblenz, Germany.

CHAPTER 2 DEVELOPMENT OF NGVA STANDARD

The NATO Generic Vehicle Architecture (NGVA) Standard was developed under the auspices of the Military Vehicle Association (MILVA).

MILVA is an association of government agencies and industries promoting Vehicle Electronics (Vetronics) in the military environment. MILVA provides an open forum to its members and publishes guidelines and standards on Vetronics issues. MILVA works in close co-operation with NATO through the Land Capability Group on Land Engagement of the NATO Army Armament Group (NAAG).

2.1. NGVA Standard Structure

Figure 1 below illustrates the Standard structure, the Volumes relationships and technical areas covered under each Volume.

NGVA Standard AEP-4754	
Volume I:	NGVA Architecture Approach (Describes the NATO Generic Vehicle Architecture (NGVA) concept)
Volume II:	NGVA Power Infrastructure (Defines the design constraints on power interfaces which form the NGVA Power Infrastructure)
Volume III:	NGVA Data Infrastructure (Defines the design constraints on the electronic interfaces that form the NGVA Data Infrastructure)
Volume IV:	NGVA Crew Terminal Software Architecture (Defines the design guidelines and constraints for standardized "Crew Terminal Software Applications")
Volume V:	NGVA Data Model (Describes the NATO GVA Data Model (NGVA DM), the Model Driven Architecture (MDA) approach used to produce the NGVA DM, the toolset required to produce and manage the configuration control of the NGVA DM and finally the applicability of the NGVA DM to Data Distribution Service (DDS) middleware installed on a GVA compliant platform.)
Volume VI:	NGVA Safety (Outlines the generic procedures to incorporate system safety related planning, development, implementation, commissioning and activities in systems engineering)

Volume VII: NGVA Verification and Validation
(Provides guidance for the verification and validation of NGVA systems regarding their conformity to the AEPs associated with this STANAG)

Figure 1: NGVA Standard AEP-4754

2.2. General Notes

2.2.1. Scope

NGVA is the approach taken by NATO and related industry to standardize the interfaces and protocols for military vehicle systems integration. The Vehicle Architecture (including data and power architectures) is considered as the fundamental enabler that can provide new capabilities on military platforms so as to improve overall effectiveness (including cost) and efficiency within the whole vehicle life cycle. The NGVA Standard does not include standard automotive electronics and power related information.

2.2.2. Warning

National governments, like their contractors, are subject to laws of their respective countries regarding health and safety. Many NATO STANAGs and Standards set out processes and procedures that could be hazardous to health if adequate precautions are not taken. Adherence to those processes and procedures in no way absolves users from complying with their national legal requirements.

2.3. Normative References

The documents and publications shown in Table 1 below are referred to in the text of this AEP Volume. Documents and publications are grouped and listed in alpha-numeric order:

1. AAP-03	PRODUCTION, MAINTENANCE AND MANAGEMENT OF NATO STANDARDIZATION DOCUMENTS
2. IAWG-AJT-301	System of System certification (related to avionic)
3. IEC 61508	Functional safety of electronic electrical/electronic/programmable electronic safety-related systems
4. ISO 26262:	Road vehicles – Functional safety. Management of functional safety.
5. JSP 454	Land Systems Safety and Environmental Protection Part 2
6. MIL-STD-882E 11 May 2012	System Safety

Table 1: Normative References

Reference in Standard AEP-4754 and its Volumes to any normative references refers to, in any Invitation to Tender (ITT) or contract, the edition and all amendments current at the date of such tender or contract, unless a specific edition

is indicated. For some standards, the most recent editions shall always apply due to safety and regulatory requirements.

In consideration of the above and as best practice, those setting the requirements shall be fully aware of the issue, amendment status and application of all normative references, particularly when forming part of an ITT or contract.

2.4. Conventions

For the purposes of all AEP Volumes all requirements are specifically detailed in tables with each requirement classified as in the paragraph 2.6. Where an AEP Volume contains no specific requirement tables they should serve as implementation guidance until technical standardization requirements are developed and included.

2.5. Requirements Classifications

The following classifications are to be used for all NGVA related requirements.

2.5.1. Compulsory Requirement (CR)

The requirement needs to be implemented in order to conform to Standard AEP- 4754 and to gain certification. Compulsory requirements are listed in the Requirements Tables inside the AEPs and marked as “CR”.

2.5.2. Optional Enhancement (OE)

Optional Enhancements do not need to be implemented in order to conform to Standard AEP-4754. However, if such a capability is present, it needs to be implemented according to the stated specification in order to be compliant. Optional Enhancements are listed in the Requirements Tables inside the AEPs and marked as “OE”.

2.6. Abbreviations

Abbreviations referred to in this AEP Volume are given in Annex A.

2.7. Terms and Definitions

2.7.1. NGVA Definitions

1. **Base Vehicle:** The basic vehicle structure and those systems needed to enable it to perform its automotive functions and mobility. Where fitted it also includes those systems needed to control turrets and other physical elements e.g. a mine plough.
2. **Base Vehicle Sub-System:** A system that forms part of the base vehicle
3. **Electronic Architecture:** The combination of the electronic based sub-systems and electronic infrastructure that supports the vehicle crew to undertake their operational tasks
4. **NATO Generic Vehicle Architecture (NGVA):** The term ‘NATO Generic Vehicle Architecture’ refers to the open, modular and scalable architectural approach applied to the design of vehicle platforms.
5. **Hard Switching:** The ability to control or operate a sub-system using physically based means.

6. **Measure of Effectiveness:** A description of how effective a solution candidate is for a particular assessment criterion.
7. **Measure of Performance:** A statement that describes the assessment criterion or criteria needed to satisfy a given requirement.
8. **Modular:** A modular architecture is designed in such a way as to allow the replacement or addition of sub-systems and upgrades as required without any undesirable emerging properties.
9. **NGVA Compliant:** NGVA Compliance applies to the whole vehicle platform and means that any sub-system existing on the platform complies with the requirements defined in STANAG 4754 and associated AEPs.
10. **NGVA Electronic Infrastructure:** The physical cables and connectors that provide means of distributing data around a base vehicle. It also includes any enabling logical components and functions e.g. Core platform management software, interface software, transport protocols and message definitions.
11. **NGVA Power Infrastructure:** The physical cables, connectors and other components that provide the means of distributing and controlling electrical power around a vehicle platform.
12. **NGVA Ready:** NGVA Ready applies at a sub-system level and means that sub-systems and components have been developed to a level where they can be efficiently integrated within a “NGVA Compliant” whole vehicle Electronics. This would mean passing an incremental process with two sequentially-related Compatibility levels:
 - a. **Connectivity Compatibility:** Ensures that the (sub-) system can be physically integrated into the NGVA architecture without any negative impacts to existing NGVA components. Physical power and network interfaces comply with the requirements of Power and Data Infrastructure AEPs.
 - b. **Communication Compatibility:** Connectivity Readiness and data interfaces (DDS/Video) with associated NGVA Data Model implementation that comply with the requirements of Data Model and Data Infrastructure AEPs.
13. **Operator:** Any person required to interface and control vehicle platform sub-systems.
14. **Power Management:** The means of prioritizing and controlling the electrical power loads throughout the vehicle platform.
15. **Scalable:** The trait of a system in being able to scale in order to handle increased loads of work.
16. **Soft Switching:** The ability to control or operate a sub-system using software functionality.
17. **Sub-System:** Separable elements or collections of equipment or software added to a base vehicle that provide operationally required capabilities over and above those delivered by the base vehicle.
18. **System:** A combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate.
19. **Vehicle Crew:** All personnel located in the vehicle platform with defined roles needed to fulfil the necessary operational functions.
20. **Vehicle Platform:** The vehicle and all its integrated sub-systems.

21. **Vehicle Users:** The individuals and groups of people who interact locally to operate, support, sustain, maintain or otherwise interface directly with the Vehicle Platform and its sub-systems. It includes Service personnel, Reserve personnel, and Civilian employees, and may include personnel under other service supply contracts.

2.7.2. AEP Specific Definitions

1. **ALARP:** As Low As Reasonably Practicable. A risk is ALARP when it has been demonstrated that the cost of any further Risk Reduction, where the cost includes the loss of defense capability as well as financial or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction. [Def Stan 00-56 Issue 4]
2. **Audit:** An examination of implemented process.
3. **Certification of Safety Case (or Safety Case Certification):** Process and declaration of the acceptance of a safety case by a certification authority.
4. **Downgraded mode:** Degraded mode of operation that is actively entered by a system or subsystem in response to a detected error, in order to reduce the error. Degradation can include reduced functionality, reduced performance, or both in order to permit survivability capabilities.
5. **Error:** An error is a deviation from the required operation of the system or sub-system
6. **Fault:** A defect within a system
7. **Hazard:** A hazard is a situation in which there is actual or potential danger to people or to the environment.
8. **Hazard Analysis:** The process of describing in detail the hazards and accidents associated with a system, and defining accident sequences. [Def Stan 00-56 Issue 4]
9. **Hazard Identification:** The process of identifying and listing the hazards and accidents associated with a system. [Def Stan 00-56 Issue 4]
10. **Hazard Log:** The continually updated record of the hazards, accident sequences and accidents associated with a system. It includes information documenting risk management for each hazard and accident. [Def Stan 00-56 Issue 4].
11. **Independent Safety Auditor:** An individual or team, from an independent organization, that undertakes audits and other assessment activities to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose. [Def Stan 00-56 Issue 4]
12. **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].
13. **Mitigation Strategy:** A measure that, when implemented, reduces risk. [Def Stan 00-56 Issue 4]
14. **Mode:** A designated system condition or status (e.g., maintenance, test, operation, storage, transport, and demilitarization). [MIL-STD-882E].
15. **Modular:** A modular architecture is designed in such a way as to allow the replacement or addition of sub-systems and upgrades as required without any undesirable emerging properties, which could impact the safety of the other, non-independent sub-systems or the safety of the vehicle overall.

16. **Risk:** An assessment of the significance of a hazard based on a function of its probability of occurrence and an appropriate numerical indication of the severity of its consequences
17. **Risk Acceptance:** The systematic process by which relevant stakeholders agree that risks may be accepted. [Def Stan 00-56 Issue 4]
18. **Risk and ALARP Evaluation:** The systematic determination, on the basis of Tolerability Criteria, of whether a risk is broadly acceptable, tolerable or unacceptable, and whether it is ALARP or whether any further Risk Reduction is necessary. [Def Stan 00-56 Issue 4]
19. **Risk Estimation:** The systematic use of available information to estimate risk. [Def Stan 00-56 Issue 4]
20. **Risk level:** The characterization of risk. [MIL-STD-882E].
21. **Risk Management:** The systematic application of management policies, procedures, and practices to the tasks of **Hazard Identification, Hazard Analysis, Risk Estimation, Risk and ALARP Evaluation, Risk Reduction and Risk Acceptance**. [Def Stan 00-56 Issue 4].
22. **Risk Reduction:** The systematic process of reducing risk. [Def Stan 00-56 Issue 4]
23. **Safe:** Risk has been demonstrated to have been reduced to a level that is ALARP and broadly acceptable or tolerable, and relevant prescriptive safety requirements have been met, for a system in a given application in a given operating environment. [Def Stan 00-56 Issue 4]
24. **Safety:** The expectation that a system does not, under defined conditions, lead to a state in which human life or the environment is endangered. [Def Stan 00-56 Issue 2].
25. **Safety Audit:** A systematic and independent examination to determine whether safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.
26. **Safety Case:** A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. (definition from Def Stan 00-56 Issue 4)
27. **Safety Case Report:** A report that summarizes the arguments and evidence of the Safety Case, and documents progress against safety. [Def Stan 00-56 Issue 4]
28. **Safety and Environmental Case Report:** A report that summarizes the arguments and evidence of the Safety Case, and documents progress against the safety program. [Def Stan 00-56 Issue 4]
29. **Safety Integrity:** The likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time
30. **Safety Integrity Level:** A classification of the required level of safety integrity defining the processes that must be applied to the development of system.
31. **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].
32. **Survivability:** Ability of a system to fulfil its mission in a timely manner in presence of attacks, failures, or accidents.

- 33. **System:** A combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate.
- 34. **System Failure:** A system failure occurs when the system fails to perform its required function.
- 35. **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].
- 36. **System safety engineering:** An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated. [MIL-STD-882E].

INTENTIONALLY BLANK

CHAPTER 3 SYSTEMS SAFETY

This Volume provides guidance on the design and certification of safe vehicle platform. The document can be applied to the entire vehicle platform (NGVA-compliant) or a vehicle sub system (NGVA ready), current and future. The guidelines specified in this Volume are based on existing, industry wide, open standards and practices.

Specifying safety guidelines and procedures forms the basis of the future. Standardising aspects of certification throughout NGVA member nations enables cost savings. For example, safety case modules for NGVA ready sub systems could be provided by NGVA member nations against these shared safety and certification guidelines will simplify vehicle reconfiguration and recertification.

This section of the Volume outlines the generic procedures to incorporate system safety related planning, development, implementation, commissioning, and activities in systems engineering. The development of safety related/critical system should start with using a system lifecycle model. Examples of system life cycle models are Systems Engineering 'V' model, waterfall model, etc.

The development of safety related/critical systems should commence by using the following process:

1. Requirements capture.
2. Record system requirements in a formalized system requirements document.
3. Identify and separate the functional and non-functional requirements and manage configuration within the requirements document.
4. Perform a hazard and risk analysis on both the functional and non-functional requirements to identify hazards.
5. Safety requirements must be produced from hazard analysis and identification.
6. System specifications should be produced from the safety requirements.
7. System specifications must include measures for safety assurance in order to keep safety in-line and protect against the identified hazards.

3.1. Safety Requirements

In order to derive safety requirements for a system the series of tasks identified below have to be performed:

1. Identification of hazards associated with the system;
2. Classification of the hazards;
3. Determination of methods for dealing with the hazards;
4. Assignment of appropriate reliability and availability requirements;
5. Determination of appropriate safety integrity level;
6. Specification of development methods appropriate to the integrity level.

3.2. Hazard Analysis

Hazard analysis on the identified potential hazards must be carried out at the early stage of the design life cycle. In addition, the hazard analysis should normally continue throughout the development process. This section describes the hazard analyses that can be used when designing a safety related/critical system

3.2.1. Preliminary Hazard Identification

1. Preliminary Hazard Identification (PHI) should be carried out at the earliest stage of system development to identify the potential hazards related to the system.
2. The results of PHI should be recorded in a preliminary hazard list.
3. Preliminary hazard list should be retained as evidence to be used in the system certification.

3.2.2. Preliminary Hazard Analysis

1. The identified hazards from PHI should be considered association with the functional requirements of the system.
2. Safety implications should be considered and design alternatives should be evaluated.
3. If possible attempts should be made to classify severity of hazards and to assign integrity level requirement for each major function.
4. The findings of preliminary hazard analysis must be documented in a preliminary hazard analysis report.
5. The preliminary hazard analysis report should consider the following:
 - a. Description of the system and its environment;
 - b. Overview of system's function and the safety features;
 - c. Safety objectives of the system;
 - d. Justification of the risk and integrity levels assigned;
 - e. Target failure rates and safety levels;
 - f. Sources of any data used within the analysis;
 - g. Bibliography of all the documents used.

3.3. Safety Reviews

Safety reviews should be conducted throughout the development process of a safety related/critical system.

1. The review should encompass all aspects of safety.
2. Safety reviews must consider data and analysis from all the available records. For example, hazard log, etc.
3. The first safety review should commence after the preliminary hazard analysis stage.
4. The assessment of allocated integrity levels and safety requirements should be addressed during the initial safety reviews.
5. Where the allocated integrity levels and safety requirements are addressed as modest, further system level hazard analysis should be performed to identify further issues or confirm the initial assessment.

3.4. Safety Management Plan

1. Safety management plan should be produced for a safety related/critical system on how the safety for the system is achieved;
2. Safety management plan should also define the management structure responsible for safety related tasks such as hazard and risk analysis;
3. The detailed safety planning of the system design, implementation, commissioning, operation and maintenance should be documented in the safety plan;

4. Safety management plan should also include the control measures designed/applied to achieve the relevant level of safety for the system;
5. It also includes various standards and codes of practice that is to be followed during the development of the system;
6. Safety management plan should be maintained and updated throughout the project.

Examples of safety management plan are presented in section 4.1.

3.5. Independent Safety Audit

1. For systems with higher level of criticality, independent assessors should be employed to perform safety audits;
2. Independent safety audits should use data from hazard logs and hazard analysis reports to verify whether the chosen safety mitigation strategies are adequate and whether the required documentation is sufficient;
3. Outcomes of the independent safety audit should be documented into an independent safety audit report;
4. The degree of independence when performing the assessment for safety audit can be an independent person, department or an organization;
5. It is understandable that the degree of independence allocated to the safety audit can be limited due to proprietary reasons, in such cases adherence to relevant safety standards can be shown as an assessment of safety related/critical systems (for instance IEC 61508).

3.6. Safety Risk Analysis

The identified hazards from the hazard analysis should be further studied to determine the risks associated from them. Risk associated with the hazards can be determined in qualitative or quantitative ways. For example, in case of quantitative approach used then the numerical approximates of both the frequency of hazard and the severity of hazards should be combined to produce a single measure of risk, where:

- Risk = severity x frequency

3.6.1. Hazard Severity

Hazard severity is categorised into various levels by [6]. Table 1 below shows an example of the accident/hazard severity categories.

Category	Definition for Equipment	Definition for Human
Catastrophic	The equipment is destroyed.	Multiple deaths
Critical	The equipment cannot complete its mission	A single death, and/or multiple severe injuries or severe occupational illnesses
Marginal	The equipment is degraded but the mission can be completed	A single severe injury or occupational illness, and/or multiple minor injuries or minor occupational illness

Negligible	The equipment has a minor fault with no impact on mission	At most a single minor injury or minor occupational illness
------------	---	---

Table 1: Example of hazard severity categories

3.6.2. Probability of Hazard

In addition, to classifying hazards into various categories, the frequency of the occurrence of these hazards is also categorised. 4 below describes the accident probability ranges.

Accident Frequency	Example probability of failure for highly critical system	Occurrences during operational life considering all instances of the system
Frequent	10000 x 10 ⁻⁶ /operating hour	Likely to be continually experienced
Probable	100 x 10 ⁻⁶ /operating hour	Likely to occur often
Occasional	1 x 10 ⁻⁶ /operating hour	Likely to occur several times
Remote	0.01 x 10 ⁻⁶ /operating hour	Likely to occur some time
Improbable	0.0001 x 10 ⁻⁶ /operating hour	Unlikely, but may exceptionally occur
Incredible	0.000001 x 10 ⁻⁶ /operating hour	Extremely unlikely that the event will occur at all

Table 2: Example of accident probability ranges

Note that, the probability of the hazardous events is also expressed in terms of events per hour or per year operation.

3.6.3. Risk Classification

The United Kingdom (UK) Health and Safety Executive (HSE) recognizes three approaches to making a claim that risk is As Low As Reasonably Practicable (ALARP). These are defined as good practice arguments which demonstrate that risk control measures comply with relevant good practice as defined in Approved Code of Practice (ACoPs), HSE guidance and standards etc.

Qualitative first principles arguments based on common sense or professional judgment to weigh possible risk reduction against the necessary "sacrifice"

Quantitative first principles arguments based on numerical techniques such as Cost Benefit Analysis (CBA) to weigh possible risk reduction against the necessary "sacrifice"

Risk classification process involves classification of risk associated with the particular hazard when Numerical data is not available for hazard severity or probability. Table 3 and Table 4 below shows example of accident risk classification.

Consequences				
Frequency	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	D	D	D	D

Table 3: Example of accident risk classes

Risk Class	Interpretation
A	Intolerable
B	Undesirable, and will only be accepted when risk reduction is impracticable
C	Tolerable with the endorsement of Project Safety Review Committee
D	Tolerable with the endorsement of the normal project reviews

Table 4: Example of interpretation of risk classes

3.6.4. Acceptability of Risk

In case the levels of risk are not acceptable, it is not satisfactory to have a hazard that could have catastrophic consequences and occur frequently. However it can be acceptable to have a hazard occur frequently with negligible consequences and a catastrophic accident is improbable or remote. The acceptability of given level of risk should be determined by the benefits associated with that risk, and by the amount of effort and cost needed to reduce it i.e. the risk is ALARP.

1. Risks associated with a safety related/ critical system should be broadly acceptable/ tolerable.
2. Sufficient evidence is required to prove that the risk has been reduced to ALARP.

3.7. Safety Integrity Levels

1. Safety related/critical systems should be allocated safety integrity levels either quantitative (in terms of measure of performance) or qualitatively (in terms of system characteristics).
 2. Safety integrity levels could also be described in terms of 'failures per year' or 'failure probability during an accident'.
 3. Safety integrity levels are defined in terms of the maximum number of times that a system built to a particular integrity level would be expected to fail in a given period of time.
 4. Safety integrity levels are differentiated between continuous mode of operation and demand mode.
 5. Failures for continuous mode of operation are expressed as failures per year.
 6. Failures for demand mode of operation are expressed as failures on demand.
- Table 5 below shows an example of target failure rates for safety integrity levels.

Safety Integrity Level	Continuous mode of operation (probability of dangerous failures per year)	Demand mode of operation (probability of failures on demand)
4	$\geq 10^{-9}$ to $<10^{-8}$	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-8}$ to $<10^{-7}$	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-7}$ to $<10^{-6}$	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-6}$ to $<10^{-5}$	$\geq 10^{-2}$ to $<10^{-1}$

Table 5: Example target failures rates for safety integrity levels [3]

Safety Integrity level applies to systematic and random errors, and failures. Appropriate strategy should be employed to mitigate these errors or failures. See ANNEX B

CHAPTER 4 SAFETY MANAGEMENT SYSTEM

A Safety Management System provides the means of managing Safety and defining the processes to be followed to achieve the desired safety objectives. The Safety Management System should be fully documented within the Safety Management Plan, so that the process for the managing project safety is clearly defined and the effectiveness of the implementation of the Safety Management System can be assessed.

An effective Safety Management System will ensure co-ordination of the correct mix of resources to plan, organise, implement, monitor, review, audit and improve specified tasks. The Safety Management System should address safety policy and/or strategy, defined levels of authority, lines of communication and procedures. The Safety Management System would typically address the following:

1. The strategy for managing safety.
2. The definition of individual and organizational roles and allocation of safety authority and responsibilities including the safety committee and identification of the 'sign-off' authority.
3. The interface arrangements, particularly with other Safety Management Systems.
4. The definition of competency requirements and mechanisms for measuring and ensuring competence.
5. The identification and allocation of resources required for the Safety Management System to be implemented effectively.
6. The identification of applicable legislation, regulations and standards.
7. The interface with Occupational Health and Safety arrangements as appropriate, either directly or by reference.
8. The audit arrangements.
9. The change management arrangements.
10. The arrangements for monitoring defect/failure reports and incident/accident/near miss reports, and identifying and implementing remedial action.
11. The arrangements for managing and acting on feedback in respect of the impact of such actions on safety requirements and the Safety Case itself.
12. The arrangements for measuring the effectiveness of safety management activities.

Figure 1 shows an example of a safety lifecycle from IEC 61508.

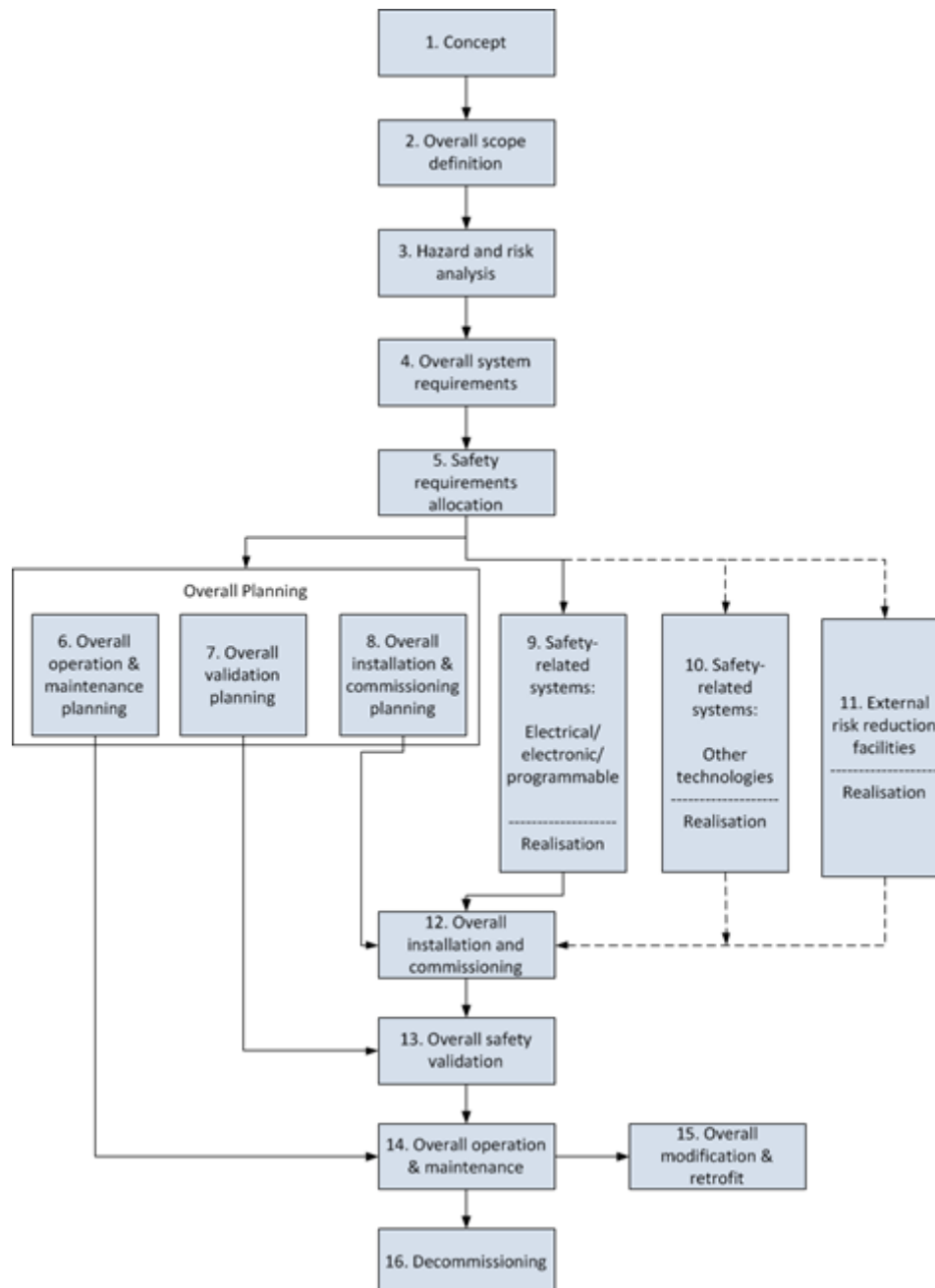


Figure 1: Example of Safety lifecycle from IEC 61508

It is important that safety is considered with all other engineering disciplines and not as a separate entity; particularly as experience has shown that poor safety management can be a significant source of project risk. As part of implementing a systems engineering approach, different processes, documents, etc., may be merged. However, the need to be able to consider safety issues independently should be recognised, particularly when involving technical experts and regulator/certification organizations. As a result, it may be necessary for safety material to be tagged as such, to enable it to be differentiated from non-safety material.

4.1. Safety Management Plan

The Safety Management Plan details the specific actions and an arrangement required to operate a Safety Management System and defines safety milestones for the project. It provides the link between safety requirements and general management processes for the project, to ensure that safety is achieved and maintained in a planned way.

4.1.1. Examples of Safety Management Plan

The Safety Management Plan would typically address the following:

1. A description of the system and its purpose sufficient to provide an understanding of what the Plan is referring to. (A full description of the system will be documented within the Safety Case.)
2. Initial definition of all key safety requirements.
3. Details of the Safety Management System to be operated.
4. A description of defined safety tasks, including:
 - a. Ownership.
 - b. Methodology
 - c. Resource requirements.
 - d. Definition of milestones.
 - e. Tolerability Criteria.
 - f. Risk management processes, including the definition of methods.
 - g. The identification of specific tools to be utilised (such as hazard log software).
 - h. The safety programme.
 - i. The safety audit plan.
 - j. The compliance matrix for this Standard, indicating procedures and methods to be used.
 - k. A list of deliverables and their format.

The safety program usually comprises a 'Gantt' chart depicting timescales, safety milestones and deliverables. It should also include a treatment of potential unprogramed activities such as analysis of incidents and accidents. The programme can be developed as required e.g., it could include the safety audit plan. The Safety Management Plan should contain an adequate level of information and detail to provide a comprehensive understanding of the way safety management will be implemented and maintained.

When defining the management and technical tasks to be conducted the following aspects should be considered and described in the Safety Management Plan.

1. The definition of the important stages of the safety program, their duration and phasing with other design, development, production and support activities, and with design and program reviews. The precise content of the safety program will be dependent upon the type of system being analyzed and the scale of the hazard analysis and assessment program. The Safety Management Plan should accurately reflect the program to be employed.
2. The Safety Management Plan should describe the overall organizational structure to indicate the involvement of the Contractor's design, development, production and service support staff with the safety program. It should identify the key

appointments referred to in this Standard and describe their levels of responsibility. The interface between the key appointments and other project staff should also be described.

3. The Safety Management Plan should describe the procedures and resources to be employed when carrying out the safety tasks. References should be made to appropriate Contractor procedures, national and international standards, and details of procedures for conducting particular analyses such as Fault Tree Analysis (FTA) and Failure Modes Effects and Criticality Analysis (FMEA). References should also be made to project specific quality plans and configuration management plans, where appropriate, to describe the quality and configuration management measures that are relevant to the safety program. The Contractor should state the deliverables that are appropriate to the work program phase.
4. Identification of the safety tasks; e.g. System Change Hazard Analysis, required for the integration and installation of the equipment into other systems.
5. The means by which all staff concerned with the contract, including sub-contractors, are made aware of the safety requirements and their specific responsibilities.
6. Anticipated problems and the possible means by which they may be overcome.
7. The methods by which the Contractor will interface with the Platform Equipment (MOD PE) Project Manager (MOD PM) in order that the Safety Management Plan is reviewed and modified as necessary.

CHAPTER 5 RISK MANAGEMENT

Risk management is the process of ensuring that hazards and potential accidents are identified and managed. It is a process managed within the Safety Management System. The outputs from the risk management process are a key part of the Safety Case. All hazards and potential accidents should be identified, as far as reasonably practicable, and the associated risks managed as appropriate. All safety risks should be reduced to levels that are ALARP. In addition, it is important to ensure that all risks are broadly acceptable. Where this is not possible, risks should be reduced to levels that are both tolerable and ALARP.

Risk management consists of the following processes:

1. Hazard Identification and Hazard Analysis
2. Risk Estimation
3. Risk and ALARP Evaluation
4. Risk Reduction
5. Risk Acceptance

5.1. Risk Management Plan

The terminology used in the process description may vary. For example, the combination of the first three activities is often referred to as **Risk Analysis**, while that of activities a. to d. is sometimes referred to as **Risk Assessment**.

In Figure 3, the essential inter-relationships of the risk management processes, together with other activities (system development life-cycle) are illustrated. Some relationships, for example, the dependence of ALARP evaluation on knowledge of alternative designs are omitted for simplicity and clarity.

The results from each stage of the risk management process feeds into the appropriate phase of the design process. For example, "*Hazards and Accidents*" which is the result from the **Hazard identification and Hazard Analysis** phase, is used in generating the safety requirements.

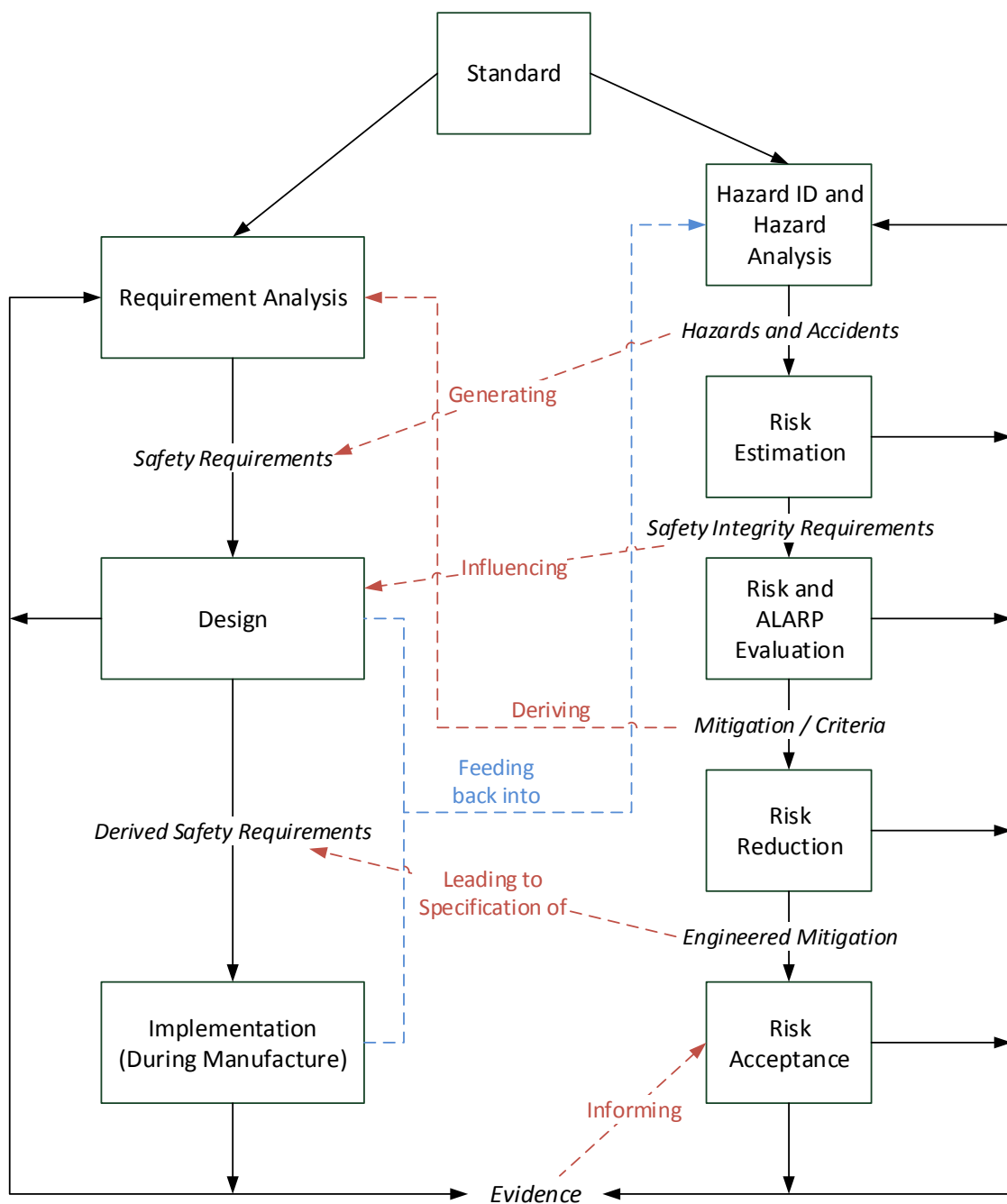


Figure 2The inter-relationship of Risk Management processes

CHAPTER 6 SAFETY REQUIREMENTS AND EVIDENCE

In order to implement a demonstrably safe system, a set of safety requirements should be formulated and then satisfied, with evidence being produced that they have been met. These safety requirements will be derived from a number of sources through the life of the system, from the initial legislative and contractual requirements, through the risk management activities, to subsequent safety demands that emerge as development proceeds. A safety requirement can be any requirement that relates to the safety of the system; it can be high- or low-level, simple or detailed, so long as it contributes to the achievement or evidence of safety and it can be adequately demonstrated that the requirement has been met.

Due to the diverse nature of the origin of safety requirements, it is necessary to provide traceability to the source of each safety requirement. The means of recording traceability is not prescribed; however, traceability should be demonstrated within the Safety Case.

In developing systems it may be necessary, to refine safety requirements into detailed requirements that are specific to the chosen implementation (see Figure 3); this will usually be the case for complex electronic systems.

The relationship between safety requirements and derived safety requirements can be informally expressed as:

1. A safety requirement is imposed on the system as a whole, irrespective of the solution and is realised as one or more derived safety requirements in the implementation (for software applications) or manufacture.
2. A derived safety requirement is something that can be specified at the level of the implementation or design of a system. (The derived safety requirement reflects the specific means being used to prevent the system entering a hazardous state, which could lead to, or fail to protect against, an accident.).

Demonstration of safety includes finding the credible evidence that shows that the derived safety requirements are correctly implemented and hence that safety requirements are satisfied. Evidence should demonstrate that implementation has not adversely affected the safety of the system. The traceability of the derived safety requirements to the top level safety requirements is essential for the Safety Case.

The evidence should consist of one or more forms of the following types:

1. Direct evidence from analysis.
2. Direct evidence from demonstration (testing and/or operation), including quantitative evidence.
3. Direct evidence extracted from the review process.
4. Process evidence showing good practice in development, maintenance and operation.
5. Qualitative evidence for good design, including expert testimony etc.

INTENTIONALLY BLANK

CHAPTER 7 INTERFACES

There are a number of interfaces that are particularly important for the management of safety. These include interfaces such as those between:

1. Organizations;
2. Safety Management Systems;
3. Safety Cases;
4. Elements of a system;
5. Systems and Sub-systems, Regarding the safety, interfaces have to be analysed because the composition of two safe elements may introduce failure or errors;
6. Systems;
7. Super-systems and Systems;

The methodology for managing interface issues should be included within the Safety Management Plan. However, the technical details of interfaces may be included within one or more specific integration or interface documents. The arguments and evidence demonstrating the effective management of interfaces should be included within the Safety Case.

INTENTIONALLY BLANK

CHAPTER 8 MANAGING CHANGE AND FEEDBACK

Change is an inevitable part of the system lifecycle and should be planned for and managed in a systematic way. It is important that an adequate level of analysis is carried out to determine the safety impact of any change. Safety impact means that a safety requirement, the safety argument or an item of safety evidence is affected. All changes, whether to the system or the environment in which it operates, should be assessed for safety impact by the Contractor and an appropriate response implemented where necessary. This response may include re-working earlier stages in the design or safety process, this can be managed within the Quality and Improvement process management.

Due to the interpretation of “what is safe” changes over time, there is potential for a system that was considered to be safe to cease to be considered safe. This may be due to changes in, for example, the operating environment, legislation, regulations, policies, technology or good practice. Such changes may cause difficulties by imposing new safety requirements or affecting existing ones, but they may also provide opportunities for implementing new safety features. To ensure that such changes are detected and addressed, a monitoring process under the Safety Management System and Quality System should be implemented. All parties involved in the development process should agree on a way forward where such changes are assessed to have a safety impact. Details of any resultant changes should be recorded in the Safety Case and feedback on specific actions should be notified to all interested parties.

INTENTIONALLY BLANK

CHAPTER 9 SAFETY AUDITS

Safety audits provide assurance that safety is being managed effectively and that safety management complies with relevant legislation, regulations, standards, policies, specific contractual requirements and the documented Safety Management System. Audits to be carried out should be identified within an audit plan.

A safety audit should include a review of the Safety Management System and any Safety Case Reports produced since the previous audit. It should also include a review of a sample of the major safety activities and outputs since the previous audit. To be effective, a safety audit will include consideration of:

1. Compliance with the Safety Management System, safety standards, etc.
2. The effectiveness of the safety processes being followed (including progress made against the Safety Plan).
3. The adequacy of the Safety Case.

The sampling policy and the frequency and extent of audits should be stated in the audit plan. The scope of these audits may be influenced by the scope of Independent Safety Auditor activity if an Independent Safety Auditor is appointed (e.g. to avoid duplication of effort).

The audit report should usually address the audit activities undertaken, the anomalies or non-conformances found, areas of particular strength and areas for improvement, recommended actions and the status or resolution of previous recommendations.

INTENTIONALLY BLANK

CHAPTER 10 SAFETY CASE

According to definition [26], a safety case is a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.

The safety case is a record of all the safety activities associated with a system, throughout its life. This is initially created early in the development process and is then expanded to include details of all aspects of the development work that are relevant to safety. Following development the safety case must be maintained throughout the operational phase, to document any alterations to the system or its use. As requirements change, or the system is modified, it will be necessary to justify such changes in terms of their implications for system safety.

One of the most important uses of the safety case is to support an application for certification. Here the regulatory authority will be looking for evidence that all potential hazards have been identified and that appropriate steps have been taken to deal with them. The safety case must also demonstrate that appropriate development methods have been adopted and that these have been performed correctly.

A safety case typically contains the following:

1. A description of the safety-related system;
2. Evidence of competence of personnel involved in any safety activity;
3. A specification of safety requirements;
4. The results of hazard and risk analysis;
5. Details of risk reduction techniques employed;
6. The results of design analysis showing that the system design meets all the required safety targets;
7. The verification and validation strategy;
8. The results of all verification, validation activities and traceability;
9. Records of safety reviews and audits;
10. Records of any incidents which occur throughout the life of the system;
11. Records of all changes to the system and justification of its continued safety.

A Safety Case is required for all systems, whether being acquired or already in-service. Safety Cases may be produced at the system, super-system or sub-system level. Where a system includes sub-systems that have separate Safety Cases, these Safety Cases should be integrated and reconciled within the higher level system Safety Case. This will assist in demonstrating that interface and other safety issues have been managed effectively, and that assumptions and cascaded safety requirements have been properly addressed.

There may be Safety Cases already in existence for related systems, sub-systems or even super-systems, and these should be reviewed before beginning work on a new Safety Case. Existing safety cases for sub-systems should be reviewed in the light of the role of the sub-system within the system and the existing arguments justifying the safety of the sub-system should be fully utilized.

10.1. Safety and Environmental Case Report (SEC Report)

A Safety and Environmental Case (SEC) report summaries the safety case at a particular point in time. It is an important deliverable that provides assurance that the safety is being managed effectively, highlights areas of safety-related project risk requiring management attention and gives stakeholders visibility of the status of the Safety Case.

The contents of the SEC Report will vary according to the maturity of the Safety Case and the intended readership. It has two functions:

1. To assure that safety risks are being managed effectively, so it should include a clear and concise summary of the Safety Case and safety progress;
2. To highlight key areas of risk to the operators and users, so it should provide information that will support operational decision-making, such as a decision to operate outside the design envelope.

The SEC Report should contain meaningful information and be as concise as possible, without sacrificing the need to provide the necessary information. References should be provided to supporting material within the Safety Case. It should be structured as follows:

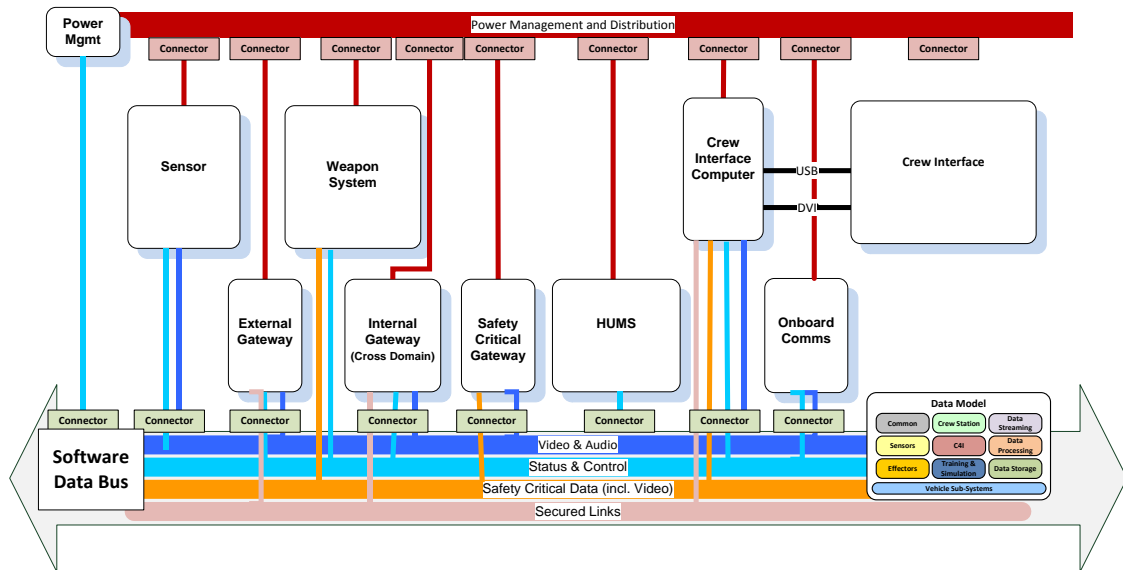
1. Executive Summary;
2. Summary of System Description;
3. Assumptions;
4. Progress against the Program;
5. Meeting safety requirements;
6. Emergency/Contingency Arrangements;
7. Operational Information;
8. Independent Safety Auditor (ISA) Report;
9. Environmental report;
10. Conclusions and Recommendations;
11. References.

CHAPTER 11	NGVA SPECIFIC SAFETY CONSIDERATIONS
-------------------	--

The adoption of NGVA will provide a common open vehicle platform electronic architecture. This enables the integration of vehicle sub-systems from diverse suppliers/manufacturers. The integration and interoperation of these sub-systems may also provide safety-critical functions for the vehicle platform.

To ensure safe system operations across the NGVA architecture and efficient provision of these safety-critical functions, the system integrator which is responsible for the overall vehicle safety must ensure that a methodical approach to safety is followed:

1. Architecture - develop a concept of the overall system architecture and consider:
 - a. Modularity and interchangeability – consider the platform concept, its role and intended future use. If it has not yet been defined consider what else it could be used for in future. If changes are frequent what additional platform configuration tasks could be required?
 - b. Future enhancements – what mission system could you expect to install on the platform in future .i.e. HUMS, HMI or RWS. These share physical resources.
 - c. Non-deterministic, deterministic and safety-critical data. This will lead to the selection of suitable technologies which provide the required systematic capabilities. Typical such capabilities are real-time performance and deterministic behaviour in terms of latency/jitter of data transmission. If these are not provided by standard Ethernet and DDS then technology enhancements have to be considered. Middleware (software data bus) can provide an information backbone between the different subsystems using the underlying (Ethernet) network.
 - d. Robust partitioning of resources.
 - e. Testability – consider how to verify and validate different configurations and then future changes.



2. Dedicated safety management based on the generic guidelines presented in CHAPTERS 1-10.
3. Allow for modular safety cases wherever feasible:
 - a. Ensure non-dependence of individual safety-cases so that one function does not interfere with the other in terms of resources (including data and power infrastructure), real-time behaviour or random failures and therefore safety.
 - b. This objective is supported by robust partitioning of resources between functions which may have a shared access to NGVA data. It allows in due course the replacement of one sub-system by another providing the same or less functions or the integration of new safety-critical functions without compromising the overall safety case.
 - c. Ensure strict configuration control.
4. Manage overall safety margins with respect to:
 - a. Data bandwidth.
 - b. Power consumption.
 - c. Diagnostic coverage and sub-system failure rates. It is highly recommended to use fault containment so that faults do not propagate within the data network. Fault containment and decoupling should be a requirement for central data network elements like switches.
 - d. Redundancy is required where single faults are not tolerable.
 - e. Safety margins for individual functions have to be defined and effectively communicated to the sub-system providers.

5. Allow for a trade-off between system availability and safety for exceptional cases where the safety of the crew may be safeguarded more effectively by the availability of one or more sub-systems (for example an active protection system) as opposed to the overall E/E system safety.
6. Full life-cycle support – consider how new safety information may develop across the whole life of the platform and how that could be shared between NATO partners:
 - a. Failure modes, effects and criticality analysis (FMECA) – how do the vehicle platform stakeholders capture and share information on the platform configuration and safety performance?
 - b. Lessons identified – What observations and measurements have you made as you change sub-systems in the architecture. What effects do specific sub-systems from specific manufacturers make to data and power performance? What works well together, what does not. How where integration issues overcome.
 - c. Emergent properties – what unexpected properties have been observed through the performance of platform sub-system configurations?

INTENTIONALLY BLANK

ANNEX A ABBREVIATIONS

ACoP	Approved Code of Practice
ALARP	As Low As Reasonably Practicable
CAE	Claims Arguments Evidence
CBA	Cost Benefit Analysis
COTS	Commercial Off The Shelf
CR	Compulsory Requirement
DDS	Data Distribution Service
DM	Data Model
FMEA	Failure Modes Effects and Criticality Analysis
FTA	Fault Tree Analysis
GSN	Goal Structuring Notation
GVA	Generic Vehicle Architecture
HMI	Human Machine Interface
HSE	Health and Safety Executive
HUMS	Health and Usage Monitoring System
IAWG	Industrial Avionics Working Group
IOC	Initial Operating Capability
ISA	Independent Safety Auditor
ISO	International Standards Organization
MILVA	Military Vehicle Association
MOD	Ministry of Defense
MOTS	Military Off-The-Shelf
NAAG	National Army Armament Group
NATO	North Atlantic Treaty Organization
NGVA	NATO Generic Vehicle Architecture
NSA	NATO Standardization Authority
NSO	NATO Standardization Office
OE	Optional Enhancement
PE	Platform Equipment
PHI	Preliminary Hazard Identification
PM	Project Manager
SEC	Safety and Environmental Case
SIL	System Integrity Level
SS	System Specific
WAN	Wide Area Network

INTENTIONALLY BLANK

ANNEX B TOOLS RELATED TO SAFETY CASE

B.1. SAFETY CASE EDITORS

A number of tools are available to support the construction of safety cases using GSN. The website of the Goal Structuring Notation Working Group provides a list of known tools.

AEP-4754(A)(1)
VOL VI