NATO STANDARD

AEP-4754

NATO GENERIC VEHICLE ARCHITECTURE (NGVA) FOR LAND SYSTEMS

VOLUME VI: SAFETY

Edition B Version 1
FEBRUARY 2023

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

3 February 2023

1. The enclosed Allied Engineering Publication AEP-4754, Volume VI, Edition B, 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 (AC/225 NAAG), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4754.

2. AEP-4754, Volume VI, Edition B, Version 1 is effective upon receipt and supersedes AEP-4754, Volume VI, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

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

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

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

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

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

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]

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

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-systems, 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 by 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 1 through 7.

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) approach used to produce the NGVA DM, the delivery and change management processes and finally gives implementation and deployment guidance)
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 automotive 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 as normative. Documents and publications are grouped and listed in alpha-numeric order:

1. AAP-03	PRODUCTION, MAINTENANCE AND MANAGEMENT OF NATO STANDARDIZATION DOCUMENTS - Edition J Version 2 – NOVEMBER 2011
2. IAWG-AJT-301	System of System certification (related to avionic)
3. IEC 61508:2010	Functional Safety of Electronic Equipment
4. ISO 26262:2018	Road vehicles – Functional safety
5. JSP 454	Land Systems Safety and Environmental Protection Part 2
6. MIL-STD-882E	US DoD, System Safety
7. Def Stan 00-56: Part 1, 28-02-2017	United Kingdom MOD, Safety Management Requirements for Defence Systems Part 1: Requirements
8. IBM – Open Architecture	Technical Principles and Guidelines 1.5.8
9. RTCA DO-297, 08-11-2005	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

Table 1: Normative References

Reference to NGVA Data Model implementation-related standards, e.g. OMG standard versions, will be included in the Reference Model Delivery Package.

Reference in NGVA Standard AEP-4754 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 2.5. 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 NGVA 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 NGVA 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. **Crew Terminal**: An electronic hardware device that is used for entering data into and presenting visual and audio data from the NGVA Data Infrastructure connected to the Base Vehicle and all its Mission Sub-Systems.

4. **Electronic Architecture**: The combination of the electronic based sub-systems and electronic infrastructure that supports the vehicle crew to undertake their operational tasks.
5. **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.
6. **Mission Sub-System:** Separable elements or collections of equipment or software added to a Vehicle Platform that provides operationally required capabilities over and above those delivered by the base vehicle.
7. **Modular**: A modular (Electronic) Architecture is designed in such a way as to allow the replacement or addition of Mission Sub-Systems and upgrades as required without any undesirable emerging properties.
8. **NGVA Compliant:** NGVA Compliance applies to the whole Vehicle Platform and all added Mission Sub-Systems and means that the Electronic Architecture of the Vehicle Platform complies with the requirements defined in NGVA Standard AEP-4754.
9. **NGVA Data 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.
10. **NGVA Power Infrastructure:** The physical cables, connectors and other components that provide the means of distributing and controlling electrical power around a Base Vehicle.
11. **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" vehicle Electronic Architecture. This would mean passing an incremental process with two sequentially-related Compatibility levels:
    a. **Connectivity Compatibility**: Ensures that the (sub-) system can be physically connected to the NGVA Power and Data Infrastructure without any negative impacts to existing NGVA (sub-) systems. Physical power and network interfaces comply with the requirements of Power and Data Infrastructure AEPs.
    b. **Communication Compatibility**: Connectivity Readiness and data interfaces (DDS/PLEVID) with associated NGVA Data Model implementation that comply with the requirements of Data Model and Data Infrastructure AEPs.
12. **Operator:** Any person required to monitor and control vehicle sub-systems.
13. **Power Management:** The means of prioritizing and controlling the electrical power loads throughout the Vehicle Platform.
14. **Scalable**: The trait of a system in being able to scale in order to handle increased loads of work.
15. **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.
16. **Vehicle Crew:** All personnel located in the Vehicle Platform with defined roles needed to fulfil the necessary operational functions.

17. **Vehicle Platform**: The platform for the Mission Sub-Systems, which comprises all Base Vehicle Sub-Systems, the NGVA Power and Data Infrastructure and all common sub-systems, such as; crew terminals, processing units and other common platform resources (e.g. sighting systems).

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 defence capability as well as financial or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction [Def Stan 00-56].
2. **Audit**: An examination of implemented process.
3. **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 effects of 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].
9. **Hazard Identification:** The process of identifying and listing the hazards and accidents associated with a system [Def Stan 00-56].
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].
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].
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].
14. **Mode:** A designated system condition or status (e.g., maintenance, test, operation, storage, transport, and demilitarization) [MIL-STD-882E].
15. **Reconfiguration:** is a modification of a NGVA system based on pre-defined and certified configuration options. Reconfiguration does not include an update or enhancement of a NGVA system.
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].

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].
19. **Risk Estimation**: The systematic use of available information to estimate risk [Def Stan 00-56].
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]..
22. **Risk Reduction**: The systematic process of reducing risk [Def Stan 00-56].
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].
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].
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).
27. **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].
28. **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
29. **Safety Integrity Level:** A classification of the required level of safety integrity defining the processes that must be applied to the development of system.
30. **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].
31. **Survivability:** Ability of a system to fulfil its mission in a timely manner in presence of attacks, failures, or accidents.
32. **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.
33. **System Failure**: A system failure occurs when the system fails to perform its required function.
34. **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].

35. **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].

CHAPTER 3 NATO GENERIC VEHICLE ARCHITECTURE SYSTEM SAFETY

3.1. NGVA System Safety Introduction

This AEP-4754-Volume VI provides guidance to design safety in systems aligned to the fundamental concepts of NGVA in terms of modularity and openness. The document can be applied to the entire vehicle platform or a vehicle sub system, current and future. The guidelines and requirements specified in this AEP-4754-Volume VI are based on existing, industry wide, open standards and practices.

Specifying guidelines and safety related requirements forms the basis of modular platform architectures capable of safety certification. It allows standardizing aspects of certification throughout NGVA member nations enabling cost savings. For example, safety case modules for NGVA ready sub systems could be provided by NGVA member nations and having specified guidelines on system safety and certification allows cost savings in terms of vehicle reconfiguration and recertification.

This AEP-4754-Volume VI is divided into two sections:

Section 1 in chapter 3 refers specifically to the modularity and openness of NGVA approach to safety and includes:

- Introduction to the concept of modular safety cases;
- Outlines the generic procedures to incorporate modular safety within the system lifecycle phases such as:
    - Concept;
    - Realization;
    - In-service;
    - Upgrade/enhancement;
    - Decommissioning.
- Requirements for the different lifecycle phases related but not limited to:
    - Organization, approach, and planning;
    - System safety programme planning;
    - Risk acceptance;
    - Configuration management;
    - Human factors;
    - Integration.

Section 2 in chapter 4 offers direct correlation of the NGVA modular system safety concept presented in this AEP Volume to the rest of the AEP Volumes. Thus, this section will present considerations and highlights potential safety issues within the NGVA Architecture, Power and Data Infrastructure, Crew Terminal Software Architecture, Data Model, and associated Verification and Validation approach.

3.2. Introduction to the concept of modular safety cases

3.2.1. Safety Cases Fundamental Concepts

Safety case is a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment. Implementation of safety cases for a system requires certain set of actions. These actions are as follows:

- Distinct set of claims about the system
- Production of supporting evidence
- A safety argument linking the claims about the system and the produced evidence
- Clarity of assumptions and judgements underlying the arguments.
- Different viewpoints and levels of detail.

Safety cases are one of the most well-established types of cases used for assurance of claims. Traditionally, safety cases dealt with monolithic, non-reconfigurable systems that made a single claim such as “the system is acceptably safe”. This monolithic single-attribute case is one in which only one aspect of the system is in focus, i.e. its top-level claim concerns only safety. It may be decomposed to the characteristics of the system (and its component) availability, reliability and performance. This should only be done when they impact/support the top-level claim. Furthermore, the concept of safety case has been expanded to cover a variety of domains such as security, dependability, reliability, etc.

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. Adopted from avionics, important aspects of this definition are the following:

- **Argument**: It is used to demonstrate how someone can reasonably conclude that a system is acceptably safe from the evidence available.
- **Clear**: A safety case is a device for communicating ideas and information, usually to a third (e.g. a regulator) party. In order to do this convincingly, it must be as clear as possible.
- **System**: The system to which a safety case refers can be anything from a network of pipes or a software configuration to a set of operating procedures. The concept is not limited to the consideration of conventional engineering design.
- **Acceptably**: Absolute safety is an unobtainable goal. Safety cases are there to convince that the system is safe enough (when compared against some definition or notion of tolerable risk).
- **Context**: context-free safety is impossible to argue. Almost any system can be unsafe if used in an inappropriate or unexpected manner. (Consider arguing the safety of a conventional house-brick.).

In general, a safety case can be considered as consisting of the following four elements. These are:

- **Objectives** – the safety requirements that must be addressed to assure safety
- **Argument** – showing how the evidence indicates compliance with the requirements
- **Evidence** – information from study, analysis and test of the system in question
- **Context** – identifying the basis of the argument presented

3.2.2. Safety Cases Fundamental Concepts

Modular safety cases (MSC) provide a means of organising large and/or complex safety cases into separate but interrelated component modules of argument and evidence. They can offer potential benefits of improved flexibility in function allocation, reduced development costs and improved maintainability. However, it poses significant considerations in certification. The traditional approach to certification relies heavily upon a system being statically defined as a complete entity and the corresponding (bespoke) system safety case being constructed. Nevertheless, a principal motivation behind MSC is that there is through-life (and potentially run-time) flexibility in the system configuration. A MSC system can support many possible mappings of the functionality required to the underlying digital platform.

A MSC attempts to establish a modular, compositional, approach to constructing safety arguments that has a correspondence with the structure of the underlying system architecture. However, to create such arguments it requires a system architecture that has been designed with explicit consideration of enabling properties such as independence (e.g. including both non-interference and location ‘transparency’), increased flexibility in functional integration, and low coupling between components ie an interoperable open and modular architecture. An additional issue is that these properties are non-orthogonal and trade-offs must be made when defining the architecture.

The key feature of the modular approach to safety assessment is that the structure of the safety case reflects the modular architecture of the vehicle platform. Furthermore, to address the desire for a reconfigurable system, it is postulated that a monolithic case is inadequate, because it must be re-evaluated following any change to the system configuration or its operational environment. A key conclusion and resulting benefit is that a modular argument allows the size of a change to the argument to be proportional to the size of the change to the system.

3.2.3. Safety Cases Modules

Defining a safety case ‘module’ involves defining the objectives, evidence, argument and context associated with one aspect of the safety case. Assuming a top-down progression of objectives-argument-evidence, safety cases can be partitioned into modules both horizontally and vertically:

- **Vertical (Hierarchical) Partitioning** - The claims of one safety argument can be thought of as objectives for another. For example, the claims regarding software safety made within a system safety case can serve as the objectives of the software safety case.
- **Horizontal Partitioning** - One argument can provide the assumed context of another. For example, the argument that “All system hazards have been identified” can be the assumed context of an argument that “All identified system hazards have been sufficiently mitigated”.

In defining a safety case module, it is essential to identify the ways in which the safety case module depends upon the arguments, evidence or assumed context of other modules. A safety case module should therefore be defined by the following interface:

1. Objectives addressed by the module;
2. Evidence presented within the module;
3. Context defined within the module;
4. Arguments requiring support from other modules;

Inter-module dependencies:

5. Reliance on objectives addressed elsewhere;
6. Reliance on evidence presented elsewhere;
7. Reliance on context defined elsewhere.

The principal need for having such well-defined interfaces for each safety case module arises from being able to ensure that modules are being used consistently and correctly in their target application context (i.e. when composed with other modules).

Figure 2 presents a simple example where two different crew stations (M1 and M2) are designed to fit a platform (base vehicle M3). C1 and C2 are in essence the interfaces or as explained in the paragraphs below the ‘Contract’ between the Crew Stations and the Base Vehicle. The standard interface where each of M1 and M2 Crew Stations is to adhere to is the M3 side of the C1 and C2 Contracts. Hence, when M1 Crew Station is to be replaced by M2, then only M2 is required to be verified against the C2 contract for Certification.

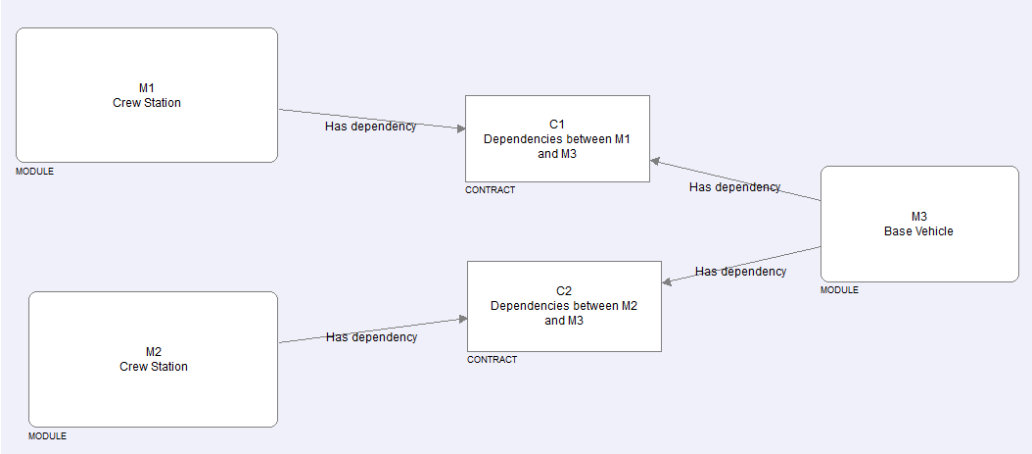

Figure 2: Example for system safety case modules

3.2.4. Safety Case Module Composition

Safety case modules can be usefully composed if their objectives and arguments complement each other – i.e. one or more of the objectives supported by a module match one or more of the arguments requiring support in the other. For example, the software safety argument is usefully composed with the system safety argument if the software argument supports one or more of objectives set by the system argument. At the same time, an important side-condition is that the collective evidence and assumed context of one module is consistent with that presented in the other. For example, an operational usage context assumed within the software safety argument must be consistent with that put forward within the system level argument.

The definition of safety case module interfaces and satisfaction of conditions across interfaces upon composition is analogous to the long established rely-guarantee approach to specifying the behaviour of software modules. For a safety case module, the rely-guarantee conditions can be thought of as items 4 to 7 (from section Safety Case Modules) of the interface, whilst item 1 (objectives addressed) defines the guarantee conditions. Items 2 (evidence presented) and 3 (context defined) must continue to hold (i.e. not be contradicted by inconsistent evidence or context) during composition of modules.

The defined context of one module may also conflict with the evidence presented in another. There may also simply be a problem of consistency between the system models defined within multiple modules. For example, assuming a conventional system safety argument / software safety argument consistency must be assured between the state machine model of the software (which, in addition to modelling the internal state changes of the software will almost inevitably model the external – system – triggers to state changes) and the system level view of the external stimuli. As with checking the consistency of safety analyses, the problem of checking the consistency of multiple, diversely represented, models is also a significant challenge in its own right.

3.2.5. The Challenge of Compositionality

It is widely recognised that relatively low risks are posed by independent component failures in safety-critical systems. However, it is not expected that in a safety case architecture where modules are defined to correspond with a modular system structure that a complete, comprehensive and defensible argument can be achieved by merely composing the arguments of safety for individual system modules. Safety is a whole system, rather than a ‘sum of parts’, property. Combination of effects and emergent behaviour must be additionally addressed within the overall safety case architecture (i.e. within their own modules of the safety case). Modularity in reasoning should not be confused with modularity (and assumed independence) in system behaviour.

3.2.6. Safety Case Module ‘Contracts’

Where a successful match (composition) can be made of two or more modules, a contract should be recorded of the agreed relationship between the modules. This contract aids in assessing whether the relationship continues to hold and the (combined) argument continues to be sustained if at a later stage one of the argument modules is modified or a replacement module substituted. This is a commonplace

approach in component-based software engineering where contracts are drawn up of the services a software component requires of, and provides to, its peer components, e.g. as in Meyer's Eiffel contracts.

In software component contracts, if a component continues to fulfil its side of the contract with its peer components (regardless of internal component implementation detail or change) the overall system functionality is expected to be maintained. Similarly, contracts between safety case modules allow the overall argument to be sustained whilst the internal details of module arguments (including use of evidence) are changed or entirely substituted for alternative arguments provided that the guarantees of the module contract continue to be upheld.

Safety Case Module Contract			
Participant Modules (e.g. Modules A, B, C, etc.)			
Goals matched between Participating Modules			
Goal	Required By	Addressed By	Goal
(e.g. Goal 1)	(e.g. Module A)	(e.g. Module B)	(e.g. Goal 2)
Collective Context and Evidence to be held Consistent between Participating Modules			
Context		*Evidence*	
(e.g. Context C1, Assumption A2, etc.)		(e.g. Sn1, Sn3, etc.)	
Resolved away Goal, Context and Solution References between Participating Modules			
Cross-Referenced Item	*Source Module*	*Sink Module*	
(e.g. Away Goal AG3)	(e.g. Module B)	(e.g. Module A)	

Figure 3: Safety Case Module Contract

3.2.7. Safety Case Architecture

Safety case architecture can be defined as the high-level organisation of the safety case into modules of argument and the interdependencies that exist between them. In deciding upon the partitioning of the safety case, many of the same principles apply as for system architecture definition, for example:

- **High Cohesion / Low Coupling** – each safety case module should address a logically cohesive set of objectives and (to improve maintainability) should minimise the amount of cross-referencing to, and dependency on, other modules.
- **Supporting Work Division & Contractual Boundaries** – module boundaries should be defined to correspond with the division of labour and organisational /

contractual boundaries such that interfaces and responsibilities are clearly identified and documented.

- **Isolating Change** – arguments that are expected to change (e.g. when making anticipated additions to system functionality) should ideally be located in modules separate from those modules where change to the argument is less likely (e.g. safety arguments concerning operating system integrity).

The principal aim in attempting to adopt a modular safety case architecture for NGVA-based systems is for the modular structure of the safety case to correspond as far as is possible with the modular partitioning of the system and its sub-systems.

3.3. System Safety considerations for modular systems

The NGVA basic principles of a open modular architecture, as describes in Volume I of this AEP, induce a change from today's system safety approach in the defence sector. Although the principles applied for system safety are also valid for a NGVA system development, some additional NGVA specific requirements need to be considered.

To ensure that the modular approach of the NGVA can be implemented in a (sub-) system development, this approach also needs to be applied to the system safety considerations.

To be able to ensure a modular approach to system safety the following issues shall be considered:

- The modular approach will promote a more distributed development of NGVA Systems, with the result that the number of stakeholders in a project will increase. Therefore, appropriate procedures to ensure information flow, interchange of requirements between the system/subsystem level and contractor/subcontractor management, shall be implemented in the project organisation of a distributed NGVA system development.
- Safety relevant functions and non-safety relevant functions should be segregated, to ensure that possible future updates of the NGVA system (e.g. software update of the crew terminal) in the in-service phase, do not result in a safety relevant system modification.
- The reconfiguration of an existing NGVA system in the in-service phase is a new concept in the defence industry and should be considered in particular for its safety implications.

The following subclauses will take these issues under consideration and define specific requirements for a modular system safety approach.

3.3.1. Introduction to the meta-lifecycle

The meta-lifecycle describes a basic life cycle model, which can be applied to any safety related system development, regardless of the specific safety standard applied to the development activities. Applying the meta-lifecycle to the safety considerations for NGVA (sub-) systems allows for specifying requirements and

considerations for each lifecycle phase. It also provides the means to consolidate different safety approaches, and life cycle models from different safety standards, in an overall “NGVA system safety program”.

For each meta lifecycle phases safety requirements from applicable industry wide, open standards and practices shall be tailored to the NGVA (sub-) system development activities.

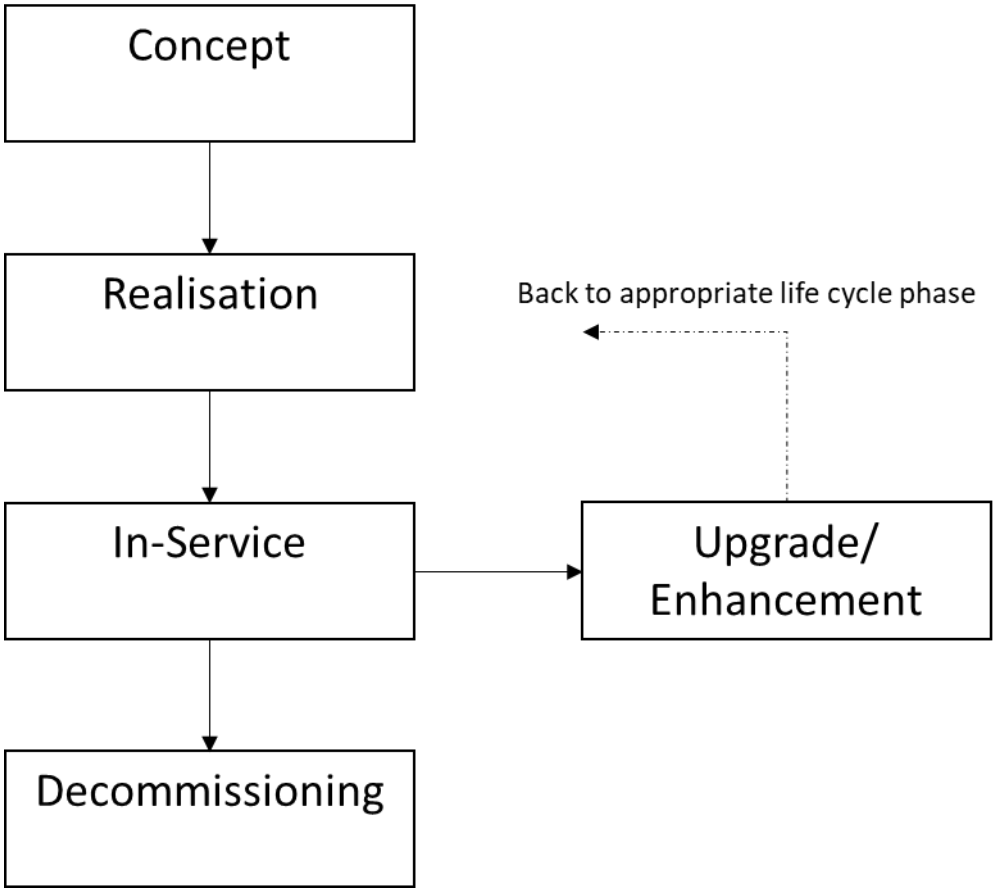

Figure 4: meta lifecycle

Note:

The following requirements defined in the meta-lifecycle are relevant on system level and are not necessarily intended to be used on module level.

3.3.1.1. Concept Phase

The concept phase of the meta-lifecycle includes all the activities with regards to planning the relevant safety activities (incl. verification planning), definition of (sub-) system boundaries, safety analysis and the definition of safety requirements on system level as well as safety requirements for sub-systems.

To ensure an appropriate system safety approach for a NGVA (sub-) system development, the modular concept of NGVA shall be considered. Therefore, the information flow, the overall requirements management, the overall configuration management, the acceptance criteria and the contactor/sub-contractor relationship shall be defined in the beginning of the NGVA (sub-) system development.

Table 2 lists the NGVA specific requirements for the concept phase.

Unique ID	Requirement Type	Requirement Text
Reference Model Delivery Package		
NGVA_SAF_CP1	CR	For each phase of the meta-LC as described in AEP-4754-Volume VI, NGVA specific safety requirements shall be defined (please also refer to chapter 4 and the other Volumes of this AEP).
NGVA_SAF_CP2	CR	It shall be demonstrated, that the applied safety standard (e.g. ISO26262/IEC61508/…) meets the NGVA specific requirements.
NGVA_SAF_CP3	CR	An appropriate system safety standard (e.g. DEF-STAN 00-56, MIL-STD 882E) shall be applied to any NGVA (sub-) system development activities
NGVA_SAF_CP4	CR	An appropriate configuration management process (e.g. according to ISO 10007) shall be applied for any NGVA (sub-) System development. *NOTE:* *Also refer to other standards (e.g. ISO 262626/IEC 61508) for further requirements.*
NGVA_SAF_CP5	CR	An appropriate requirements management process (e.g. according to ISO 12207) shall be applied for any NGVA (sub-) System development. *NOTE:* *Also refer to other standards (e.g. ISO 262626/IEC 61508) for further requirements.*
NGVA_SAF_CP6	CR	The intended use and the environment for the NGVA (sub-) System shall be defined for all possible NGVA-System configurations
NGVA_SAF_CP7	CR	The NGVA-(sub-) System boundaries shall be defined and agreed upon by all relevant stakeholders

		for all possible system configurations (e.g. acc. to ISO 15288).
NGVA_SAF_CP8	CR	A contractor (system integrator)/ subcontractor (sub-system development) management shall be defined and agreed upon by all relevant stakeholders for all possible system configurations (for examples please refer to ISO26262).
NGVA_SAF_CP9	CR	A procedure shall be defined how hazards and associated risks are formally accepted by the appropriate risk acceptance authority.
NGVA_SAF_CP10	CR	An overall safety concept shall be developed by the main- contractor (system integrator). The overall safety concept shall include all possible configurations on system level. Safety requirements for NGVA sub-systems shall be specified by the overall safety concept on NGVA system level.
NGVA_SAF_CP11	CR	The modular safety case approach shall be applied to any NGVA (sub-) System development.
NGVA_SAF_CP12	CR	NGVA Sub-system safety requirements shall be refined by sub-system developer and agreed by system developer.
NGVA_SAF_CP13	CR	A safety verification plan shall be developed by NGVA System developer for all possible system configurations.
NGVA_SAF_CP14	CR	NGVA system developer shall derive requirements from the safety verification plan and allocate these requirements to the NGVA sub-system level for all possible system configurations.
NGVA_SAF_CP15	CR	NGVA relevant ILS information and requirements shall be defined (e.g. mounting/dismounting of mission specific equipment).
NGVA_SAF_CP16	CR	Safety Assessments for NGVA sub-systems shall be planned and agreed with sub-system developer (please also refer to NGVA_SAF_CP8)
NGVA_SAF_CP17	CR	Human factors considerations shall be observed for the overall safety concept.
NGVA_SAF_CP18	CR	Human-Machine interfaces shall be developed in accordance to appropriate standards or nation specific guidelines.

Table 2: Requirements from concept phase

Note:
The safety requirements specified by AEP-4754-Volume VI only cover the NGVA specific requirements. For compliance with regulations and laws applicable industry wide, open standards and practices shall be considered for the development activities.

3.3.1.2. Realisation phase

The realisation phase of the meta-lifecycle includes the design of the system in accordance to the requirements developed in the concept phase, as well as the validation and tests as defined by the verification plan (see NGVA_SAF_CP13). The realisation phase concludes with the finalisation of the modular safety case and the delivery into service.

Appropriate safety standards for the realisation phase of the NGVA (sub-) system shall be applied (as defined by requirements NGVA_SAF_CP2 and NGVA_SAF_CP3).

3.3.1.3. In-service phase

The in-service phase addresses three sub-phases which only in part include NGVA specific requirements. The three sub-phases are as follows

a) Usage
b) Maintenance
c) Reconfiguration

For sub-phases a) and b) no NGVA specific requirements are defined. Please refer to applicable safety standards to address these sub-phases in an appropriate way.

Reconfiguration:

The reconfiguration of an existing in-service system is an NGVA specific benefit of an open and modular system architecture. It is not defined as a modification of the NGVA (sub-) system. As this option is not available in today's existing non-NGVA systems, an appropriate safety approach is defined by this AEP.

The following table describes the NGVA specific safety requirements for the reconfiguration of an in-service NGVA system.

Unique ID	Requirement Type	Requirement Text
Reference Model Delivery Package		
NGVA_SAF_IS1	CR	A reconfiguration (e.g. mission equipment) of a in-service NGVA system shall only be performed within the scope of NGVA system configurations given by the safety statement of the NGVA system.
NGVA_SAF_IS2	CR	A safe mode of operation, for reconfiguring the NGVA system, shall be incorporated by the system developer.
NGVA_SAF_IS3	CR	Procedures, test steps, manual configuration identification, interface tests or any other safety relevant measures, as defined by the NGVA system safety concept, shall be defined by the NGVA system developer and are to be observed by in-service personnel at all times.
NGVA_SAF_IS4	CR	The minimum level of staff training, to perform safety relevant tasks when reconfiguring the NGVA system, shall be defined by the NGVA system developer and agreed with the in-service representative.
NGVA_SAF_IS5	CR	A restriction of access to reconfiguration relevant functions and data shall be incorporated by the system developer, in accordance to recommended practices for security from the procuring nation.

Table 3: Requirements from in-service phase

3.3.1.4. De-commissioning phase

Standard procedures shall be applied. Please refer to appropriate standards (e.g. IEC 61508:2010).

3.3.1.5. Upgrade/Enhancement

The upgrade/enhancement phase includes modifications on the NGVA (Sub-) System configuration options. Standard procedures shall be applied. Please refer to appropriate standards (e.g. IEC 61508:2010)

CHAPTER 4 GUIDANCE FOR THE APPLICATION OF MODULAR SAFETY

This chapter provides guidance for applying safety related requirements from this AEP-4754-Volume VI to NGVA (sub-) system development activities, as well as guidance for applying industry wide, open standards and practices to modular system development.

4.1. Application of the modular safety case considerations

As detailed in section 3.1.1, traditional safety cases dealt with monolithic, non-reconfigurable systems that made a single claim such as “the system is acceptably safe”. Essentially, a component or a system is looked upon as a ‘black box’ that as soon as it is connected to ‘something’ (eg a component to a system, or a system to power) then the safety case should provide the evidence that it is tolerably safe. To do that the component and the system have to be finalised and implemented before a safety case is to be developed. Hence, the safety case structure is organised according to the analysis used to provide evidence to support the claims made, in this situation, for a military land platform with no clear distinction between the arguments and evidence concerning different subsystems and components. Thus, when this analysis cuts across several subsystems, composed of various components, then a small change even to a single component would require the need to repeat the original analysis resulting to increased costs and complexity of the recertification process.

The modular approach presented here entails breaking down the safety case into modules corresponding to the modular architecture of the vehicle. Essentially the modular safety case is developed and applied in parallel and at the same time as the vehicle system architecture with standard interfaces (hardware and software) reflecting on the system, sub-systems and individual components (hardware and software) referred to as modules. Therefore, developing or updating a module (component/ sub-system/ system) implies that the safety case can be largely developed as a ‘black box’ in monolithic safety cases even before the module is connected to ‘something’. In this case, the ‘black box’ is the module itself and the connection are the standard interfaces with their requirements as published in STANAG 4754.

In general, as the safety case size increases, so does the complexity. In almost every way, safety cases for large systems (especially military vehicle systems) are inherently more difficult to design, build, and manage than for smaller systems. The evolution of vehicle system architectures encourages ongoing changes so that vehicle capabilities can be enhanced as and when technology is able to do so (eg high definition video distribution with real time image analysis for local situation awareness). However, these changes also affect the safety case and changes breed complexity that has to be managed. The modular approach provides a way of addressing this problem but the granularity in defining within the vehicle system architecture the safety case modules is highly important. The more modules (black boxes) implies the more interfaces (connections) and therefore the probability of failure increases. Hence, there has to be a balance between modularity and granularity to the point where the safety tolerance is not compromised.

For example, if a component (e.g. a camera or image processing algorithm) in a single network video distribution subsystem is to be replaced by a better similar functional component then the safety case of the whole subsystem should be updated. However, if the video distribution network is segmented (e.g. multiple instances for different types of video distribution such as target acquisition, storage, processing etc) to enhance its performance, the safety case architecture design should consider the complexity of producing the safety case for each of the segments or the level of the capability as a subsystem.

4.2. Safety consideration for applying the other AEP- 4754 Volumes

4.2.1. Volume I: Architecture

The complexity of future military land vehicles and addition of in-service upgrades through incremental technology development, insertion and rapid role change requires vehicle safety cases to be re-assessed and re-issued. The need for rapid response to Urgent Operational Requirements (UOR) is an additional challenge. The costs for re-assessing and re-issuing safety cases for these systems are high. This is because traditional safety cases are monolithic and to some extent current modular safety case approaches are too tightly coupled. Therefore, changes to platform systems require that the safety case be developed from scratch; hence, incurring huge cost and extended maintenance and recertification time, which eventually affect platform availability for any contingency plans.

Modularity involves breaking a large safety case into separate physical/logical entities that ultimately makes the overall safety case easier to comprehend. By understanding the behaviour of a module, it is easier to identify and assess the ramification of change. This gives rise to a number of potential advantages.

Firstly, although the initial development cost of modular safety cases are higher because of the additional effort, this cost is quickly recovered within the vehicle lifetime. Indeed, the cost associated with recertifying the system after an upgrade or role change/rapid reconfiguration process, is greatly reduced due to the intrinsic reusability nature of modular safety cases. This is quite significant because military land platforms can have long lifespan. Thus, the adoption of the modular approach would offer a significant reduction in maintenance costs.

Secondly, the modular structure minimises the impact of inter-dependencies associated with conventional monolithic safety case construction.

Thirdly, the approach supports the mandates of the NATO Generic Vehicle Architecture (NGVA) requiring all military land platforms to possess safety cases that support the optimisation of fleet inventory, permit rapid role change, and the implementation of in-service upgrades. Hence, modular safety cases are seen as a key enabler if the full benefits of NGVA are to be realised.

The potential benefits from adopting Modular Safety Cases methodology in the design and development military vectronics architectures include:

- Platform availability through rapid recertification: The approach allows safety case modules to be replaced without requiring modifications to the entire safety case of the platform when the vehicle undergoes role change thus enabling rapid recertification and maintaining platform availability for any eventuality.
- Upgradability: A legacy platform can undergo a sub-system upgrade, thus requiring the safety case to be modified. The approach allows safety case modules to be extended or completely replaced to suit the upgrade and aid in recertification
- Costs: The approach promises through life cost savings during system integration, re-certification. The dependencies between modules are identified and hence known when modules are replaced.
- International Interoperability: The approach is a key enabler for NATO GVA STANAG 4754 by incorporating modular safety cases within the equipment life cycle right from the start of the development process.

The benefits of modular safety cases are genuinely achieved when the safety case life cycle is carried out in parallel with the design life cycle. This allows identifying dependencies between safety case modules early on in the life cycle. The modular nature of the platform/system architecture plays a vital role in gaining cost and time benefits during reconfiguration and role change. Thus, system integrators, sub-system contractors must strictly adhere to the NGVA requirements, which are based on the concepts of modularity, openness, scalability to achieve the same benefits in the certification/re-certification process. Figure 5 attempts to illustrate the link between safety case development and system development.

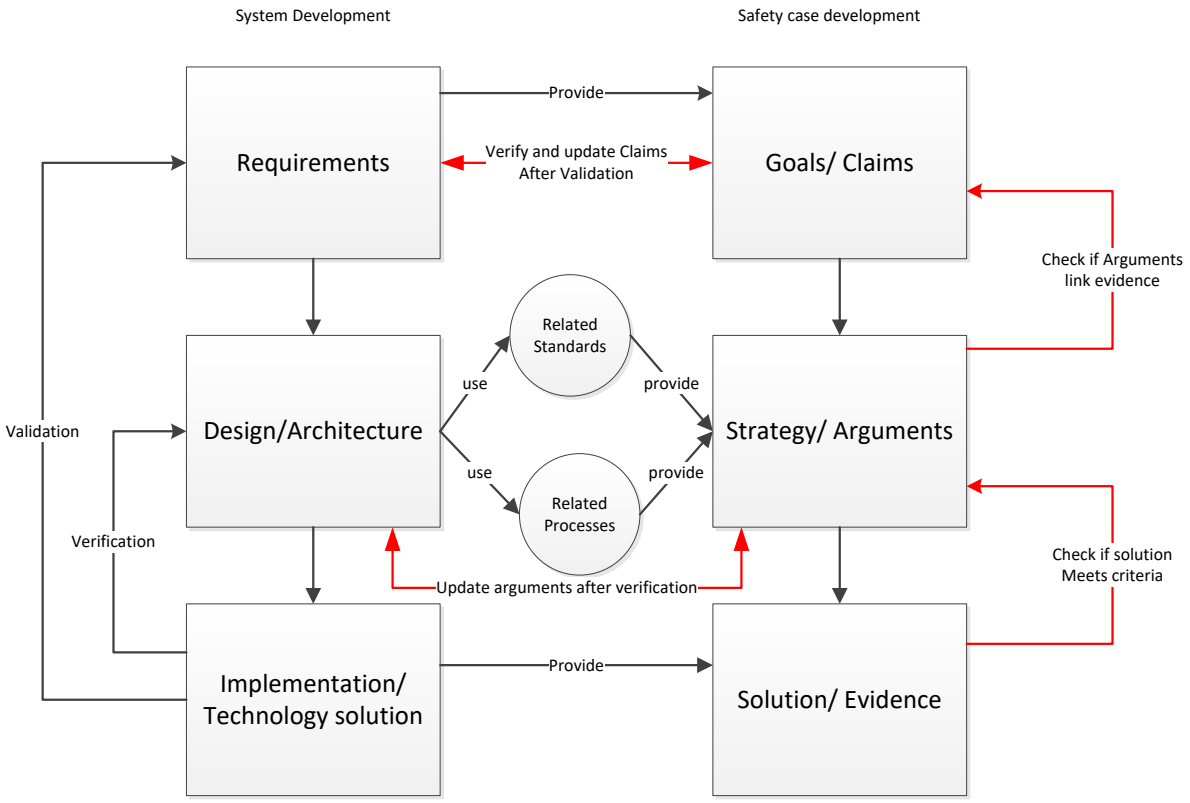

Figure 5: Link between safety case and system development

4.2.2. Volume II: Power

No NGVA specific requirements are to be considered, other than already listed in Volume II of this AEP.

Topics to be included:

- Draft of Volume II (Safety related information to be included in Volume VI)
- Identify DELTAs which are not covered by the Vol.2 Draft
- Reference to EN 13849-2
- Power Management Issues

4.2.3. Volume III: Data Infrastructure

To ensure the open and modular approach of the NGVA, safety relevant data needs to be considered when planning and designing an NGVA (sub-) System. Otherwise modularity of NGVA (sub-) Systems may be severely limited.

Safety critical systems require reliable and deterministic behaviours in their communication operations, therefore the following safety goals shall be considered for the safety relevant communication within the NGVA network topology:

- Prevent unnoticed repetition of messages
- Prevent unnoticed loss of messages
- Prevent unnoticed message insertion
- Prevent unnoticed data corruption
- Prevent unnoticed delay of messages
- Prevent unnoticed masqueraded messages

The safety goals listed above describe basic principles of safe communication but are not necessarily definitive. As defining a technical solution is not in the scope of AEP-4754 Volume VI, NGVA System developer will need to choose an adequate network topology and communication to achieve safety (c.f. NGVA_INF_006).

For safety relevant communication requirements listed in Volume III and Volume V of this AEP should be considered, when choosing the safety relevant network. The safety related communication is not bound to the requirements regarding data infrastructure and data models as defined in this AEP. The reason for this exemption, is the circumstance, that as of 2018, no certifiable safety related communication system that also matches the requirements defined by Volume III and V of this AEP is available.

Therefore, other options shall be considered for system integration, depending on the safety requirements of the NGVA (sub-) System.

Please note that this head space regarding the properties of a NGVA (sub-) System is creating a risk for the interoperability of NGVA (sub-) Systems from different manufacturers and therefore is an issue for further consideration. Please also see chapter 4.5 in Volume III of this AEP.

One possible option to ensure interoperability of NGVA (sub-) Systems from different manufacturers, is to use the defined Data infrastructure and Data models and implement a black channel communication for the safety related communication in acc. to IEC 62280 (c.f. figure 6).

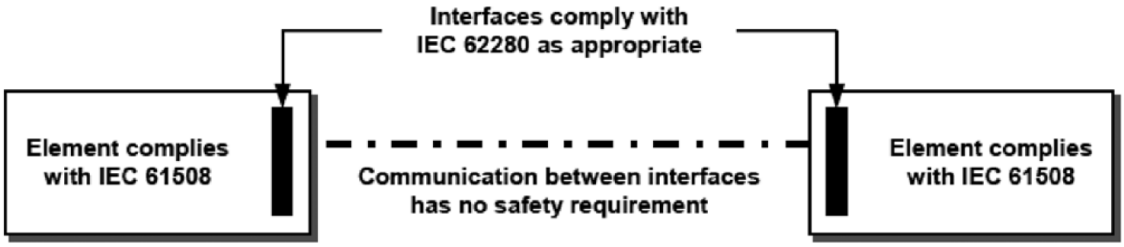

Figure **6**: black channel communication from IEC 61508
The design of complex integrated system with safety-relevant functions, hosted on common shared computing and networking resources may require additional safety considerations and activities, related to data infrastructure and data models.

For integrated applications with a large number of functions hosted on shared computing and networking infrastructure, additional measures complementary to black channel approach may be considered.

Integration Type	**Safety Communication Implementation Approach**	**Assumptions**
Safety function (or few functions) hosted on its own data/computing/ networking infrastructure	Black Channel safety communication	we can detect faults with required probability
Complex Function (many safety-relevant, real-time and non-safety functions) with partial reliance on physically separated safety data infrastructure	Black Channel safety communication Optional: partial reliance on increased fault diagnostic coverage provided by the data infrastructure	1) Backup mechanisms should be considered to bring integrity and availability to required levels. 2) The fault diagnostic and reporting at the data infrastructure level can help to avoid fault propagation and interference between hosted safety-relevant and non-safety functions.
Very complex functions (many safety-relevant, and Nx10 real-time and non-safety functions on few computers, with high resource utilization)	Black channel safety communication including reliance on fault diagnostic coverage provided by the (white channel) data infrastructure	As above, but the complexity of the system requires additional data infrastructure analysis on interference and common mode faults related to the computing/networking platform and data infrastructure.

4.2.4. Volume IV: Crew Terminal Software

The NGVA Crew Terminal Software Architecture standard, as defined in Volume IV of this AEP, supports the principles of open modular architectures embodied in the goals of NGVA.
Volume IV however, does not consider the safety implications of these open modular architectures and the flexible composition of CT systems built of software modules. Therefore, safety principles for software architectures shall be considered for CT systems to ensure the NGVA goals of open modular architectures. The following properties for the software design should be considered:

- Completeness with respect to software safety requirements specification
- Correctness with respect to software safety requirements
- Freedom from intrinsic design faults
- Simplicity and understandability
- Predictability of behavior
- Verifiable and testable design
- Fault tolerance
- Defence against common cause failure from external events

In order to avoid safety issues and possible restrictions for the open and modular architecture, the “hazard identification step” in the concept-phase of the meta-lifecycle, shall consider possible hazards in relation to the CT system for all possible NGVA system configurations.

If hazards are in evidence and mitigation measures need to be implemented, to reduce the risk to an acceptable level, options shall be considered during the development of the safety concept, to ensure modularity. A common approach to this issue is the segregation of safety relevant functions and non-safety relevant functions. This principle is already applied to “integrated modular avionics” (IMA) for the past decades. For specific requirements please refer to IEC61508:2010-3 ANNEX F or DO-297.

4.2.5. Volume V: Data Model

The NGVA Data Model (DM) is a set of modular objects, i.e. modules, called PIMs (Platform Independent Modules) which are defined in compliance with the Model Driven Architecture (MDA) open standard developed and maintained by the Object Management Group (OMG). PIMs are highly abstract, modular definitions, completely independent of software architectures and messaging technologies.
PIMs need to be translated into Platform Specific Modules (PSMs) to take account of the Data Distribution Service (DDS) technology that is used in NGVA. The PSMs generated by the translation process actually embed the DDS software architecture (e.g. the publish/subscribe mechanism) but still need one further processing step.
In fact, PSMs must be translated into a Platform Specific Implementation (PSI) to be compiled in software libraries understood by the DDS Middleware of choice.

Therefore, the overall process defined in Volume V of this AEP includes a system development environment to design the PIMs (currently IBM Rhapsody) and two translators (PIM to PSM, and PSM to PSI) to produce the Interface Description Language (IDL) files used by the DDS middleware to implement the exchange of data, events and commands among the nodes.

Safety relevant functions embedded in the modular architecture of the DM shall be analysed considering at least the following aspects:

a) the development of the PIMs,
b) the conversion process that produces the PSI,
c) the DDS middleware that uses the PSI.

Aspect a) shares all software related properties already described in section 4.2.4 (Volume IV: Crew Terminal Software) and the PIMs that deal with safety relevant functions shall be clearly identified and their behaviour analysed.

Aspect b), however, encompasses a different challenge. Transforming abstract models (the PIMs) into an actual implementation (the PSI) might have, and in fact has, impacts on the architecture of the system that shall be carefully considered with respect to functional safety. For instance, any hierarchical interactions between the PIM are subject to flattening once transformed into a serverless, publish-subscribe architecture like DDS.

Aspect c) is mostly covered by the considerations on the NGVA Data Infrastructure (DI) expressed in section 4.2.3 (Volume III: Data Infrastructure), with particular regard to the option to implement black channel communications on the dedicated Safety data bus.

Moreover, at the moment of writing these notes, there are few connectivity frameworks to comply with functional safety standards, and even less are off-the-shelf products (see RTI Connext DDS Cert, which is certifiable to IEC 61508 SIL 3, Connext DDS Cert | Software for Safety Critical Systems | RTI).
Qualifying not only the DM but also the tools to produce it may not prove to be the most convenient way to ensure that the system is reasonably free from systematic faults.

4.2.6. Volume VII: Validation & Verification

For requirements regarding validation and verification please refer to the concept phase and realization phase as described in this Volume of the AEP. Please also refer to appropriate safety standards for further requirements (e.g. IEC61508:2010 – 1, chapter 7.14 or DO-297) and chapter 3.2.

Note: Please consider that the V&V process covers all requirements (incl. safety related requirements).

4.3. Further safety considerations in the NGVA context

4.3.1. Re-Use of existing software

The aim of the open and modular architecture of NGVA is to enable the re-use and portability of software modules. The requirements for CT systems are described in Volume IV of this AEP.
However, Volume IV does not provide any requirements regarding safety relevant software modules. Table 4 provides basic requirements to ensure safety while re-using existing safety relevant software modules (please also refer to IEC61508:2010-3, Chapter 7.4.2.12):

Unique ID	Requirement Type	Requirement Text
Requirements SW re-use		
NGVA_SAF_SW1	CR	A sufficient precise and complete description of the SW module shall be available.
NGVA_SAF_SW2	CR	If the pre-existing safety relevant software module is planned for use in a existing NGVA System, an appropriate modification process shall be applied (e.g. IEC61508:2010, LC-phase 15)
NGVA_SAF_SW3	CR	If the pre-existing safety relevant software module is planned for implementation in a NGVA (Sub-) system development the following approach shall be applied: Refer to NGVA_SAF_SW3.1
NGVA_SAF_SW3.1	CR	Requirements analysis shall be performed to identify any deviations between NGVA (sub-) system development and pre-existing software.
NGVA_SAF_SW3.2	CR	Evidence of compliance to an appropriate standard for the avoidance and control of systematic faults in the software module shall be available.
NGVA_SAF_SW3.3	CR	The Validation of the pre-existing software module in the new environment shall be performed, as defined by the validation plan (refer to concept phase of meta-lifecycle)
NGVA_SAF_SW4	CR	If requirements NGVA_SAF_SW3.1 – 3.3 do not apply due to lack of information, a requalification of the software module shall be performed (please refer to IEC61508:2010 – 3, 7.4.2.13)

Table 4: Requirements for re-use of existing software

4.3.2. Legacy modules

Development cycles of (sub-) systems in the defence sector are typically more time consuming than development efforts for industry products. Also the service life of defence (sub-) systems surpasses the service life of industry products.
On this account, NGVA systems will need to be able to integrate legacy systems, which are not NGVA ready. From a safety perspective this can cause issues, as legacy systems often do not comply to the current safety standards.

To integrate legacy modules / sub-systems in a NGVA system, the following approach is suggested, to ensure an appropriate safety approach:

Step 1: Information baseline

To be able to identify a baseline for the safety approach, the following information should be available for the NGVA system integrator:

a) Information on intended use and environment of the legacy module for which it was originally developed
b) Information on modes of operation for the legacy module
c) Information on hazards and risks associated with the legacy module
d) Information on safety measures implemented in the legacy module
e) Detailed interface description
f) Results from safety validation
g) Safety statement stating the possible in-use restriction
h) User documentation

If the information above is not available to the NGVA system integrator, the system integrator should create the information by means of analysis, reverse engineering, research of similar modules or other possible measures.

Step 2: Identify scope of modification

On basis of the information from step 1 (“Information Baseline”), NGVA system integrator should identify the scope of the modification by performing an impact analysis. Depending on the result of the impact analysis, the NGVA system integrator should return to the appropriate life cycle phase of the meta life cycle (please also refer to e.g. IEC 61508:2010 – 1, 7.16).

Step 3: Realisation of modification

In most cases the impact analysis will require a return to the hazard identification “step” in the lifecycle. Should new hazards arise from the integration of a legacy module, the measures for mitigation will most likely be the scope of the NGVA system integrator, as a modification on an existing system (legacy module) is often not feasible.

Note:
When analysing the modification of a NGVA system, all possible system configurations shall be considered.

For the realisation of the modification additional requirements derived from the hazard identification step and refined by the safety concept (please refer to NGVA requirements in chapter 3), will need to be implemented in the NGVA system.

As a modification of a existing NGVA system may also not be feasible with regard to the modular concept, the allocation of these new safety requirements for the modification will most likely “target” the NGVA gateway. With this approach a modification of the existing NGVA system can be contained to the “legacy gateway”.

4. Validation of modification

There are no NGVA specific issues regarding validation of modification. Please refer to an appropriate standard (e.g. IEC 61508:2010).

5. Update of the modular safety case

To conclude the modification process, the modular safety case will need to be updated as well as the safety statements and user documentation for the NGVA system incl. all possible NGVA system configurations.

ANNEX A ABBREVIATIONS

AAP	Allied Administrative Publication
AEP	Allied Engineering Publication
ALARP	As Low As Reasonably Practicable
CM	Configuration Management
COTS	Commercial Off The Shelf
CR	Compulsory Requirement
CT	Crew Terminal
DDS	Data Distribution Service
DI	Data Infrastructure
DoD	Department of Defence
DM	Data Model
EN	European Norm
GVA	Generic Vehicle Architecture
IAWG	Industrial Avionics Working Group
IDL	Interface Description Language
IEC	International Electrotechnical Commission
ILS	Integrated Logistic Support
ISO	International Standards Organization
ITT	Invitation to Tender
JSP	Joint Service Publication
LC	Life Cycle
MDA	Model Driven Architecture
MILVA	Military Vehicle Association
MOD	Ministry of Defense
MSC	Modular Safety Case
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
OMG	Object Management Group
PIM	Platform independent Modules
PSI	Platform Specific Implementation
PSM	Platform Specific Module
RTCA	Radio Technical Commission for Aeronautics
SEC	Safety and Environmental Case
SIL	System Integrity Level
STANAG	Standardization Agreement
UOR	Urgent Operational Requirements

ANNEX B MAPPING OF LIFECYCLE PHASES TO OTHER STANDARDS

In order to fulfill the requirement NGVA_SAF_CP1 - NGVA_SAF_CP3 a mapping between the meta-lifecycle and the lifecycle of the applied safety standard should be considered. The following subclauses of ANNEX C provide examples for the mapping of lifecycles.

B.1. MAPPING TO MIL-STD-882E

The eight elements of the system safety process as defined by MIL-STD-882E (please refer to chapter 4.3 of the standard) describe the system safety process as defined by MIL-STD-882E.
To be able to include the MIL-STD882E system safety process into a NGVA system development the following mapping of “Elements” to the meta-lifecycle can be performed:

a) Concept phase of the meta-lifecycle
The following Elements of the system safety process from MIL-STD-882E can be mapped to the concept phase of the meta-lifecycle:

- Element 1: Document the System Safety Approach
- Element 2: Identify and Document Hazards
- Element 3: Assess and Document Risk
- Element 4: Identify and Document Risk Mitigation Measures

b) Realisation Phase of the meta-lifecycle
The following Elements of the system safety process from MIL-STD-882E can be mapped to the realisation phase of the meta-lifecycle:

- Element 5: Reduce Risk
- Element 6: Verify, Validate and Document Risk reduction
- Element 7: Accept Risk and Document

c) In-Service Phase of the meta-lifecycle
The following Elements of the system safety process from MIL-STD-882E can be mapped to the in-service phase of the meta-lifecycle:

- Element 8: Manage Life-Cycle Risk

d) De-commissioning Phase of the meta-lifecycle
The following Elements of the system safety process from MIL-STD-882E can be mapped to the de-commissioning phase of the meta-lifecycle:

- Element 8: Manage Life-Cycle Risk

B.2. MAPPING TO IEC61508:2010

The sixteen phases of the safety lifecycle as defined by IEC61508:2011 (please refer to Part 1 of the standard) describe the safety approach for E/E/PE systems (functional safety). To be able to include IEC61508:2010 safety lifecycle into a NGVA system development the following mapping of lifecycle phases to the meta-lifecycle can be performed:

a) Concept phase of the meta-lifecycle
The following phases of the safety lifecycle from IEC61508:2010 can be mapped to the concept phase of the meta-lifecycle:

- LC-phase 1: Concept
- LC-phase 2: Overall scope definition
- LC-phase 3: Hazard and risk analysis
- LC-phase 4: Overall safety requirements
- LC-phase 5: Overall safety requirements allocation
- LC-phase 6: Overall operation and maintenance planning
- LC-phase 7: Overall safety validation planning
- LC-phase 8: Overall installation and commissioning planning
- LC-Phase 9: E/E/PES system safety requirements specification
- LC-phase 11: Other risk reduction measures: Specification

b) Realisation phase of the meta-lifecycle
The following phases of the safety lifecycle from IEC61508:2010 can be mapped to the realisation phase of the meta-lifecycle:

- LC-phase 10: Realisation
- LC-phase 11: Other risk reduction measures: Realisation
- LC-phase 12: Overall installation and commissioning
- LC-phase 13: Overall safety validation (“keyword: risk acceptance”)

c) In-service phase of the meta-lifecycle
The following phases of the safety lifecycle from IEC61508:2010 can be mapped to the in-service phase of the meta-lifecycle:

- LC-phase 14: Overall operation, maintenance and repair
- LC-phase 15: Overall modification and retrofit

d) De-commissioning phase of the meta-lifecycle
The following phases of the safety lifecycle from IEC61508:2010 can be mapped to the de-commissioning phase of the meta-lifecycle:

- LC-phase 16: Decommissioning or disposal

NOTE:
Please consider that IEC61508 has its origin in the process industry, thus some LC-phases may not apply entirely for the defence sector.

AEP-4754 VOLVI (B)(1)