NATO STANDARD

AEP-4754

NATO GENERIC VEHICLE ARCHITECTURE (NGVA) FOR LAND SYSTEMS

VOLUME III: DATA INFRASTRUCTURE

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 III, Edition B, Version 1 NATO GENERIC VEHICLE ARCHITECTURE (NGVA) FOR LAND SYSTEMS VOLUME III: DATA INFRASTRUCTURE, 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 III, Edition B, Version 1 is effective upon receipt and supersedes AEP-4754, Volume III, 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 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) 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. DDS	OMG - Data Distribution Service (DDS) (http://www.omg.org/spec/DDS)
2. DDSI-RTPS	OMG – The Real-Time Publish-Subscribe Protocol DDS Interoperability Wire Protocol (DDS-RTPS) Specification (http://www.omg.org/spec/DDSI-RTPS)
3. EN 4531	Aerospace series - Connectors, optical, circular, single and multi-pin, coupled by triple start threaded ring - Flush contacts
4. EN 3745	Aerospace series – Fibres and cables, optical, aircraft use – Test methods – Test methods
5. EU Directive 2011/65/EU RoHS	Restriction on the Use of Certain Hazardous Substances in Electrical and Electronic Equipment
6. IEC 60793-2-10	Optical fibres – Part 2-10: Product specifications – Sectional specification for category A1 multimode fibres
7. IEEE 1588 (PTP v2)	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
8. IEEE 802.3	IEEE Standard for Ethernet

9. MIL-DTL-38999	Detail Specification: Connectors, Electrical, Circular, Miniature, High Density, Quick disconnect (Bayonet, Threaded, or Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for
10. STANAG 4697/ AEP-79	Platform Extended Video Standard (PLEVID)
11. USB v2.0	Universal Serial Bus Revision 2.0 (http://www.usb.org/developers/docs/usb_20_071012.zip)
12. RFC 768	User Datagram Protocol
13. RFC 791	DARPA Internet Program Protocol Specification
14. RFC 793	Transmission Control Protocol
15. RFC 1034	Domain Names - Concepts and Facilities
16. RFC 1035	Domain Names – Implementation and Specification
17. RFC 1122	Requirements for Internet Hosts – Communication Layers
18. RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
19. RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP
20. RFC 5227	IPv4 Address Conflict Detection
21. RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
22. RFC 6093	On the Implementation of the TCP Urgent Mechanism
23. RFC 6274	Security Assessment of the Internet Protocol
24. RFC 6528	Defending against Sequence Number Attacks

Table 1: Normative References

Reference to NGVA Data Model implementation-related standards, e.g. OMG standard versions, will be included in the Data 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 national 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 provide 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 emergent 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. **Audio Data**: Data used for real-time audio distribution which may be generated by audio sensors. Voice data is a specific subset of Audio Data.
2. **Automotive Data**: Data related to the pure automotive capability which may be distributed on an automotive bus based network as part of the Base Vehicle. The automotive bus based network lies outside of the NGVA Data Infrastructure but needs to be interfaced to the NGVA Data Infrastructure via an Automotive Network Gateway.
3. **Automotive Network Gateway**: A component that provides a controlled data bridge between an automotive bus based network and the NGVA Data Infrastructure.
4. **External Gateway**: A component which enables data connections to or from the outside world (e.g. other vehicles, dismounted soldiers, etc.).
5. **Gateway to Non-NGVA Systems**: A component which enables data connections to or from legacy Mission Sub-Systems and/or Mission Sub-Systems which are not NGVA Ready.
6. **NGVA Data**: Data which is defined in the NGVA Data Model and distributed via the NGVA Data Infrastructure.
7. **Video Data**: Data used for streaming video.
8. **Voice Communications**: Voice Communications applies to both the intercom systems inside a vehicle and also the audio communication with the outside world.
9. **Voice Data**: Voice data is a subset of Audio Data and may also be raw or compressed data using an audio codec.
10. **NGVA Network**: One of the networks within the NGVA Data Infrastructure. The NGVA Data Infrastructure may consist one or more (local area) networks (e.g. VLAN or physical separated NGVA Networks for security and/or safety reasons)

CHAPTER 3 OVERVIEW

3.1. Scope

As described in AEP-4754 Volume I, the role of a military vehicle has evolved dramatically over the last few years. The historic approach is to integrate each Mission Sub-System as a stand-alone system into a Base Vehicle. Thereby each Mission Sub-System had its own infrastructure, services and displays and controls (Figure 2).

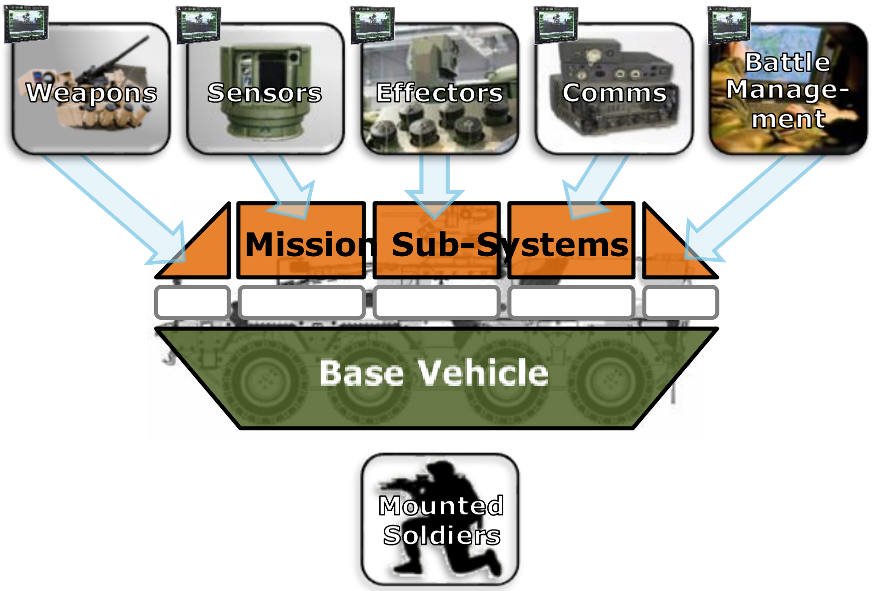


Figure 2: Stovepipe Sub-System Integration

A key objective of the NGVA is to fundamentally change this historic approach. Defining and standardizing a common data-bus enables interoperability between all connected sub-systems and also reduces the time taken to integrate new sub-systems. The aim however, is to constrain design options as little as possible to allow for flexibility and innovation.

This Volume defines the design constraints on the electronic interfaces and protocols that form the NGVA Data Infrastructure, which consists of one or more data networks including cables, plugs, the packet layer up to data exchange middleware and network devices with their provided network services which are used for the interconnection of Mission and Base Vehicle Sub-Systems inside the vehicle (Figure 3).

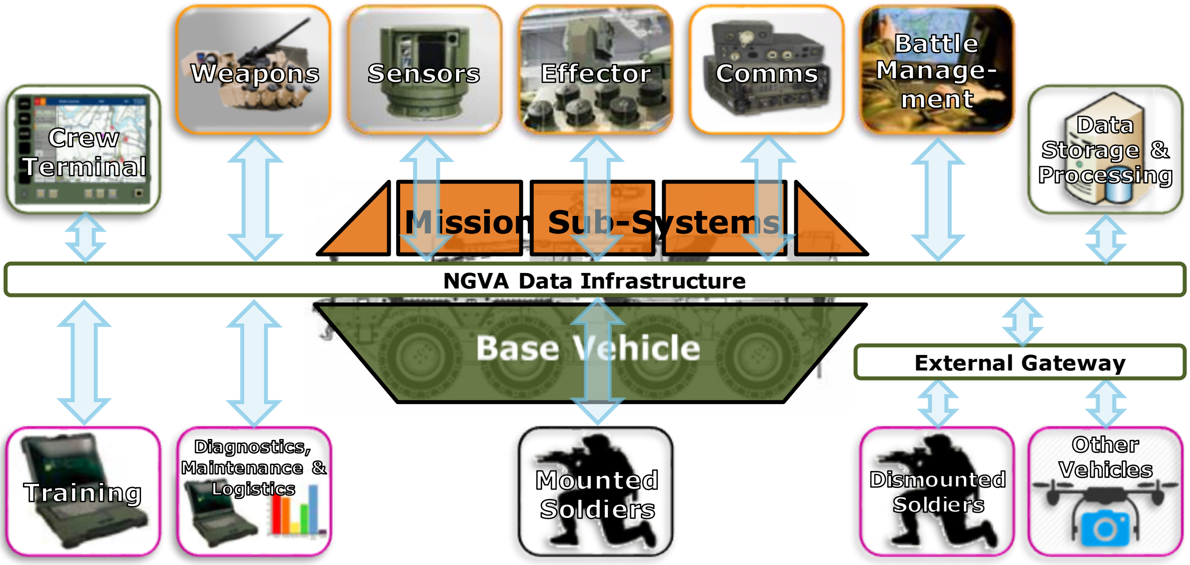


Figure 3: Integrated Mission sub-Systems

The Crew Terminal (CT) in Figure 3 plays a special role in the NGVA as it is used to interact with multiple vehicle sub-systems for control, display and the fuse of information, instead of sub-system specific operating units and displays. The comprehensive networking enables the use of multi-role/multi-purpose CTs for Vehicle Crew members to operate the system. As a part of the inherent modularity of future vehicles, one or several CTs can be added to or removed from the initial Vehicle Platform configuration.
For example, an IFV basically outfitted with a Driver CT, a Gunner CT and a Commander CT may be temporarily fitted with an extra dismounting Squad Leader CT due to operational requirements. This extra Squad Leader CT could be removed afterwards, or not. Such modularity shall not adversely affect the functioning of the Vehicle Platform.

The NGVA Data Infrastructure consists of:

1. One or more Local Area Networks (LANs); i.e. NGVA Networks;
2. Data Exchange Mechanism based on DDS/DDSI wire protocol and the NGVA Data Model (cf. AEP-4754 Volume V) with the appropriate Quality of Service (QoS) Profiles;
3. Network Services (e.g. Time Service);
4. Physical Interfaces, network connectors;
5. Audio and video streaming data and control protocol;
6. Data Interfaces; Data interface definition for NGVA Ready sub-systems and gateways. Gateways can be applied between NGVA Networks, for NGVA external data communications, for connection to security networks, for connection to non-NGVA safety critical or automotive networks, and for connection to legacy and/or non-NGVA ready sub-systems (as required);
7. Data stream between the Crew Terminal and remote applications.

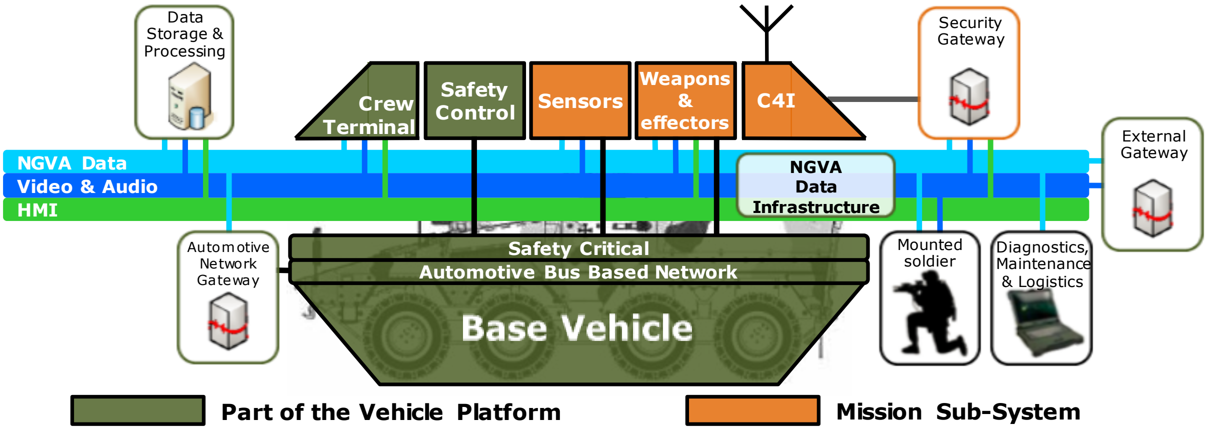


Figure 4: Example of NGVA Data distribution within an NGVA Network

As shown in Figure 4, the following data streams are identified as being part of the NGVA Data Infrastructure:

1. NGVA Data
2. Video & Audio
3. HMI

NGVA Data is data shared on an NGVA Network using the DDS/DDSI wire protocol and structured in line with the NGVA Data Model (AEP-4754 Volume V).

Video Data and Audio Data are based on STANAG 4697 (PLEVID), extended by digital voice type specific control and codecs (VoiP).

Mission Applications may run directly on a Crew Terminal or may run remote on a central Virtual Machine (VM) server (shown as Data Storage & Processing in Figure 4) or on the individual sub-systems (e.g. Weapon System). An HMI connection is used as the data connection between the Crew Terminal and remotely running applications. Note that the Mission Applications are not part of the NGVA. The NGVA Data Infrastructure only defines an HMI connection as the data connection between Crew Terminal and the remotely running applications.

Different (physical or virtual) networks may be used for handling different security classifications in order to achieve the necessary separation dependent on national requirements. Security gateways are used to provide cross domain data exchange between these separated domains. Depending on the protocols used for the data streams in the higher classified network the security gateway could be a security bridge between two NGVA Networks or a Gateway to Non-NGVA Systems.

Another reason for network separation could be a dedicated high bandwidth network for video.

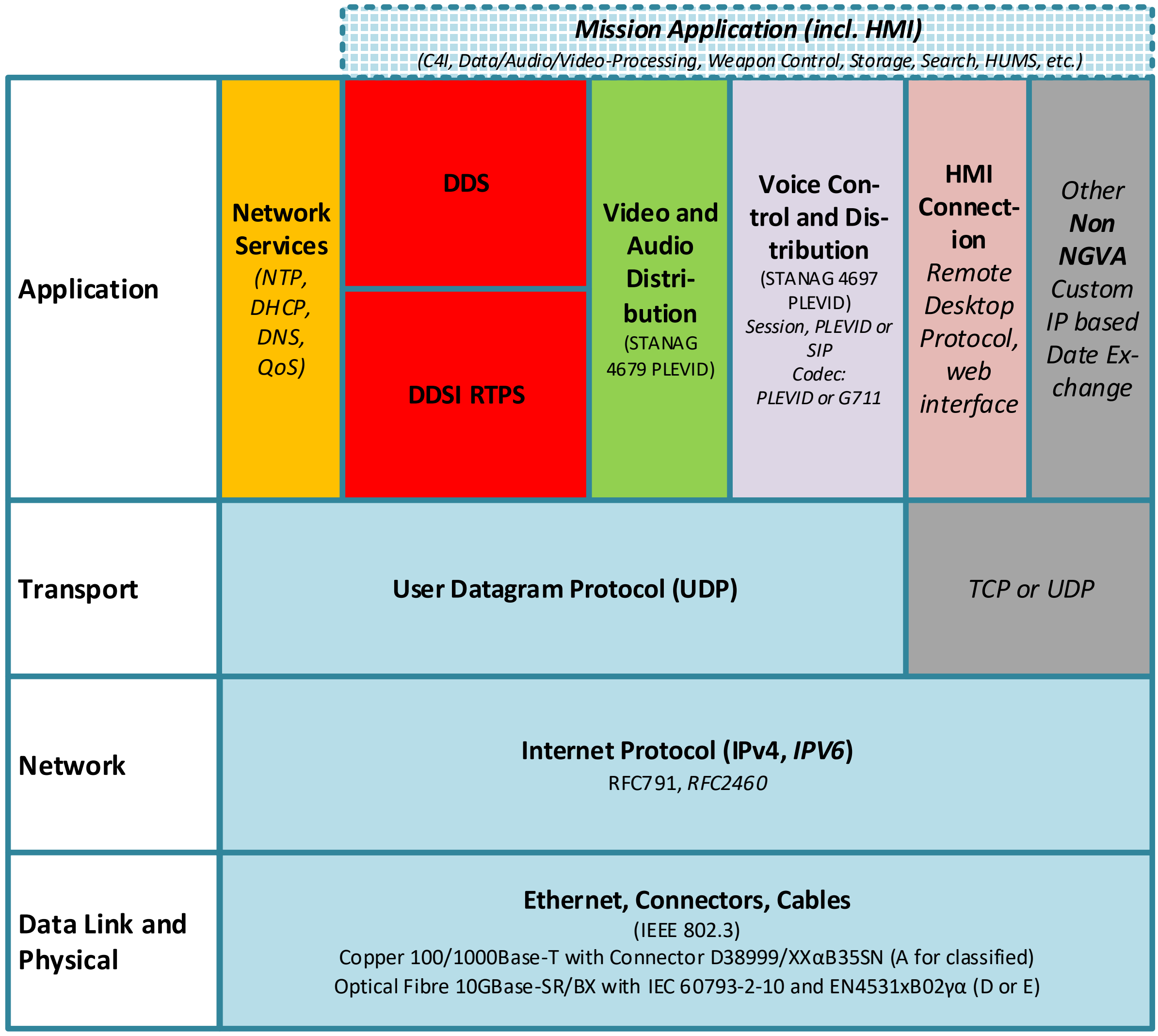
Safety and Operation Critical Solutions are solutions which use communication technology other than the NGVA protocols/mechanisms required by this AEP. Safety and Operation Critical Solutions could be direct wiring, a CAN bus based system, or Ethernet based enhanced protocol solutions like AFDX (Avionics Full-Duplex Switched Ethernet) and potentially TSN (Time-Sensitive Networking developed for Automotive). Information could be extracted from Safety and Operation Critical Systems to the NGVA Data Infrastructure making use of a safety gateway. A safety gateway shall prevent degradation of performance of a Safety and Operation Critical System in all circumstances. Thereby an Automotive Network Gateway is in essence a safety gateway as driving, braking and steering are Safety and Operation Critical Functions.

The overall system aspects are described in CHAPTER 4.

Figure 4 is just an example. Nations are free to develop their own Electronic Architecture philosophy conforming to NGVA Standard AEP-4754 Volumes I through VII and to derive their national requirements from that.

3.2. NGVA Data Infrastructure Layer View

Figure 5 shows a layer view of the main elements of the NGVA Data Infrastructure.



Mission Application (incl. HMI)
(C4I, Data/Audio/Video-Processing, Weapon Control, Storage, Search, HUMS, etc.)

Application

Network Services *(NTP, DHCP, DNS, QoS)*

DDS

DDSI RTPS

Video and Audio Distribution (STANAG 4679 PLEVID)

Voice Control and Distribution (STANAG 4697 PLEVID) *Session, PLEVID or SIP* *Codec: PLEVID or G711*

HMI Connection *Remote Desktop Protocol, web interface*

Other ***Non NGVA*** *Custom IP based Date Exchange*

Transport

User Datagram Protocol (UDP)

TCP or UDP

Network

Internet Protocol (IPv4, *IPV6*)
RFC791, *RFC2460*

Data Link and Physical

Ethernet, Connectors, Cables
(IEEE 802.3)
Copper 100/1000Base-T with Connector D38999/XXαB35SN (A for classified)
Optical Fibre 10GBase-SR/BX with IEC 60793-2-10 and EN4531xB02γα (D or E)

**Figure 5: NGVA Data Infrastructure Layer View
(Optional Enhancements are shown in italic)**

Figure 5 shows following layers:

1. **Data Link and Physical:** Cable, Connectors, Ethernet (see section 5.1 and 5.2)
2. **Network:** Internet Protocol (see section 5.3)
3. **Transport:** Mechanism to Transmit, Receive, Synchronize, etc. Data (see section 5.4)
4. **Application:** Common Naming, Understanding and Structure of the Data to be exchanged (see section 5.5)
   As the technologies chosen for the different layers differ depending on application areas, the application areas are indicated at the top:
   a. **DI Services:** Data Infrastructure Services (see section 5.5.1)
   b. **NGVA Data:** Exchange of data defined in the NGVA Data Model (see section 5.5.2)
   c. **Video / Audio:** Video and Audio distribution inside the NGVA networks (see section 5.5.3)
   d. **Voice:** Voice Communication (see section 5.5.4)
   e. **HMI:** Optional Enhancement for exchange of HMI data between remote applications and the Crew Terminal (see section 5.5.5)
   f. **Other:** Optional Enhancement with other IP based Data Exchange Mechanisms (see section 5.5.6)

The NGVA Data Infrastructure will be the link between the software running on all the end devices; i.e. the mission applications. These mission applications are however not part of the NGVA Data Infrastructure and therefore out of scope of this AEP.

3.3. NGVA Layout Example

Figure 6 depicts a simplified layout of an NGVA Network indicating the possible interfaces to the NGVA Data Infrastructure.

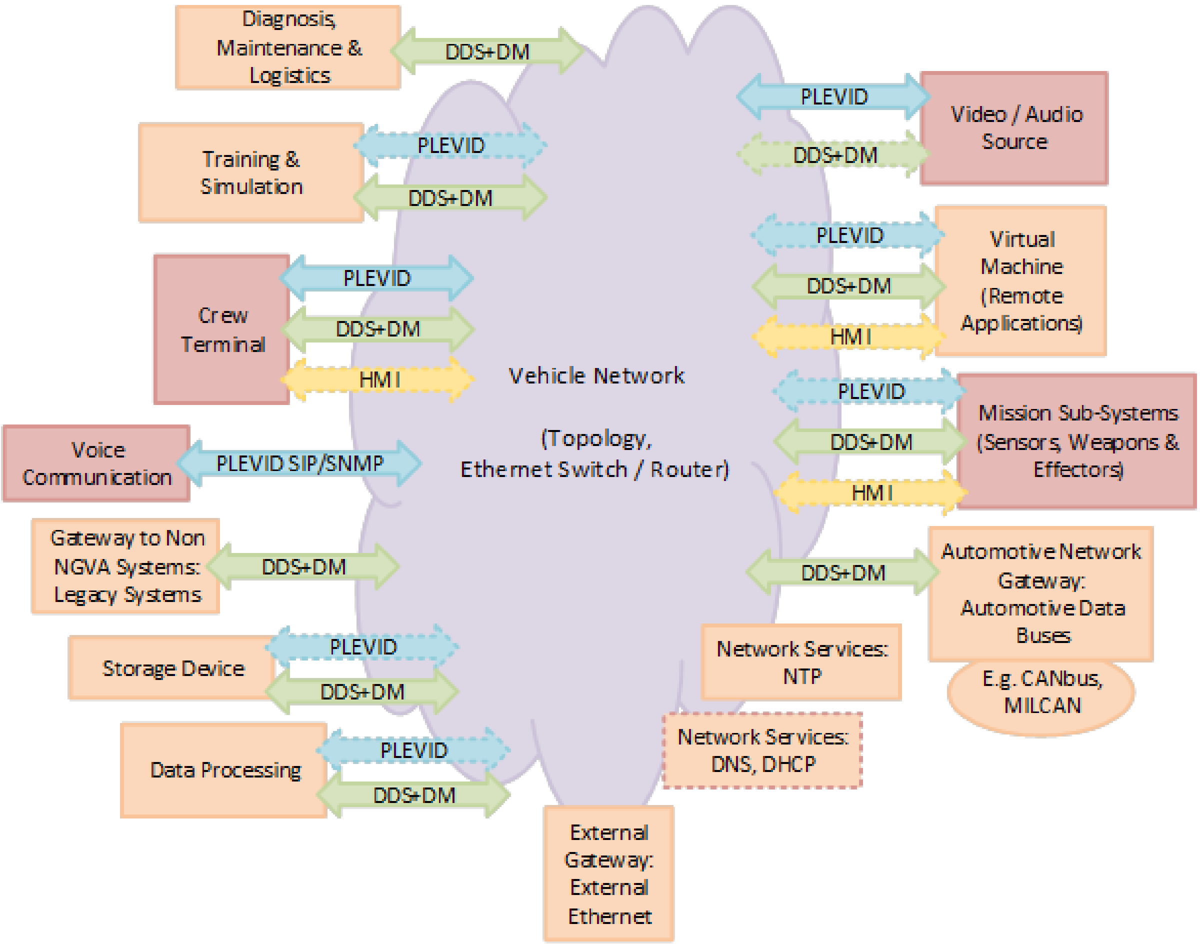

Diagnosis, Maintenance & Logistics
DDS+DM
Training & Simulation
PLEVID
DDS+DM
Crew Terminal
PLEVID
DDS+DM
HMI
Voice Communication
PLEVID SIP/SNMP
Gateway to Non NGVA Systems: Legacy Systems
DDS+DM
Storage Device
PLEVID
DDS+DM
Data Processing
PLEVID
DDS+DM
Vehicle Network
(Topology, Ethernet Switch / Router)
PLEVID
DDS+DM
Video / Audio Source
PLEVID
DDS+DM
HMI
Virtual Machine (Remote Applications)
PLEVID
DDS+DM
HMI
Mission Sub-Systems (Sensors, Weapons & Effectors)
DDS+DM
Automotive Network Gateway: Automotive Data Buses
E.g. CANbus, MILCAN
Network Services: NTP
Network Services: DNS, DHCP
External Gateway: External Ethernet

Figure 6: Data Infrastructure Example (dashed lines – to be used if applicable)

The interfaces to the NGVA Data Infrastructure are discussed in CHAPTER 6.

3.4. Document Structure

The overall system aspects are described in CHAPTER 4.

CHAPTER 5 is dedicated to Ethernet based LAN and contains subsections for the:

- Physical Layer (Section 5.1);
- Data Link Layer (Section 5.2);
- Network Layer (Section 5.3);
- Transport Layer (Section 5.4);
- Application Layer (Section 5.5).

The Application Layer completes the Ethernet based LAN and covers:

- Network Services;
- NGVA Data distribution;
- Video / Audio distribution;
- Voice distribution;
- HMI distribution;
- Other LAN services and/or distribution which is not covered by NGVA.

The interfaces to the NGVA Networks are discussed in CHAPTER 6. To be able to communicate with the NGVA Data Infrastructure the interface is described to explain NGVA Readiness. Connected equipment can be NGVA Ready sub-systems, sub-systems connected via a Gateway to Non-NGVA Systems, the Base Vehicle connected via the Automotive Network Gateway, Safety and Operation Critical Systems or these can be systems or networks connected via an External Gateway, e.g. to other Vehicle Platforms, dismounted soldiers, higher echelons etc..

Finally, CHAPTER 7 covers Peripheral Device Connections, which specifies a USB connector that should be available, with certain NGVA sub-systems, in order to connect with peripheral devices such as Joysticks, Keyboards, Buttons, and Printers.

INTENTIONALLY BLANK

CHAPTER 4 SYSTEM ASPECTS

4.1. General Considerations

The overall setup of an NGVA Compliant Vehicle Platform should include a suitable Electronic Architecture depending on requirements, covering for example:

- segregation between real-time and non-real-time data by using different networks or Virtual Local Area Networks (VLANs);
- separate networks for high volume streaming data.

It is important to consider scalability and allow for future additions to the Vehicle Platform and provision for growth by designing in reserve capacity, which will enable flexibility and innovation.

Vehicle Platform level assessment requires the consideration of:

- real time performance;
- vehicle safety;
- security issues.

Overall performance coupled with safe and secure operation of the vehicle platform is paramount. A system level assessment is needed to determine the level of performance that the infrastructure must provide in terms of both, static capacity, dynamic loading and throughput. The assessment must take into account the role and needs of the Vehicle Platform and consider future capability enhancement.

The system integrator must ensure the reliable, smooth and quick start-up time of the important sub-systems in accordance with specific vehicle requirements, and may need to tune the NGVA network by using Quality of Service (QoS), Bandwidth Control, Traffic Shaping and use of VLANs as measures to achieve the desired performance.

4.1.1. Vehicle Buses and Networks

The NGVA Data Infrastructure is based on an Ethernet Internal LAN. Automotive and other bus based networks and technologies are not within the scope of this AEP.

Non-NGVA networks and buses (e.g. IP radios, Mil Std 1553, ARINC 429, STANAG 4628) shall require an NGVA Ready gateway. This is described in CHAPTER 6 of this document.

4.1.2. External Data Communications

An External Gateway shall provide the access to any services inside the Vehicle Platform that are required or need to be accessible from outside the Vehicle Platform or to any services outside the Vehicle Platform that need to be accessible from inside the Vehicle Platform. These services may include voice communication, Blue Force tracking, etc.

Specific external communication, including non-IP based communications (e.g. specific applications, security gateways or HF Radios) which do not directly transmit NGVA Data might be necessary. The NGVA Data Infrastructure does not cover these special implementations.

Mission applications available on a Vehicle Platform such as Battle Management System, Voice Communication, etc. shall also fulfil the requirements for NGVA Readiness as stated in CHAPTER 6.

External Gateways could be used for close connections to other vehicles or dismounted soldiers to exchange NGVA Data, video and audio, enabling higher data throughput solutions which might differ from today's standard Command, Control, Communications Computer, and Intelligence (C4I) data as used e.g. in

1. the Multilateral Interoperability Program (MIP),
2. MIL-STD-6017 "Variable Message Format (VMF)",
3. STANAG 4406 "Military Message Handling System (MMHS)"

A special external communications case might be a wired connection used for linking static Vehicle Platforms to provide high data throughput capabilities, e.g. for static forward tactical Headquarters.

Table 2 below describes the requirements for NGVA External Data Communications.

Unique ID	Requirement Type	Requirement Text
NGVA External Data Communications		
NGVA_INF_001	CR	Any NGVA Data, Video Data and/or Audio Data inside the Vehicle Platform which is required outside the Vehicle Platform and which the Vehicle Platform may provide or any NGVA Data, Video Data and/or Audio Data outside the Vehicle Platform which is required inside the Vehicle Platform shall be implemented through an External Gateway.

Table 2: NGVA External Data Communications Requirements

4.2. Overall Requirements

4.2.1. NGVA Compliance

All NGVA sub-systems shall be NGVA Ready which means that they need to natively comply with the compulsory requirements of the NGVA Data Infrastructure or use an NGVA Ready gateway (Gateway to Non-NGVA Equipment) to achieve compliancy.

4.2.2. NGVA Sub-Systems Control

An NGVA Compliant Vehicle Platform will be comprised of common sub-systems, such as Crew Terminal, processing units, and other platform resources (e.g. sighting systems and rangefinders). In order to communicate with and control these Vehicle Platform resources without conflict, the NGVA Data Model defines an arbitration protocol. The protocol is based on DDS and its behaviour is described in a module within the NGVA Data Model. The arbitration protocol standardizes the way controlling resources, such as a crew station, gain control of individual sighting systems, rangefinders to avoid control conflicts.

DDS operates using a "publish and subscribe" protocol, where publishers are not aware of the subscribers that are using their published data. However, NGVA operation also requires publishers to direct messages to specific resources for system integration purposes. Therefore, the NGVA Data Model defines a system for providing unique Resource IDs and Descriptors to a specific Mission Sub-System implementation to identify Resources connected to the Mission Sub-System. The allocation of Resource IDs to the connected Resources is performed by the NGVA Registry Service.

Table 3 below describes the requirements for NGVA Sub-Systems Control.

Unique ID	Requirement Type	Requirement Text
NGVA Sub-Systems Control		
NGVA_INF_002	CR	NGVA Ready sub-systems shall comply with the NGVA Arbitration Protocol as defined in the NGVA Data Model.
NGVA_INF_094	CR	NGVA Ready sub-systems shall comply with the NGVA Registry Service as defined in the NGVA Data Model.

Table 3: NGVA Sub-Systems Control Requirements

4.2.3. Failure of NGVA Infrastructure

Failure of the NGVA Data Infrastructure or its components shall not degrade the performance of the Base Vehicle or any safety critical sub-system that exists on the vehicle.

Table 4 below describes the requirements for Failure of NGVA Infrastructure.

Unique ID	Requirement Type	Requirement Text
Failure of NGVA Infrastructure		
NGVA_INF_003	CR	Failure of the NGVA Data Infrastructure or its components shall not degrade the performance of the Base Vehicle or any safety critical sub-system that exists on the Vehicle Platform.

Table 4: Failure of NGVA Infrastructure Requirements

4.3. Network Topology

The local network topology needs to be carefully designed and implemented so that the required data rates and latencies can be achieved while providing robustness and graceful degradation in the case of faults or damage. The safety and security issues need to be considered as well as provision of gateways between NGVA Networks, to external, to legacy or to automotive systems.

It might be necessary to provide several Ethernet switches and/or separate different networks on a single Vehicle Platform, e.g. for video streaming or real time data or for data at different security levels. These NGVA Networks shall be designed for scalability to cater for the range of operational missions for which the Vehicle Platform is expected to support through life.

The core Ethernet cabling and network infrastructure shall provide for at least 1 Gb/s Ethernet transmission speed. In specific cases, such as data transmission through slip rings, a lower transmission speed may be necessary.

For details of the minimum requirements on switches or routers, refer to the Switch Specifications in STANAG 4697.

It is recommended that Ethernet switches provide some fibre optic data ports with at least 10Gb/s capability.

Table 5 describes the NGVA Network topology requirements.

Unique ID	Requirement Type	Requirement Text
NGVA Network Topology		
NGVA_INF_004	CR	The NGVA Network topology shall be such that the required data rates and latencies requirements can be achieved.
NGVA_INF_005	CR	The NGVA Network topology shall be such that robustness and graceful degradation in case of faults or damage shall be provided.
NGVA_INF_006	CR	The NGVA Network topology shall be such that safety and security issues are considered and evidence shall be provided.
NGVA_INF_007	CR	When there is a need to connect to non-NGVA or external networks the NGVA Network topology shall use gateways to connect to these networks.
NGVA_INF_008	OE	The NGVA Network shall be designed for scalability to cater for the range of operational missions for which the Vehicle Platform is expected to support through life.
NGVA_INF_009	CR	Ethernet cabling and network infrastructure shall support data transfer at a minimum transmission speed of 1Gb/s.

Unique ID	Requirement Type	Requirement Text
NGVA Network Topology		
NGVA_INF_010	CR	The used switches or routers shall fulfil the minimum requirements listed in STANAG 4697 PLEVID in the section “Switch Specifications”.

Table 5: NGVA Network Topology Requirements

4.3.1. Flow Control or Data Throughput Management

Real-Time data (e.g. video, audio, voice communications, and vehicle sensor and control data) typically needs low latency distribution. Especially, video streaming with its high data throughput requirement requires fast networks. Recording and storage functions generally accept higher latencies and slower networks.

Network flow control and traffic management techniques are useful for managing the data rates inside a network in a way that ensures the network transmits all the data within the specific requirements. Flow control is especially useful for video data with its naturally high data volume requirements. However as stated in STANAG 4697, flow control should not be employed to compensate for the use of undersized networks but rather ensure that the required data transmission runs smoothly on a correctly sized network capacity.

Flow Control is an optional enhancement and shall be implemented according to STANAG 4697. Table 6 below describes the NGVA flow control requirements.

Unique ID	Requirement Type	Requirement Text
NGVA Flow Control		
NGVA_INF_011	OE	Flow Control should be implemented according to STANAG 4697 PLEVID.

Table 6: NGVA Flow Control Requirements

4.4. Cyber Security Guidance

Security of operation and protection of data is considered essential for all military vehicles. Security has to consider anything that could compromise the confidentiality, integrity and availability of data or operation of the vehicle. Nations have different approaches to the assessment and management of security risks. A generic approach is on its way to be defined.

However, every nation will need to consider threats to the vehicle, its technology, data, or its operation. Every nation is now becoming much more aware of the potential for security attacks and will have robust techniques for assessing the threats and risks they are prepared to take.

Therefore, a security concept needs to be developed that considers possible threats and possible counter measures, which results in a security architecture. From the perspective of a Vehicle Platform with an NGVA Electronic Architecture, the following are measures are likely to be considered in any security approach.

Physical Measures describe anything tangible that is used to prevent or detect unauthorized access to physical areas, systems, or assets:

1. Prevention of unauthorized access to the Vehicle Platform, e.g. physical access control
2. Anti-tamper or tamper evident mechanisms

Administrative Measures refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals:

1. Security Operating Procedures
2. Careful control of maintenance activities
3. Design & development measures
4. Audit and Accounting controls
5. Adequate clearance of personnel
6. Data classification

Technical Measures (also known as logical measures) include hardware or software mechanisms used to protect assets:

1. Operating system lockdowns
2. Network security measures
3. Anti-Virus
4. Intrusion detection and prevention
5. User authorisation
6. Authentication and access control
7. Gateways and cross-domain controls
8. Data encryption
9. Firewall

This NGVA standard implies separate networks for different security domains. Physical network infrastructure/cabling can be separated by specifying different keyway polarisations for connectors for different security domains (unclassified and classified).

Generally, there is a need for the basic, usually “unclassified” NGVA functions and data associated with vehicle operation to be rapidly and highly available with the minimum need for authentication by Operators. However, the data and systems associated with battlespace information, which are likely to attract a higher security classification, will require standard authentication and access controls. Table 7 describes the NGVA security requirements.

Unique ID	Requirement Type	Requirement Text
Security		
NGVA_INF_012	CR	A security concept needs to be developed which considers possible threats and possible counter measures which shall result in a security architecture.
NGVA_INF_013	OE	The Security Architecture should include physical measures.
NGVA_INF_014	OE	The Security Architecture should include administrative measures.
NGVA_INF_015	OE	The Security Architecture should include technical measures (also known as logical measures).

Table 7: NGVA Security Requirements

The Vehicle Platform specific Security Architecture shall assess the implementation of the solutions listed in Table 8.

Unique ID	Requirement Type	Requirement Text
Optional Security Enhancements		
NGVA_INF_016	OE	The IP-Stacks of all network devices shall be hardened as described in RFC 6274.
NGVA_INF_017	OE	All switches shall be capable of Dynamic ARP Inspection (DAI).
NGVA_INF_018	OE	If DHCP is intended to be used, all switches shall be capable of DHCP Snooping.
NGVA_INF_019	OE	All device communication via DDS shall be compliant with the OMG DDS Security specification.
NGVA_INF_020	OE	If IGMP is intended to be used, all network devices employing it should support IGMP-AC.
NGVA_INF_021	OE	The architecture separates physical network infrastructure/ cabling for different security domains by specifying different keyway polarisations for connectors for different security domains (unclassified and confidential).

Table 8: Optional Security Enhancements for the NGVA Data Infrastructure

4.5. Safety in NGVA Data Infrastructure

The standardized NGVA Data Infrastructure protocols/mechanisms are not sufficient to realize Safety and Operational Critical assurance of data distribution within a safety case where equipment/systems are interconnected. Safety Case critical performance can be realized using a (non-NGVA) Safety Bus to assure distribution of safety critical data between equipment/sub-systems and/or when the Safety Critical performance/ functionality is contained within the sub-systems itself, i.e. fail safe behaviour in case of failing/erroneous communication between system elements in the Safety Case thread.

Use of Ethernet infrastructure technology within the IEEE 802.3 standard to enable assured safety critical data exchange is still in the research and standardization phase. State of the art candidates for Safety critical Ethernet, augmented standard or enhanced protocols on standard Ethernet, are Time Triggered Ethernet SAE AS 6802, AFDX (Avionics Full-Duplex Switched Ethernet) and potentially TSN (Time-Sensitive Networking developed for Automotive).

Safety-critical systems are those systems whose failure could result in loss of life, significant property damage or damage to the environment. A safety system comprises everything (hardware, software, and human aspects) needed to perform one or more safety functions, in which failure would cause a significant increase in the safety risk for the people and/or environment involved.

Safety-related systems are those that do not have full responsibility for controlling hazards such as loss of life, severe injury or severe environment damage. The malfunction of a safety-related system would only be that hazardous in conjunction with the failure of other systems or human error.

Safety Aware functionality (as used further in this document as relevant safety definition) is defined as islands of functionality/performance outside the Safety Critical or -related systems domain of a solution but an operational important part of the Safety Case Hazard Analyses identified thread/flow within the total solution.

Remark:
Safety in networked solutions is very much dependent of the security aspects within that solution. Safety Aware considerations are likely only possible/allowed for MIL-STD 882E defined Severity Categories III Marginal or IV negligible.

The Safety Aware relevance is applicable because the NGVA Data Infrastructure is involved in distributing data related to the situational awareness for the Vehicle Crew and status of the Vehicle Platform and Mission Sub-Systems. For acknowledged safety cases like gun related target tracking and shot activation trigger, communication means are within the sub-system and/or using dedicated bus technologies placed in the (non-NGVA) Safety Bus. This type of information, as well as other safety critical information, can be interfaced via a Safety Gateway or the Automotive Network Gateway to the NGVA Data Infrastructure for usage by registered applications (Conversion to NGVA Data by e.g. DDS wrappers may be required).

Since a key objective of the NGVA is to minimize equipment in the Vehicle Platform and therefore size, weight and power demands, system integrators may want to maximize the use of the NGVA Data Infrastructure and connected Crew Terminals. This approach could seek to re-use platform infrastructure and equipment to support system functionality for safety-related or safety-aware systems. In that case, sufficient safety enforcing functionality should be placed outside the NGVA Data Infrastructure and/or strictly within the (non-NGVA) Safety Bus context.

The Safety Case for e.g. situations where manual intervention is allowed can have a different safety enforcing solution compared to the classical implementation.

Examples for such situations are given in Table 9 below. To minimize the probability for an unsafe situation, Safety Aware performance must be provided by the NGVA Data Infrastructure within potential Safety Cases for the overall Vehicle Platform and integrated Mission Sub-Systems. “Safety Aware” is defined as islands of functionality outside the Critical Safety domain of a solution but an adjacent important part of the Safety Case Hazard Analyses identified thread/flow within the total solution.

Possible Safety Aware use-case examples to substantiate the need for Safety Aware performance are given below.

Case	Issue	Safety ensuring function
Observation/ surveillance camera	No valid or timely unavailable Situational Awareness	• Deterministic delay/jitter • Bandwidth control/supervision • Delivery assurance • Sensor-application Identity assurance • Content Integrity assurance
C2IS Instrumentation panel	Unavailability of information	• Deterministic delay and timeliness on technical application-sensor-information presentation.
Platform supervision	Consistency & integrity of information	• Information time synchronized accuracy/ relationship • Information (fused) state situational life cycle integrity
Driver Assistance System camera	No valid or timely unavailable video feed.	• Deterministic delay/jitter • Bandwidth control/supervision • Delivery assurance • Sensor-application Identity assurance • Content Integrity assurance

Table 9: Examples of NGVA Network “Secure Aware” Performance in potential safety cases

NGVA safety aware data distribution within the NGVA Data Infrastructure can be detailed to the following (performance) characteristics:

A. Availability of network (routes) and (distributed/redundant) transmission protocols, servers and clients;
B. Deterministic behavior of the data delivery process;
C. Several real-time classes supporting enabling and the timing requirements of applications/services;
D. Specific Data Model topic QoS patterns supporting the potential different information delivery assurance specific characteristics in a defined safety aware use case;
E. Integrity of the distributed data, i.e. assurance on correct information transfer;
F. Confidence that the information is distributed between intended & trusted equipment/processes/services on the network.

Like security, Safety (Aware) solutions can be characterized with the CAI (Confidentiality, Availability and Integrity) triangle in mind.

Confidentiality:
This standard and its associated AEP Volumes do not cover the inter application/ process/equipment trust mechanisms (Safety Aware characteristic F) on NGVA Data Infrastructure level preventing malicious non expected applications (hosts) to interact with the vehicle applications using the NGVA Data Infrastructure. Potential recommended mechanism are using the DDS security capability and/or based on the capability of the Vehicle Platform central Registration and resource Arbitration Service allowing devices/applications into the Vehicle Platform.

Availability:
The segregation of the NGVA Data Infrastructure in several NGVA Networks in addition to proper QoS configuration of the network elements and flows, as explained in Section 3.1 and 4.1 of this AEP, are considered providing the ”Availability” basis for safety aware characteristics A, B and C. Refer to NGVA_INF_003, NGVA_INF_004, NGVA_INF_006 and NGVA_INF_007.

Within a defined safety aware implementation the different classes of distribution of NGVA Data on the information bus (DDS) is a critical design consideration. Therefore, AEP-4754 Volume V defines DDS Topic QoS patterns for NGVA Data distribution improving the (high) probability/assurance of safety aware information distribution performance for the following examples of Data Model topic types:

- States:
  - Assurance of (persistent) state integrity from or shared amongst (sub)system/processes.
- Commands:
  - Assurance of triggered critical stimulus.
- Alarms:
  - Assurance of triggered critical events.
- Periodic data with deterministic delay/jitter guaranties:
  - Assurance of (absolute) time window synchronized sensitive information.
- Events:
  - Assurance of triggered operational status & state (change) information.

DDS/DDSi supports mechanisms to create such patterns for topics which are used/meaningful for the applications/services exchanging information over the NGVA Infrastructure in a safety aware use-case.
Examples of these mechanisms are Durability, Reliability, Destination order, History, Writer Data lifecycle, Deadline, Latency, Lifespan.
The configuration and/or use of these patterns in a Vehicle Platform solution are depending on the vehicle specific safety aware use-cases and the solution dependent equipment/systems.

Integrity:
DDS including error detection/correction mechanisms provides the basis for D and E. Augmenting (the limited) integrity provisions are as defined in this AEP and within the IEEE 802.3 standard Transmission Protocols. Using encrypted network communication flows can also be used to strengthen the integrity.

CHAPTER 5 ETHERNET BASED INTERNAL NGVA LAN

5.1. Physical Layer

5.1.1. NGVA Interface Panel

NGVA Interface Panels shall be used inside the Vehicle Platform for Mission Sub-Systems that are installed on the Vehicle Platform for dedicated missions or shall be installed to foresee growth potential for connecting future NGVA Ready Mission Sub-Systems. The NGVA Interface Panels (see Figure 7) shall be available at suitable locations inside the Vehicle Platform. There may be multiple panels within a Vehicle Platform with varying connector points and types. These panels shall be equipped with the NGVA Power and Data Connectors specified. NGVA Ready Mission Sub-Systems must use these panels to receive power and to exchange NGVA Data.

A sub-system or gateway which is permanently connected to the NGVA Data Infrastructure may physically use other connectors which are better suited to the specific purpose or constraint.

This approach provides a standardized way to interface NGVA Ready sub-systems and Gateways to Non-NGVA Equipment with the NGVA Data Infrastructure and will improve configurability and flexibility. The NGVA Interface Panel also enables cost efficient addition of sub-systems and potential replacement of obsolete sub-systems.

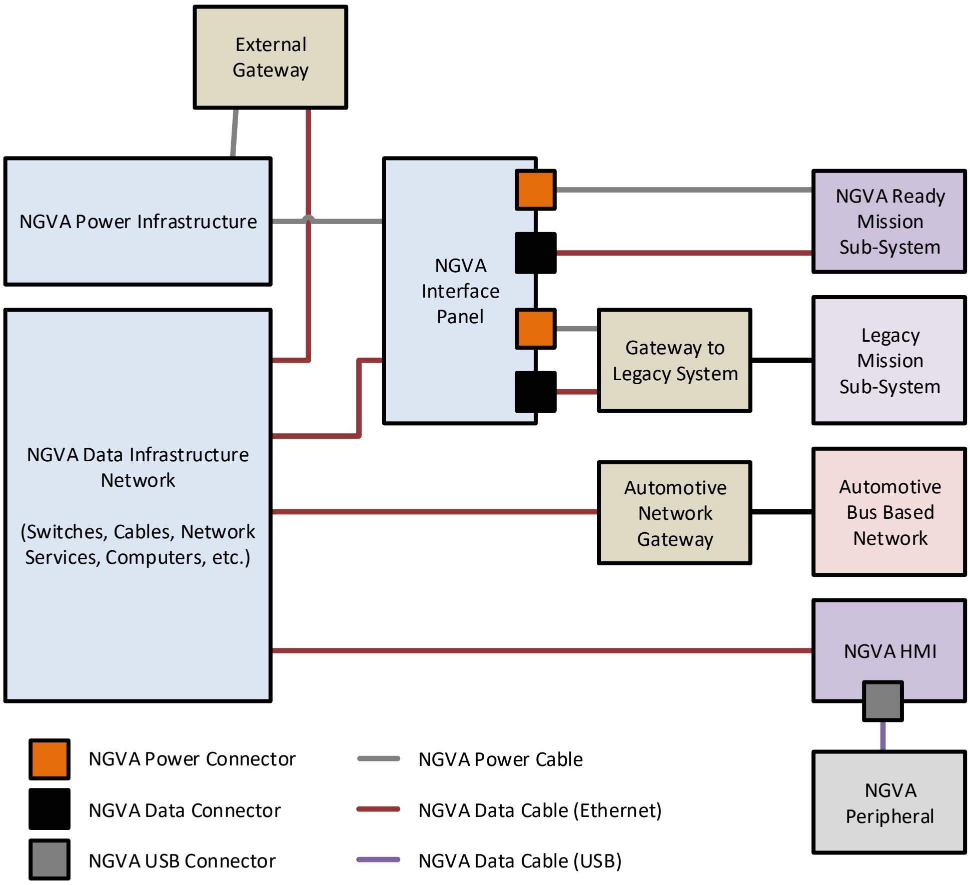

External Gateway
NGVA Power Infrastructure
NGVA Interface Panel
NGVA Ready Mission Sub-System
Gateway to Legacy System
Legacy Mission Sub-System
NGVA Data Infrastructure Network
(Switches, Cables, Network Services, Computers, etc.)
Automotive Network Gateway
Automotive Bus Based Network
NGVA HMI
NGVA Peripheral
NGVA Power Connector
NGVA Data Connector
NGVA USB Connector
NGVA Power Cable
NGVA Data Cable (Ethernet)
NGVA Data Cable (USB)

Figure 7: NGVA Interface Panel Concept for Networking of Sub-Systems

Table 10 below shows the requirements for the NGVA Interface Panel.

Unique ID	Requirement Type	Requirement Text
NGVA Interface Panels		
NGVA_INF_022	CR	NGVA Interface Panels shall be equipped with Data Connectors described in Section 5.1.2.1 and Section 5.1.2.2. Single and Dual connectors are chosen as needed.
NGVA_INF_023	CR	NGVA Interface Panels providing power and data connection shall be made available at suitable locations inside the Vehicle Platform with connectors which are specified in AEP-4754 Volume II; NGVA Power Infrastructure and this AEP.
NGVA_INF_024	CR	NGVA Ready sub-systems must be capable of using the NGVA Interface Panels to receive power and to exchange NGVA Data.
NGVA_INF_025	OE	NGVA Ready sub-systems which are permanently connected to the NGVA Data Infrastructure may also use other connectors which are better suited to the specific purpose.
NGVA_INF_026	OE	Spare NGVA Data interface outlets should be provided to meet growth requirements as specified in the Vehicle Platform specific system requirements.
NGVA_INF_027	CR	Any NGVA Data interface outlet requiring disconnection of cables under normal usage or any spare outlet shall be provided with a suitable protective cap for protection when disconnected. A storage location for the protective cap (e.g. dummy connector) shall be provided.

Table 10: NGVA Interface Panels Requirements

5.1.2. Data Connectors (Ethernet)

In order to ensure that there is physical connectivity standardization between an NGVA Compliant Vehicle Platform and NGVA Ready sub-systems, a set of common data connectors is defined. This also helps to prevent connecting the wrong (commercial) equipment to the NGVA Data Infrastructure.

Although this AEP specifies the connectors to be used, system performance is highly dependent on the cabling and construction methods for the complete wiring harnesses. MIL-DTL-38999 connectors were not specifically designed for high capacity data transmission so extreme care needs to be taken in the cable terminations and shielding. Each vehicle integrator will have a standard for cable harness construction for their Vehicle Platforms and NGVA based harnesses should comply as much as possible with those specifications. However, it may be necessary to deviate from the normal standards to maintain network data performance.

5.1.2.1. 100/1000Mb/s Ethernet

Keyway Polarisation: Different Keyway Polarisations are specified in this standard to add a physical layer of protection against the accidental connection of equipment to an incorrect security domain.

Single Connector: Where a single Ethernet connection is required the connector shall be of type MIL-DTL-38999 Series III, D38999/XXαB35SN (or A) with the pin out as defined in Table 11 and the detailed specification of:

1. Shell Style – where XX depends on application;
2. Plating – α (where α is not W);
3. Shell Size - B;
4. Insert Arrangement - 11-35;
5. Contact Style – S (Socket);
6. Keyway Polarisation:
   a. N – For the basic security domain
   b. A – For higher security domain
      (subject to approval of national security authority).

D38999/XXα B35SN (or A) Contact Position ID	**Ethernet Channel**	**Signal**
1	N/C	N/C
2	A	BI_DD-
3	N/C	N/C
4	A	BI_DC-
5	A	BI_DC+
6	N/C	N/C
7	A	BI_DA+
8	N/C	N/C
9	A	BI_DB+
10	A	BI_DB-
11	A	BI_DD+
12	A	Isolated Screen
13	A	BI_DA-

Table 11: Single Ethernet Connector Pinout

NOTES: *The contacts highlighted in grey can be used as a 2-pair option used for 100Mb connections.*
Next to the connection to contact 12 the cable screen shall be electrically connected to the connector shell

Dual Connector: Where a dual Ethernet connection is required (e.g. for maximizing available switch space) the connector shall be of type MIL-DTL-38999, D38999/XXαC35SN (or A) with the pin out as defined in Table 12 and the detailed specification of:

1. Shell Style – where XX depends on application;
2. Plating – α (where α is not W);
3. Shell Size - C;
4. Insert Arrangement - 13-35;
5. Contact Style – S (Socket);
6. Keyway Polarisation:
    a. N – For the basic security domain
    b. A – For higher security domain
    (subject to approval of national security authority).

Note: The NGVA interface panel shall present the socket gender as defined by the socket connector part number.

D38999/XXαC35SN (or A) Contact Position ID	Ethernet Channel	Signal
1	A	BI_DD-
2	N/C	N/C
3	B	BI_DA-
4	N/C	N/C
5	A	BI_DA-
6	B	BI_DC-
7	B	BI_DC+
8	A	BI_DC+
9	A	BI_DC-
10	B	BI_DB-
11	N/C	N/C
12	A	BI_DB-
13	N/C	N/C
14	B	BI_DD-
15	A	BI_DD+
16	B	BI_DA+
17	A	BI_DA+
18	B	Isolated Screen
19	B	BI_DB+
20	A	BI_DB+
21	B	BI_DD+
22	A	Isolated Screen

Table 12: Dual Ethernet Connector Pinout

NOTES: The contacts highlighted in grey can be used as a 2-pair option used for 100Mb connections.
Next to the connection to contacts 18 and 22 the cable screen shall be electrically connected to the connector shell

5.1.2.2. 10Gb/s Ethernet

To allow future expansion in the amount of data transmitted across Vehicle Platforms, in particular the uptake of Digital Video and higher definition video, this standard specifies a high bandwidth, 10Gb Ethernet network.

The fibre optic is the only media that can support mid-term and long-term future requirements in terms of data transmission (> 100Gb/s and in future prospective up to 450Gb/s, speed is highly dependent on transceiver technology and Optical Multi-mode level, however it would provide sufficient bandwidth to any foreseeable future application). An additional benefit of fibre optic is their intrinsic immunity to EMI, which e.g. eliminates security concerns from a cabling galvanic cross coupling.

Keyway Polarisation: Two different Keyway Polarisation are specified in this standard to add a physical layer of protection against the accidental connection of equipment to an incorrect security domain.

Single Channel Optical Connector: The single channel optical Ethernet connector shall be of type EN4531xB02yα (D or E) with specification:

1. Connector specification – EN 4531-001
2. Contact specification:
    a. EN 4531-101 for multimode fibre
    b. EN 4531-201 for singlemode fibre
3. Shell Style – where x depends on application;
    a. 0: square flange receptacle,
    b. 7: jam nut receptacle,
    c. 5: plug
4. Shell Size – B
5. Insert Arrangement – 02 (2 cavities);
6. Contact Style – where y depends on shell style:
    a. A for receptacle and male insert
    b. C for plug with female insert
7. Plating – α (where α is not W);
8. Keyway Polarisation:
    a. D – For the basic security domain
    b. E – For higher security domain
    (subject to approval of national security authority).

Contact Position ID	Function
1	Tx Ethernet
2	Rx Ethernet

Table 13: Fibre Ethernet Connector Pin out (fibre pair, “SR”) for NGVA Interface Panel

Contact Position ID	Function
1	Tx/Rx Ethernet

Table 14: Fibre Ethernet Connector Pin out (single fibre, “BX”)

The two fibre version "SR" described in Table 13 shall be used. Exception would be for data transmission via small rotary joints (slip-rings) when simplex fibres described in Table 14 may be used.

Dual Channel Optical Connector: The dual channel optical Ethernet connector shall be of type EN4531xC04yα (D or E) with specification:

1. Connector specification – EN 4531-001
2. Contact specification
   a. EN 4531-101 for multimode fibre
3. Shell Style – where x depends on application;
   a. 0: square flange receptacle
   b. 7: jam nut receptacle
   c. 5: plug
4. Shell Size – C
5. Insert Arrangement – 04 (4 cavities);
6. Contact Style – where y depends on shell style:
   a. A for receptacle and male insert
   b. C for plug with female insert
7. Plating – α (where α is not W);
8. Keyway Polarisation:
   a. D – For the basic security domain
   b. E – For higher security domain
   (subject to approval of national security authority).

The pin-out for the dual channel optical Ethernet connector shall be as indicated in Table 15.

Contact Position ID	Function
1	Tx Ethernet 1
2	Rx Ethernet 1
3	Tx Ethernet 2
4	Rx Ethernet 2

Table 15: Fibre Ethernet Dual Connector (two fibre pairs, "SR") Pin out

5.1.3. Connectors for Video and Audio

The connectors listed above are valid for the NGVA Interface Panel. Different connector types may be used on the sub-systems connected to the panel when appropriate adapter cables are provided.

Note that PLEVID specifies different connectors for cameras and audio devices in STANAG 4697.

5.1.4. Network Cabling

All NGVA Ethernet cabling shall be capable of at least 1000BASE-T operation.

Category 5e cable (ANSI/TIA/EIA-568-A) is suitable for most varieties of Ethernet over twisted pair up to 1000BASE-T, where Category 6a cable (ANSI/TIA-568-C.1) is capable to be used up to 10GBASE-T. These maximum speeds can only be achieved when its construction respects certain quality levels.

To ensure the right quality in terms of signal integrity, EMI shielding and speed in particular for the Category 6a cable, the NGVA Ethernet copper cabling should be compliant to the EN 50288-10-2 standard.

To work correctly, 10Gb/s Ethernet over fibre optic cable requires a cable of a certain specification. IEC 60793 is the international standard which defines the characteristics that optical fibre used for 10Gb/s Ethernet, this standard must be supported.

Given the challenging operational environment, NGVA Platforms should feature only crush resistant fibre optic compliant with the EN-3745 standards, this to ensure a standardized level of the fibre optic mechanical performances and foster their adoption.

The NGVA network cabling must comply with the requirements in Table 16.

Unique ID	Requirement Type	Requirement Text
Network Cabling		
NGVA_INF_028	CR	All NGVA Ethernet copper cabling shall be capable of at least 1000BASE-T operation.
NGVA_INF_029	OE	If 10Gb/s operations are necessary, then optical fibres which comply with IEC 60793 shall be used.
NGVA_INF_030	CR	Optical fibres used for Ethernet interfaces shall comply with one of the following two specifications: • multimode, graded-index optical fibre waveguide with nominal 50/125 µm core / cladding diameter and numerical aperture complying with Ala.2 (OM3) optical fibre as defined in IEC 60793-2-10 dated 1 Mar 2011. • singlemode, graded-index optical fibre waveguide with nominal 9/125 µm core/cladding diameter and numerical aperture complying with B1 (OS1) optical fibre as defined in IEC 60793-2-50 dated 25 October 2013.

Table 16: NGVA Network Cabling Requirements

5.1.5. Network Devices

The NGVA network devices must comply with the requirements in Table 17.

Unique ID	Requirement Type	Requirement Text
Network Devices		
NGVA_INF_031	OE	10Gb/s transceiver on multimode fibre should comply with the following requirements: - 1 fibre for Rx, 1 fibre for Tx as defined by 10GBASE-SR in standard IEEE 802.3ae 2002 - bit rate : 10.3125Gb/s - wavelength : 850 nm
NGVA_INF_032	OE	10Gb/s transceiver on singlemode fibre should comply with the following requirements: - 1 fibre only for Rx/Tx as defined by 10GBASE-BX in standard IEEE 802.3ae 2002 - bit rate : 10.3125Gb/s - wavelength : Tx / Rx: 1270 nm / 1330 nm +/- 10 nm

Table 17: NGVA Network Devices Requirements

5.2. Data Link Layer

The NGVA Data Infrastructure shall be based on Ethernet[1]. Table 18 describes the NGVA Data Link Layer requirements.

Unique ID	Requirement Type	Requirement Text
Data Link Layer		
NGVA_INF_033	CR	IEEE 802.3 compliant Ethernet technology shall be used for NGVA Data distribution (except for the connectors specified in Section 5.1.2).

Table 18: NGVA Data Link Layer Requirements

5.3. Network Layer

Either IPv4 or IPv6 shall be used as the default standard.

All NGVA Data Infrastructure network devices shall support:

1. ICMP (for error message transmission on network device level)
2. IGMP (incl. IGMP snooping; for multicast management, e.g. for DDS)
3. Diffserv or equivalent (for network traffic management, e.g. flow control and QoS).

[1] **IEEE 802.3 - Ethernet Standards Collection**

Table 19 below describes the NGVA Network Layer requirements.

Unique ID	Requirement Type	Requirement Text
Network Layer		
NGVA_INF_034	CR	The NGVA Data Infrastructure shall support Internet Protocol IP Version 4 (RFC 791) or IP Version 6 (RFC 2460).
NGVA_INF_036	CR	The NGVA Data Infrastructure shall support ICMP for error message transmission.
NGVA_INF_037	CR	The NGVA Data Infrastructure shall support IGMP for multicast management.
NGVA_INF_038	CR	Layer 3 network devices shall support Diffserv or equivalent for network traffic management.

Table 19: NGVA Network Layer Requirements

5.3.1. IP Addressing

Address resolution mechanisms used to create a manageable network are:

1. ARP for local address resolution.
2. DHCP for local IP address allocation
3. DNS for global network naming
4. NAT/NATP to decouple local address space from external network addresses

Either fixed predefined IP-Configuration or dynamic addressing using DHCP may be used.

If STANAG 4697 Part 2 is the chosen standard for video distribution, the addressing scheme and requirements defined in that standard need to be considered and implemented, i.e. the use of static IP addresses and the multicast IP addresses derived from them. Table 20 below describes the IP Addressing requirements.

Unique ID	Requirement Type	Requirement Text
IP Addressing		
NGVA_INF_039	CR	The NGVA Data Infrastructure shall support ARP for local address resolution.
NGVA_INF_040	OE	The NGVA Data Infrastructure may support DHCP for local IP address allocation.
NGVA_INF_041	OE	The NGVA Data Infrastructure may support DNS for (global) network naming.
NGVA_INF_042	OE	The NGVA Data Infrastructure may support NAT/NATP to decouple local address space from network addresses.
NGVA_INF_043	CR	If static IP addresses are used they shall be excluded from the DHCP domain.

Table 20: NGVA IP Addressing Requirements

5.4. Transport Layer

This AEP-4754 Volume III and STANAG 4697 require the use of UDP, RFC 768. The NGVA Data Infrastructure thus needs to support unicast, multicast, and broadcast UDP for IPv4. If IPv6 is also provided, unicast and multicast UDP needs to be supported.

DDS shall be configured to use Multicast UDP for discovery. Specific implementations may also use unicast UDP and shared memory for discovery.

NGVA Data distribution in the Vehicle Platform shall use Multicast UDP for NGVA Data, if supported by the DDS implementation. Publishers targeting Multicast UDP for NGVA Data, however, must also support unicast subscription for potential Subscribers that cannot take advantage of Multicast UDP for NGVA Data delivery.

Next to UDP, the Transport Layer requirements include the Transmission Control Protocol for end-to-end acknowledged and sequenced data transfer (Unicast only).
Table 21 describes the NGVA Transport Layer requirements.

Unique ID	Requirement Type	Requirement Text
Transport Layer		
NGVA_INF_044	CR	If IPv4 is provided, the NGVA Data Infrastructure shall support Unicast, Multicast and Broadcast UDP. RFC 768
NGVA_INF_045	CR	If IPv6 is provided, the NGVA Data Infrastructure shall support Unicast and Multicast UDP. RFC 768
NGVA_INF_095	OE	The NGVA Data Infrastructure should support the Transmission Control Protocol. RFCs 793, 1122, 3168, 6093, 6528.

Table 21: NGVA Transport Layer Requirements

5.5. Application Layer

5.5.1. Network Services

5.5.1.1. Time Service

The local clocks of the NGVA Ready sub-systems need to be synchronized such that a common time is used throughout the network inside the vehicle. The DDS exchange mechanism requires a monotonic increasing clock to operate correctly with timestamps and timeouts. Therefore, a protocol is required which avoids discontinuous steps and rather speeds up or slows down the clock frequency in order to synchronize time between the NGVA Network nodes.

Therefore, the Vehicle Platform shall not allow Operators to change the time of individual sub-systems. Specific functionality shall be implemented to set an initial time or to correct the time during run-time for the complete network.

Time synchronization shall be implemented as a standard service, using NTP (RFC 5905). The network shall provide at least one NTP-Server, and preferably a second one for redundancy. A sufficiently accurate time source needs to be available to the NTP server, e.g. GPS based time signal. Connected computer systems shall use NTP clients.

The initial date of devices in the network shall be a date near the development date of the device in order to avoid a faulty behaviour after the “wrap around” of NTP in the year 2036.

Implementations shall avoid the “UNIX Millennium Bug” and use 64bit timestamps on the whole network.

Where NTP is insufficient and high accuracy time synchronization is required, PTP (IEEE 1588-2008) shall be used.

5.5.1.2. Dynamic IP Allocation Service

If dynamic IP allocation is required, the Dynamic Host Configuration Protocol (DHCP) shall be used. For reliability reasons, redundant DHCP servers shall be made available in the network in order to avoid a single point of failure.

If STANAG 4697 Part 2 is chosen for video streaming static IP address allocation shall be implemented accordingly. The specific requirements need to be considered by configuring DHCP accordingly for the nodes specific to the video streaming system. DHCP shall then not provide addresses in the video node address range.

A network node needs to be able to detect the usage of the same IP address on the network and to act according to RFC 5227 (send a DHCPDECLINE, a SNMP message or use of another conflict resolution mechanism).

5.5.1.3. Domain Naming Service

The Domain Name System (DNS) is described in RFC 1034 and RFC 1035 and translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices inside the network.

DNS is an optional enhancement to the NGVA Data Infrastructure which needs to be used with care. The use of domain names makes the network depend on the functioning of the DNS service. For reliability reasons, redundancy for the DNS service may be considered for the NGVA Data Infrastructure when using DNS.

DNS is especially needed if DHCP is used and addresses are dynamically assigned depending on the actually available stack of addresses. Table 22 below describes the NGVA Application Layer requirements.

Unique ID	Requirement Type	Requirement Text
Application Layer		
NGVA_INF_066	CR	Time synchronization shall be used for the devices using date or time for their operation and for all devices using DDS.
NGVA_INF_067	CR	Operators shall not be allowed to change time settings of individual Vehicle Platform sub-systems directly.
NGVA_INF_068	CR	A specific functionality shall be implemented for the Operator to set an initial time during run-time covering the complete NGVA Compliant Electronic Architecture. Preferably, automatic time setting by a common time source (e.g. based on GPS), shall be available.
NGVA_INF_069	CR	A specific functionality shall be implemented to maintain time during run-time covering the complete NGVA Compliant Electronic Architecture. Automatic time synchronization by a common time source shall be available.
NGVA_INF_096	OE	The common time source should be based on a global time source (e.g. based on GPS or based on an accurate clock).
NGVA_INF_070	CR	Both for IPv4 and IPv6, a time server using NTPv4 (RFC 5905) shall be available for time synchronization and used by the NGVA Network devices unless a more precise time is needed.
NGVA_INF_071	CR	The NTP Server and the common time source shall avoid discontinuous changes of the clock and going backwards in time.
NGVA_INF_072	OE	For higher precision timing PTPv2 (IEEE 1588-2008) shall be used.
NGVA_INF_073	CR	The NGVA Data Infrastructure and connected equipment/sub-systems shall not be sensitive to known time bugs and services such as the 2036 NTP overflow and the “UNIX Millennium Bug”.
NGVA_INF_075	CR	If dynamic IP address allocation is required then DHCP shall be used.
NGVA_INF_076	OE	If the DHCP service is used then redundant DHCP servers may be implemented.
NGVA_INF_077	OE	A DNS server may be used for address resolution with the required reliability (may need several redundant servers).
NGVA_INF_078	CR	All NGVA Data Infrastructure network nodes shall be able to detect and handle IP address conflicts as described in RFC 5227.

Unique ID	Requirement Type	Requirement Text
Application Layer		
NGVA_INF_063	CR	If DHCP is chosen, IP address allocation and video, audio, or voice is transmitted according to STANAG 4697 part 2, the DHCP servers shall be configured such that IP address allocation is compatible with the fixed addressing specified in IEEE 802.3.

Table 22: NGVA Application Layer Requirements

5.5.2. NGVA Data distribution

NGVA Data is formalized in the NGVA Data Model and may have some real time or streaming characteristics.

NGVA Data shall be formatted in accordance with the NGVA Data Model and use DDS middleware utilising the DDSI (RTPS) wire for distribution across the NGVA Data Infrastructure.

DDS is an OMG Data Standard and defines a data-centric publish-subscribe architecture for interconnecting sub-systems (composed of data providers and consumers) that promotes loose coupling between these sub-systems. A data provider publishes on typed data channels called 'topics', to which data consumers can subscribe. A sub-system may simultaneously fulfil the roles of data provider and consumer. A typical DDS application architecture can be represented as a software data bus.

DDSI is the Wire Protocol Specification that enables interoperability between different vendor DDS applications. The specification is part of the open OMG DDS Standard.

The NGVA Data Model defines a set of data topics for military for communication between sub-systems of the NGVA Electronic Architecture. The NGVA Data Model is further described in AEP-4754 Volume V. Table 23 below describes the NGVA Data distribution requirements.

Unique ID	Requirement Type	Requirement Text
NGVA Data Distribution		
NGVA_INF_046	CR	DDS shall be configured to use Multicast UDP for discovery.
NGVA_INF_047	CR	NGVA Data distribution in the Vehicle Platform shall use Multicast UDP for DDS Configuration Data, if supported by the DDS implementation.
NGVA_INF_048	CR	If NGVA_INF_047 is required, publishers targeting Multicast UDP for NGVA Data shall also support unicast subscription for potential Subscribers that cannot take advantage of Multicast UDP for DDS Configuration Data delivery.

Unique ID	Requirement Type	Requirement Text
NGVA Data Distribution		
NGVA_INF_049	CR	NGVA Data shall be exchanged on the NGVA Data Infrastructure using DDS middleware [1] conforming to the DDSI-RTPS wire protocol [2]
NGVA_INF_050	CR	The DDS middleware shall use the default configuration listed in the DDSI-RTPS wire protocol [2]. (E.g. see Section 9.6.1 of DDSI-RTPS version 2.3)
NGVA_INF_051	CR	When a vehicle sub-system realizes capabilities that are covered by the NGVA Data Model, DDS Topics generated from the NGVA DM shall be used and implemented as specified in AEP-4754 Volume V

Table 23: NGVA Data Distribution Requirements

5.5.3. Video and Audio distribution

5.5.3.1. Video Data

Video data is defined as streaming data used for real-time video distribution which generally requires low latency and a relatively high data throughput capability. The data may be raw or compressed using a video codec.

Video Data shall be distributed through the NGVA Network using STANAG 4697 or DDS. The STANAG 4697 describes two alternatives:

1. a specifically configured GigE Vision and
2. Def Stan 00-082 VIVOE[2]

Unique ID	Requirement Type	Requirement Text
Video Data Distribution		
NGVA_INF_055	CR	Video Data shall be distributed in the NGVA Data Infrastructure as specified in STANAG 4697 or using the NGVA Data Model Video Module and DDS.

Table 24: Video Data Distribution Requirements

5.5.3.2. Audio Data

Audio Data is defined as streaming data used for real-time audio distribution which may be generated by audio sensors but may also include digital voice communication data. Audio Data generally requires low latency and requires a much lower data throughput capability than Video Data but still much higher than NGVA Data. The data may be raw or compressed using an audio codec.

[2] It should be noted that Def Stan 00-082 requires a specific scheme for IP addresses and addressing which needs to be considered when setting up the network.

STANAG 4697 Part 2 describes the transmission of Audio Data and defines the protocols to be used but not the audio encodings. For NGVA, Audio Data, especially from audio enabled video sensors, shall be transmitted according to STANAG 4697[3].

Unique ID	Requirement Type	Requirement Text
Data Distribution		
NGVA_INF_056	OE	Audio Data not being Voice Data associated with automotive and C2ISR sensors shall be distributed in the NGVA Network as specified in STANAG 4697[4].

Table 25: Audio Data Distribution Requirements

5.5.4. Voice Data distribution

Voice Communications describes the intercom systems inside a Vehicle Platform and also the communication outside the Vehicle Platform, e.g. to higher echelons, to other vehicles, or to dismounted soldiers. Voice Data is distributed for Voice Communications but specific requirements need to be fulfilled such as maximum latency and a suitable session management for the voice connections. Voice Data is a subset of Audio Data and may be seen separate and be raw or compressed using an audio codec.

STANAG 4697 or VoIP technologies shall be used for this Voice Data. For VoIP the de-facto standard is Session Initiation Protocol (SIP) with the ITU G.711 A-law and L16 audio codecs. Therefore, for digital voice communication services, the modifications and extensions to STANAG 4697 described in the following sections (5.5.4.1 and 5.5.4.2) may be used.

Unique ID	Requirement Type	Requirement Text
Voice Data Distribution		
NGVA_INF_057	OE	Vehicle Platform internal Voice Communication may use SIP for session control.
NGVA_INF_058	OE	Vehicle Platform internal Voice Communication may use the codecs specified STANAG 4697.
NGVA_INF_059	OE	Vehicle Platform internal Voice Communications may use ITU G.711 A law as the audio codec.
NGVA_INF_060	OE	Vehicle Platform internal Voice Communications may apply audio codec with small jitter buffers with 10 ms frames.
NGVA_INF_062	OE	Vehicle Platform internal persistent voice sessions should be established at system start up.

Table 26: Voice Data Distribution Requirements

[3] Audio Data is not included in the Data Model but if added in the future it may do so as described in 5.5.2.

[4] If audio data is included in the NGVA Data Model, audio may also be distributed as described in Section 5.5.2

5.5.4.1. Session Control

STANAG 4697 uses SNMP for session control, which may be used for digital Voice Communications in the NGVA Data Infrastructure. The SIP standard (providing e.g. SIP-INVITE, SIP-BYE, and other relevant supporting messages) is widely used and provides a much richer and standardised set of capabilities for voice session control and therefore may also be used for voice communications in more enhanced solutions where interoperability with standard devices and gateways is required.

It is recommended to establish and maintain Vehicle Platform internal voice communication sessions at system start up. This improves the response time and effectiveness of the internal Voice Communication service.

5.5.4.2. Coding and Decoding

The codecs used when implementing audio streaming according to STANAG 4697 are limited to the mandatory L16, a basic Pulse-Code Modulation (PCM) and the optional MPEG-4 Part 3, also known as Advanced Audio Coding (AAC). These codecs may also be used for voice communication data.

The ITU G.711 A-law standard describes a widely used codec for digital telephony systems with 160 byte packet sizes and a delay of 20 ms. This codec may be used for Voice Data.

For all codecs small jitter buffers with 10 ms frames may optionally be used for lower latency applications.
For Vehicle Platform centric sessions/stream, latency values between 50 ms and 100 ms are recommended which may require smaller packet sizes for Voice Data frames compared to standard SIP/RTP. IETF specifies 120 ms as the max delay in full duplex conversation delay.

5.5.4.3. Digital Voice Communication Services

The scope of Voice Communication services is the distribution of Voice Data via the NGVA Data Infrastructure between Voice Communication devices, such as crew audio gear/phones, radios, loudspeakers and audio alerting devices. Voice streams could be ad-hoc or semi-permanent to selected end points. For safety reasons, some sessions could also need to be persistent (usual in vehicles).

Depending on the operational use cases, communication groups can be automatically or manually established. Communication groups act like ad-hoc conference groups with 1 to n participants.

Established communication group sessions could support late entry and drop out for any participant without reconfiguration.

The voice communication service device and the end point application should support the following characteristics:

1. Full duplex
2. Half duplex with external signalling handshake
3. Monitoring

The voice communication service could include noise reduction, external trigger and Voice Operated Transmission (VOX) activation mechanisms suitable for the noisy vehicle environment.

5.5.5. Human Machine Interface Data

HMI Applications may run directly on a Crew Terminal (CT) or may run remote on a central VM server or the individual sub-systems (e.g. Weapon System). An HMI connection is used as the data connection between the CT and remotely running applications. Applications running remotely shall not require dedicated displays but shall display their information on the CTs. The connection between the CT and remote running applications can be established e.g. by a Remote Desktop Interface, Thin Client (potentially via a security gateway), a simple Web Interface, or any other means.

As a part of the inherent modularity of future vehicles, one or several Mission Sub-Systems can be added to or removed from the initial Vehicle Platform configuration.
For example, an armoured vehicle may be temporarily fitted with an additional sensor system or for example an extra Augmented Reality application which combines Video Data with NGVA Data. These additional Mission Sub-Systems could be removed afterwards, or not. Such modularity shall not adversely affect the functioning of the Vehicle Platform and in particular shall not adversely affect the Crew Terminal functionality.

For further details see AEP-4754 Volume IV; NGVA Crew Terminal Software Architecture.

5.5.5.1. NGVA Sub-Systems Software

NGVA Sub-Systems are connected to the NGVA Data Infrastructure. They may be Crew Terminals which provide an interface to the Vehicle Crew or other systems such as sensor, processing, storage or gateway systems.

The software applications on NGVA Ready sub-systems need to perform the specific functions needed for a specific military vehicle. This software and these functions are therefore not within the scope of this AEP or the NGVA standardization. Neither the internal architecture of sub-system software nor the operating system and its configuration is defined within NGVA. The applications within NGVA Ready sub-systems could range from a complex workstation computer or a fire control system to a very small and simple embedded computer. However, software interfaces to the NGVA Data Infrastructure need to comply with its requirements.

5.5.6. Non-NGVA Data Exchange

The Ethernet based infrastructure provided by NGVA may also be used to distribute non-NGVA information packets as long as the NGVA Data, Video Data, Audio Data and HMI exchange functions are not adversely impacted.

Examples of such data exchanges might be data via other web protocols, e.g. http, ftp for configuration of network nodes, file transfer, e.g. Technical Documentation, and Web Services for higher level, less time critical functions.

As described in Section 4.1, the system integrator must ensure the reliable, smooth and quick start-up time of the important sub-systems in accordance with specific vehicle requirements, and may need to tune the NGVA network by using Quality of Service (QoS), Bandwidth Control, Traffic Shaping and use of VLANs as measures to achieve the desired performance.

Unique ID	Requirement Type	Requirement Text
Non-NGVA Data Distribution		
NGVA_INF_065	CR	If the Ethernet based infrastructure provided by NGVA is used to distribute other non-NGVA information packets the desired performance of the NGVA Data, Video Data, Audio Data and HMI exchange functions shall not be adversely impacted.

Table 27: Non-NGVA Data Distribution Requirements

CHAPTER 6 NGVA DATA INTERFACES

Where the NGVA Data Infrastructure with one or more NGVA Networks is discussed in CHAPTER 5, this CHAPTER will discuss all equipment directly connected to the NGVA Data Infrastructure. To be able to connect to an NGVA Network these equipment must be NGVA Ready. In general, the equipment can be split into NGVA Ready sub-systems directly connected to one of the NGVA Networks and other (non-NGVA Ready) sub-systems and networks which are connected using a gateway.

6.1. NGVA Ready sub-systems

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.

An NGVA Ready sub-system must ensure that it does not adversely affect operation or performance of an NGVA Network, e.g. by excessive traffic generation. Also care shall be taken to limit access to the NGVA Network only to the desired communication and thus reduce the risk of unforeseen influences, especially for security purposes.

Connectivity Compatibility means the NGVA Ready Sub-System shall use a mating connector on its interconnection cable. The connector shall be the mating part of what is required in sections 5.1.2 and 5.1.3.

Communication Compatibility means the NGVA Ready Sub-System shall use the same protocols as specified in sections 5.2, 5.3, 5.4 and 5.5.

6.2. Gateways

Gateways shall be used to connect non-NGVA compliant sub-systems or networks to the NGVA Data Infrastructure (see Figure 8). Their task is to convert physical, electrical, protocol, data and service interfaces from the non-NGVA domain to the NGVA domain. The same rules apply for gateways as for NGVA Ready sub-systems. In that sense gateways shall be NGVA Ready as well. Also, the gateway must ensure that it does not adversely affect operation or performance of an NGVA Network, e.g. by excessive traffic generation. Gateways can also be used as barriers to limit access to the NGVA Network and thus reduce the risk of unforeseen influences, especially for security purposes.

Examples of where gateways must be used for connecting to the NGVA Data Infrastructure:

1. Legacy or non-NGVA Mission Sub-Systems not using NGVA Data and/or Audio/Video Data according to this STANAG,
2. Automotive bus based networks or non IP based networks, or
3. External devices or networks.

A specific application of gateways is the separation of different NGVA Networks for security reasons (Security Gateway) or safety reasons (Safety Gateway).

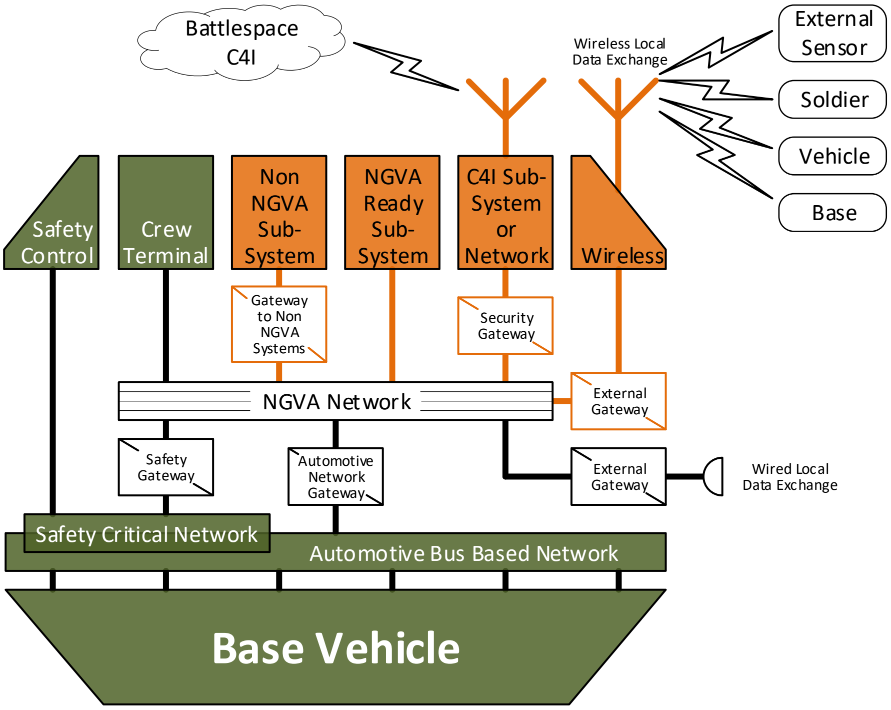


Figure 8: Example of NGVA Gateways

6.2.1. Gateways to Non-NGVA Equipment

There will be requirements to connect sub-systems or devices to the NGVA Data Infrastructure, which were developed before this STANAG was ratified. The development or use of upgraded sub-systems which natively comply with NGVA is strongly encouraged.

In order to integrate a Non-NGVA Ready sub-system or component into an NGVA Compliant Vehicle Platform, a Gateway to Non-NGVA Systems must be provided. The Gateway to Non-NGVA Systems on one side will be compatible with the NGVA Data Infrastructure and on the other side compatible to the specific data connection of the Non-NGVA Ready sub-system. The Gateway to Non-NGVA Systems will ensure that the sub-system or component will provide and receive NGVA Data, Video Data, Audio Data and/or Voice Data.

This is especially important;

1. if the sub-system needs to be operated by an NGVA Ready Crew Terminal,
2. if it provides data (potentially) required to be consumed by other sub-systems, or
3. if it needs access to data which is available on the NGVA Network.

Gateways to Non-NGVA Systems need to fulfil certain minimal requirements to be connected to the NGVA Data Infrastructure as listed in Table 28.

6.2.2. Automotive Network Gateway

It is expected that automotive bus based networks, e.g. CAN or STANAG 4628, will still be widely used in the near future as part of the Base Vehicle because of its broad distribution in all major civilian and military vehicles. Especially, for low level data exchange and control, there are major advantages in using these bus protocols. These are low cost widely available products with worldwide knowledge in using these technologies. However, it could be that these bus based networks may be replaced by new technologies or will be based on Ethernet in the future.

Multiple sub-systems connected to the NGVA Data Infrastructure may need to use some of the data available on the automotive bus based networks such as speed of the vehicle, motor rotation speed, faults, wear and maintenance data, HUMS data, logistic data, etc. An Automotive Network Gateway shall transfer the required data to the NGVA Data Infrastructure and makes them available.

In some cases the automotive bus based network may need some data from the NGVA Data Infrastructure which also needs to be addressed by the Automotive Network Gateway functionality.

If an NGVA based data infrastructure does not provide the necessary safety level, multiple redundant CAN or STANAG 4628 buses (or other safety critical networks) may be used to implement the safety critical functions which then interfaces to the NGVA Data Infrastructure with the Automotive Network Gateway described here.

6.2.3. External Data Communications

External networks are typically part of a battlespace C4I system. However, when vehicles are in close proximity, non-C4I system communications may be used providing fast transmission, high level of details, and information that may require high data throughput.

An External Gateway may also integrate Voice Communication to the outside world. VoIP may be used for this connection (see Section 5.5.4). End to end voice session management, including naming and addressing using SIP mechanisms, a set of widely used codecs and RTP for transmission will increase interoperability.

Another function of an External Gateway may be to connect to external sensors, like unattended ground sensors or drone sensors.

6.2.3.1. C4I System Integration

Generally, data exchange with other units, e.g. vehicles, dismounted soldiers or headquarters is carried out with C4I systems. Such systems are widely used today but they usually constitute a distributed information exchange network, which is driven by high echelons requirements and are less specific to the specific needs of a vehicle or a group of nearby vehicles (e.g. patrols or convoys).

Future C4I systems need to be integrated onto the NGVA Data Infrastructure because they will need to use the same Crew Terminals and standardised NGVA Data services. This means they do not need to provide an additional screen or control unit or duplicate functions and services on the vehicle.

Data and services on the NGVA Data Infrastructure may be used by the C4I sub-system and also C4I sub-system data may need to be consumed by NGVA Ready sub-systems. For example, C4I systems may deal with sensor and effector data, which is part of NGVA. C4I on the other hand may provide Red Force position data which can be used to direct cameras and/or effectors connected to the NGVA Data Infrastructure.

A gateway between the C4I system and the NGVA Data Infrastructure is recommended as Optional Enhancement. A full integration of the C4I system into the NGVA Data Infrastructure has the benefit of reusing the common vehicle services, functions and resources. However, separated networks may be required in case they belong to different security domains. In this case an accredited security gateway may be necessary to bridge the C4I secure network and the NGVA Network.

6.2.3.2. Direct connection to other Platform Networks

The exchange of NGVA Data could especially be useful for nearby vehicles on the same level of command or with nearby dismounted or mounted soldiers. For them, data is required fast and with high level of detail. Sometimes also high data volumes are required such as video or imagery data.

These connections could be implemented in a wired or wireless manner. Dedicated short range data capable radios with high data rates could be used for a wireless interface.

For these direct platform to platform connections, an External Gateway to transmit NGVA Data is always necessary. The other external network could be non-NGVA Network, meaning NGVA Data should be converted into the other end protocol and data format. Also in case the other external network is NGVA based an External Gateway is necessary to avoid conflicts between NGVA Data topics of both networks. The gateway will also need to shield the NGVA Data Infrastructure from outside intrusions.

As such an External Gateway depends on the specific implementation or standard for the outside communication, and is out of scope of this AEP.

Unique ID	Requirement Type	Requirement Text
Gateways		
NGVA_INF_079	CR	An External Gateway shall be used to connect any external network to the NGVA Data Infrastructure.
NGVA_INF_080	CR	Gateways shall be used to connect non-NGVA compliant networks to the NGVA Data Infrastructure.
NGVA_INF_081	CR	Gateway to Non-NGVA Systems shall be used to connect non-NGVA Ready sub-systems to the NGVA Data Infrastructure.
NGVA_INF_082	CR	A gateway connected to an NGVA Network must ensure that it does not adversely affect operation or performance of an NGVA Network.
NGVA_INF_083	CR	Gateways shall also be used as barrier to limit access to the NGVA Network (e.g. refuse all unauthorized data connections) and thus reduce the risk of unforeseen influences.
NGVA_INF_084	CR	Gateways shall avoid unauthorised access or disclosure of data for security purposes.
NGVA_INF_086	CR	When connecting an automotive bus based network on the Base Vehicle which can provide NGVA relevant data, e.g. STANAG 4628, it shall be connected to the NGVA Data Infrastructure via an Automotive Network Gateway.
NGVA_INF_097	CR	When connecting a safety network, it shall be connected to the NGVA Data Infrastructure via a Safety Gateway.
NGVA_INF_089	CR	Connections to networks of other Vehicle Platforms shall use an External Gateway which shields the NGVA Data Infrastructure from the off Vehicle Platform network.
NGVA_INF_090	CR	Connections to NGVA Compliant networks of other Vehicle Platforms shall use an External Gateway which prepares the NGVA Data exchange for the transmission characteristics of the specific connection.
NGVA_INF_091	OE	Battlespace Voice Communications may be part of an External Gateway (C4I or Direct Connection to Other Platforms).
NGVA_INF_092	OE	The External Gateway may use SIP for session control and provide ITU G.729 or MELPe as possible codecs.

Table 28: NGVA Gateway Requirements

INTENTIONALLY BLANK

CHAPTER 7 PERIPHERAL DEVICE CONNECTIONS

Peripheral devices, such as joysticks, keyboards, roller wheels, buttons, etc. may be connected to the crew stations using Universal Serial Bus (USB) technology.

USB is an open industry standard defining the communication protocols, cabling and connectors between a host computer and other electronic devices. A common interface will facilitate standardisation and inter-changeability of peripheral devices.

Table 29 defines the pinout of the standard NGVA USB connector. It shall be of type MIL-DTL-38999 Series III, D38999/XXαA35N with the specification:

1. Shell Style – where XX depends on the specification;
2. Plating – α (where α is not W);
3. Shell Size – A;
4. Insert Arrangement – 9-35;
5. Contact Style – S (Socket);
6. Keyway Polarisation – N;

Contact Position ID	Function
1	USB_Ground
2	USB_2_D-
3	USB_2_D+
4	USB_1_D-
5	USB_1_D+
6	USB_+5V

Table 29: NGVA Standard USB 2.0 Connector Pinout

Table 30 details the requirements relating to peripheral devices attached to the NGVA Data Infrastructure.

USB 3.x, although widely used in the civil world, is not be supported yet, since there is no military, vendor independent connector standardized at the time this document was written. The much higher speed of USB 3.x is mainly useful for USB connected mass storage and camera devices. Such devices connected via USB are not considered in this AEP yet. Typically, the peripheral devices considered in this CHAPTER require only very low data throughput.

Unique ID	Requirement Type	Requirement Text
Peripheral Devices		
NGVA_INF_093	OE	Peripheral Devices may be connected to an NGVA Ready sub-system using USB 2.0 with a connector as described in this CHAPTER.

Table 30: NGVA Peripheral Devices Requirements

INTENTIONALLY BLANK

ANNEX A ABBREVIATIONS

AAC	Advanced Audio Coding
AEP	Allied Engineering Publication
AFDX	Avionics Full-Duplex Switched Ethernet
Amdt	Amendment
ARP	Address Resolution Protocol
ARINC	Aeronautical Radio, INCorporated
BIT	Built-in-Tests
BX	Bi-Directional
C2ISR	Command, Control, Intelligence, Surveillance and Reconnaissance
C4I	Command, Control, Communications, Computers and Intelligence
CAI	Confidentiality, Availability and Integrity
CAN	Controller Area Network
CR	Compulsory Requirement
CT	Crew Terminal
DAI	Dynamic ARP Inspection
DC	Direct Current
DDS	Data Distribution Service
DDSI	Data Distribution Service Interoperability
Def Stan	Defence Standard
DHCP	Dynamic Host Configuration Protocol
DI	Data Infrastructure
DiffServ	Differentiated Services
DNS	Domain Name System
DM	Data Model
DTL	Detail specification
DTMF	Dual-Tone Multi-Frequency
EN	European Norm
Gb	Gigabit
Gb/s	Gigabit per second
GPS	Global Positioning System
GVA	Generic Vehicle Architecture
HF	High Frequency
HMI	Human Machine Interface
HQ	Head Quarter
HUMS	Health and Usage Monitoring System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IFG	Infantry Fighting Vehicle
IGMP	Internet Group Management Protocol
IGMP-AC	Internet Group Management Protocol with Access Control
INF	Infrastructure
IP	Internet Protocol
ITT	Invitation to Tender

ITU	International Telecommunication Union
LAN	Local Area Network
LAVOSAR	Land Vehicle with Open System Architecture
Mb	Megabit
MELPe	Mixed-Excitation Linear Predictive enhanced
MIP	Multilateral Interoperability Program
MMHS	Military Message Handling System
Ms	millisecond
N/C	Not Connected
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NGVA	NATO Generic Vehicle Architecture
NTP	Network Time Protocol
OE	Optional Enhancement
OMG	Object Management Group
PCM	Pulse-Code Modulation
PLEVID	PLatform Extended Video Standard
PTP	Precision Time Protocol
QoS	Quality of Service
Rev	Revision
RFC	Request for Comments
RoHS	Restriction of Hazardous Substances
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
RTPS	Real-Time Publish-Subscribe
Rx	Receive
SA	Situational Awareness
SAE	Society of Automotive Engineers
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SR	Short Range
STANAG	STANdardization AGreement
STD	Standard
TSN	Time-Sensitive Networking
Tx	Transmit
UDP	User Datagram Protocol
USB	Universal Serial Bus
VIVOE	Vetronics Infrastructure for Video Over Ethernet
VoIP	Voice over IP
VOX	Voice Operated Transmission
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMF	Variable Message Format

INTENTIONALLY BLANK

AEP-4754 VOLIII (B)(1)