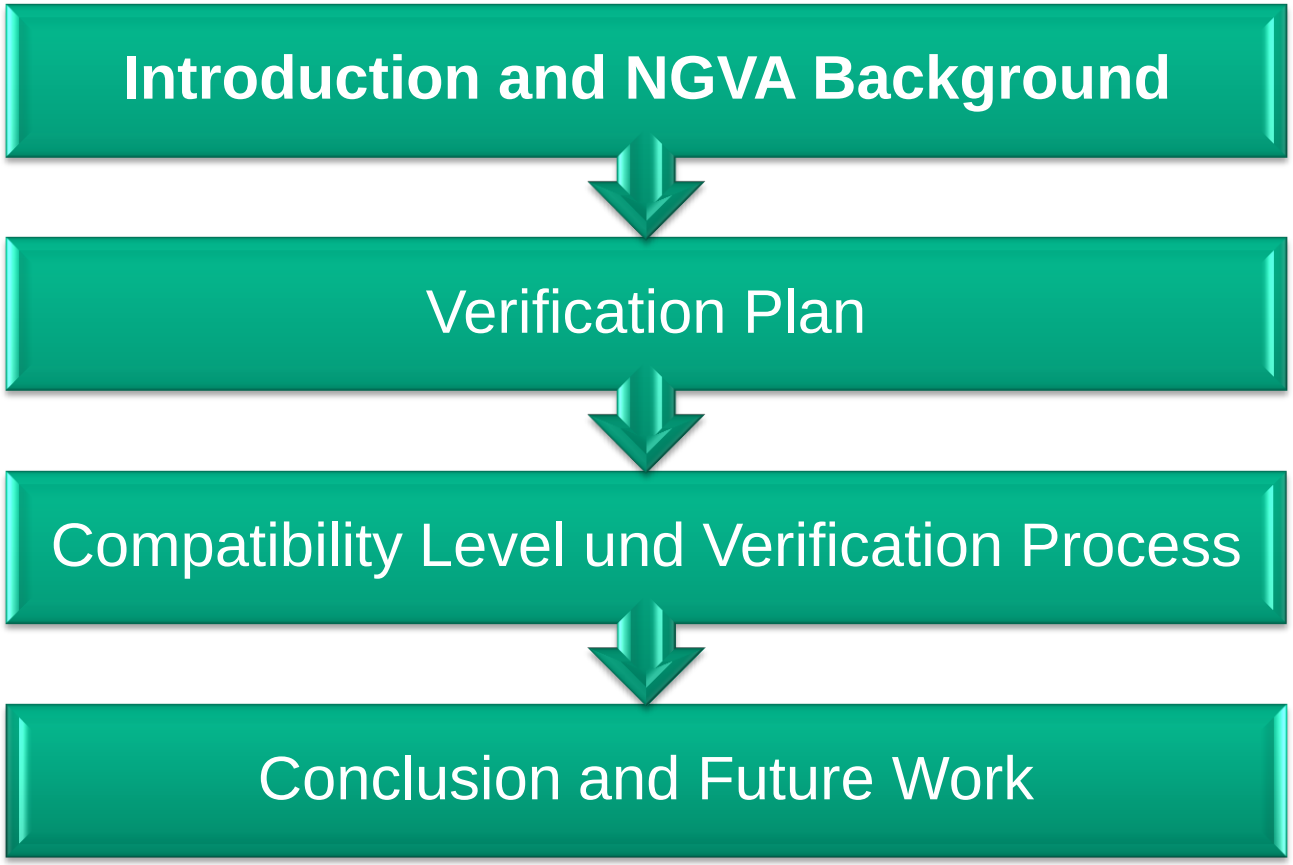
TOWARDS VERIFICATION OF NATO GENERIC VEHICLE ARCHITECTURE-BASED SYSTEMS

Fraunhofer
FKIE

Daniel Ota

21st International Command and Control Research and Technology Symposium (ICCRTS)
London, United Kingdom, 6th - 8th September 2016

OVERVIEW

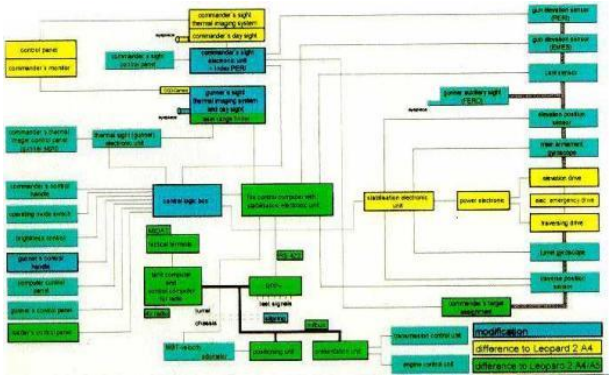


Introduction

- Lack of interoperability between components
- Either no or proprietary interfaces
- Variety of standards and protocols
- Poorly documented interfaces
- Specific operator panels per sub-system

Introduction

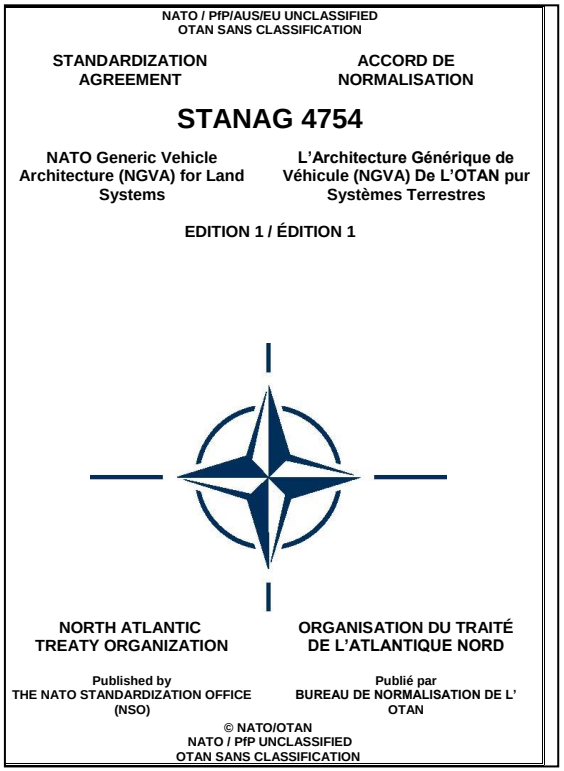
- Lack of interoperability between components
- Either no or proprietary interfaces
- Variety of standards and protocols
- Poorly documented interfaces
- Specific operator panels per sub-system



- National Initiatives on Open System Architectures
  - Modular Open Systems Approach to Acquisition
  - Future Airborne Capability Environment
  - Vehicle Integration for C4ISR/EW Interoperability
  - Generic Vehicle Architecture

NATO Generic Vehicle Architecture STANAG Aims

- Enable member nations to realize the benefits of an open architecture approach to land vehicle platform design and integration
  - Improve operational effectiveness
  - Reduce integration risks
  - Reduce cost of ownership
- Mandating appropriate interface standards and design constraints
  - Vehicle platform electronic data and power infrastructure
  - Associated safety guidelines and verification & validation process



NATO / PfP/AUS/EU UNCLASSIFIED
OTAN SANS CLASSIFICATION

STANDARDIZATION AGREEMENT

ACCORD DE NORMALISATION

STANAG 4754

NATO Generic Vehicle Architecture (NGVA) for Land Systems

L'Architecture Générique de Véhicule (NGVA) De L'OTAN pur Systèmes Terrestres

EDITION 1 / ÉDITION 1

NORTH ATLANTIC TREATY ORGANIZATION

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD

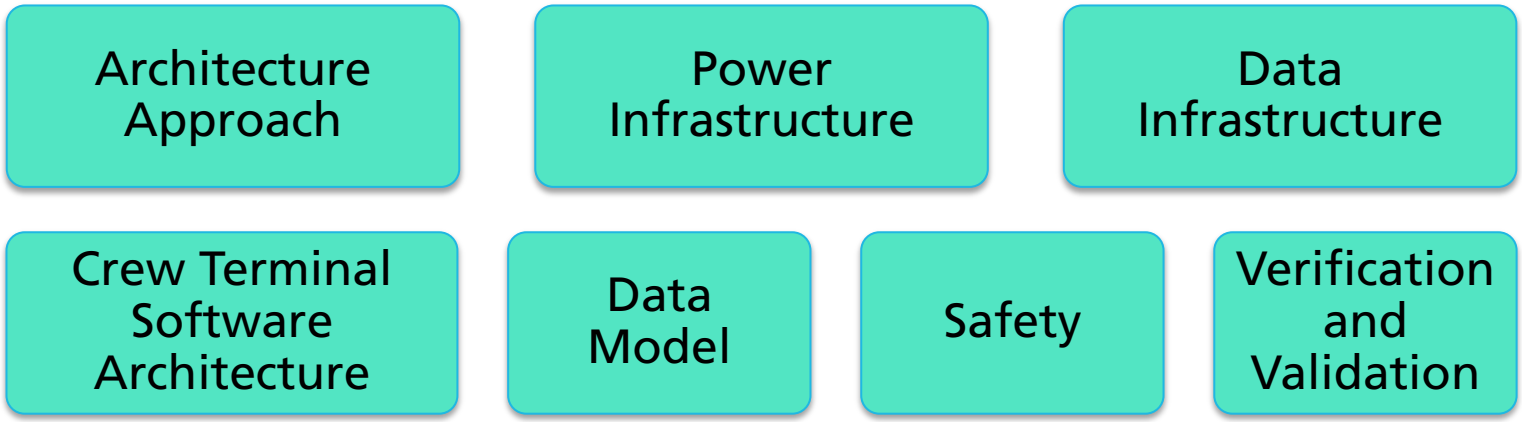
Published by THE NATO STANDARDIZATION OFFICE (NSO)

Publié par BUREAU DE NORMALISATION DE L' OTAN

NATO / PfP UNCLASSIFIED
OTAN SANS CLASSIFICATION

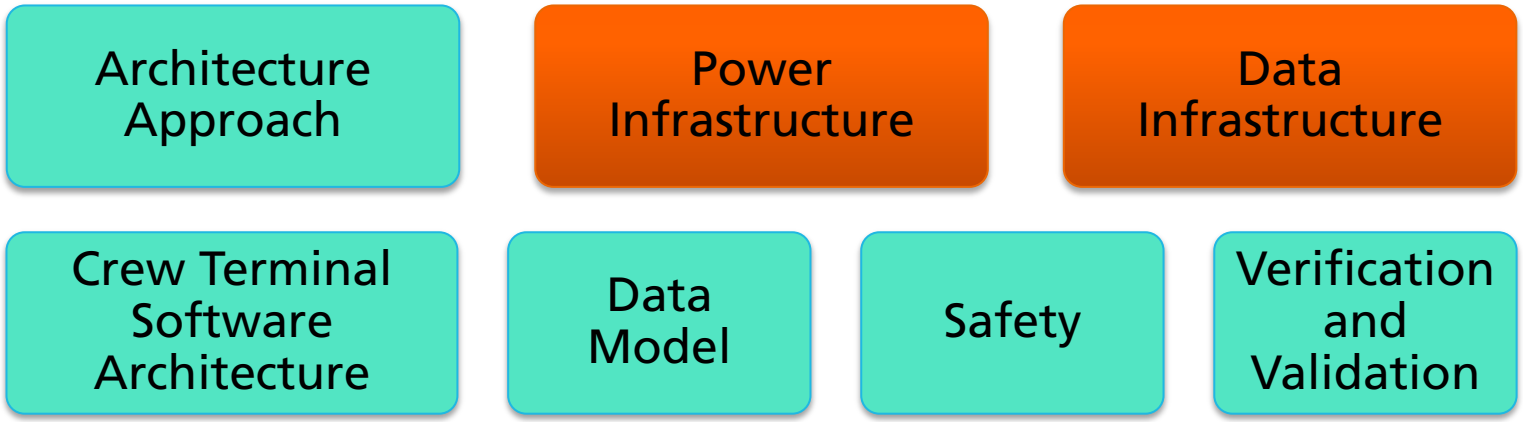
NGVA STANAG Structure

- NGVA consists of a main STANAG document and seven associated Allied Engineering Publications (AEP) Volumes



NGVA STANAG Structure

- NGVA consists of a main STANAG document and seven associated Allied Engineering Publications (AEP) Volumes



- Power Infrastructure and Data Infrastructure contain formal requirements to be verified for NGVA compliance

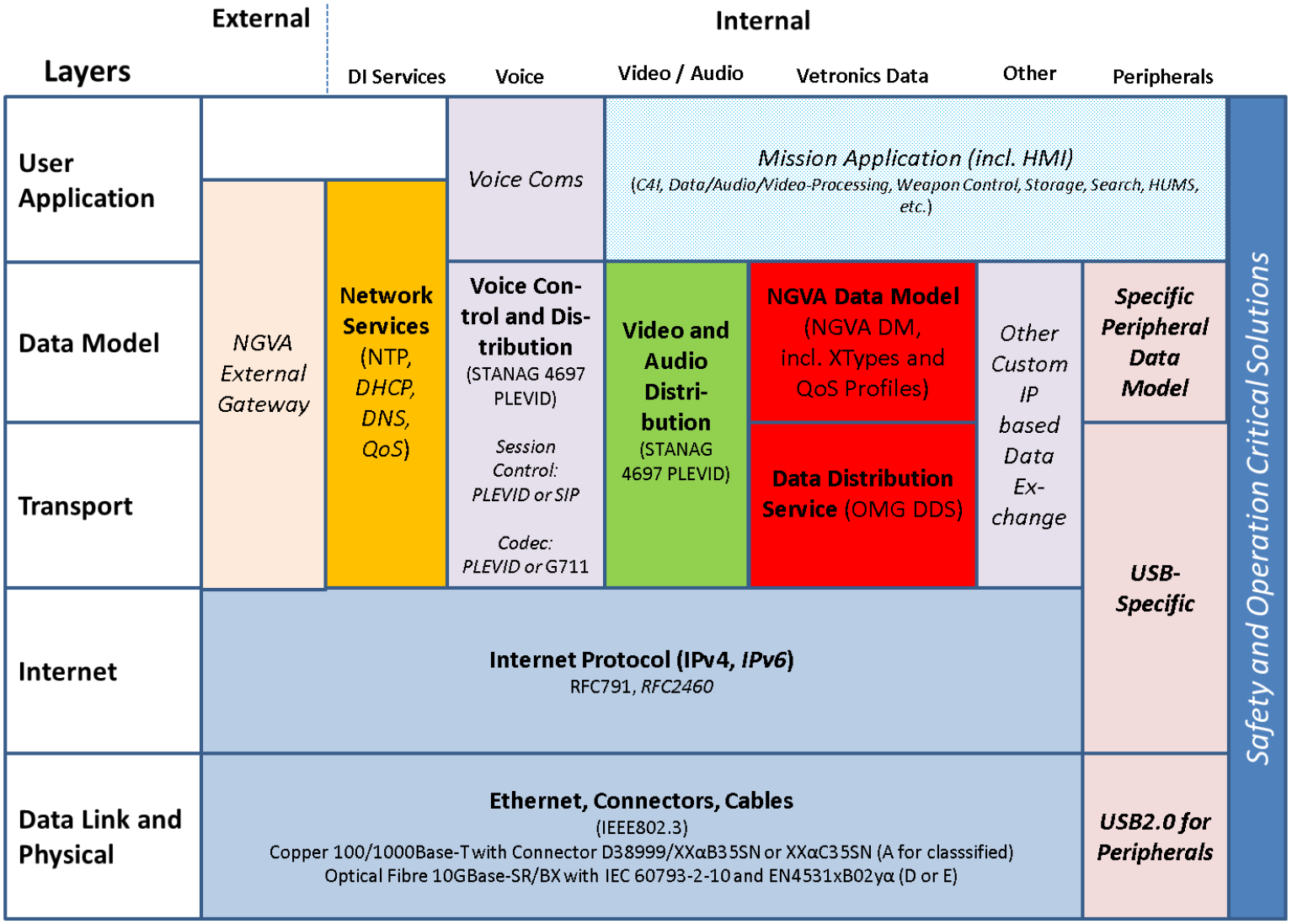
AEP-4754 Volume 2: Power Infrastructure

- NGVA Power Infrastructure refers to
  - Physical cables, connectors and other components that provide the means of distributing and controlling electrical power

- NGVA Power Infrastructure covers
  - Interfaces and connectors
  - Power conditioning
  - Power management
  - Power advice
  - Power control

	MIL-DTL-38999	VG 95234	VG 95328	
8A			D 14-19 SN	Low power and hardwired signals
13A			M 14-19 PN	
25A	C4SA			
60A	E06SN			Medium power
90A		B1 32-1 SN		High power
120 A	G48SN			
130 A		M 32-1 PN		

AEP-4754 Volume 3: Data Infrastructure



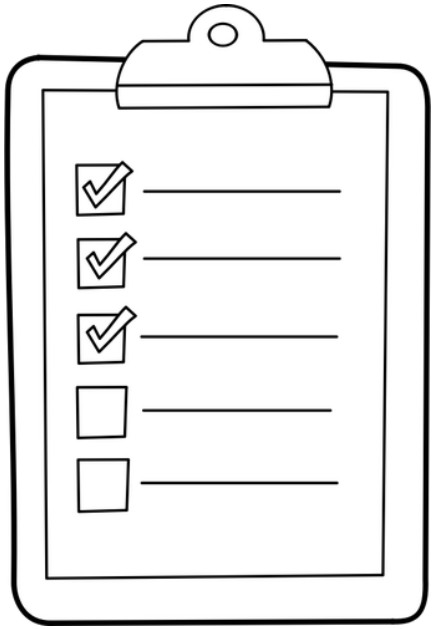
Fraunhofer FKIE

Example Requirements for Power and Data Distribution

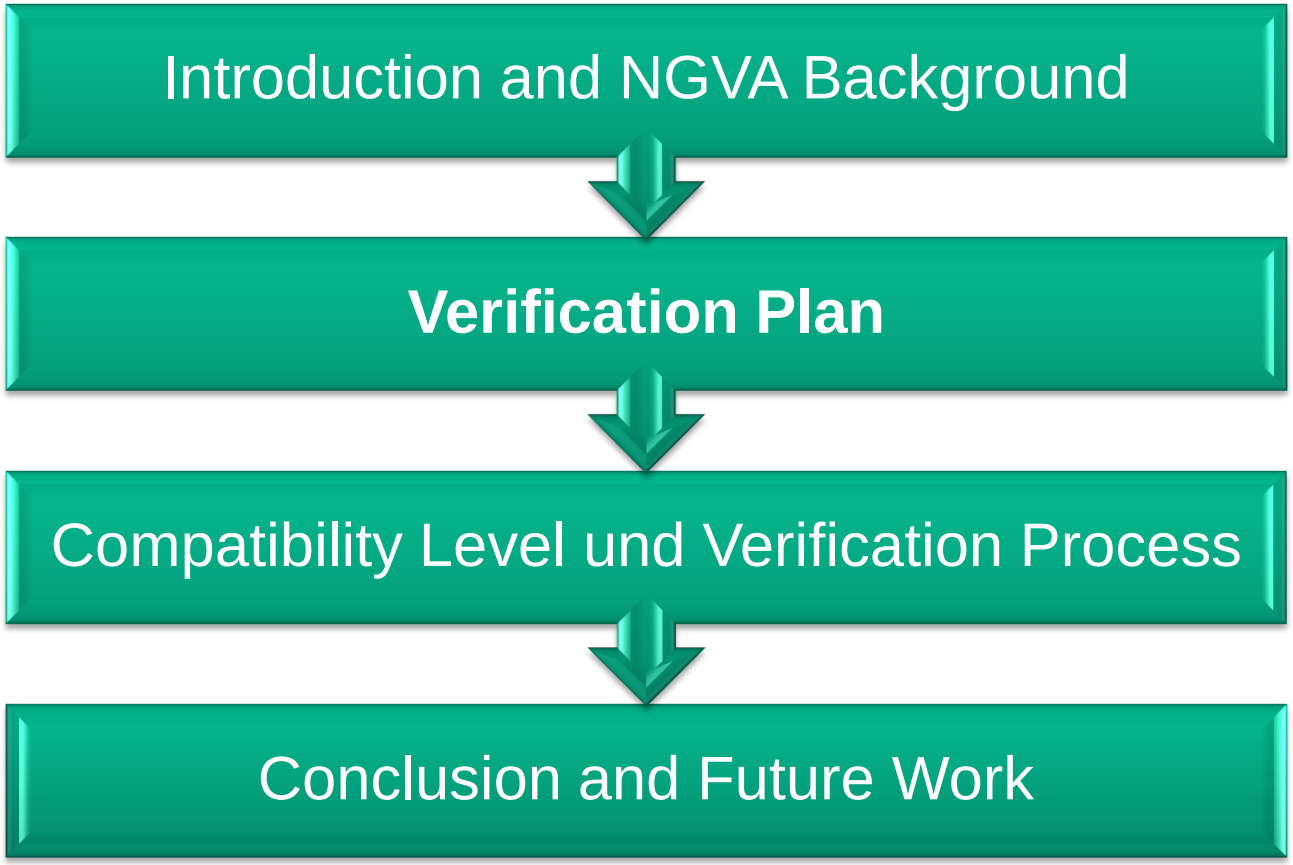
ID	Type	Requirement Description
NGVA_POW_008	CR	The NGVA 28V DC 25 ampere low power connector shall be of type MIL-DTL-38999 series III Rev L Amdt (07/2009), D38999/XX C98SA [...]
NGVA_POW_027	OE	The NGVA power [sub-system] shall inform the [vehicle crew] of the battery life remaining in hours and minutes at the current load.
NGVA_INF_002	CR	NGVA ready sub-systems shall comply with the NGVA Arbitration Protocol as defined in the NGVA Data Model.
NGVA_INF_009	CR	The NGVA network topology shall be such that the required data rates and latencies requirements can be achieved.
NGVA_INF_032	CR	Vetronics Data shall be exchanged by DDS topics using the "QoS pattern" attached to it in the NGVA Data Model to assure assignment of DDS topics.

AEP-4754 Volume 7: Verification and Validation

- Volume outlines a generic framework for verification and validation of NGVA systems
  - Common **terminology**
  - Guidance on the development of a **verification plan**
  - Incremental **certification process** for NGVA conformity based on three sequentially-related compatibility levels
  - Specification of a five-stage **verification process**



OVERVIEW

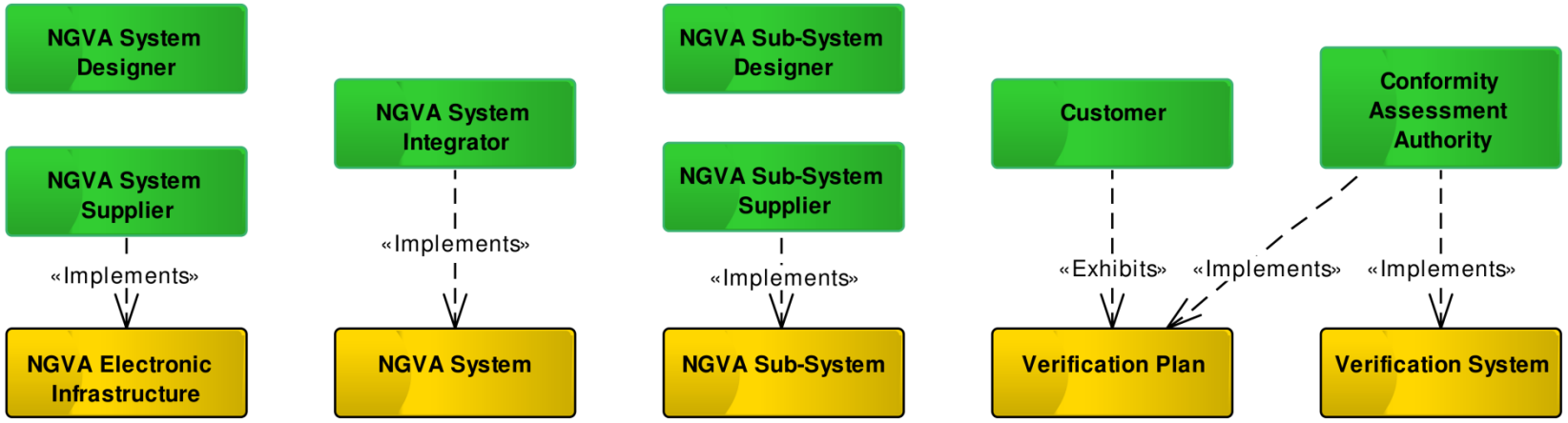


Verification Plan

- Detailed guidance on the development of a verification plan
  - Verification roles and responsibilities
  - Verification methods (Inspection, Analysis, Demonstration, Test)
  - Review methods (formal system reviews)
  - Analysis methods (traceability/coverage analysis)
  - Verification tools and techniques
  - Verification independence
  - Re-Verification guidelines
  - Legacy equipment guidelines

Verification Roles and Responsibilities

- Development of a verification plan needs
  - Definition of different stakeholders involved
  - Specification of stakeholder responsibilities



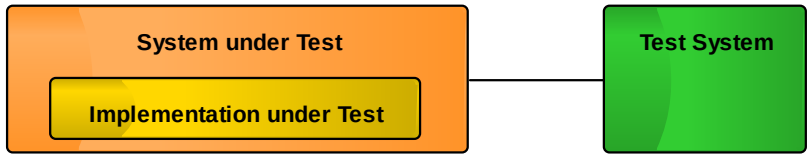
Verification Tools and Techniques

- Use of hardware and software tools to assist and automate verification processes
  - Test coverage analysis, regression testing

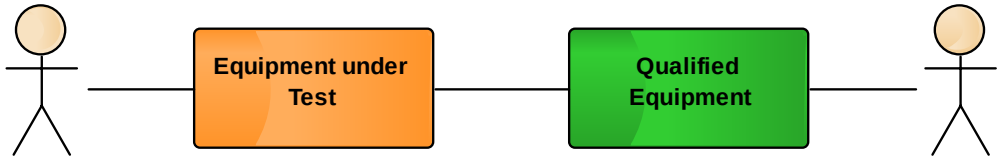
- Guidelines for these tools and any hardware test equipment
  - Detailed description of tools needed
  - Explanations of tool's performance
  - Required inputs and generated outputs
  - Test facilities and test labs, e.g. specific conformance or interoperability test labs

Conformance and Interoperability Tests

- NGVA main objective: assurance of interoperability
- Typically conformance and interoperability testing are used
  - Both techniques are complementary
- Conformance testing addresses protocols and lower-layer communication



- Interoperability testing selected for entire systems and applications



Test Labs and Test Beds

- Vendors as well as vendor-independent authorities should maintain test beds
  - Conduct tests prior to the initial release or upgrades
  - Provide infrastructure to which NGVA systems have to be interoperable with
  - Allow collocated testing to verify real-time, safety, and security requirements

Demonstrators and Experiments

- Confirmation of functional and operational requirements
- Verification as well as validation to prove the intended use
- Defined concept of use of the system is validated in predefined operational scenarios.

Independent Verification and Validation (IV&V)

- Verification by independent authorities necessary for but not limited to requirements that are safety-critical or of high-security nature
- Independent verification and validation is defined by three parameters:
  - Technical, Managerial und Financial Independence

Independent Verification and Validation (IV&V)

- Verification by independent authorities necessary for but not limited to requirements that are safety-critical or of high-security nature
- Independent verification and validation is defined by three parameters:
  - Technical, Managerial und Financial Independence

- Different forms of independence for a V&V organization should be used depending on the complexity of the NGVA system to be verified
  - Classical IV&V (embodies all three independence parameters)
  - Modified IV&V (no managerial independence)
  - Integrated IV&V (no technical independence)
  - Internal IV&V and Embedded IV&V (all three independence parameters are compromised)

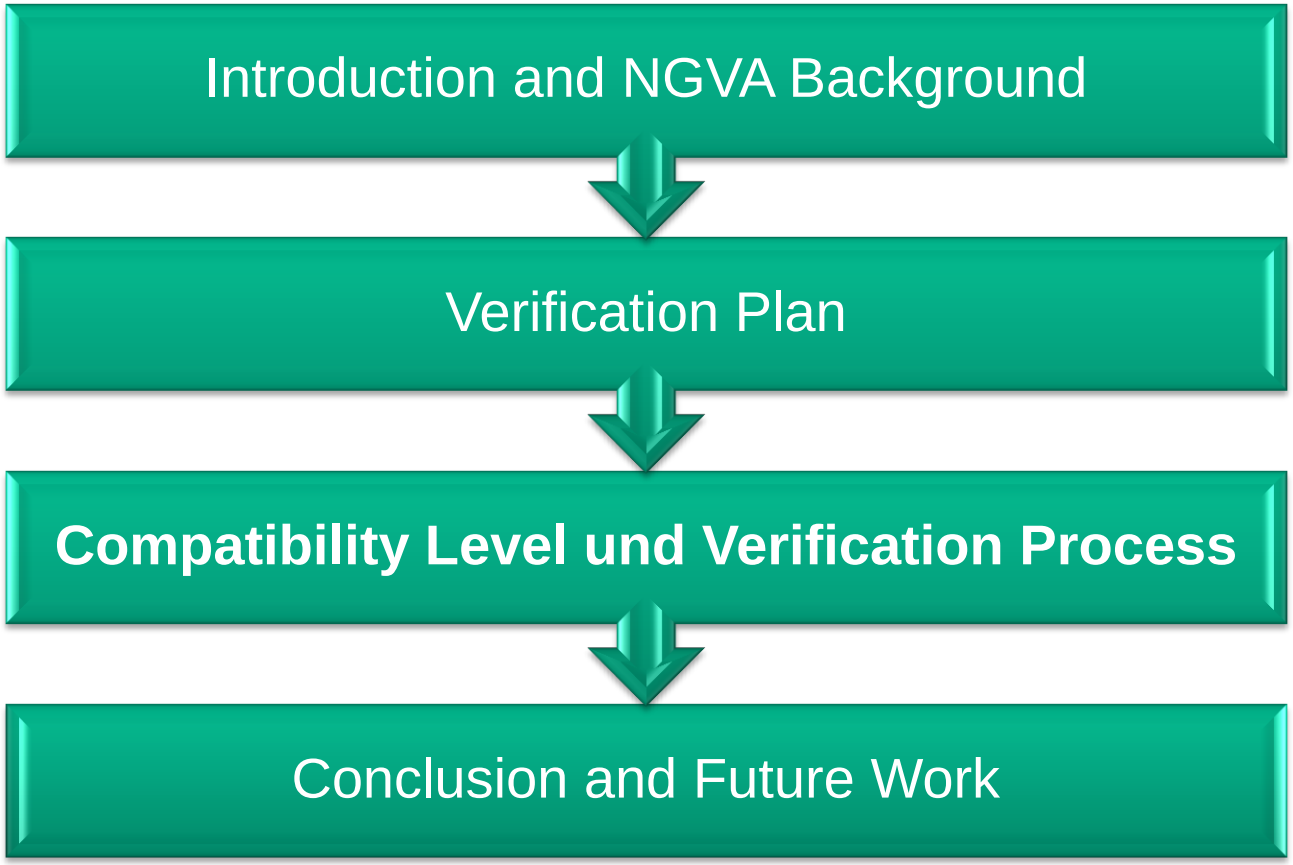
Re-Verification Guidelines

- After modifications of design or implementation, NGVA equipment needs to be re-verified
  - Depending on the level of change, in case of doubt the complete system needs to be re-verified



- Verification plan should describe re-verification guidelines depending on the type and level of (sub-) system changes
- If there are no guidelines given, the whole system has to perform the complete verification process again

OVERVIEW



Introduction of Conformity Levels

- Design of an incremental process for systems verification and certification
- Based on three sequentially-related levels:

- Different levels allow evaluation of specific system requirements in a structured manner by arranging the verification order
- Levels are sequential; Communication Readiness includes Connectivity Readiness and Functional Readiness includes all others.

NGVA Compatibility Levels – Certification

Connectivity Compatibility

Ensures sub-systems can be physically integrated without negative impacts to existing infrastructure

Communication Compatibility

Refers to correct implementation of the NGVA DM (e.g. Topic Types, QoS) and video streaming standards

Functional Compatibility

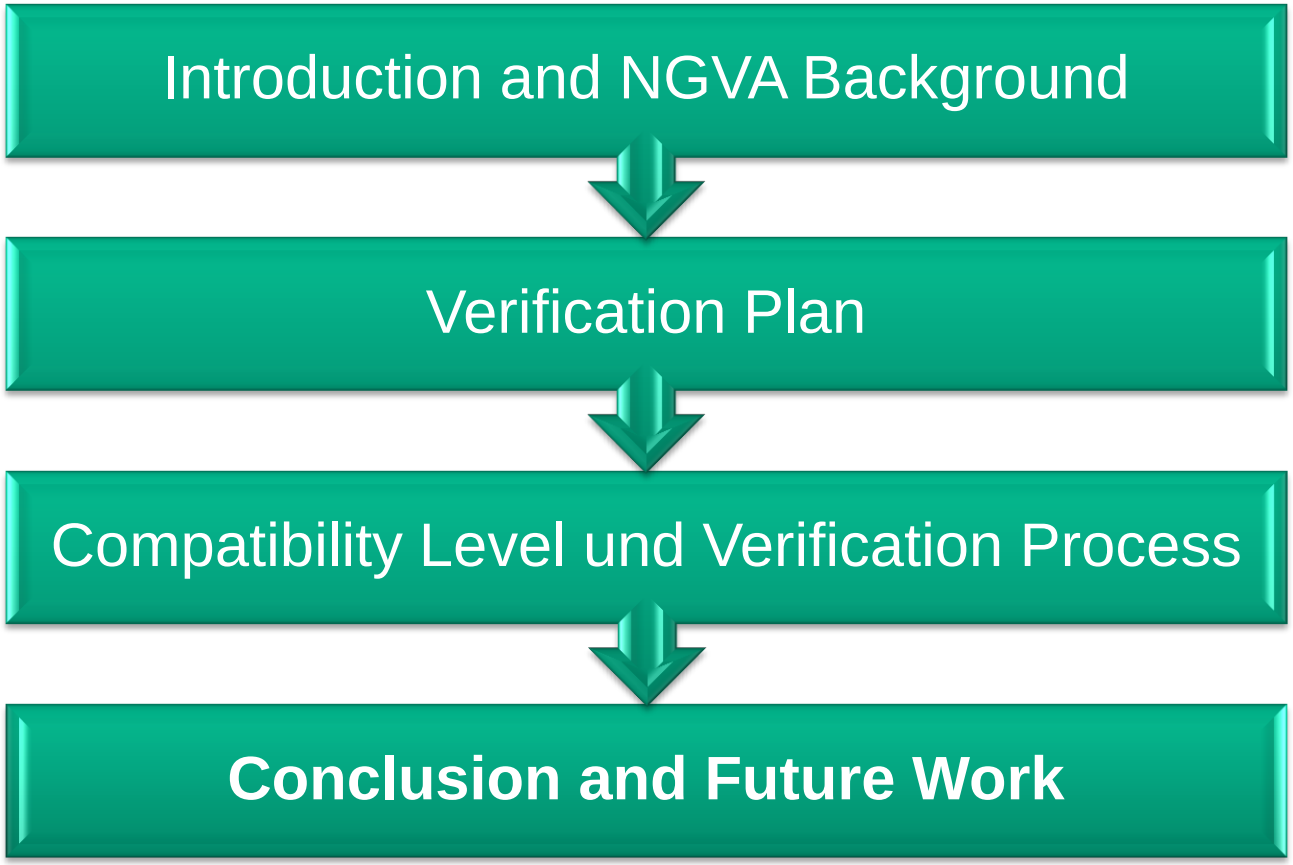
Verifies functional and performance requirements, e.g. NGVA DM tests covering component responses for valid, inopportune and invalid inputs

Verification Process

- Definition of a five-stage verification process

Planning	• System-specific requirements are collected and verification types are established; plan review
Preparation	• Allocation to NGVA Readiness Levels • NGVA system/enabling resources are acquired
Performance	• Conformance to requirements sequentially established • Test procedures and outcomes are linked to requirements
Outcomes Analysis	• Collected results are analysed for quality and correctness • Re-performing of affected verification steps if necessary
Capturing of Results	• System Id; Procedures/ Requirements passed or failed; Corrective Actions, Traceability Analysis; Lessons Learned;

OVERVIEW

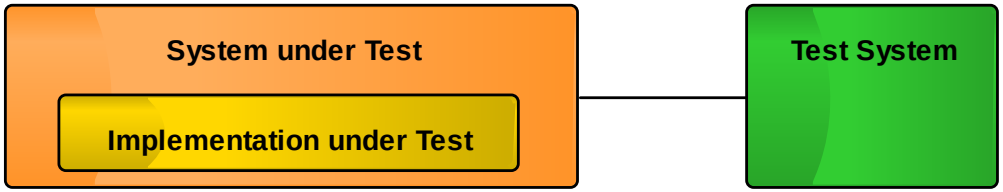


Conclusion

- Generic verification framework in order to deal with all types of (sub-) systems designed according to the emerging NGVA STANAG
  - Introduction of detailed Verification Plan
  - Conformity assessment by three sequentially-related NGVA Compatibility Levels
  - Development of a Verification Process consisting of five steps from verification planning to the capturing of the results
- Verification framework discussed and agreed in the NGVA community
- Accepted as the study draft for the Verification and Validation AEP Volume of the NGVA STANAG

Future Work – NGVA DM Test Reference System

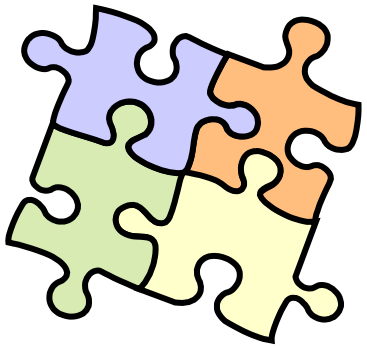
- Verification key aspect: NGVA Data Model Conformance Testing
  - Each vehicle subsystem is considered as a black box
  - Does the System under Test conform to the NGVA Data Model?
  - Functionality and behaviour for valid, inopportune and invalid input



- Independent conformity assessment bodies provide appropriate test systems
- Assure that all vendors have always access the latest release of the test suite
  - Perform automatic execution of test cases
  - Obtain automatic and unbiased assignment of test verdicts

Future Work – Guidelines for Modular (Re-) Verification

- No guidelines for modular verification of NGVA systems
- No differentiation between the verification of complete systems and NGVA sub-systems so far



- Concepts needed to avoid complete re-verification of the entire NGVA system if only some portions change
  - Describe subsystems capabilities as service contracts
  - Consider of Modular Safety Cases
  - Examine Modular Certification approaches from avionics domain

Thank You
for Your Attention!

Contact

Fraunhofer
FKIE

Daniel Ota
Dipl.-Inf.
Team Lead Platform Capability Integration

Information Technology for Command and Control

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE

Fraunhoferstraße 20 | 53343 Wachtberg | Germany
Phone +49 228 9435-732
Fax +49 228 9435-685
daniel.ota@fkie.fraunhofer.de