TOWARDS VERIFICATION OF
NATO GENERIC VEHICLE
ARCHITECTURE-BASED SYSTEMS

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

Introduction and NGVA Background

Verification Plan

Compatibility Level und Verification Process

Conclusion and Future Work
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
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
NGVA STANAG Structure

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

  - Architecture Approach
  - Power Infrastructure
  - Data Infrastructure
  - Crew Terminal Software Architecture
  - Data Model
  - Safety
  - Verification and Validation
NGVA STANAG Structure

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

  - Architecture Approach
  - Power Infrastructure
  - Data Infrastructure
  - Crew Terminal Software Architecture
  - Data Model
  - Safety
  - Verification and Validation

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

<table>
<thead>
<tr>
<th>Current (A)</th>
<th>MIL-DTL-38999</th>
<th>VG 95234</th>
<th>VG 95328</th>
</tr>
</thead>
<tbody>
<tr>
<td>8A</td>
<td></td>
<td></td>
<td>D 14-19 SN</td>
</tr>
<tr>
<td>13A</td>
<td></td>
<td></td>
<td>M 14-19 PN</td>
</tr>
<tr>
<td>25A</td>
<td>C4SA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60A</td>
<td>E06SN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>90A</td>
<td></td>
<td>B1 32-1 SN</td>
<td></td>
</tr>
<tr>
<td>120A</td>
<td></td>
<td></td>
<td>G48SN</td>
</tr>
<tr>
<td>130A</td>
<td></td>
<td></td>
<td>M 32-1 PN</td>
</tr>
</tbody>
</table>
## AEP-4754 Volume 3: Data Infrastructure

### Data and Network Infrastructure

<table>
<thead>
<tr>
<th>Layers</th>
<th>External</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Link and Physical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### External Layers
- **DI Services**
- **Voice**

#### Internal Layers
- **Video / Audio**
- **Vetronics Data**
- **Other**
- **Peripherals**

#### Data Model
- **NGVA External Gateway**
- **Network Services** (NTP, DHCP, DNS, QoS)
- **Voice Control and Distribution** (STANAG 4697 PLEVID)
  - Session Control: PLEVID or SIP
  - Codec: PLEVID or G711
- **Video and Audio Distribution** (STANAG 4697 PLEVID)
- **NGVA Data Model** (NGVA DM, incl. XTypes and QoS Profiles)
- **Data Distribution Service** (OMG DDS)
- **Mission Application (incl. HMI)**
  - (C4I, Data/Audio/Video-Processing, Weapon Control, Storage, Search, HUMS, etc.)

#### Transport Layer
- **Internet Protocol (IPv4, IPv6)**
  - RFC791, RFC2460

#### Internet
- **Ethernet, Connectors, Cables** (IEEE802.3)
  - Copper 100/1000Base-T with Connector D38999/Xxα35SN or XXαC35SN (A for classified)
  - Optical Fibre 10GBase-SR/BX with IEC 60793-2-10 and EN4531xB02yα (D or E)

**Specific Peripheral Data Model**

**USB-Specific**

**USB2.0 for Peripherals**
## Example Requirements for Power and Data Distribution

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Requirement Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGVA_POW_008</td>
<td>CR</td>
<td>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 [...]</td>
</tr>
<tr>
<td>NGVA_POW_027</td>
<td>OE</td>
<td>The NGVA power [sub-system] shall inform the [vehicle crew] of the battery life remaining in hours and minutes at the current load.</td>
</tr>
<tr>
<td>NGVA_INF_002</td>
<td>CR</td>
<td>NGVA ready sub-systems shall comply with the NGVA Arbitration Protocol as defined in the NGVA Data Model.</td>
</tr>
<tr>
<td>NGVA_INF_009</td>
<td>CR</td>
<td>The NGVA network topology shall be such that the required data rates and latencies requirements can be achieved.</td>
</tr>
<tr>
<td>NGVA_INF_032</td>
<td>CR</td>
<td>Vetronics Data shall be exchanged by DDS topics using the &quot;QoS pattern&quot; attached to it in the NGVA Data Model to assure assignment of DDS topics.</td>
</tr>
</tbody>
</table>
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

Introduction and NGVA Background

Verification Plan

Compatibility Level und Verification Process

Conclusion and Future Work
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

![Diagram showing the relationships and roles in a verification plan, including NGVA System Designer, NGVA System Supplier, NGVA System Integrator, NGVA System, NGVA Sub-System Designer, NGVA Sub-System Supplier, NGVA Sub-System, Customer, Conformity Assessment Authority, Verification Plan, and Verification System.]
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 and NGVA Background

Verification Plan

Compatibility Level und Verification Process

Conclusion and Future Work
Introduction of Conformity Levels

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

- 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

Introduction and NGVA Background

Verification Plan

Compatibility Level und Verification Process

Conclusion and Future Work
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

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